Edited by
Vladan Pantović
Dušan Starčević

# INFOTECH

Powered by ASIT

## 2020 - 2024
## Selected Papers

2025.


# INFOTECH 2020 - 2024

# SELECTED PAPERS

Edited by

Vladan Pantović

Dušan Starčević

Belgrade, 2025

# International Conferences

# INFOTECH 2020-2024

**Organizer**

**ASIT** - *Association for Computing, Informatics, Telecommunications and New Media of Serbia*

**Co-organizers of the scientific part of the conference:**

- Faculty of Project and Innovation Management prof. dr Petar Jovanović, Belgrade
- Faculty of Information Technology and Engineering, Belgrade
- Faculty of Business Economy and Entrepreneurship, Belgrade
- Laboratory for multimedia communication, FON, Belgrade
- University "Bijeljina", Bijeljina, Bosnia and Herzegovina
- "Dositej" Faculty of Economics and Informatics, Belgrade

# INFOTECH 2020 - 2024 Selected Papers

**Edited by Vladan Pantović & Dušan Starčević**

**Publisher:** ASIT, Belgrade, Nikola Mirković, President

**Co-Publisher**: Faculty of Project and Innovation Management prof. dr Petar Jovanović, Belgrade

Cover Design**:** Vladimir Jablanov / Digital printing: GRAFOPAN doo Belgrade / Circulation: 200

ISBN-978-86-900491-5-8

CIP - Каталогизација у публикацији Народна библиотека Србије, Београд

004(082)
007:004(082)
659.23:681.324(082)
681.324(082)

**INFOTECH. Selected papers (34-39 ; 2000-2024)**

Zbornici radova INFOTECH 2020 - 2024 [Elektronski izvor] : selected papers / editori Vladan Pantović, Dušan Starčević. - Beograd : ASIT : Faculty of Project and Innovation Management, 2025 (Beograd : Grafopan). - 179 str. : ilustr. ; 30 cm

Tiraž 200. - Str. 5: Preface / Nikola Mirković, Vladan Pantović. - Bibliografija uz svaki rad. - Registar.

ISBN 978-86-900491-5-8

a) INFOTECH (35-39 ; 2000-2024) b) Информациона технологија -- Зборници

v) Информациони системи -- Зборници g) Рачунарске мреже -- Зборници

d) Електронска размена података -- Зборници đ) Пројектовање -- Примена рачунара -- Зборници

COBISS.SR-ID 170034185

# Table of Contents

# P R E F A C E

This year marks the 40th edition of INFOTECH, a regular annual international scientific and professional conference in the field of the development and application of information technologies. ASIT - the Association for Computing, Informatics, Telecommunications and New Media of Serbia, the organizer of the INFOTECH conferences, on the occasion of the aforementioned important jubilee, published this special publication.

The international conferences INFOTECH fulfill the mission of their founder, ASIT, to be a meeting point for exchanging ideas, knowledge and solutions of professional individuals from academics and business, to promote the possibilities and significance of information techology in the digital transformation of society.

A total of nine invited keynote lectures and 21 selected papers by 55 authors are published in the INFOTECH 2020 - 2024 Selected Papers publication. After the first Chapter, Invited Keynote Lectures, selected papers are classified according to their subject matter into an additional six chapters: 2. Artificial Intelligence, 3. Information Security, 4. IT in the COVID Crisis Time and Digital Health Technologies 5. IT and Project Management, 6. Information Technology Application, 7. Management and Information Systems.

Keynotes and selected papers are penned by authors from Serbia and abroad (USA, Mauritius, United Arab Emirates, Qatar, India, United Kingdom, Croatia and Bosnia and Herzegovina). A certain number of lectures by authors from abroad were presented in a hybrid mode of work due to the Covid pandemic.

We would like to thank everyone who actively participated in the preparation of the INFOTECH 2020 - 2024 conferences, and we expect good cooperation in the coming years as well.

Chairman of the Organizing Board

Nikola Mirković

Chairman of the Scientific Program Board

Prof. dr Vladan Pantović

## PROGRAM COMMITTEE

- Dr Vladan Pantović, Faculty of Project and Innovation Management, Belgrade

## PROGRAM COMMITTEE MEMBERS

- Dr Dušan Starčević, Faculty of Organizational Sciences, Belgrade
- Dr Aca Aleksić, "Dositej" Faculty of Economics and Informatics, Belgrade
- Dr Maja Anđelković, Faculty of Information Technology and Engineering, Belgrade
- Dr Zoran Avramović, University of Belgrade, Belgrade
- Dr Olja Arsenijević, Institut for serbian culture, Priština – Leposavić
- Dr Robin Singh Bhadoria, *Hindustan College of Science and Technology, Mathura, India*
- Dr Zoran Bojković, Faculty of Transport and Traffic Engineering, Belgrade
- Dr Milan Brković, Association of Serbian Banks, Belgrade
- Dr Vladimir Brusić, *University of Doha for Science and Technology, Qatar*
- Dr Miodrag Brzaković, Faculty of Applied Management, Economics and Finance, Belgrade
- Dr Maja Cogoljević, Faculty of Business Economy and Entrepreneurship, Belgrade
- Dr Danijela Ćirić-Lalić, Faculty of Technical Sciences, Novi Sad
- Dr Anastasios Dagiuklas, *London South Bank University, London, United Kingdom*
- Dr Velimir Dedić, Faculty of Information Technology and Engineering, Belgrade
- Dr Vlado Delić, Faculty of Technical Sciences, Novi Sad
- Dr Gordana Djordjević, Faculty of Business Economy and Entrepreneurship, Belgrade
- Dr Viviana Fernández Marcial, *Universidade da Coruña, España*
- Dr Jovan Filipović, Faculty of Organizational Sciences, Belgrade
- Dr Pawan Fowdur, University of Mauritius, Republic of Mauritius
- Dr Borko Furht, *Florida Atlantic University, Boca Raton, USA*
- Dr Gordana Gardašević, Faculty of Electrical Engineering, Banja Luka
- Dr Milan Gligorijević, Alfa BK University, Belgrade
- Dr Zagorka Gospavić, Faculty of Civil Engineering, Belgrade
- Dr Zvezdan Horvat, *Adizes Institute Worldwide, Santa Barbara, USA*
- Dr Miloš Jelić, Foundation for Quality Culture and Excellenc, Belgrade
- Dr Emil Jovanov, *University of Alabama, Huntsville, USA*
- Dr Filip Jovanović, Faculty of Project and Innovation Management, Belgrade
- Dr Siniša Jovanović, Imtel Komunikacije, Belgrade
- Dr Marina Jovanović-Milenković, Faculty of Project and Innovation Management, Belgrade
- Dr Asutosh Kar, *Indian Institute of Information Technology, Kancheepuram, Chennai, India*
- Dr Tihomir Katulić, University of Zagreb, Croatia
- Dr Jelena Kočović, Faculty of Economics, Belgrade
- Dr Petar Kočović, Faculty of Information Technology and Engineering, Belgrade
- Dr Bojan Kostandinović, Mokra Gora School of Management, Belgrade
- Dr Boro Krstić, University "Bijeljina", Bijeljina, Bosnia and Herzegovina
- Dr Dejan Kršljanin, Center for Applied Mathematics and Electronics, Belgrade
- Dr Goran Lazarov, Higher Colleges of Technology, Dubai, United Arab Emirates
- Dr Dragan Lončar, Faculty of Economics, Belgrade

- Dr Zoran Marjanović, Faculty of Organizational Sciences, Belgrade
- Dr Vera Marković, Faculty of Electronic Engineering, Nis
- Dr Miodrag Mesarović, Energoprojekt Entel, Belgrade
- Dr Danijela Milošević, Faculty of Technical Sciences Čačak
- Dr Mladen Milošević, Faculty of Security Studies, Belgrade
- Dr Miloš Milovanović, Faculty of Organizational Sciences, Belgrade
- Dr Miroslav Minović, Faculty of Organizational Sciences, Belgrade
- Dr Cvetko Mitrovski, Faculty of Technical Sciences, St. Kliment Ohridski University – Bitola, North Macedonia
- Dr Vojislav Mišić, *Ryerson University, Toronto, Canada*
- Dr Vladimir Mladenović, Faculty of Technical Sciences Čačak
- Dr Boško Nikolić, Faculty of Electrical Engineering, Belgrade
- Dr Srđan Nogo, University of East Sarajevo, Bosnia and Herzegovina
- Dr Deasún Ó Conchúir, *Scatterwork GmbH, Switzerland*
- Dr Mladen Opačić, Metropolitan University, Belgrade
- Dr Miroslav Perić, Singidunum University, Belgrade
- Dr Vladimir Petrović, *Robert Bosch GmbH, Germany*
- Dr Milan Prokin, Faculty of Electrical Engineering, Belgrade
- Dr Jelica Protić, Faculty of Electrical Engineering, Belgrade
- Dr Zoran Radojičić, Faculty of Organizational Sciences, Belgrade
- Dr Milan Radosavljević, Faculty of Business Studies and Law, Belgrade
- Dr Radoslav Raković, Engineering Academy of Serbia (EAS), Belgrade
- Dr Muthu Ramachandran, *Leeds Becket University, United Kingdom*
- Dr Marko Savković, Studiopro, Belgrade
- Dr Dejan Simić, Faculty of Organizational Sciences, Belgrade
- Dr Svetozar Sofijanić, Technical Academy for Applied Studies, Belgrade
- Dr Svetlana Stevović, Faculty of Mechanical Engineering, Belgrade
- Dr Velimir Štavljanin, Faculty of Organizational Sciences, Belgrade
- Dr Vladimir Terzija, *University of Manchester, United Kingdom*
- Dr Ana Trbović, FEFA, Belgrade, Grid Singularity, Berlin, Germany
- Dr Mladen Veinović, Singidunum University, Belgrade
- Dr Dejan Vidojević, Academy of Professional Studies Sumadija, Kragujevac
- Dr Nikola Vojtek, Daon, Belgrade
- Dr Slađana Vujićić, Faculty of Business Economy and Entrepreneurship, Belgrade
- Dr Dušan Vujošević, School of Computing, Belgrade
- Dr Ivan Vulić, Faculty of Project and Innovation Management, Belgrade
- Mr Dragorad Milovanović, School of Computing, Belgrade, Program Committee Secretary

# 1.

# Invited Keynote Lectures

# FIFTEEN YEARS OF eGOVERNMENT IN SERBIA

Assistant Professor Dejan Vidojević, PhD, University of Criminal Investigation and Police Studies,
dejan.vidojevic@me.com

**Apstrakt:** *U okviru rada je dat kratak istorijski pregled razvoja eUprave u Republici Srbiji u odnosu na osnovne preduslove i postavljene dugoročne i kratkoročne ciljeve. Polazna osnova za analizu realizovanih pravaca razoja i dostignutog nivoa su svakako teorijske osnove, zatim primeri najbolje prakse u svetu kao i sprovedena istraživanja u prethodnom periodu na koja se referencira ovaj rad. Prioriteti razvoja i značaja su svakako osnovni parametri za analizu trenutnog stanja i niova, kao i ulazni parametri za definisanje budućih ciljeva i planova unapređenja i razvoja eUprave. Rezultat ovog istraživanja su predlozi i preporuke koje bi mogle da doprinesu kvalitetu procesa implementacije primenjenog koncepta eUprave.*

**Ključne reči:** *eUprava, usluge, koncept, ciljevi, infrastruktura.*

**Abstract:** *The paper provides a brief historical overview of the development of eGovernment in the Republic of Serbia in relation to the basic preconditions and set long-term and short-term goals. The starting point for the analysis of the realized directions of development and the achieved level are certainly the theoretical bases, then the examples of best practice in the world as well as the conducted research in the previous period to which this paper refers. Priorities of development and importance are certainly the basic parameters for the analysis of the current situation and levels, as well as the input parameters for defining future goals and plans for the improvement and development of eGovernment. The result of this research are proposals and recommendations that could contribute to the quality of the process of implementation of the applied concept of eGovernment.*

**Keywords:** *eGovernment, services, concept, goals, infrastructure.*

## 1. INTRODUCTION

The transformation of business and the transformation of society itself conditioned the beginning of the creation of conditions for the development of electronic business in public administration at the beginning of this century. Considering that the business within the state administration was burdened with documentation that monitors business processes, within the European Union, the creation of conditions for the development of e-government began, which conditioned the setting of new goals for the development of administration in the Republic of Serbia. The transition to e-business in public administration has become an imperative and a basic goal in all developed countries.

The basic precondition for the development of e-government is legislation whose adoption and implementation have paved the way for the development of e-government in Serbia. A chronological overview of the regulatory framework that is the basis for the development of e-government in Serbia is given:

- 2002 - The European regulatory framework for electronic communications comprehensively regulates the electronic communications sector of the European Union;
- Since 2003, the regulatory framework has been mandatory in the EU Member States, and the Republic of Serbia is obliged to harmonize its national legislation with the relevant acquis in the accession process;
- In 2004, the Law on Electronic Signature was adopted;
- In 2006, the Strategy for the Development of the Information Society in the Republic of Serbia was adopted, which is the first act that comprehensively regulates the field of the information society in the Republic of Serbia;
- In 2009, the e-Government Development Strategy for the period from 2009 to 2013 was adopted, together with the Action Plan;
- In 2009, the Law on Electronic Document and Trademark was adopted;
- In 2010, the e-Government portal of the Republic of Serbia officially started operating;
- The Law on Information Security was adopted in 2016;
- In 2017, the Regulation on the implementation of the new law on general administrative procedure was adopted and the eZUP system was established;
- In 2018, the Law on Electronic Administration was adopted and the Service Highway of Organs (SMO) was established;
- In 2020, the eGovernment Development Program for the period 2020-2022 and the Action Plan for its implementation were adopted.

In the technical and technological sense, the overview of the development of eGovernment with key events is presented chronologically:

- In 2005, the individual development of eGovernment infrastructure and services in state administration bodies began;
- In 2007, the organized development of eGovernment infrastructure and services under the authority of the Ministry of State Administration and the Ministry of Telecommunications began;
- In 2010, the eGovernment portal was launched;

- In 2012, the process of development and implementation of the basic infrastructure of eGovernment was completed to the greatest extent;
- In 2017, the eZUP system was established;
- In 2018, the Service Highway of Organs was established;
- In 2019, the central ePayment system and the Open Data system were established;
- In 2020, the Office for IT and eGovernment was entered in the Register of Electronic Identification Service Providers and Electronic Identification Schemes in the Republic of Serbia.

## 2. SIGNIFICANCE, GOALS AND PRIORITIES OF eGOVERNMENT [1]

The importance of introducing eGovernment is reflected in the results and effects achieved by implementing the concept:

- Improving the efficiency and effectiveness of business processes in public administration;
- Acceleration and simplification of administrative procedures of public administration;
- Increasing the degree of transparency in the functioning of public administration;
- Simplification of the process of interaction between public administration and service users by applying the principle of interoperability.

Priorities for the implementation of the eGovernment concept in Serbia are reflected in long-term and short-term project implementation plans:

- Development of optical infrastructure and development of broadband internet on the entire territory of Serbia;
- Construction of the State Data Center as the basic infrastructure unit of the e-government system;
- Development of the Central Population Register and the Address Register;
- Development of Meta-registers and Registers of Administrative Procedures;
- Further development of the e-Government Portal through constant improvement of service quality;
- Development of an electronic archiving system;
- Development and improvement of public administration information systems on the principles of interoperability, a Single Administrative Place and a "Single Service Desk".

The general goals of the application of the eGovernment concept in Serbia are:

- Reducing costs by applying electronic services and transactions;
- Shortening the duration of administrative procedures;
- Increasing the speed and level of reliability by applying electronic services in business processes;
- Economic development through higher quality of interaction of public administration with the economy and citizens and direct impact on the development of the economy through the application of modern technologies;
- Increasing the level of transparency and availability of information to users of public administration services;
- Increasing the level of availability of services by increasing the availability and content;
- Increasing the level of service availability through integration, cost management and increasing the efficiency of business processes;
- Formation of the information society through the processes of integration and digital transformation.

## 3. eGOVERNMENT CONCEPT, INFRASTRUCTURE AND SERVICES [2]

The concept of eGovernment presented through the methodological framework and general direction of development - from institutional architecture to public services is presented in Figure 1.

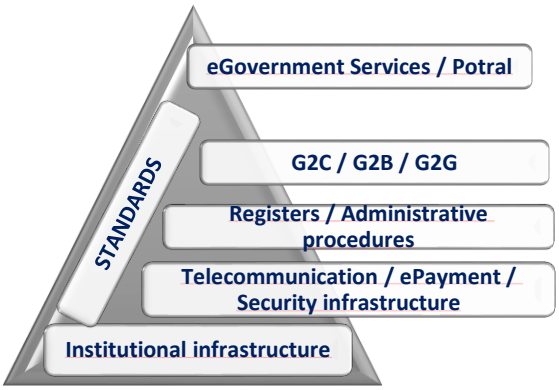



**Figure 1. The concept of eGovernment development**

In Serbia, the standard concept and methodology of e-government development has been applied, the basis of which is the institutional infrastructure, and the direction of development is from technological and security infrastructure to public services.

The architecture of the eGovernment system in the technical-technological sense consists of 4 layers:

- Access layer / Communication channels with service users;
- eGovernment layer / integrated services through a single eGovernment portal;
- eBusiness layer / data sources and data processing applications;
- Infrastructure layer / Public administration infrastructure.

The implementation of the concept of e-government is implementing through 5 typical stages of development presented through the so-called "Stages of online presence"

---

(Figure 2): [1] Model *Web Measure Assesment* of the United Nations organizations *UNPAN - United Nations Public Administration Network*

- "emergging presence" - a limited amount of information,
- "enchanced presence" - more information on different spheres of action,
- "interaction" - participation of target groups in IT-supported processes and availability of certain services,
- "transaction" - two-way online exchange of information and provision of various services,
- "transformation" - full integration of processes and transformation of changes (joined-up e-government).

In relation to the stages of development, Figure 2 shows the corresponding stages of implementation of the eGovernment system.

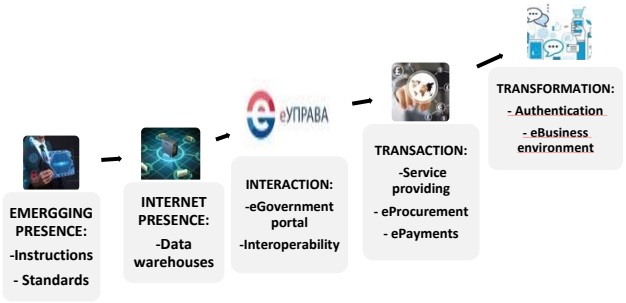



**Figure 2. Implementation of the eGovernment concepte**

In relation to the above, the levels of eGovernment / administration development can be defined (level 0 to level 5), which is presented in Figure 3. Level 0-1 is characterized by referring to services within the administration that are distributed via the intranet. Level 2-5 is referring to customer services distributed via the Internet and Extranet.

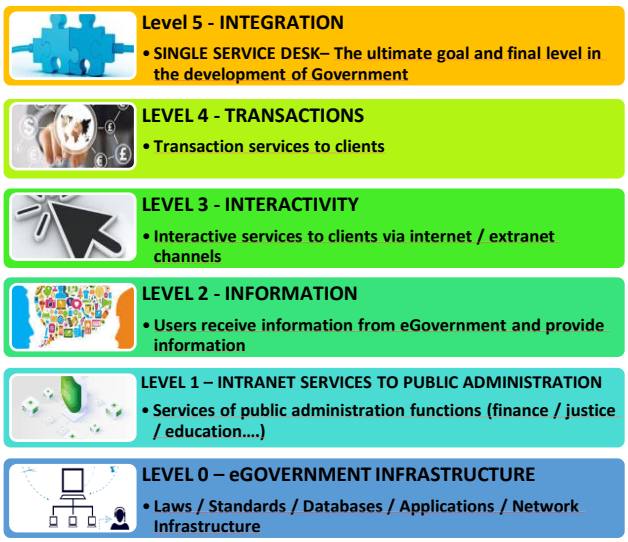



**Figure 3. Levels of eGovernment development**

The key level of eGovernment development is level 3, ie establishing interactivity - the client can get information from a state body or organization, and also provide them with information. The final goal and the final stage of eGovernment development is level 5, ie full integration through the establishment of a single channel of communication – *Single Service Desk*.

The infrastructural elements of the implemented eGovernment concept are (Figure 4.):

- eGovernment portal;
- Computer network and Data center;
- eIdentification infrastructure;
- Knowledge management infrastructure.

Infrastructure elements are grouped and make up 3 layers of infrastructure:

- User layer;
- Middle layer and
- (Backend) background layer.

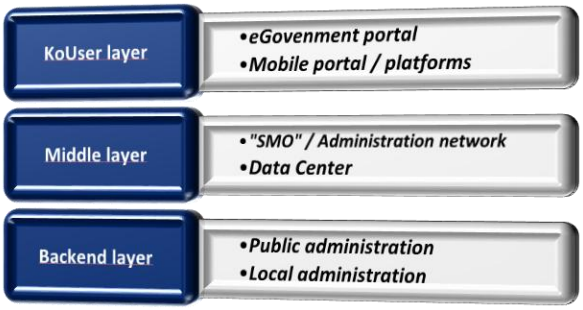



**Figure 4. Infrastructure elements of eGovernmente**

Elements / layers are integrated using interoperability standards.

The applied concept of implementation of the eGovernment system in Serbia implies the establishment of a single communication channel (Single Service Desk) - eGovernment portal (*euprava.gov.rs*).

The eGovernment portal should be a single access point, whose services are grouped according to users:

- Citizens;
- Business;
- State - public administration bodies.

## 4. OVERVIEW OF THE CURRENT SITUATION OF eGOVERNMENT IN SERBIA [3] [4] [5]

The United Nations Department of Economic and Social Affairs conducts a biennial survey on the level of development of eGovernment in all member countries (*UN e-Government Surveys*).

Based on the *eGovernment Developmentmnet Index (EDGI)*, the development of eGovernment at the national level is assessed, which is based on three components:

- *Online Service Index* (*OSI*);
- *Telecommunication Infrastructure Index* (*TII*) and
- *Human Capital Index* (*HCI*).

---

The results of the research (Figure 5.) are available in the report as of 2018 and Serbia is in the 49th position – Index EDGI (0-1) - 0,7155

According to the report[2] , eGovernment is a key factor in improving the implementation of a country's sustainable development goals. The results of the research unequivocally indicate that the lowest ***Telecommunication Infrastructure Index (TII) – 0,6208*** and that in the future the priority will be the development of eGovernment infrastructure. Based on the parameters and previously mentioned research results, and observed from the aspect of the *level of implementation of the concept*, it is estimated that eGovernment in Serbia is currently at the transition between ***level 3 and 4 (interactivity - transaction)***.

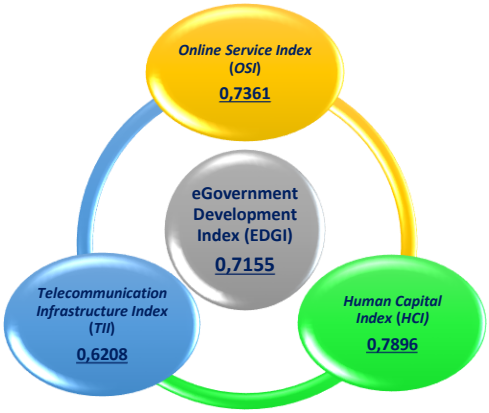



**Figure 5. Results of the e-Government Survey 2018 survey**

The current state of development of eGovernment in Serbia can be observed from the following aspects [1]:

1. Current state of application of information technologies:
   According to the estimates of the Republic Bureau of Statistics, less than 35% of the population uses eGovernment services, while approximately 99% of economic entities use these services.

2. Levels of eGovernment development in state administration and local government bodies:
   - Insufficient number of professional IT staff;
   - Insufficient level of training of employees to use IT services;
   - Insufficient level of standardization and unification of e-government services in terms of establishing a Single Service Desk;
   - Inadequate allocation of IT resources, especially in local governments in relation to central Government;
   - Insufficient level of application of technologies related to electronic documents and archives, electronic business procedures and security procedures;
   - Insufficient customer support for using the eGovernment service.

3. Users of eGovernment - citizens, business:
   - Insufficient instructions and information on administrative procedures and duration;
   - Insufficient level of accessibility and visibility of the eGovernment portal;
   - Insufficient level of standardization and unification of eGovernment services in terms of establishing a Single Service Desk;
   - Insufficient level of digitization of key administrative procedures for citizens;
   - Insufficient level of implemented system security measures and personal data protection;
   - Insufficient level of development of electronic payment system for the business.

Based on the previously mentioned research results, the current state of eGovernment in Serbia can be presented in the form of summarized conclusions:

- Insufficient level of quality of e-government services due to difficult digital interaction between state bodies, as well as eGovernment with users;
- Insufficient level of implementation of key IT solutions in public administration bodies;
- Insufficient profesional human resources in the eGovernment system;
- Insufficient level of readiness of users to use eGovernment services / refers primarily to citizens.

## 5. RECOMMENDATIONS FOR FURTHER DEVELOPMENT OF eGOVERNMENT IN SERBIA

According to previously performed analyzes and assessment of the current situation, two basic directions of further development of eGovernment in Serbia are imposed, taking into account the international environment:

1. Further organized and systemic development of e-government infrastructure;
2. Further development and improvement of the level of knowledge and capacity human resources of e-government.

The development of e-government infrastructure should be developed from the middle layer to the user, in accordance with the following priorities:

- Development of a state Data Center;
- Development of eIdentification and ePayments infrastructure;
- Development of a Network of public administration;
- Improving the eGovernment Portal;
- Development of mobile portals and applications for mobile platforms.

Infrastructure development implies the application of interoperability standards and is ultimately focused on the establishment of mobile platforms and applications.

Human resources development implies quantitative and qualitative improvement within the eGovernment system. The high level of quality of human resources enables the accelerated development of the eGovernment system and the high level of support to users, which in this segment should be the priorities of the development process.

The key thing in the further process of eGovernment development is the continuous development of infrastructure and improvement of human resources, which in the future will enable *harmonization of the process and level of eGovernment development on the entire territory of Serbia using the principle of resource sharing*.

In the processes of further development of eGovernment, it is necessary to *apply a systematic approach in the planning and implementation of plans* in order to increase efficiency and effectiveness and enable accelerated development.

## 6. CONCLUSION

The development of eGovernment in Serbia must be accelerated in the future in order to enable the integration of the system into a brodar framework with the systems of European countries, by applying interoperability standards within the system level and towards other systems outside Serbia.

It is very important for eGovernment to be efficient and user-oriented in order to create conditions for the digital transformation of the entire society and faster economic development in the existing environment.

## REFERENCES

[1] „eGovernment Development Program 2020 - 2022 and Action Plan for implementation", *Government of the Republic of Serbia*, Belgrade, June 2020.
[2] D. Vidojević, „Material for lectures from the course eGovernment“, *University of Criminal Investigation and Police Studies*, Zemun, Serbia, 2020.
[3] „eGovernment Survey 2018“, Department of Economic and Social Affairs ,*United Nations*, New York, 2018, (*publicadministration.un.org*).
[4] „eGovernment Assessment (eGovernment Development Index)“, *Swiss Pro*, Serbia, 2019.
[5] "Analysis of the state of digital skills of citizens in the use of eGovernment services", *Ministry of State Administration and Local Self-Government - Key4s doo Belgrade*, Serbia, 2019.

# A CLOUD BASED IOT SYSTEM FOR REAL-TIME AND ADAPTIVE WEATHER FORECASTING IN MAURITIUS

*Dr. Tulsi Pawan Fowdur, Associate Professor, PhD, CEng, MITP, MIEEE,*

*Department of Electrical and Electronic Engineering, University of Mauritius, p.fowdur@uom.ac.mu*

**Abstract:** The Internet of Things (IoT) coupled with cloud computing and AI are bringing about revolutionary technological changes in almost all spheres of life. This work considers the application of these three pervasive technologies to a well-known but very challenging problem which is weather forecasting. With the advent of global warming and other climatic imbalances, several countries are experiencing drastic weather conditions such as flash-floods which can lead to major collateral damage and life loss. Predicting such weather conditions with conventional forecasting systems is not possible because these systems provide predictions for large regions over hours. Lately, a number of real-time weather forecasting systems based on IoT have been developed to provide short-term real-time forecasts also known as Nowcasts. The main challenge in these systems is to use appropriate prediction algorithms that can predict different weather parameters with the highest possible accuracy as well as providing adequate storage requirements and processing power for real-time operation. In this work, three IoT based weather forecasting systems have been employed to provide short-term weather forecasts in Mauritius at intervals ranging from 20 minutes to one hour. The first two IoT systems are microcontroller based and make use of the Arduino and Raspberry-Pi microcontroller, while the third one is a dedicated weather forecasting device from Davis instruments. A cloud notification system based on the IBM Bluemix platform has also been set up to provide real-time weather predictions to users on their mobile phones as well as for storing weather parameters on the cloudant database and running the prediction algorithms on the Devops Insight services, respectively. Several adaptive forecasting algorithms based on variants of the Multiple Linear Regression technique as well as K-Nearest Neighbors scheme, have been experimented. Moreover, three adaptive selection criteria for selecting the most appropriate prediction algorithm for a given Nowcast have been developed and tested. Tests were performed in three different regions in Mauritius namely Reduit, Terre Rouge and Vacoas. The best adaptive schemes were able to predict these parameters with a very low percentage error in real-time, making the system particularly suitable for predicting the weather for micro-climatic regions.

Note: The work presented in this keynote speech is based on a research project entitled "**An Adaptive Short-term Localised Weather Forecasting System for Mauritius"**, that was funded by the Mauritius Research and Innovation Council and completed in September 2019. The project reference is MRIC/ HPC-RIG-A06. It has also led to the following publications:

1. T.P. Fowdur, Y. Beeharry, V. Hurbungs, V. Bassoo, V. Ramnarain-Seetohul, E. Chan Moo Lun, "Performance analysis and implementation of an adaptive real-time weather forecasting system", ELSEVIER, Internet of Things 3–4 (2018) 12–33. https://doi.org/10.1016/j.iot.2018.09.002

2. Y. Beeharry, T.P. Fowdur, and J.A. Sunglee, " A Cloud-Based Real-Time Weather Forecasting Application" Proceedings of IEEE TELSIKS 2019, 14th International Conference on Advanced Technologies, Systems and Services in Telecommunications, Serbia, Nis, 23-25 October 2019. DOI: https://doi.org/10.1109/TELSIKS46999.2019.9002327

# USE OF WEARABLES AND IOT TECHNOLOGY IN THE FIGHT AGAINST COVID-19 AND FUTURE PANDEMICS

*Dr. Emil Jovanov, Professor, IEEE Fellow*

*Electrical and Computer Engineering Dept, The University of Alabama in Huntsville,*

*emil.jovanov@uah.edu, http://www.ece.uah.edu/~jovanov*

**Abstract:** The COVID-19 pandemic has accelerated the adoption of digital health technologies and emphasized the urgent need for scalable, continuous, and unobtrusive health monitoring systems. We present the pivotal role of wearable sensors and Internet of Things (IoT) technologies in addressing current and future public health challenges through personalized, predictive, preventive, and participatory (P4) healthcare.

The integration of wearable sensors with ambient intelligence and cloud-based analytics enables novel applications such as remote physiological monitoring, mobility assessment, behavioral tracking, and real-time detection of disease onset. Examples include smartwatch-based mobility tests, physiological monitoring through smart objects (e.g., smart water bottles), and safe medication adherence technologies. Additionally, emerging sensing modalities, such as capacitive sensing and radar-based remote monitoring, facilitate seamless monitoring and contactless and opportunistic health assessments, which is particularly important for vulnerable populations.

The synergy of data from wearable and environmental sensors, supported by AI-driven interpretation and IoT infrastructure, fosters the development of personalized health management platforms. These systems facilitate early detection of illness, improve adherence, and empower individuals with actionable insights derived from continuous monitoring. Case studies and pilot experiments illustrate the feasibility and promise of such systems in everyday settings.

The convergence of wearable technologies and the Internet of Things (IoT) is reshaping the landscape of healthcare by enabling continuous, context-aware, and unobtrusive monitoring of physiological and behavioral parameters. This transformation is particularly critical in the context of global health crises such as the COVID-19 pandemic, where early detection, remote patient management, and population-level surveillance are essential. By embedding intelligence into everyday objects, such as smartwatches, rings, and even water bottles, we can facilitate seamless health data acquisition during normal daily activities, overcoming limitations of traditional episodic and facility-based care. The integration of wearable and ambient sensors, enhanced by cloud-based analytics and machine learning, allows for the development of adaptive, personalized health management systems.

# TOWARDS AI-NATIVE ARCHITECTURE IN 6G

*Professor Tasos Dagiuklas,*

*School of Computer Science and Digital Technologies, London South Bank University,*

*tdagiuklas@lsbu.ac.uk*

**Abstract:**

The evolution from 5G to 6G is driven by the imperative to embed intelligence and autonomy at the core of future networks. This trajectory sets the foundation for networks that are not only faster and more efficient but also self-aware, adaptive, and aligned with societal and industrial demands.

This talk explores the shift towards AI-native and cloud-native networking architectures that redefine how future networks are designed, operated, and optimized. While 5G has introduced key enablers—such as Software-Defined Networking (SDN), Network Function Virtualisation (NFV), edge cloud computing, and network slicing—to support application verticals like eMBB, URLLC, and mMTC, 6G builds on this by embracing distributed intelligence and pervasive automation.

AI becomes an intrinsic component across all layers, enabling Intent-Based Networking (IBN), autonomous decision-making, and real-time optimization through frameworks such as federated and transfer learning. The convergence of AI with cloud-native principles supports scalable, resilient, and programmable infrastructures, particularly at the network edge. Additionally, 6G introduces key technologies such as Reconfigurable Intelligent Surfaces (RIS), cell-free massive MIMO, and integrated Terrestrial/Non-Terrestrial Networks (TN/NTN) to underpin the vision of ubiquitous and intelligent connectivity.

# IoT-BASED AI ADAPTIVE CONTROL OF BUILDING PASSIVE MEASURES THE NEXT STEP IN PROMOTING ENERGY EFFICIENCY IN BUILDINGS

*Dr Mahendra Gooroochurn*

*CEng, LEED AP BD+C, Edge Expert, MIET, MIEEE, MASHRAE*

*Associate Professor, University of Mauritius,* M.Gooroochurn@uom.ac.mu

**Abstract:**

A key attribute of a sustainably designed built environment is its ability to integrate in the local context of the site, and therewith be able to harness the natural resources available as much as possible, while preventing the site conditions and ambient conditions from adversely affecting the indoor environmental conditions. Whereas passive measures have been a key approach to design green buildings for providing indoor environments with requisite indoor environmental quality for occupant health and well-being, with the combined effect of climate change and microclimates, the efficacy of passive measures cannot be ascertained at all times, especially for fixed techniques such as cool roofs and external shading devices. Indeed, literature findings confirm that our built environment are ill-prepared to deal with the consequences of climate change, with an expected impoverishment of the indoor conditions, to the detriment of the health, productivity and general well-being of occupants, be it for commercial or residential premises.

The emerging fields of IoT sensing, AI and 5G have allowed the holistic integration of technology with decision-making aligned with precepts of Industry 4.0, and opened opportunities to control these building passive measures by relying on a knowledge base derived from prior knowledge of the underlying building physics with respect to the thermal characteristics of the envelope and variation of climate parameters at the project location. This configuration allows to dynamically modulate the building passive measures and cope with daily variations in the prevailing climate to provide a further step towards curtailing the building carbon footprint intelligently. Research findings in applying this design paradigm for concrete constructions in the tropical context of Mauritius have shown the effectiveness of automating passive measures for providing proper indoor environmental quality. This design paradigm relying on adaptiveness of passive measures will certainly enable better adaptation to climate change effects and hence stronger climate resilience in the face of weather extremes.

**Keywords:** Green building design, automated passive design, building physics, AI, Mechatronics, Climate adaptation

# TECHNICAL EVOLUTION OF 5G MOBILE CONNECTIVITY NETWORKS: 3GPP 5G-ADVANCED STANDARDIZATION PROJECT

Dragorad Milovanović, University of Belgrade, Serbia, dragoam@gmail.com

**Abstract:** *This article provided a comprehensive overview of technical evolution in 3GPP (3rd Generation Partnership Project) standardization process of 5G-Advanced mobile communication systems. The next significant phase in the 5G development accelerate research efforts toward achieving 6G global connectivity. 3GPP standardization methodology and publication of particular Releases-18&19&20 as results of work on thousand technical reports (TRs) and technical specifications (TSs) are outlined. Significant takeaway from this decade-long evolution is the importance of collaboration in driving consensus and technical progress.*

**Keywords:** *5G mobile networks, 3GPP standardization*

## 1. INTRODUCTION

The goal of research and integration of new digital information and communication technologies is to progressively improve the performance of mobile networks and applications. Wireless communication has undergone significant advancements. Over the past 5 years, we have published chapters covering the development of 5G multimedia communications technologies, standardized network architectures as well as advanced technical specifications [1-4]. Key strategies for achieving network efficiency, fundamental and practical limitations are explored. At the system constraints level, unavoidable fundamental constraints and optimization trade-offs, as well as current activities on standardization of global technical specifications are considered [5].

3GPP standardization organization plays a major part in the once-every-decade generational progression since the first phase of mobile standards in the 1980s. Each generation has collected improvements throughout the system, measured in 3GPP Releases. In 2024, 3GPP is finalized its specification for Release-18 focusing on 5G-Advanced systems, while making progress to publication Release-19 December 2025. 3GPP also prepares for the transition to 6G standardization with Release-20 publication by June 2027.

The paper is organized as follows. After an introduction, section presents 3GPP standardization methodology. Next, 5G-Advanced standardization project timeline and results are outlined as well as start of normative work on 6G scenarios, use cases and service requirements.

## 2. 3GPP STANDARDIZATION METHODOLOGY

The 3GPP (3rd Generation Partnership Project) unites telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), providing stable framework to produce technical reports (TR) and specifications (TS) that define radio access, core network and service capabilities. Global convergence towards the 3GPP specifications of complete system description has allowed mobile telecom market growth on stable standardization platform.

3GPP started work in 1998 with scope to maintenance and development of technical specifications and technical reports for evolved mobile technologies, from 3G to 6G. A 3GPP Project agreement describes the basic principles and ideas on which the development is based. 3GPP Working procedures cover description and purpose of the project, participation, structure, responsibilities of the groups, work programme and technical coordination, deliverables, reporting, external relations. 3GPP Technical specification group (TSG) plenary meetings are maintain quarterly four times a year and 3GPP specifications are made available. At each TSG round, specifications can be brought under change control, unchanged from their previous versions, revised as a result of incorporating approved change requests, or upgraded to that Release with no technical change [6].

3GPP Work plan provides details of the co-operation between all the TSGs. These targets are *features* or study items (SI) that add new or enhanced functionality to the existing mobile system. Feature development is based around Releases (R). The work plan is driven by the estimated freeze date of current and future releases and the functional content of each release. It is possible that features may span more than one release. These features are divided into building blocks and work tasks, which lead to the production of technical specifications or reports. Specifications are then brought under change control – where a *change request* is needed to propose any modifications to a specification for approval to the technical specification groups. The official work item (WI) description is maintained by the responsible TSG. The work plan is a table that contains all of the deliverables being worked on, with the most recent WIDs and SIDs at the top of the plan and earlier items listed at the bottom [7].

The 3GPP production of specifications and studies are contribution-driven, by member companies, in working groups WG and at the technical specification group TSG level. Technical specification groups are Radio Access Networks (RAN), Services & Systems Aspects (SA), Core Network & Terminals (CT) as shown in the Fig. 1. The working groups WG, within the TSGs, meet regularly and come together for their quarterly plenary meeting, where their work is presented for information, discussion and approval. Technical specification group TSG SA is responsibility for the overall coordination of the technical work and for the monitoring of its progress.

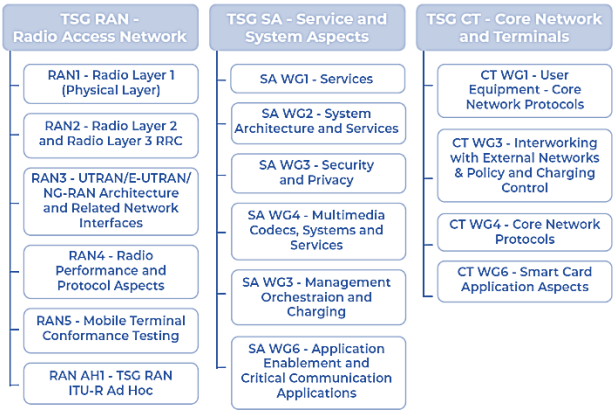



Figure 1. 3GPP technical specification groups TSG and working groups WG.

Real progress on 3GPP standards is monitored by publication a particular Releases. When Release is completed, new features are functionality *frozen*, ready for global implementation. 3GPP works on a number of Releases in parallel, starting future work well in advance of the completion of the current one. Such a concept ensures that progress is continuous and stable. The major concern for all 3GPP Releases is to make the mobile system backwards/forwards compatible, to ensure that the operation of user equipment is livelong.

The 3GPP completed the first release of fifth generation (5G) mobile communications in its **Release-15** in June 2018, and fully specified by September 2019 laying the groundwork for global commercial 5G deployments. Release-16 introduces significant enhancements that improve existing features and address new use cases and deployment scenarios. The primary new use cases and deployment scenarios addressed in **Release-16** include enhanced support of ultra-reliable low-latency communications (URLLC) and IIoT. 3GPP's submission to the International Mobile Telecommunications-2020 (IMT-2020) encompassed Release-15 and Release-16 functionality. The International Telecommunication Union Radiocommunication Sector (ITU-R) officially approved 3GPP's submission as 5G technology in February 2021 [8, 9]. Subsequently, 3GPP has been working on evolving 5G technology in its releases to achieve further performance improvements and cater to new use cases. In transitional **Release-17**, 5G features are significantly enhanced, with new use cases and deployment scenarios, including robust support for IoT RedCap and non-terrestrial networks (NTN).

The 5G system is described in over a thousand technical reports (TRs) and technical specifications (TSs). 3GPP specifies RAN air-interface, protocols and network interfaces that enable the entire mobile system: call and session control, mobility management, service provisioning, etc. Thanks to this approach 3GPP networks can operate in an inter-vendor and inter-operator context.

5G system (5GS) includes user equipment (UE), radio access network (RAN) and core network (5GC), as shown in the Fig. 2. 5G's radio technology is called NR (New Radio). The main entity of the RAN is the gNB which further splits into a central unit (CU) and one or more distributed unit(s) (DU). The 5GC is here schematically represented by user plane function (UPF), handling the user data and, in the signaling plane, access and mobility management function (AMF) that accesses the UE and the RAN. The user plane functions are distributed and geographically close to the RAN to minimize user plane latency, while the control plane functions are centralized to take advantage of virtualization [10, 11, 12].

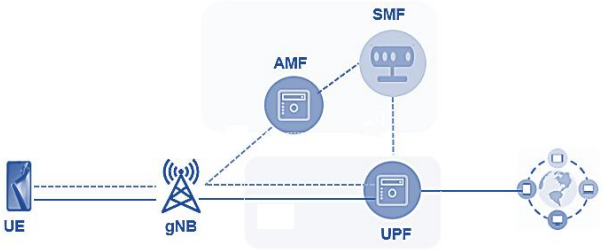



Figure 2. Overview of 5G system: user equipment (UE), radio access network (RAN) and core network (5GC).

The 5GC relies on a service-based architecture (SBA), where the architecture elements are defined in terms of network functions (NFs) and interfaces of a common framework. A protocol stack is defined for communications between several NFs as shown in the Fig. 3. Such an SBA approach offers modularity and reusability [13, 14].

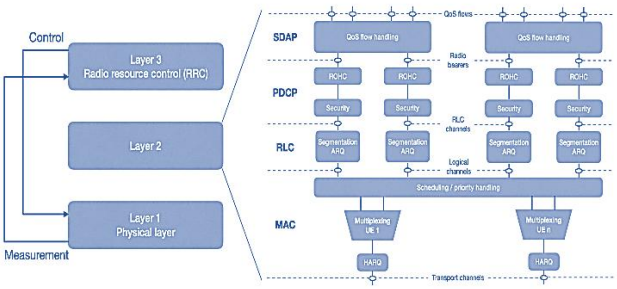



Figure 3. Overview of 5G NR protocol architecture.

## 3. 5G-ADVANCED EVOLUTION

The 5G-Advanced evolution promises improvements in **Release-18** NR, AI/ML integration, advanced network features, satellite communications. Further progress continues in **Release-19** and transitional **Release-20**, focusing on expanding AI/ML use cases and exploring 6G capabilities [15, 16, 17].

### 3.1 3GPP Release-18

The initial release for 5G-Advanced was functionally frozen in March 2024, and specifications were published in June 2024. In December 2021, 3GPP approved 5G-Advanced as a working items package following six months of intensive discussion. The package comprises 27 diverse study or work items, aimed at enhancing network performance and addressing novel use cases. In particular, The release aims to promote a balanced evolution of 5G across key technology areas. This approach has resulted in the definition of many study items SI and their setup as work items WI in later releases. Significant topics include MIMO enhancements, evolved duplexing, AI/ML data-driven designs. Release-18 is considered an advanced version of 5G and covers the following aspects:

- NS (Network Slicing) enhancements aim to improve the flexibility and scalability of existing network slicing technologies, including multi-domain and multi-provider slicing.
- NTN (Non-Terrestrial Networks) supports satellite communications, thus enabling 5G services in underserved and remote/rural areas where traditional terrestrial networks may not be feasible.
- Enhanced AI and automation aim to improve the efficiency and performance of 5G networks by introducing advanced features to optimize network performance and automate network management tasks.
- Mission-critical services introduce new features that improve the reliability and performance of services, such as public safety communications and emergency response.
- Advanced energy efficiency features aim to reduce the environmental impact of 5G and lower operating costs.

Release-18 introduces several new features and enhancements to the performance, efficiency, and capabilities of 5G networks. Moreover, 5G-Advanced brings new use cases and applications that demand higher data rates, lower latency, and improved reliability. It is designed to fully realize the system's capabilities and encompasses numerous technological innovations that benefit network and system operators, end-users, and various industries. The key features include improved coverage and capacity, enhanced end-user experience, and enhancements necessary for more demanding applications. 5G-Advanced leverages ML to adapt to the environment, enhance performance, and manage complex optimizations. It also focuses on energy efficiency to reduce network power consumption and maximize device battery life. Furthermore, it includes industrial IIoT enhancements to support industrial use cases that require high reliability, low latency, and high availability.

### 3.2 3GPP Release-19&20

The second release for 5G-Advanced, started in early 2024. Items SI/WI were decided in December 2023 after 500 presentations were submitted to the two dedicated workshops. The deadline for the functional freeze of features is September 2025, with the ASN.1 & Open API freeze completed and publication by December 2025.

From the 2026, Release-20 take center stage, with its accent on projects for both 5G-Advanced and 6G. This dual-track transitional framework allows 3GPP working groups to innovate within 5G-Advanced, while simultaneously initiating the research phase for 6G.

The decision on Release-20 content are made in the first half of 2025, with approved deadlines for functional freeze by March 2027 and publication specification by June 2027.

## 4. 6G RESEARCH & STANDARDIZATION

Global 6G technology standardization is about to get started. The first 3GPP Workshop on 6G was organized in March 2025, a decade after the first 5G Workshop in September 2015 [18, 19]. Mobile network operators, industry associations, hardware/software vendors, academia, system integrators, and technology providers assembled to discuss the focus of the upcoming Release-20 study items. Participants focused on narrowing the scope of 6G, introducing more constraints around use cases and architecture.

Following on from the first 6G Workshop March 2025, studies in TSG RAN on *Scenarios and requirements* and in WG SA1 on the *Use cases and service requirements* are underway. Further Release-20 technical studies will start in June 2025 by approval the first 6G Working Group at the Plenary meeting. This is an important moment in time that sets the stage for commercialization around 2030 [20, 21].

The Release-20 study items offer a comprehensive framework for 6G development by outlining the key use cases and service requirements for the future mobile system. TSG RAN approved in December 2024 6G study items supported by over 50 companies from diverse countries and regions from the broader telecommunications sector to make a global interoperable standard. This study items (SIs) investigates a candidate set for minimum technical performance requirements (TPRs) based on the ITU-R recommendation and, where applicable, the associated target values and key

assumptions for the identified minimum requirements. 3GPP technical report (TR) presents a study on 6G use cases and service requirements in its Stage 1 phase for Release-20 [21]. This document serves as a foundational study to guide the future development of the 6G mobile communication system. It outlines key use cases and service requirements, providing comprehensive framework for 6G development. Each use case provides a structured analysis including descriptions, pre-conditions, service flows, and potential new requirements for 6G system:

- It explores key aspects of the future mobile system, starting with system and operational factors such as migrating from existing networks, roaming, interconnection, and interworking.
- 6G security significantly focuses on network security, base station validity, and user privacy.
- Technical report also emphasizes network resilience, promotes sustainability through energy efficiency, and supports a variety of user equipment UE types.
- Additionally, the document explores technologies such as Integrated Sensing and Communication (ISAC) and artificial intelligence (AI) integration for network optimization and intelligent services.
- It aims to provide ubiquitous connectivity through integration terrestrial and non-terrestrial networks NTN, enabling services in underserved and remote areas.
- Use cases around immersive and massive communication are also detailed, related to smart homes, factories, transportation, and smart cities and countries.

The official start of normative work on 6G will be **Release-21**, producing the first 3GPP technical specifications. The Release-21 timeline is expected to be finalized by June 2026, with the ASN.1 & Open API freeze projected no earlier than March 2029. Release-21 normative 6G specification work is expected to align with submission of next generation radio-interface technologies (RIT) for the terrestrial component of IMT-2030 standard [22, 23].

## 5. CONCLUDING REMARKS

The evolution of 3GPP from Release-15 to Release-20 has been a decade-long path of innovation and collaboration. Each release has contributed uniquely to building a global and versatile technology ecosystem that has advanced connectivity, expanded possibilities, and prepared the base for the next generation of mobile networks. One of the most significant takeaways is the importance of adaptability and collaboration.

The first 3GPP Workshop on 6G was organized in March 2025, a decade after the first 5G Workshop in September 2015. In the past decade, lessons learned and foundations serve as important guidelines for future 6G hyper-connected world where communication, sensing, and AI converge to create seamless and immersive experiences.

## REFERENCES


[1] D.A.Milovanovic, T.P.Fowdur, Z.S.Bojkovic, (Eds.), *Towards integration 6G NTN Non Terrestrial Networks with 5G satellite connectivity*, CRC Press 2026.

[2] T.P.Fowdur, D.A.Milovanovic, Z.S.Bojkovic, (Eds.), *Intelligent and sustainable engineering systems for Industry 4.0 and beyond*, CRC Press 2025.

[3] D.A.Milovanovic, Z.S.Bojkovic, T.P.Fowdur, (Eds.), *Driving 5G Mobile communications with Artificial Intelligence towards 6G*, CRC Press 2022.

[4] Z.S.Bojkovic, D.A.Milovanovic, T.P.Fowdur, (Eds.), *5G Multimedia communications: Technology, multiservices, deployment*, CRC Press Oct. 2020.

[5] H.Holma, A.Toskala, T.Nakamura, *5G technology: 3GPP evolution to 5G-Advanced*, 2E Wiley, 2024.

[6] 3GPP TS21.900, *Technical specification group working methods*, Sept. 2020 – March 2025.

[7] 3GPP TR21.801, *Specification drafting rules*, Sept. 2020 – March 2025.

[8] ITU-R Recommendation M.2083, IMT-Vision *Framework and overall objectives of the future development of IMT for 2020 and beyond*, Sept. 2015.

[9] ITU-R Recomm. M.2150, *Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-2020* (IMT-2020), 2021-2023.

[10] 3GPP TS22.261, *Service requirements for the 5G system*, Aug. 2016 – March 2025.

[11] 3GPP TS23.501, *System architecture for the 5G System (5GS)*, Dec. 2016 – March 2025.

[12] 3GPP TS38.401, *NG-RAN; Architecture description*

[13] 3GPP TS38.300, *NR; NR and NG-RAN Overall description; Stage-2*, March 2017 – March 2025.

[14] 3GPP TS 23.502, *Procedures for the 5G System (5GS)*, Dec. 2016 – March 2025.

[15] 3GPP TR 21.918, *Release 18 Description, Summary of R18 Working Items*, March 2025.

[16] 3GPP *Release 19 and Release 20 Work Plan*, 2025.

[17] 3GPP TS 22.261, *Release 20, Service requirements for the 5G system*, March 2025.

[18] 3GPP *6G Workshop*, Incheon, South Korea, March 2025.

[19] 3GPP *5G Workshop*, Phoenix, United States, Sept. 2015.

[20] 3GPP TSG RAN RP-243327, *New SID: Study on 6G scenarios and requirements*, Dec. 2024.

[21] 3GPP TR 22.870 *Release 20, Study on 6G use cases and service requirements*, Stage 1, March 2025.

[22] ITU-R Recommendation M.2160, *Framework and overall objectives of the future development of IMT for 2030 and beyond*, Nov. 2023.

[23] X.Lin et al., "Embracing AI in 5G-Advanced toward 6G: A joint 3GPP and O-RAN perspective", IEEE *Communications Standards Magazine*, vol.7, no.4, pp.76-83, Dec. 2023.

# THE POSITION, ROLE AND COMPETENCES OF DATA PROTECTION OFFICERS IN THE EU LAW

Izv. prof. dr. sc. Tihomir Katulić, University of Zagreb Faculty of Law, tkatulic@unizg.pravo.hr

**Abstract:** *The Data Protection Officer (DPO) is an important role provided by the General Data Protection Regulation (GDPR) to oversee compliance with data protection legislation and ensure the safety of personal data. The DPO position is mandated for public authorities, organizations handling substantial volumes of sensitive data, and those engaged in extensive tracking of data subjects, introduced to rectify inconsistencies in the prior regulation and establish a common EU data protection standards. DPOs need comprehensive expertise in data protection law, processing practices and information security. Their responsibilities encompass providing compliance guidance, training employees, and collaborating with regulatory bodies. DPOs need to maintain independence and prevent conflicts of interest in order to promote a culture of data protection within organizations. This position is crucial for establishing confidence in the digital economy and safeguarding individuals' fundamental rights and liberties.*

**Keywords:** *Personal data, data protection officer, data protection impact assessment, privacy by design and by default.*

## 1. INTRODUCTION

The European legislators embarked on the development of the General Data Protection Regulation (GDPR) motivated by a series of different goals, motives and needs that became apparent during the application of national regulations based on the 1995 Data Protection Directive, the first general purpose EU data protection law. One of the main motives arose from the Union's desire to establish uniform rules for better protection of personal data within the Union. Prior to the implementation of the GDPR, different national rules were applied, which made it difficult for commercial companies and other entities operating in multiple EU countries to conduct business due to often unpredictable regulatory and oversight standards and behavior.

After GDPR went into application, there were several significant changes in the behavior of European data controllers and processors – efforts to adapt their business processes were actively intensified, which enabled the emergence and development of a new category of legal and business services – services for compliance with the requirements of the legal framework for personal data protection. Among data subjects, there is a continuous trend of increasing awareness about the data subject rights and ways to exercise the rights arising from the GDPR. Supervisory authorities very quickly began to impose high administrative fines on organizations that failed to align their data processing procedures with the GDPR [1].

In short, the start of the application of the GDPR (as well as similar national laws in EU Candidate Member States) usually marks a significant change in how companies and other organizations manage personal data, with an emphasis on greater transparency, security, and accountability. This change historically created a lot of uncertainty and misunderstanding regarding the scope, content and enforcement of the new legal framework.

The GDPR entered into force in May, 2016 and into application on 25h of May 2018. In the period leading up to the entry into application, many an European organization experienced an unprecedented state of regulatory confusion and panic, mostly about the anticipated high financial penalties, along with ongoing debates on topics more familiar to the general public such as legitimate interest or the right to be forgotten [2]. The Data Protection Officer or DPO, as defined in the General Data Protection Regulation, is a comparatively less visited topic, undeservedly so as it represents an important compliance function and new aspect of interaction between regulation, technology and practice. At the same time it represents a novel career direction for young lawyers and technical experts in the field of data protection [3].

In the first part of the paper, we will review the institute of the DPO as it was regulated in European legislation before the entry into force of the General Data Protection Regulation, and present the reasons for its establishment within the framework of the General Data Protection Regulation.

The central part of the paper details the provisions of the GDPR relating to the appointment and qualifications of the DPO. Within these chapters, special emphasis is placed on difficulties in interpreting certain provisions, as well as on recommendations where they exist.

It should be noted that the main part is based on the Guidelines on Data Protection Officers of the Article 29 Data Protection Working Party [4], which, along with the Regulation itself and applicable administrative decisions by national data protection authorities and ultimately judicature of national courts and the CJEU, represent the official legal sources for interpreting and understadning the role of the DPO.

## 2. DATA PROTECTION OFFICER BEFORE THE ADOPTION OF THE REGULATION

Although the institute of the Data Protection Officer first appeared in West Germany in the 1970s [5], it only came to life with the adoption of Directive 95/46/EC [6]. It provided for the possibility for member states to simplify or exempt the controller from the obligation to notify the supervisory authority about processing activities by appointing a DPO. *"(...) when the controller, in accordance with the national legislation governing its operations, appoints a DPO who is specifically responsible for ensuring, in an independent manner, the internal application of national provisions adopted in accordance with this Directive, maintaining a record of processing operations carried out by the controller, containing certain information from Article 21(2) of this Directive, thereby ensuring that the processing operations do not adversely affect the rights and freedoms of the data subjects."* The Directive opens up the possibility but does not create an obligation for his appointment, from which it can be concluded that the Directive aimed to encourage the creation of the DPO position as a means of a kind of compromise between the stricter and financially burdensome obligation of direct notification of processing to the supervisory authority and the simplicity of daily operation of the data processing supervisor. Many EU Member States embraced this solution in their adaptations of the Directive into their own legislation, but due to the vagueness of the position itself, as well as the legal nature of the directive as an EU legislative act without direct application, the provisions were not uniform. In the Croatian legal system, the DPO was introduced as an institute through amendments to the Personal Data Protection Act (PDPA) in 2008 and 2011 under the name of Personal Data Protection Officer [7]. With the first amendment to the Act, namely the creation of Article 18a, the possibility of appointing a DPO was provided, and it was determined that *"(...DPO) takes care of the legality of personal data processing and the realization of the right to personal data protection and cooperates with the Personal Data Protection Agency regarding the supervision of personal data processing."*

The second amendment made in 2011 completely changed the text of the DPO provision and expanded the provisions on the appointment, position, and tasks of the DPO, providing for the possibility of his appointment for controllers with fewer than 20 employees and as an obligation for controllers with more than 20 employees, obliging the data controller to report the appointment to the Personal Data Protection Agency, a standard obligation that was renewed by the provisions of Article 37 of the GDPR. PDPA excluded the possibility of appointment of a person against whom proceedings are being conducted or a measures have been imposed for breach of official duty or work obligations, or to whom a measure has been imposed for breach of the employer's ethical code. The DPO was obliged to maintain the confidentiality of all information and data he becomes aware of in the course of his duties, which are as follows: to take care of the legality of personal data processing in terms of compliance with the provisions of this Act and other relevant regulations, to warn the personal data controller about the necessity of applying relevant regulations in cases of planning and actions that may have an impact on privacy and personal data protection issues, to inform all persons employed in processing about their legal obligations, to ensure the fulfillment of obligations from Articles 14 and 17 of the Act, to enable the exercise of data subjects' rights from Articles 19 and 20 of the Act, to cooperate with the Personal Data Protection Agency regarding the supervision of processing [8].

With these and other amendments from the Act on Amendments to the Personal Data Protection Act of 2011, it was brought into line with Directive 95/46/EC. This determination of the Personal Data Protection Officer lasted until the PDPA was repealed with the entry into force of the GDPR and the adoption of the accompanying implementing act, in which the legislator chose not to specify the role of the DPO and to leave the normative of the institute to the GDPR through its direct and complete application [9].

## 3. WHY THE DATA PROTECTION OFFICER?

As Directive 95/46/EC proved ineffective in creating a common legal framework for data protection due to differences in its implementation and application in the national legislation of Member States, a need for a direct application approach through a Regulation became pressing.

Such fragmentation, as observed from 1998 to 2014 in the EU, can lead to hindering the flow of personal data, as well as representing an obstacle to conducting economic activities and disrupting market competition in the EU. The

adoption of the GDPR was presented as an ideal solution to these problems by establishing directly applicable rules in Member States, which were left with the possibility of only additional determination by national provisions. The Member States could only add additional obligations to the data controllers in their competence, but not disregard standards set by the GDPR. This would ensure a consistent application of rules for the protection of individuals' fundamental rights and freedoms in relation to the processing of personal data [10].

Since achieving the goals set by the Regulation requires expertise and skills not many employees have, the legislator provided the situations where having the benefit of a DPO advice was mandatory to data controllers and data processors. The appointment, position, and tasks of the officer are regulated by Articles 37 to 39 of the GDPR.

## 4. APPOINTMENT OF THE DATA PROTECTION OFFICER

### 4.1. Mandatory designation of a DPO

Article 37.1 of the GDPR states: *"The controller and the processor shall designate a data protection officer in any case where the processing is carried out by a public authority or public body, except for courts acting within their judicial competence."*

Public authorities and public bodies are obliged to appoint a DPO, taking into account the higher level of responsibility expected from state bodies, the increased significance and scope of their work, and the need to maintain trust in state institutions; individuals often will not have a significant influence over the controller in such processing cases, so it is in their interest to have an increased level of protection from potential breaches of personal data when being processed by public bodies [11].

The obligation to appoint a DPO does not apply to courts acting within their judicial competence, with the purpose of protecting the independence of the judiciary in performing judicial tasks, which includes official decision-making, but the possibility of supervising data processing actions by a special body within the judicial system of the member state is not excluded. Given that the Regulation generally does not apply to judicial authorities, it makes sense that these bodies do not need a DPO whose main task is to monitor compliance with that same Regulation. This rule applies to both the controller and the processor. Although it is not always necessary for the processor to appoint a DPO if the controller meets one of the conditions for mandatory appointment, in this case, it will be mandatory, even if the processor is not a public authority, but processes data for a controller who is [12].

### 4.2 Regular and Systematic Monitoring On a Large Scale

Further, another mandatory designation situation is when *"... the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, scope, and/or purposes, require regular and systematic monitoring of data subjects on a large scale."*

In extensive and long-term data processing, the dangers in terms of possible abuse and data breach are much more prevalent and require a higher level of protection, which the DPO can help ensure. It is important to pay attention to the following elements: processing of personal data is a core activity, requires regular and systematic monitoring, and its implementation on a large scale. [13]

The Regulation briefly explains what is considered as a core activity: *"(...) the core activities of the controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities"*, so they can be considered key actions necessary to achieve the objectives of the controller or processor. It is clear that the Regulation distinguishes between primary and ancillary activities and that only the primary obligation is considered a core activity in terms of the obligation to appoint; although the provision mentions the processing of personal data as an ancillary activity, this does not mean that it cannot also be primary (if it forms an integral part of the activities carried out by the controller or processor), but also that data processing that has a factually essential role in the operation of the controller or processor (for example, keeping employee records for payroll purposes) can be considered an ancillary activity. The Regulation does not define what is considered regular and systematic monitoring; the closest it comes to this is in Recital 24, where it sets criteria for determining the monitoring of data subjects' behavior, with the understanding that, given the focus on internet monitoring techniques, they should be considered as an example, not an exclusive provision. WP29 in its guidelines addresses this vagueness by defining 'regular' as ongoing or occurring at specific intervals over a certain period, recurring at precisely defined times, and/or maintained continuously or periodically, while 'systematic' is defined as occurring according to a system, predetermined, organized, or methodical, as part of a general plan for data collection and/or carried out as part of a strategy. The guidelines also contain examples of activities that could be considered regular and systematic [14].

As in previous cases, the Regulation does not define the term 'large scale', although Recital 91 mentions *"processing operations of large scope"*, which could be

used as a guideline for determining that term. Practically speaking, it is not possible to determine an exact amount of data being processed or the number of persons covered by the processing that would be considered large scale, in a way that can be applied to all cases. It is possible that over time, a practice will develop for determining the necessary amount/number or their approximation for certain, more common, processing procedures. WP29 recommends that the criteria for determining the scale of processing include the number of subjects (either as an exact number or as a ratio of the relevant population), the volume of data and/or the range of different data being processed, the duration or permanence of the processing activity, and the geographical scope of the processing activity. As with the previous elements of this point, the guidelines provide several examples for easier interpretation [15].

**4.3 Special Categories of Data**

Finally, Article 37.1 stipulates: *"The controller and the processor shall designate a data protection officer in any case where the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10."*

In this case, the mandatory appointment of a DPO is provided because it involves data whose processing could lead to significant risks for the fundamental rights and freedoms of the individual, given their particularly sensitive nature with regard to fundamental rights and freedoms. In this point, it is important to emphasize that it must relate to the core activities of the controller or processor and that the processing is extensive; it can be expected that these facts will be determined on a case-by-case basis. Special categories in Article 9 of the Regulation are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health, or data concerning a natural person's sex life or sexual orientation. Personal data in Article 10 of the Regulation relate to criminal convictions and offences or related security measures [16].

In addition to the reasons in Article 37(1), the Regulation provides for another, additional case in paragraph 4 of the same article where the appointment of a DPO is mandatory as imposed by EU law or the law of a member state. In this way, the Regulation authorizes member states to independently regulate cases of mandatory DPO appointment outside the framework of the Regulation itself, as well as the possibility of expansion through EU law, such as judgments of the European Court, directives, and the like.

**4.4. Professional Qualifications**

Previously, before the GDPR, the DPD did not provide qualification criteria for DPOs. GDPR in Article 37.5 now provides: *"The data protection officer shall be designated on the basis of professional qualifications, in particular expert knowledge of data protection law and practices, and the ability to fulfil the tasks referred to in Article 39."* WP29 clarifies the concepts of professional qualifications, level of expert knowledge, and ability to perform tasks [17].

Professional qualifications represent expertise in national and European data protection legislation and adequate knowledge of the provisions of the Regulation. They also refer to the understanding of the practice of data protection where it is important to understand the business processes of an organization, its data systems and processing activities, security needs, and specific risk profile. Therefore DPO skills include a combination of legal, organizational, and technical knowledge. The supervisory authority can assist in acquiring some of this knowledge through appropriate and regular training for DPOs, especially where the DPO performs duties with a public authority or public body, and should be well acquainted with the appropriate administrative rules and procedures.

Expert knowledge needs to be proportional to the sensitivity, complexity, and amount of personal data being processed; the DPO should be carefully selected considering the data protection challenges expected to arise in the organization. Accordingly, the necessary level of expert knowledge should be determined specifically in relation to the data processing procedures being carried out and the protection required for the processed data by the controller or processor.

The ability to perform tasks relates to the qualities of the DPO (such as personal integrity or a high level of professional ethics) and knowledge, but also to their position within the organization. Given the wide range of abilities and knowledge that the DPO must have, there is a problem of finding the right experts, as well as the way of acquiring and proving the required abilities and knowledge. A solution to this problem could be found in the certification process, which the Regulation itself recommends in Recital 100 and regulates in Articles 42 and 43. This process has many advantages: it can serve authorities as confirmation that the appointed DPO meets the conditions set by the Regulation, as a way to build and maintain a high level of compliance with the Regulation

across Europe, and as a way to achieve legal certainty for organizations that want to demonstrate compliance. A notable disadvantage of certification is the cost; individuals who wish to prove with a certificate that they possess the necessary competencies must do so before employment, i.e., bear the costs of training themselves, which can have a discriminatory effect [15].

Although it is possible to acquire the necessary abilities and knowledge through regular education, universities and law schools usually do not adapt to the needs of the labor market quickly enough, although educational institutions in some member states have begun to introduce specialized courses and training focused on DPO education. In the Croatian higher education system, the curriculum necessary for training the adequate future DPOs is covered by courses and training at the Faculty of Law and the Faculty of Electrical Engineering and Computing of the University of Zagreb; there are also targeted courses and training provided by private companies and there are regional and global industry associations and education providers [16].

### 4.5. Other Relevant Provisions

GDPR provides that a group of undertakings may appoint a single DPO provided that he is easily accessible from each establishment. The concept of accessibility in this context is not determined as strict physical presence at the processing location, but is linked to the role of the DPO as a contact person with data subjects, with the supervisory authority, but also within the organization of the controller or processor. To enable the DPO to fulfill these roles, he must be able to communicate effectively with data subjects and cooperate with the supervisory authority. This is achieved in several ways, one of which is the use of the language used by the supervisory authority or data subjects. Given that much of the data processing today is done digitally and using the internet, the DPO's obligations often spill over beyond his home country, and it is unreasonable to expect one person to be physically available in all establishments, to master the knowledge of all necessary languages, and the specifics of the normative arrangements of member states. For this purpose, the DPO may have team members located in the respective countries, who, in addition to meeting language needs, can also provide support in terms of legal expertise for their home countries. If such teams are formed, it is considered that the DPO's knowledge of the English language is sufficient to meet the accessibility requirement [17].

In order to facilitate the accessibility of the officer, the GDPR in Article 37 determines the obligation to publish the contact details of the DPO and to communicate them to the supervisory authority. The DPO needs to be able to be contacted independently of the rest of the organization in which he performs that duty, both within the organization and outside it, and the confidentiality of those communications must be maintained. WP29 states that the aforementioned contact details should include a postal address, a separate telephone number, and/or an email address, and other means of contact as necessary, such as a contact form on the website. Publishing the officer's name is not mandatory under the Regulation, but communicating it to the supervisory authority is necessary to enable cooperation and fulfill the officer's function as a contact person with it. Good practices include publishing the name in contact details, developing an internal network for contacting the DPO in organizations where he performs that duty, informing data subjects about the DPO at the time of processing, and establishing a separate mailbox for the DPO.

Article 37.6 provides that "… *data protection officer may be a member of the staff of the controller or processor or perform tasks on the basis of a service contract."*

This opens the option for controllers and processors to appoint an internal or external DPO. The guidelines of WP29 emphasize that the external DPO is in no way different from the internal one, enjoying the protection provided by the GDPR such as protection of independence in action and protection from unjustified dismissal or penalty. In choosing between these two models, DPOs as employees or outsourced DPOs, controllers or processors decide based on their needs regarding data processing, as well as the size of their organization and available financial resources. The advantages of an internal DPO are that he has better insight into the operations and ongoing processing activities of the organization, facilitates the establishment of a system for handling personal data that meets the needs of the organization, facilitates internal contact in the organization (especially if the organization consists of several separate units), and as such is recommended for large enterprises, groups of undertakings, and enterprises engaged in high-risk data processing. On the other hand, the external DPO is characterized by previously acquired expert knowledge and a professional approach, often has insurance for possible damage caused by breach of contract, has a more liberal relationship with the organization as not being retained on the basis of an employment contract, and this solution is recommended for small and medium-sized enterprises [18].

## 5. TASKS OF THE DATA PROTECTION OFFICER

### 5.1 Tasks According to Article 39

The tasks of the DPO, as listed in Article 39(1) of the Regulation, represent the minimum duties they perform, with the provision that they may perform other actions provided that the condition of avoiding conflicts of interest is met.

*"Monitoring compliance with this Regulation and with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits."*

Here, it is necessary to emphasize again that the organization handling the personal data, the data controller or data processor is responsible for the compliance of their actions with the GDPR, not the DPO as an individual. Activities that the DPO could carry out for this purpose are collecting information with the aim of identifying processing activities, analyzing and checking the compliance of processing activities, and informing, advising, and issuing recommendations to the controller or processor. Although conducting a data protection impact assessment is the task of the controller, not the officer, DPO has the task of providing advice regarding that assessment and monitoring its performance in accordance with Article 35, and as such, has an important and useful role in assisting the controller facilitating the *data protection by design* approach as envisaged by the Article 25 of the GDPR [19].

The guidelines suggest that the controller should seek advice from the DPO on the following issues related to assessments: whether to conduct an assessment, how to conduct it, whether to conduct it internally or entrust its implementation to an external collaborator, what precautions (including technical and organizational ones) to apply in order to reduce the risks to the rights and interests of data subjects, whether the assessment was carried out accurately, and what its outcome is, i.e., whether processing can continue. If the controller decides to refuse to act on the DPO's advice, the documentation related to the Assessment should contain justification for such a position of the controller; it is useful to record all advice given by the DPO in order to facilitate their argumentation later.

The DPO cooperates with the supervisory authority and act as a contact point on issues regarding processing, including prior consultation under Article 36, and consulting on any other issues as needed. These tasks relate to the role of the DPO as a facilitating factor for the supervisory authority in terms of access to documents and data necessary for performing its tasks under Article 57 of the GDPR, as well as exercising investigative, corrective, and advisory powers and those related to approval under Article 58. Although the DPO is bound by confidentiality, this obligation does not prohibit the DPO from contacting the supervisory authority for advice on any issue, as needed. Such a relationship between the DPO and the supervisory authority creates a kind of parallel structure, in which the DPO reports both to the organization in which he performs his duty and to the supervisory authority, which can cause dissatisfaction with the organization that pays the DPO and, accordingly, expects his dedication to their interests. It is necessary to emphasize that the DPO's obligation to cooperate with the supervisory authority does not include the obligation to report to it about personal data breaches, since that is the obligation of the controller, although the DPO will perform the role of a contact person for the supervisory authority in such situations [20] [21].

In performing his tasks, the DPO takes into account the risk associated with processing operations and considers the nature, scope, context, and purposes of processing. This task represents a requirement for the DPO to prioritize activities and direct his efforts to issues that present a greater risk to data protection; in this sense, it represents a general, common-sense principle that can be applied to many aspects of the DPO's daily work. This, of course, does not mean that they should neglect monitoring compliance with lower-risk processing procedures, but it indicates that the emphasis of their actions should be on higher-risk areas. Using such a selective and pragmatic approach should help DPOs advise controllers on the methodology for conducting assessments, which areas should be subjected to internal or external data protection audits, what internal training activities to provide for staff or management personnel in charge of data processing activities, and which processing actions to devote more time and resources to. The application of such an approach is especially important for small and medium-sized enterprises, which are likely not to have a large amount of funds and resources for data protection activities.

This approach is surprising on the one hand because the protection of individuals with regard to the processing of personal data is a fundamental right established by the Charter of Fundamental Rights of the European Union and the Treaty on the Functioning of the European Union, but, on the other hand, the Regulation itself emphasizes that the right to data protection is not an absolute right, but must be considered in relation to its function in society and

balanced with other fundamental rights in accordance with the principle of proportionality. There is also an interpretation of the concept of risk in the Regulation as the risk of non-compliance with the Regulation itself rather than the risk of violating the fundamental rights and freedoms of individuals in processing activities.

**5.2 Other Tasks**

In Article 39(1) of the GDPR, a list of the DPO tasks is provided, the performance of which is considered the minimum, and the controller or processor are generally not prevented from assigning other tasks to the DPO. An example of such an assigned task is maintaining records of processing activities, for which the controller or processor is otherwise responsible.

In the practice of numerous existing national regulations and according to the data protection rules applicable to EU institutions and bodies, DPOs compile lists and maintain records of processing activities based on information provided to them by various departments in their organization responsible for processing personal data. Such records can be considered one of the tools that enable the DPO to perform his tasks in terms of monitoring compliance, informing, and advising the controller or processor. [22],

Other examples where the officer could perform tasks for which the controller is otherwise responsible include enabling data subjects' rights to access their personal data, correcting inaccurate or supplementing incomplete personal data of data subjects upon their request, deleting personal data of data subjects upon their request, performing tasks of transferring personal data to another controller, etc.

**6. CONCLUSION**

GDPR and many of the new generation of data protection laws modelled upon the GDPR, from those from EU candidate members to laws developed by legal systems of Gulf Countries, South East Asian democracies or countries of Latin America, are often taken as a living example of the so called Brussels effect [23].

More specifically, we can conclude that provisions regarding appointment and competence of the DPO have become an international legal standard. GDPR and related laws have taken a step towards ensuring an independent and unimpeded DPO function, which is indispensable for safeguarding of data subject rights.

Given a relatively (in legislative terms) short period that has elapsed since GDPR entered into force, it is not surprising that there is comparatively little scientific research on the practical performance of data protection officers under the GDPR, which invites further research.

Taking into account everything established so far, the DPO will continue to be an essential part of the EU data protection legal framework, as well as an exciting development of the legal profession in general.

**7. REFERENCES**

[1] GDPR Enforcement Tracker, available at https://www.enforcementtracker.com/ .

[2] Mulley-Goodbarne, E.: "*GDPR is the biggest change in 20 years but no reason to panic*", MobileNews, 2018, available at: https://www.mobilenewscwp.co.uk/Features/article/gdpr-biggest-change-20-years-no-reason-panic, last accessed 30/04/2025.

[3] Tomaževič, N. et. al.: "*Artificial Intelligence for human-centric society: The future is here*", Zavod 14, 2023, Katulic:"*CISO, DPO, AIHO? Navigating the EU's AI regulatory efforts in pursuit of data protection and information security compliance*", p. 56, Brussels, Celje, 2023.

[4] European Data Protection Board, WP 29 Guidelines on Data Protection Officers ('DPOs') (wp243rev.01), available at: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=44100 last accessed: 30/4/2025

[5] Recio, M.: "*Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability"*; European Data Protection Law Review, no. 1/2017, p. 114., Lexxion, Karlsruhe, 2017.

[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L 281, 23/11/1995 P. 0031 - 0050*

[7] The Law on the Amendment of the Personal Data Protection Law, Official Gazette of the Republic of Croatia OG 41/2008 and OG 130/2011.

[8] Ibid, Art. 5

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88

[10] GDPR Art. 37-39.

[11] *Ibid.*

[12] *Ibid* Guidelines on DPOs, p. 10.

[13] *Ibid* Guidelines on DPOs, p. 7.[14] *Ibid* Guidelines on DPOs, p. 8.

[15] *Ibid* Guidelines on DPOs, p. 20-25.[16] *Ibid* Guidelines on DPOs, p.19. See also Data Protection Lifelong Learning Program established by the UNIZG Faculty of Law available at: https://www.pravo.unizg.hr/en/studiji/cjelozivotno-obrazovanje/prakticna-primjena-opce-uredbe-o-zastiti-podataka/ , the Zagreb University Specialist Program in Cybersecurity: https://www.fer.unizg.hr/en/studies/specialist/information_security. International Association of Privacy Professionals (IAPP) offers a variety of certificates and training recognized as an industry standard www.iapp.org

[17] Lambert, P.: "*The Data Protection Officer: Profession, Rules and Role*", CRC Press, Taylor&Francis, 2017.

[18] EDPB: SME Data Protection Guide: DPO Best Practices, available at: https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-officer_en last accessed 30/04/2025.

[19] Michelakaki, C., Barros Vale, S.: *Unlocking Data Protection By Design & By Default: Lessons from the Enforcement of Article 25 GDPR,* The Future of Privacy Forum, 2023. Available at: https://fpf.org/wp-content/uploads/2023/05/FPF-Article-25-GDPR-A4-FINAL-Digital.pdf

[20] Katulić, T., Katulić, A.: *Competences, Position and Role of Data Protection Officers in Ensuring Library Data Protection Compliance*, IFLA CPDWL Satellite meeting: Librarians and information professionals as (pro)motors of change: immersing, including and initiating digital transformation for smart societies Date: 20 – 21 August 2019

[21] Fritsch, C.: "*Data Processing in Employment Relations: Impacts of the European General Data Protection Regulation Focusing on the Data Protection Officer at the Worksite*". Gutwirth, S., Leenes, R., de Hert, P. (editors) *Reforming European Data Protection Law*. Law, Governance and Technology Series(), vol 20. Springer, Dordrecht. https://doi.org/10.1007/978-94-017-9385-8_6

[22] Ciclosi, F., Massacci, F.: "*The Data Protection Officer: A Ubiquitous Role That No One Really Knows*" in IEEE Security & Privacy, vol. 21, no. 1, pp. 66-77, Jan.-Feb. 2023, doi: 10.1109/MSEC.2022.3222115.

[23] Bradford, A.:"*The Brussels Effect*", Northwestern University Law Review, Vol. 107, No. 1, 2012

# SMART HEALTH HOME: TECHNOLOGY ADOPTION AND SOCIAL IMPACT

*Vladimir Brusić, PhD*
*ARGS, University of Doha for Science and Technology, Doha, Qatar, vladimir.brusic@udst.edu.qa*

**Abstract:** S*mart Health Homes (SHH) integrate wearables and environmental sensors with IoT devices to enable continuous, real-time health monitoring at home settings. SHH supports preventative care and personalized health management. Key challenges include providing meaningful reports, and ensuring medical-grade accuracy, regulatory compliance, and ethical safeguards. Scalability of SHH systems into Smart Health Communities (SHC) requires modular design, standardized data formats, and alignment with public health frameworks. The SHH–SHC model promotes a shift from curative to preventative healthcare, enhancing outcomes, reducing costs, and supporting equitable access to care.*

**Keywords:** *Ethical technology; Home health care; Sensor networks;Smart health home; Wearable technology*

## 1. INTRODUCTION

Smart Health Home (SHH) is a transformative technology impacting both healthcare and information systems. SHH connects wearable sensors, environmental sensors, and smart devices into an integrated system to monitor health, support care delivery, promote wellness, and enhance preventative care [1]. SHH combines sensor systems, the Internet of Things (IoT), and data communication technologies, enabling real-time, continuous health monitoring that extends healthcare services beyond traditional clinical setting. It is a specialized application within the broader Internet of Health Things (IoHT) framework. The IoHT has been adopted in institutional healthcare settings because it improves resource utilization, provides for faster and more efficient operations, improves data management, and enhances healthcare outcomes. SHH extends these capabilities into homes, offering significant advantages such as continuous health status monitoring and context-aware sensing. Combining health data with contextual data—such as location, environment, and activity—enables adaptive learning through data analytics and machine learning. Adopting SHH requires addressing medical, technical, regulatory, and ethical challenges. Wearable sensors measurements must be reliable and accurate. SHH must generate medically meaningful and interpretable reports. It must also comply with standards for medical software and devices. Finally, data privacy, security, and ethical concerns remain critical, alongside usability and user trust.

## 2. ADDRESSING THE CHALLENGES

The SHH model requires certified sensors and medical-grade devices (such as glucometers, heart rate sensors, blood pressure meters, or ECG devices). Their integration is based on sound software engineering principles, to ensure system reliability and interoperability. SHH must follow standardized procedures and ensure compliance with clinical standards for data accuracy and with clinical guidelines. Data should use interoperable data formats (e.g., HL7, FHIR) to ensure robust integration with healthcare systems. Structured health reports must provide a high-level overview of vital signs, observations, and trends, including key condition-specific data, summaries, reference values, and alerts. Since measurements occur without direct medical supervision, reliability assessments must be included. Medical software standards focus on a) requirements and information; b) risk management, development, and security; and c) design, manufacturing, and distribution of connected health devices. Medical device standards include a) quality management systems; b) risk management; c) biological evaluation; and d) safety and performance of electrical equipment. Six ethical requirements for SHH design include: a) safety and trust; b) privacy and data security; c) group vulnerability; d) individual autonomy; e) transparency, explainability, and fairness; and f) social responsibility. Developers must consider SHH's broader societal impact, including ethical deployment, long-term consequences, and alignment with professional codes of conduct. By embedding ethical considerations into every stage of SHH development—from design and data handling to deployment and long-term use—developers can create systems that are not only technically robust but also socially responsible and human-centered healthcare solution.

## 3. SCALABILITY

Scalability is a critical factor when transitioning from individual SHH systems to broader Smart Health Communities (SHC, Figure 1). SHH systems should be built using modular components that can be easily integrated or expanded. This allows for seamless scaling from single homes to community-wide networks. For scalability, SHH must support standardized data formats, secure cloud-based storage, and preferably the interoperability with electronic health records. With systems scalability, ethical principles such as privacy, vulnerability, autonomy, and fairness must be preserved. These principles should be embedded into the software development lifecycle to ensure they remain intact as the system grows. Risk management strategies (e.g., from ISO 14971) must evolve to address not just individual risks but also systemic risks that emerge at the community level—such as data breaches affecting multiple homes or algorithmic bias in community health analytics. Scalable SHH systems must adapt to diverse user needs across different demographics and health conditions. This includes support for vulnerable populations and ensuring equitable access to SHH technologies. For SHH to scale into SHC, the alignments with public health policies, legal frameworks, and community governance structures are essential. Software processes for SHH to SHC scaling should be designed to accommodate these broader requirements. SHH-SHC system transfers data to healthcare organizations and public health services in anonymous format. For personal healthcare the patient or carer disclose the identity of the patient directly to the healthcare provider at the time of healthcare delivery. The option of federated learning using anonymized data enables identification of patient clusters across different communities that likely share health condition and responses to intervention.

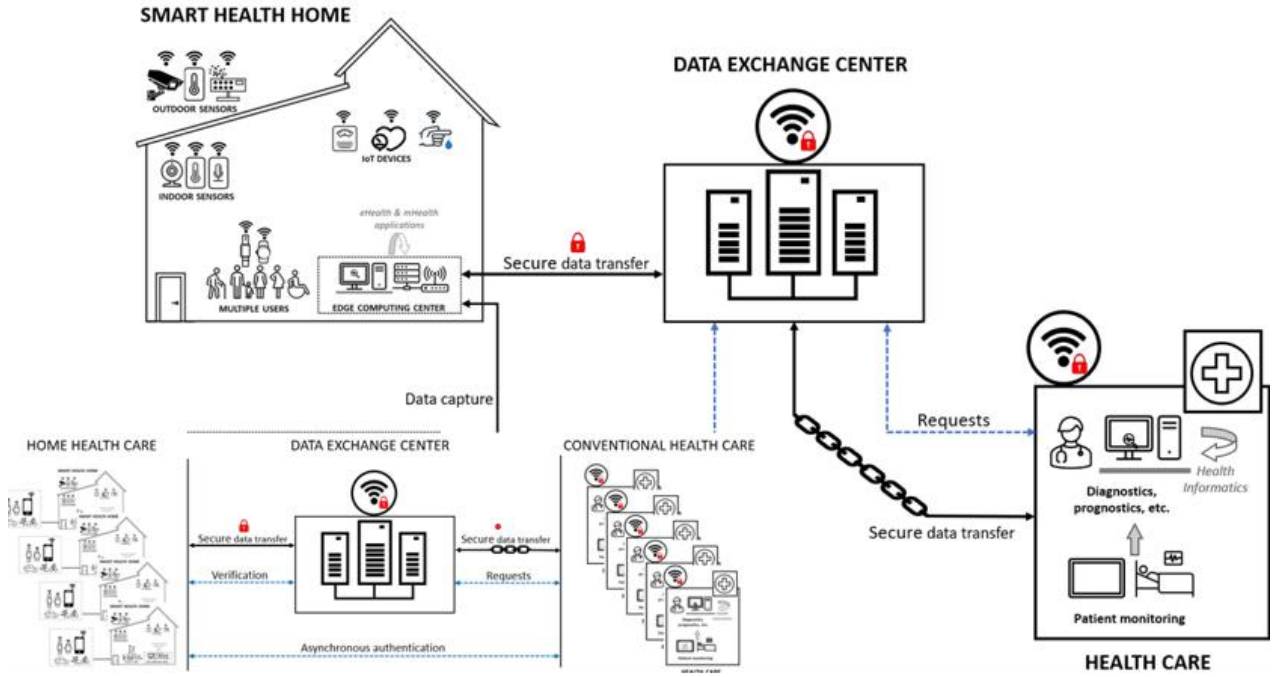



**Figure 1. Smart Health Home and Smart Health Communities (SHH-SHC).**
The schematic shows connectivity between SHH add healthcare institutions with secure anonymized data transfer and the scalable sheme where multiple SHH are interconnected to multiple healthcare providers.

## 4. CONCLUSION

Smart Health Homes (SHH) serve as the foundational units of Smart Health Communities (SHC). SHHs integrate technology into individual living spaces to monitor health, support independent living, and enable personalized care. When these homes are networked and scaled, they form SHCs—interconnected ecosystems that promote proactive, community-wide health management. The benefits of SHH-SHC system are the enhancement of personalized health care, improved preventative healthcare, and reduction of healthcare cost.

The SHH-SHC model offers a shift from curative (reactive) healthcare to preventive, participatory, and data-informed health ecosystems. We also envision a shift from isolated sensor-based monitoring systems to software engineering driven and ethically informed, intelligent, and scalable health ecosystems. SHH will increasingly integrate AI-driven analytics, context-aware sensing, and modular, interoperable platforms that support individual health monitoring and enable community-wide health intelligence. The future SHH-SHC will not be limited to monitoring health but will also predict risks, personalize interventions, and support healthy aging at home. Taken

together, SHH-SHC will make healthcare more individualized, evidence-based, proactive, participatory, and sustainable than conventional healthcare models.

**REFERENCES**

[1] Pike M, Mustafa NM, Towey D, Brusic V. Sensor networks and data management in healthcare: Emerging technologies and new challenges. In2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC) 2019 Jul 15 (Vol. 1, pp. 834-839). IEEE.

[2] Islam SR, Kwak D, Kabir MH, Hossain M, Kwak KS. The internet of things for health care: a comprehensive survey. IEEE access. 2015 Jun 1;3:678-708.

[3] Wang W, Li X, Qiu X, Zhang X, Brusic V, Zhao J. A privacy preserving framework for federated learning in smart healthcare systems. Information Processing & Management. 2023 Jan 1;60(1):103167.

[4] Carroll N, Richardson I. Software-as-a-medical device: demystifying connected health regulations. Journal of Systems and Information Technology. 2016 May 9;18(2):186-215.

[5] Ramakrishna S, Tian L, Wang C, Liao S, Teo WE. Medical devices: regulations, standards and practices. Woodhead Publishing; 2015 Aug 18.

[6] Zhang X, Pike M, Mustafa N, Brusic V. Ethically informed software process for Smart Health Home. In2022 IEEE 35th International Symposium on Computer-Based Medical Systems (CBMS) 2022 Jul 21 (pp. 187-192). IEEE.

# MODERN WEB TECHNOLOGIES AND MARKETING: POSSIBILITY AND CHALLENGES

Filip Jovanović, Faculty of Project and Innovation Management, filip.jovanovic@pmc.edu.rs

**Abstract:** *This paper explores the dynamic relationship between modern web technologies and marketing, analyzing both the opportunities and challenges they present. Leveraging a review of recent literature, the study highlights how advancements such as social media, mobile platforms, and data analytics have transformed marketing strategies, while also introducing new complexities related to privacy, integration, and talent acquisition. The findings suggest that successful digital marketing requires continuous adaptation to evolving technologies and consumer expectations. Key implications for practitioners and researchers are discussed, with a focus on future trends and best practices.*

**Keywords:** *Internet marketing, Web technologies, Social media, Digital transformation, Marketing challenges*

## 1. INTRODUCTION

In the era of digital transformation, marketing practices are increasingly reliant on technological innovation. The rapid advancement of web technologies has fundamentally reshaped the marketing landscape. Digital platforms, social networks, and data-driven tools have enabled marketers to reach and engage consumers in unprecedented ways. However, this evolution also brings significant challenges, including data privacy concerns, integration issues, and the need for specialized talent. This paper examines the possibilities and challenges associated with modern web technologies in marketing, drawing on contemporary literature and industry insights.

## 2. PROBLEM STATEMENT

While modern web technologies offer marketers powerful tools for audience targeting, engagement, and analytics, they also introduce a complex set of challenges. Organizations must navigate privacy regulations, manage data overload, adapt to rapidly changing consumer behaviors, and integrate diverse digital platforms. The central problem addressed in this paper is how marketing professionals can effectively leverage modern web technologies to achieve business objectives while overcoming these obstacles [1], [2], [3].

Despite the vast opportunities that modern web technologies offer to marketing, their implementation and use bring a range of complex challenges that require careful analysis and a strategic approach [4].

The first and most significant challenge is the rapid pace of technological change. Digital tools, platforms, and trends are evolving at an exceptional speed, which requires companies to constantly monitor innovations and continuously adapt their strategies. Organizations that fail to keep up with these changes risk losing their competitive advantage [1].

The second major issue is the integration of new technologies with existing systems. The introduction of advanced analytics, automation, and personalization tools often requires significant investments, technical expertise, and changes in organizational structure. Many companies face difficulties when connecting new digital solutions with outdated IT systems, which can lead to inefficiencies and increased costs [2].

A third challenge is managing large volumes of data. Modern marketing generates enormous amounts of information about users and their behavior. However, data collection alone is not sufficient – it is crucial to properly analyze and interpret this data to make informed business decisions. Excessive data can lead to confusion and incorrect conclusions if there is no adequate system for data management and analysis [5].

Data privacy and security have become central issues in digital marketing. Strict regulations, such as GDPR and similar laws, require companies to manage user data transparently and provide a high level of protection, which often demands additional investments and changes in business processes [5].

Another important challenge is the shortage of qualified personnel. Digital marketing requires professionals who possess a combination of knowledge in marketing, technology, and analytics. There is a shortage of such profiles in the labor market, making it difficult for companies to build effective digital teams [6].

Finally, changing consumer behavior and expectations present an additional difficulty. Consumers today expect personalized, fast, and relevant communication across all digital channels. Companies that cannot meet these demands risk losing loyalty and market share [5], [6].

For all these reasons, it is clear that the successful application of modern web technologies in marketing requires not only investments in technology, but also changes in organizational culture, continuous employee education, and the development of flexible strategies that can quickly adapt to new market conditions [4], [3].

## 3. OPPORTUNITIES AND CHALLENGES IN MODERN WEB TECHNOLOGIES AND MARKETING

Digital marketing can be understood as a dynamic process that integrates technology, data, and creativity to create value for customers and organizations. It involves not only the use of digital channels for promotion but also the strategic management of customer relationships, content, and brand reputation in the digital environment. Recent frameworks emphasize the importance of agility, customer-centricity, and the continuous adaptation of marketing strategies to technological changes [7].

Modern web technologies offer a range of solutions that empower marketers to overcome the challenges outlined above. The key to success lies in strategically leveraging these technologies, investing in human capital, and fostering a culture of continuous innovation and adaptation. Below, we explore both the opportunities and the main challenges, along with actionable approaches to address them. [4], [7]

### 3.1 Opportunities Provided by Modern Web Technologies

Enhanced Reach and Engagement: Modern web technologies have dramatically expanded marketers' ability to reach global audiences and foster meaningful engagement. Social media platforms such as Facebook, Instagram, and LinkedIn enable brands to interact directly with consumers, create communities, and encourage user-generated content. Mobile applications and responsive web design ensure that marketing messages are accessible anytime and anywhere, increasing the likelihood of customer interaction. Content management systems (CMS) further allow for the dynamic personalization of content, ensuring that each user receives relevant information based on their preferences and behavior. This multi-channel approach not only broadens the audience but also deepens engagement and loyalty through interactive and real-time communication [2].

Data-Driven Decision Making: The integration of advanced analytics and artificial intelligence (AI) into marketing platforms has revolutionized the way decisions are made. Marketers can now collect, analyze, and interpret vast amounts of data from multiple sources, including social media, website traffic, and customer transactions. AI-driven tools enable precise audience segmentation, predictive modeling, and campaign optimization in real time. As a result, companies can allocate resources more efficiently, personalize offers, and accurately measure return on investment (ROI). This data-driven approach minimizes guesswork and allows for continuous improvement based on measurable outcomes [5].

Omnichannel Marketing: Modern web technologies support the seamless integration of online and offline marketing channels, creating a unified customer journey. By leveraging customer relationship management (CRM) systems, marketing automation platforms, and cross-device tracking, companies can ensure that customers receive consistent messaging and service regardless of the channel they use. This omnichannel approach increases customer satisfaction and loyalty, as it allows for smooth transitions between digital touchpoints (such as social media, email, and e-commerce) and physical experiences (such as in-store visits or events). The result is a holistic brand experience that meets the evolving expectations of today's consumers [3].

Agility and Innovation: Cloud-based tools and composable architectures have made it possible for marketing teams to rapidly experiment with new ideas and adapt to market trends. These technologies allow for the quick deployment of new features, A/B testing of campaigns, and real-time adjustments based on customer feedback or analytics. Marketers can respond to shifts in consumer behavior or competitive actions with unprecedented speed, reducing time-to-market for new initiatives. This agility fosters a culture of innovation, where organizations are encouraged to test, learn, and scale successful strategies efficiently [4].

### 3.2 Key Challenges in Modern Digital Marketing

Intense Competition for Attention: The digital landscape is saturated with content from countless brands, influencers, and media outlets, making it increasingly difficult for marketers to capture and retain consumer attention. Users are bombarded with advertisements, notifications, and

promotional messages across various platforms, leading to shorter attention spans and higher expectations for relevance and value. As a result, marketers must develop creative, targeted, and engaging campaigns to stand out and foster genuine connections with their audience [3].

Data Privacy and Regulation: With the introduction of regulations such as the General Data Protection Regulation (GDPR) and similar laws worldwide, organizations are under greater scrutiny regarding how they collect, store, and use consumer data. Compliance requires transparent data practices, explicit user consent, and robust data security measures. These regulations limit traditional targeting methods and require marketers to rethink their data strategies, often increasing operational complexity and costs. Failure to comply can result in significant legal and reputational consequences for businesses [5].

Data Overload: The proliferation of digital channels and touchpoints generates massive amounts of data from various sources, including social media, websites, mobile apps, and CRM systems. While this data holds valuable insights, the sheer volume can overwhelm marketers, making it challenging to extract actionable information. Without effective data management and advanced analytics tools, organizations risk missing key trends, drawing incorrect conclusions, or failing to personalize their marketing efforts effectively [5].

Integration Complexity: Integrating new digital marketing technologies with existing legacy systems is often resource-intensive and technically challenging. Many organizations operate with fragmented IT infrastructures, where new tools must be carefully synchronized with older platforms to ensure seamless data flow and campaign execution. This process requires significant investment in technology, skilled personnel, and cross-departmental collaboration, and can slow down digital transformation initiatives if not managed properly [2].

Talent Shortage: There is a growing demand for professionals who possess both technological and analytical skills in addition to marketing expertise. However, the rapid evolution of digital tools has created a skills gap, with many organizations struggling to recruit and retain qualified talent. This shortage can hinder the effective implementation of digital marketing strategies and slow down innovation, as teams may lack the necessary expertise to leverage new technologies to their full potential [6].

Maintaining Consistency Across Channels: Ensuring a unified and coherent brand message across multiple digital platforms is increasingly complex. Each channel-such as social media, email, websites, and mobile apps-has its own format, audience expectations, and technical requirements. Marketers must coordinate content, timing, and tone to provide a seamless experience, which requires robust content management systems and clear brand guidelines. Inconsistencies can confuse customers and weaken brand identity [3].

Rapid Technological Change: The pace at which new digital marketing tools, platforms, and consumer behaviors emerge is accelerating. Marketers must continuously monitor trends, test new solutions, and adapt their strategies to remain competitive. This environment demands agility, ongoing professional development, and a willingness to experiment, as organizations that fail to keep up risk losing market share to more innovative competitors [4].

## 4. TRENDS IN DIGITAL MARKETING RESEARCH

A comprehensive review of internet marketing literature over the past two decades reveals several significant trends that have shaped both academic research and business practice. The volume of research and published articles on internet marketing has grown exponentially, particularly in the last eight years. This surge reflects the increasing importance of digital channels in reaching and engaging consumers, as well as the rapid evolution of technology and marketing tools. Researchers have responded to these changes by exploring new topics, methodologies, and practical applications, contributing to a richer and more diverse body of knowledge in the field [8].

Key research areas such as consumer behavior, internet strategy, and online communications have remained central to the literature. However, there has been a noticeable shift towards emerging topics, including social media marketing, mobile marketing, and the application of analytics in campaign management. These newer areas reflect the changing digital landscape, where consumers interact with brands through multiple devices and platforms, and where data-driven decision making is increasingly critical for success [8].

The most promising directions for future research and business growth are identified in the domains of mobile internet, social media and networks, and advanced analytics. Mobile marketing, in particular, is expected to play a dominant role as smartphones and mobile

applications become the primary means of accessing digital content for many users. Social networks continue to evolve, offering new opportunities for targeted advertising, influencer partnerships, and real-time engagement. Meanwhile, the integration of advanced analytics and artificial intelligence enables marketers to extract actionable insights from vast amounts of data, optimize campaigns, and deliver personalized experiences at scale [7].

From a practical perspective, the literature emphasizes the need for continuous learning, agile adaptation, and cross-functional collaboration within marketing teams. As digital marketing becomes more complex, organizations must invest in ongoing professional development and foster a culture of innovation. Effective communication and collaboration between marketing, IT, and analytics departments are essential for implementing new technologies and responding swiftly to market changes. These capabilities are seen as key drivers of competitive advantage in the digital era [9].

## 5. CONCLUSION

Modern web technologies have revolutionized the way businesses approach marketing, offering powerful tools for engagement, personalization, and performance measurement. However, alongside these benefits come significant challenges, including rapid technological change, data management complexities, privacy concerns, and a shortage of skilled professionals.

To effectively harness the potential of these technologies, companies must adopt a strategic, agile approach that integrates technological innovation with human expertise. This includes investing in staff training, fostering a culture of continuous learning, and maintaining a strong ethical framework in handling consumer data.

Looking ahead, the successful application of modern web technologies in marketing will depend not only on adopting the latest tools but also on the organization's ability to align its structure, values, and processes with the demands of the digital age. The convergence of data, creativity, and technology will continue to shape the marketing landscape, creating new opportunities for brands that are willing to adapt and innovate.

## REFERENCES

[1] SmallBizClub, "5 Marketing Technology Challenges that All Businesses must Solve", SmallBizClub, 2020. https://smallbizclub.com/technology/5-marketing-technology-challenges-that-all-businesses-must-solve/

[2] Y. K. Dwivedi et al., "Setting the future of digital and social media marketing research: Perspectives and research propositions", *International Journal of Information Management*, vol. 59, 2021.

[3] O. Niininen (ed.), *Contemporary Issues in Digital Marketing*, Routledge, 2022.

[4] D. L. Hoffman, C. P. Moreau, S. Stremersch, M. Wedel, "The Rise of New Technologies in Marketing: A Framework and Outlook", *Journal of Marketing Research*, vol. 59, no. 1, pp. 1–13, 2022.

[5] Sitecore Staff, "Your digital evolution: Top 7 digital marketing challenges and how to solve them", Sitecore Blog, 2024. https://www.sitecore.com/blog/digital-marketing/your-digital-evolution-top-7-digital-marketing-challenges-and-how-to-solve-them

[6] Testbirds Blog, "Cracking the Code: Digital marketing's challenges", Testbirds, 2024. https://www.testbirds.com/en/blog/cracking-the-code-digital-marketings-challenges/

[7] M. S. Krishen, S. Dwivedi, N. B. Dennis, "Digital Marketing: A Framework, Review and Research Agenda", *Journal of Business Research*, 2017.

[8] J. Schibrowsky, D. Peltier, K. Nill, "A review of internet marketing research over the past 20 years and future research direction", *Journal of Research in Interactive Marketing*, vol. 7, no. 3, pp. 166–181, 2013.

[9] Fomichenko, I., S. Barkova, A. Dykan, K. Kosik, K. Kozlova, "Internet Marketing as a Modern Enterprise Communication Tool", *Economic Herald of the Donbas*, no. 4 (62), pp. 97–102, 2020.

# 2.

# Artificial Intelligence

# FORECASTING SOFTWARE VULNERABILITY TOTALS USING LONG SHORT-TERM MEMORY (LSTM) NEURAL NETWORKS

Michael T. Shrove, Millennium Corporation, tshrove@gmail.com
Emil Jovanov, University of Alabama Huntsville, emil.jovanov@uah.edu

**Abstract:** *The main objective in this research is to provide a framework that will allow project managers, business owners, and developers an effective way to forecast the trend in software vulnerabilities within a software project. By providing these stakeholders with a mechanism for forecasting vulnerabilities, they can then provide the necessary resources at the right time to correct and fix vulnerabilities, which reduces the attack surface. In our research, we demonstrate forecasted trends in several open-source projects using the LSTM neural network. In this paper, we present our technique and methodologies for developing the inputs for the proposed model and the results of testing of three open-source projects. Our results show that using a long-short term memory neural network can produce a mean absolute error of 1.3 vulnerabilities. Further, we discuss the prediction model and its results*.

**Keywords:** *Machine Learning, Long-Short Term Memory, Neural Network, LSTM, Software Vulnerabilities.*

## 1. INTRODUCTION

In today's world, software has almost become a part of every job function in the market. From the food industry to the medical industry to the defense industry, software is everywhere. More and more people rely on software that is of high quality and produces accurate results. With the increase in demand for software, so are the pressures that are being put on software developers to deliver software more quickly and efficiently. This rapid pace of software development does not come without its costs. For developers to meet the demand, they are improving their processes with deployment and architecture strategies such as DevOps processes and microservice architecture designs. On the other side, if the developers are not upgrading their operations, they are taking shortcuts in their code to meet the demands, which in turn can lead to software vulnerabilities or technical debt (TD).

Cunningham first introduced the idea of TD in 1992 [1] as a concept in software development that reflects the implied cost of additional rework caused by choosing an easy solution now instead of using a better approach that would take longer. Every time TD incurs in the project; it creates additional TD cost [2, 3] that must be monitored. If these costs are ignored, they can accrue interest [2, 3] on top of the principal cost [2] of the TD item. Recurring TD costs or TD that the team members have decided not to deal with can cause the project to bankrupt [2], causing the project to fail.

In our research, our focus was around the TD costs associated with developers taking shortcuts in the security aspects of the software, which in turn causes vulnerabilities and increases the attack surface, also known as security debt [4]. A substantial portion of the attacks encountered today arise because of security debt. Given the increasing trend in software demands and complexities, vulnerabilities, and the ever-growing threat of attacks, producing secure code and monitoring security debt has become even more critical.

For our research, we wanted to produce a method for software teams and product owners to use that would allow them to monitor their security debt over time and forecast when they could expect more vulnerabilities in the software. We developed a vulnerability prediction model using time series data produced from open-source software teams. Time series analysis uses the fact that data points obtained over time in a consistent time interval appear to have an internal structure such as autocorrelation, and periodical and seasonal elements. We collected security debt items from open-source software projects. We used a time series regression model called a long short-term memory (LSTM) neural network (NN) to produce a forecasted trend line of the security debt of the software project. Using our research, software development teams and product owners could use our methods to predict future vulnerabilities, allocate their resources more efficiently than they currently are, and anticipate future releases of security patches.

## 2. RELATED WORK

In using time series data and forecasting trends, business and stock markets are using these models to forecast sales and stock prices. Though, in our research, we wanted to predict the pattern of security vulnerabilities of a particular

software project. In our literature review, we found that a majority of authors are trying to classify if a specific module of code is or will be defect prone in the future based on software metrics or authors are forecasting defect trends of a software project [6,7,8,9,10]. Time series trend forecasting seemed to be more in financial markets [12]. But one paper, [8], was very similar to our methods used in our research. In this paper, the authors took the total defect count produced throughout the project's lifecycle and used that to forecast the trend of defects totals in the future of the project. They used a statistical model approach using the ARIMA (auto-regressive integrated moving average) model.

There were a few papers that were also similar to our research and were focusing specifically on security vulnerability trend forecasting while using other methods [13,14,15], while other authors were focusing on security TD [16,17,18].

## 3. OVERALL APPROACH

In our approach, we wanted to find a method that would allow stakeholders to monitor the data, present the total number of vulnerabilities, forecast the trends in the vulnerability data, and present in a graphic format for the stakeholders to view for decision making. For the data, we focused on open-source software (OSS) project data; however, we needed to find some that had their security log data open to the public. We used OSS to apply time series-based models to forecast trends in the data, and lastly, we used open-source graphing libraries to present the patterns to the stakeholders.

### 3.1 The Training Dataset

Our training datasets are open-source software projects from three different projects, the Electron project, Kubernetes project, and the Brave Browser project. They were readily available and open to the public and were acquired using the GitHub API. Brave is a web browser project that has a goal to rid ads and trackers. Kubernetes is an open-source system for automating deployment, scaling, and management of containerized applications. Electron is an open-source framework for making desktop applications cross-platform with JavaScript and HTML. All three of these projects have been tracking their software project in GitHub with not only source code but also security-related issues. Electron had been tracking their security-related issues for 1752 days, Kubernetes for 2032 days, and Brave for 778 days.

**Table 1** - OSS Project Information used for Research

| Project Name | 1st Vulnerability | Total # Vulnerabilities |
|---|---|---|
| **Kubernetes** | 06/11/2014 | 728 |
| **Brave** | 12/05/2017 | 228 |
| **Electron** | 04/08/2015 | 72 |

### 3.2 Data Preprocessing

For these three projects, their code and issues were stored in GitHub. We used the GitHub API and an open-source library called pygithub to extract the issues from the issue tracking system within GitHub. For this research, we collected only the issues with each GitHub project that were labeled as a security issue.

We decided to calculate the security debt cost as +1 (production of vulnerability), -1 (reduction of a vulnerability or resolving the vulnerability), or 0 (no change in vulnerabilities). We arranged the security debt items by date from the earliest dated debt first, to the most recent dated debt last. We then created a cumulative sum of the security debt by the project. Our output from this stage (ex. Kubernetes project seen by Figure 2) would be a cumulative sum list of vulnerabilities of each project sorted from the oldest to the youngest security debt item. That cumulative sum would be the input into our time series model for vulnerability prediction moving forward.

### 3.3 Long-Short Term Memory Neural Network Model

In this section, we will describe our general process of applying the LSTM NN model to our time series data. We will get into more specifics during the next section labeled *Results*.

**LSTM NN Background.** Long Short-Term Memory networks or LSTM networks are a type of Recurrent Neural Network (RNN) that uses previous time events to inform the ones after it. RNNs work well if the problem requires only recent information to perform the present task. If the problem requires long term dependencies, RNN struggles to model it. The LSTM was designed to learn long term dependencies by remembering the information for long periods of time. Two people named Hochreiter and Schmidhuber [20] created them back in 1997. Over the years, the LSTM network became popular, and many different variants were produced. In this research, we used an LSTM NN to perform a regression on the security debt totals through the life of the project. The code we implemented is a stateful LSTM for time series prediction. We used Keras as a framework along with the Sequential

API within Keras to develop our LSTM model. Our code will be posted on Gitlab[1] for viewing and future use.

**Stationary Testing.** One requirement about using any time-series forecasting model is that the data is required to be as stationary as possible for the best results. Stationarity is defined as the mean, variance, and autocovariance that do not change over time. In the next section, we will show our techniques for removing non-stationarity, the most common method being differencing. To determine if our time series was stationary or not, we used the Dickey-Fuller (DF) test [19]. The DF test suggests the time series has a unit root, meaning it is non-stationary. It has some time-dependent structure. The alternative hypothesis is that it indicates the time series does not have a unit root, meaning it is stationary. It does not have a time-dependent structure. Once the DF test has been run, if the time series was stationary (p-value < alpha value), we could move on to applying the forecasting model. If not, we would have to use methods for removing non-stationarity in the data.

**Methods for Removing Nonstationarity.** Methods for removing non-stationarity are not the same each time for time series data. Different methods must be applied each time, and the results must be manually evaluated based on the results of the hypothesis test. The most common techniques for removing non-stationarity are transformation, smoothing, and differencing. Of those three techniques, we show eight methods shown in Table 2.

**Table 2** - Non-Stationarity Removal Techniques

| # | Name | Technique | Description |
|---|---|---|---|
| **1** | Natural Log | Transformation | Applying the natural logarithm to the data. |
| **2** | Log Moving Average | Transformation / Smoothing | Applying a 7-day moving average of the natural logarithm of the data. |
| **3** | Moving Average | Smoothing | Applying a 7-day moving average of the data. |
| **4** | Diff Natural Log | Transformation / Differencing | Applying differencing to the natural logarithm of the data. |
| **5** | Diff Moving Average and Data | Transformation | Applying the difference between normal data and moving average. |
| **6** | Diff Log and Moving Average | Transformation / Differencing | Applying a difference between the natural logarithm of the data and the natural logarithm moving average. |
| **7** | EWMA (Exponential Weighted Moving Average) of Log | Transformation | Applying an EWMA algorithm to the natural logarithm of the data. We used a half-life of 7 for all instances. |
| **8** | Log EWMA Differencing | Transformation / Differencing | Applying a difference between the natural logarithm of the data with the EWMA algorithm. |

In each of our hypothesis tests (applying the DF test to each technique), we used a value of 0.05. If the results of the hypothesis test returned a value of less than 0.05, we would fail to reject the null hypothesis (not stationary). Otherwise, if the p-value were equal to or greater than 0.05, we would reject the null hypothesis, and we could potentially use the technique for removing the non-stationarity in the data.

**Applying the LSTM Network.** As for the model, we used Keras to build the LSTM network. We used 100 units for each LSTM layer. With a total of two LSTM layers with one dense output layer, as seen in Figure 1.

```
model = keras.models.Sequential([
  keras.layers.LSTM(100, return_sequences=True, stateful=True,
                    batch_input_shape=[1, None, 1]),
  keras.layers.LSTM(100, return_sequences=True, stateful=True),
  keras.layers.Dense(1),
  keras.layers.Lambda(lambda x: x * 200.0)
])
```

***Figure 1*** *- LSTM model configuration.*

We used a training dataset from each open-source software project performing 500 epochs in the training session. To not over train, we applied an early stopping function on the epoch with a patience value of 50.

## 4. RESULTS

Following the process described in Section 3, we began by plotting the raw data from each OSS projects. By plotting the data, we can understand the limitations of the data and what potential techniques can be used to make the data stationary if the data is not already stationary.

Figure 2 shows plots of all three projects from our dataset. As it can be seen from the plots, all three projects have completely different security debt profile. The time increment usually needs to be consistent to have a useful time-series dataset. We altered data from each project to have a sampling frequency of 1 day.

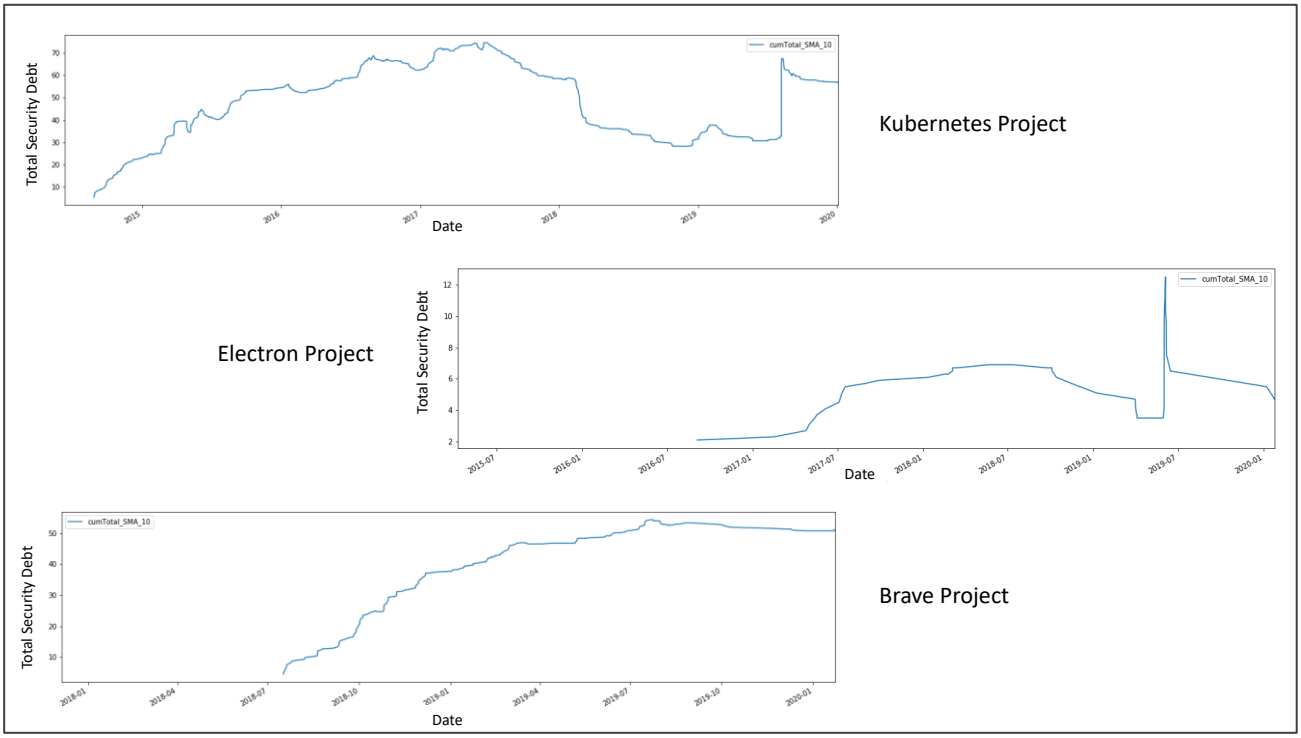



***Figure 2*** *- Total Security Debt of the Kubernetes, Electron, and Brave Open-Source Software Project.*

In step 2 of our process is to test for the stationarity or non-stationarity of each project's data. Using the Dickey-Fuller (DF) test as described in Section 3.3 under *Stationarity Testing*, the results are shown below. If the DF test for the project returns a p-value < 0.05, the data is stationary, and nothing further is required. Otherwise, we will need to apply a method to transform the data. The results of the projects are shown below in Table 3.

***Table 3*** *- Dickey-Fuller Test Results on each OSS Project.*

| Project Name | Test Statistic | *p*-value | Lag | Stationary |
|---|---|---|---|---|
| Kubernetes | -2.498172 | 0.115920 | 0.0 | Non-Stationary |
| Brave | -1.033190 | 0.740967 | 3.0 | Non-Stationary |
| Electron | -2.285791 | 0.176592 | 9.0 | Non-Stationary |

As seen from the p-values, all the projects produce non-stationary data sets. The Kubernetes project is the closest being stationary at 0.11.

Our next step was to determine an appropriate transformation method for making our time series data stationary. As described in Table 2, we tried eight different methods on each project. We only used these methods on projects with a p-value > 0.05. We then applied the Dickey-Fuller test to each dataset after each method was applied. We then applied a hypothesis test on each new dataset to determine if the p-value < 0.05 (stationary) or p-value > 0.05 (nonstationary) for stationarity checks as describe in previous sections. Our results are shown in Table 4. On the y-axis in Table 4, we have the non-stationarity removal techniques (NRTs). On the x-axis, we have OSS projects. The values represent the p-value from the Dickey-Fuller Test after the NRT was applied to the data. We rounded each p-value to the nearest two digits because we only need 2-digit significands in determining stationarity from the Dickey-Fuller test.

***Table 4*** *- Dickey-Fuller Test after NRT function applied*

| NRTs (Table 2) | Kubernetes | Brave | Electron |
|---|---|---|---|
| **Log** | $3.85e^{-09}$ | 0.21 | 0.29 |
| **Log Moving Average** | $0.30e^{-04}$ | 0.18 | 0.23 |
| **Moving Avg** | 0.12 | 0.70 | 0.42 |
| **Diff Log** | $6.42e^{-09}$ | $2.11e^{-13}$ | $6.21e^{-21}$ |
| **Diff Moving Avg** | $1.74e^{-26}$ | $2.84e^{-11}$ | $4.46e^{-29}$ |
| **Diff Log Moving Avg** | $2.07e^{-17}$ | $1.09e^{-9}$ | $1.67e^{-17}$ |
| **EWMA** | $1.14e^{-4}$ | 0.27 | 0.32 |
| **Log EWMA Diff** | $6.49e^{-10}$ | $4.68e^{-4}$ | $9.89e^{-11}$ |

We determined that using the Difference Natural Log (Diff Log) technique to make our data stationary was the best approach. It was straight forward to implement and could be undone if necessary, for further analysis of the data. Figure 3 shows the results of the Diff Log technique. Once we transformed all projects' data into stationary data using the Diff Log method, we could use the LSTM network model to forecast the data.

As described in the section labeled Applying the LSTM Network Model, we used the same data from Section 3.1.

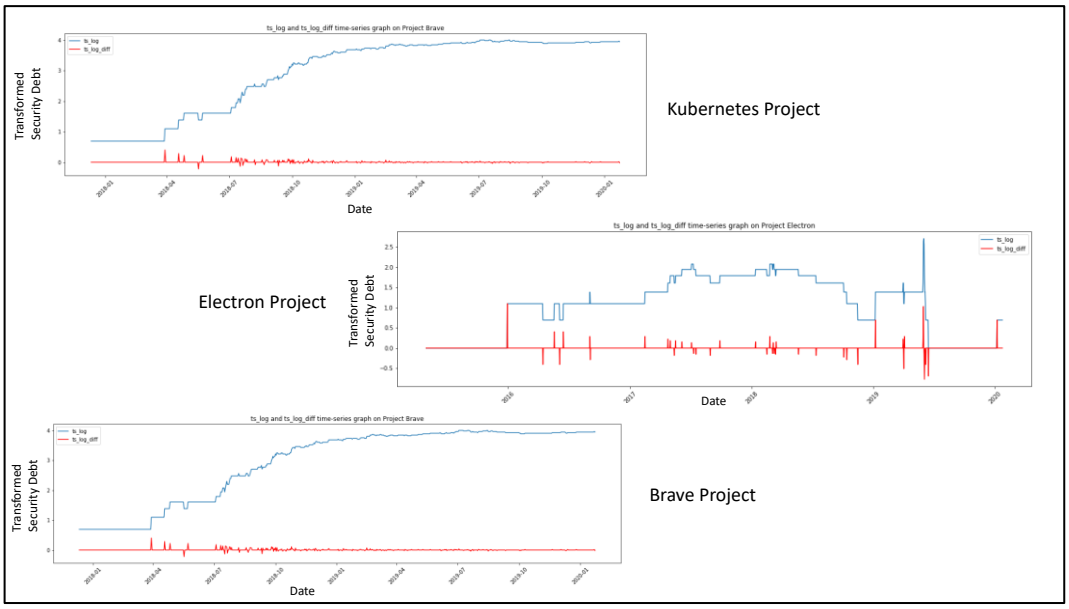



***Figure 3*** *- Diff Log Transformations of 3 OSS projects' Raw Data*

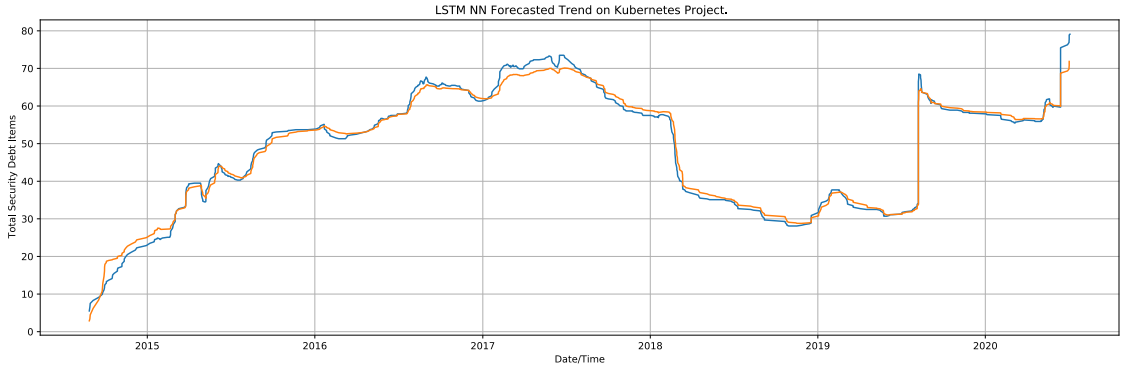



***Figure 4*** *- Kubernetes OSS Project Total Security Debt Prediction using LSTM Network*

We performed the transformation to the data described above. Our input to the algorithm was the transformed stationary project data collected in Section 3.1. After training and applying the LSTM network model, Figures 4 shows the output of the algorithm from the Kubernetes project. The blue line is the original data, and the forecast line is the orange line.

Lastly, we apply the LSTM network model to each dataset after the Diff Log transformation method was applied. The results showed that using our technique described in our research; we resulted in an average mean absolute error (MAE) of 2.95 for all three projects.

## 5. THREATS TO VALIDITY

In this section, we will discuss some threats that might hinder or contribute in a negative way towards our model or the process used for our research.

### 5.1 Data Validity

The vulnerabilities collected in our data are issues reported by people in the open-source community. These people may be amateurs to the product. We don't have any knowledge; therefore, the reported vulnerabilities may not be valid, or there may be duplicates of the same vulnerability.

### 5.2 Variation of Data

The data collected during this research was all obtained from one source, GitHub. Having different sources of data could show a broader trend in seasonality and defect reporting that is not shown in the data. Future research will collect multiple sources and perform a similar analysis and come to a more general and universal model for the general software community.

### 5.3 Reporting Mechanisms

The data collected for this research was gathered on projects' GitHub; however, each project could have another internal reporting instance of vulnerability tracking not displayed to the public. This would not reflect in our data or model development. In future research, we could reach to each project and confirm one instance of vulnerability reporting.

## 6. CONCLUSION

Prediction of software vulnerabilities is increasingly important for all software projects. A forecasting mechanism using LSTM neural network described in this paper could provide valuable insights for the stakeholders of the projects or even the open-source community. By understanding when vulnerabilities tend to arrive throughout the week and year, the stakeholders could quickly provide campaigns with the open-source community asking for additional help. Also, for-profit companies could plan part-time or temporary resources throughout the year to reduce the attack surface without paying for full-time employees, saving the organization money in the long run. In this research, we have shown that the LSTM network with proper transformation functions can forecast defect trends with confidence. In the future, we plan to use traditional technical debt along with software security to model and forecast security debt in software projects.

## REFERENCES

1. Cunningham, W., Ward, Cunningham, & Ward. (1993). The WyCash portfolio management system. ACM SIGPLAN OOPS Messenger, 4(2), 29–30. https://doi.org/10.1145/157710.157715
2. Li, Z., Avgeriou, P., & Liang, P. (2015). A systematic mapping study on technical debt and its management. Journal of Systems and Software. https://doi.org/10.1016/j.jss.2014.12.027
3. Akbarinasaji, S., Bener, A. B., & Erdem, A. (2016). Measuring the principal of defect debt. Proceedings of the 5th International Workshop on Realizing Artificial Intelligence Synergies in Software Engineering - RAISE '16. https://doi.org/10.1145/2896995.2896999
4. Campos, M., Silva, O., Valente, M. T., & Terra, R. (n.d.). Does Technical Debt Lead to the Rejection of Pull Requests? Retrieved from https://arxiv.org/pdf/1604.01450.pdf
5. Florentine, S. (2017). IT project success rates finally improving. Retrieved August 25, 2019, from https://www.cio.com/article/3174516/it-project-success-rates-finally-improving.html
6. Fenton, N., Neil, M., Marsh, W., Hearty, P., Marquez, D., Krause, P., & Mishra, R. (2007). Predicting software defects in varying development lifecycles using Bayesian nets. Information and Software Technology, 49(1), 32–43. https://doi.org/10.1016/j.infsof.2006.09.001
7. Okutan, A., & Yıldız, O. T. (2014). Software defect prediction using Bayesian networks. Empirical Software Engineering, 19(1), 154–181. https://doi.org/10.1007/s10664-012-9218-8
8. Raja, U., Hale, D. P., & Hale, J. E. (2009). Modeling software evolution defects: A time series approach. Journal of Software Maintenance and Evolution, 21(1), 49–71. https://doi.org/10.1002/smr.398
9. Vashisht, V., Lal, M., & Sureshchandar, G. S. (2015). A Framework for Software Defect Prediction Using Neural Networks. Journal of Software Engineering and Applications, 08(08), 384–394. https://doi.org/10.4236/jsea.2015.88038
10. Wang, S., & Yao, X. (2013). Using class imbalance learning for software defect prediction. IEEE Transactions on Reliability, 62(2), 434–443. https://doi.org/10.1109/TR.2013.2259203
11. Song, Q., Jia, Z., Shepperd, M., Ying, S., & Liu, J. (2011). A general software defect-proneness prediction framework. IEEE Transactions on Software Engineering, 37(3), 356–370. https://doi.org/10.1109/TSE.2010.90
12. Bou-Hamad, I., & Jamali, I. (2019). Forecasting Financial Time-Series Using Data Mining Models: A Simulation Study. Research in International Business and Finance, 101072. https://doi.org/10.1016/j.ribaf.2019.101072
13. Catal, C., Akbulut, A., Karakatič, S., Podgorelec, V., & Pavlinek, M. (2016). Can we predict software vulnerability with deep neural network? Retrieved from https://www.researchgate.net/publication/322131540
14. Clemente, C. J., Jaafar, F., & Malik, Y. (2018). Is predicting software security bugs using deep learning better than the traditional machine learning algorithms? Proceedings - 2018 IEEE 18th International Conference on Software Quality, Reliability, and Security, QRS 2018, 95–102. https://doi.org/10.1109/QRS.2018.00023
15. Last, D. (2016). Forecasting zero-day vulnerabilities. Proceedings of the 11th Annual Cyber and Information Security Research Conference, CISRC 2016. https://doi.org/10.1145/2897795.2897813
16. Fu, W., & Menzies, T. (2017). Revisiting unsupervised learning for defect prediction. 72–83. https://doi.org/10.1145/3106237.3106257
17. Rindell, K., Jaatun, M. G., & Bernsmed, K. (2019). Managing security in software or: How I learned to stop worrying and manage the security technical debt. ACM International Conference Proceeding Series. https://doi.org/10.1145/3339252.3340338
18. Nord, R. L., Ozkaya, I., & Shull, F. (2017). Software Vulnerabilities, Defects, and De-sign Flaws: A Technical Debt Perspective. Proceedings of the Fourteenth Annual Acquisition Research Symposium, 67–74. Retrieved from http://www.acqnotes.com/wp-content/uploads/2017/08/SYM-AM-17-034_Wednesday-Vol-1_5-1-2017.pdf#page=67
19. Leybourne, S., Kim, T. H., & Newbold, P. (2005). Examination of some more powerful modifications of the Dickey-Fuller test. Journal of Time Series Analysis, 26(3), 355–369. https://doi.org/10.1111/j.1467-9892.2004.00406.x
20. Hochreiter, Sepp, and Jürgen Schmidhuber. "Long Short-Term Memory." Neural Computation, vol. 9, no. 8, MIT Press, Nov. 1997, pp. 1735–80, doi:10.1162/neco.1997.9.8.1735.

# COMPARATIVE ANALYSYS OF IN-HOUSE AI DEVELOPMENT VS ARTIFICIAL INTELLIGENCE AS-A-SERVICE (AIAAS)

Milan Djordjević, PM.GURU, USA, milan@pm.guru

**Abstract:** *This paper investigates the decision-making process regarding the adoption of Artificial Intelligence (AI) in businesses. It evaluates the benefits and drawbacks of developing in-house AI systems or utilizing AI-as-a-Service (AIaaS) providers. Further, it emphasizes the significance of understanding an organization's AI maturity level and aligning its AI strategy with its broader data strategy.*

***Keywords:*** *Artificial Intelligence, AIaaS, In-house AI, AI Maturity Model, Data Strategy, Business Strategy, Cost-Benefit Analysis, Project Management, Business Intelligence*

## 1. INTRODUCTION

AI's pervasive influence across industries necessitates an informed decision-making process for businesses contemplating between in-house AI development and AIaaS. The integration of AI technologies offers a plethora of benefits, including enhanced efficiency, cost reduction, improved customer experience, and the generation of actionable insights from data, as highlighted by Rocha & Kissimoto[1]. Organizations are increasingly exploring AI to gain a competitive edge, innovate their service offerings, and optimize operational processes.

The allure of AI lies in its transformative potential. It can automate repetitive tasks, offer personalized services, enhance decision-making with predictive analytics, and drive innovations in product and service delivery. Bharadiya[2] emphasized the challenges and opportunities associated with integrating AI in business processes, underscoring the need for a comprehensive understanding of AI's value generation mechanisms. The decision to adopt AI is often motivated by the desire to enhance operational efficiency, reduce costs, and harness data for informed decision-making.

### 1.1 Literature Overview

The literature on AI adoption in businesses provides insights into the complexities and considerations involved in choosing between in-house AI development and AIaaS. Brundage et al.[3] highlighted the importance of aligning AI adoption with organizational goals and capacities. Bawack et al.[4] found that in-house AI development offers greater customization and control but comes with higher initial costs and the challenge of hiring skilled professionals. AIaaS provides a cost-effective, scalable, and quick-to-implement solution, albeit with potential limitations in customization and data security.

### 1.2 Methodology

This study employs a qualitative research approach, involving a comprehensive review of existing literature, case studies, and surveys to understand the prevailing trends and considerations in AI adoption. We analyzed data from various industries to offer a diverse perspective on the decision-making process regarding in-house AI vs. AIaaS.

## 2. NAVIGATING THE AI ADOPTION LANDSCAPE

Mukherjee[5] underscored AI's role in enhancing human resource management and productivity, illuminating the shift towards automation amidst the complexities of labor-intensive economies. The accelerated integration of AI and big data analytics in various sectors, especially healthcare, underscores the transformative potential of these technologies when strategically aligned with organizational goals[5].

### 2.1 AI and Your Data Strategy

An AI strategy should be a key component of a broader data strategy. The use and development of AI algorithms require large amounts of dana [5]. Therefore, the implementation of an effective AI strategy depends fundamentally on a robust data strategy. A well-structured data strategy is essential to fuel an effective AI strategy. Organizations must invest time and resources into developing a data strategy that ensures the right data is collected, maintained, managed, and made accessible to drive AI initiatives. In the absence of a robust data strategy, even the most advanced AI models and algorithms would be rendered ineffective. Mukherjee[5] underscored AI's role in enhancing human resource management and productivity, illuminating the shift towards automation amidst the complexities of labor-intensive economies.

Additionally, the integration of AI and big data is not only central to the advancement of intelligent systems but is also pivotal in enhancing the adaptability, efficiency, and productivity of services, especially in the healthcare sector [10].

### 2.2 Understanding Organizational AI Maturity Level

The alignment of AI strategy with organizational capacity and objectives is facilitated by an assessment of the AI maturity level, offering insights into the readiness and capability of the organization to integrate and optimize AI technologies. Fairness and ethical considerations are integral to the AI integration process, necessitating cooperation among various stakeholders including AI developers, policymakers, and patients to ensure equitable AI implementation Li et al.[7].

### 2.3 Balancing Act: Evaluating the Cost-Benefit Aspects

After determining an organization's AI maturity level, the cost-benefit analysis of in-house AI development versus AIaaS must be evaluated. The economic evaluation of in-house AI and AIaaS is intricate, shaped by variables including financial outlay, talent acquisition, and computational resources. Each option presents distinct economic implications, necessitating a comprehensive assessment to inform the decision-making process. The COVID-19 pandemic has underscored the need for resilience and sustainability in supply chains, highlighting the role of AI in enhancing the adaptability and recovery of businesses from disruptions[8].

To navigate this complex landscape, businesses must evaluate a range of factors:

- Financial Investment: In-house AI demands high initial investments and ongoing costs for training and maintenance, while AIaaS usually operates on a subscription-based model that can offer more predictable costs.
- Human Talent: In-house AI requires a team of skilled AI professionals, whereas with AIaaS, much of the expertise is provided by the service.
- Computing Resources: AI requires high computing power; this can be a constraint for in-house operations but is generally managed by the AIaaS provider.
- Time to Deployment: In-house AI projects can take a long time to deliver results, whereas AIaaS can often provide quicker wins.

#### 2.3.1 In-House AI Development

In-house AI development often entails substantial initial investment. The costs associated with hiring specialized talent, infrastructure development, and ongoing maintenance can be significant[9]. Organizations opting for this route need to be prepared for a long-term financial commitment and should have a clear vision of how AI will deliver value to their business operations and strategy.

Organizations with highly specific needs, proprietary data, or those operating in niche markets often prefer in-house AI. It offers tailored solutions, greater control over the AI development process, data security, and customization of AI applications. However, it requires a significant investment in talent and infrastructure[6].

Moreover, training machine learning models in-house requires substantial computing power, especially for complex models and large datasets. The investment in high-performance computing systems, including GPUs, can be significant[4]. The ongoing costs of upgrading and maintaining these systems, along with the energy costs, add to the economic considerations of in-house AI development.

#### 2.3.2 AI-as-a-Service (AIaaS)

AIaaS, on the other hand, offers a flexible financial model, typically subscription-based, allowing businesses to access cutting-edge AI technologies without the hefty initial investment[5]. AIaaS is particularly beneficial for SMEs or organizations looking to swiftly implement AI solutions. Providers offer a range of ready-to-use AI tools and applications, reducing the time to deployment. This model also provides access to a broader ecosystem of AI tools and applications, offering versatility and flexibility.

Furthermore, AIaaS eliminates the need for organizations to invest in high-performance computing infrastructure for training machine learning models. Organizations can leverage pre-trained models or train their models using the provider’s computing resources[2]. This not only reduces the initial investment but also accelerates the time to deployment of AI solutions.

Security is another key area of growth for AIaaS platforms. As AI and machine learning involve handling sensitive data, the issue of data privacy and security is paramount. In response, AIaaS providers are investing in robust security measures to protect user data, adopting practices such as end-to-end encryption, strict access controls, and regular security audits. As a result, organizations can trust these

platforms with their data and comply with various data privacy regulations.

However, there are limitations to consider. Utilizing pre-trained models can be restrictive as these models are often trained on general datasets and might not possess the specificity required for certain organizational needs. The lack of customization can lead to less accurate or relevant outcomes, sometimes leading to model hallucinations where the AI produces incorrect or nonsensical outputs[3].

Additionally, while pre-trained models offer a quick start, they often require fine-tuning to adapt to specific organizational data and use cases. This fine-tuning process can be complex and may necessitate additional investments, both in terms of finances and expertise, mitigating some of the cost advantages of AIaaS[1]. The balance between the ease of access to AI technologies and the need for customization and specificity is a critical consideration for organizations opting for AIaaS.

### 2.4 A Look to the Future

AIaaS platforms are a dynamic aspect of the broader AI landscape, continuously evolving in response to emerging trends, technological advancements, and client needs. This constant evolution allows AI platforms to become more sophisticated, secure, and customizable over time, reflecting the growing complexity of the AI field and providing increasingly powerful tools to those who use them.
This increasing sophistication allows businesses to leverage AI for more advanced use cases and solve more complex problems, thereby increasing the overall value of their AI investment.

Moreover, the customization features of AIaaS platforms are also improving. This includes customizable algorithms, adjustable parameters, and the ability to integrate with other business systems.

### 2.5 Enhancing Oraganizational Strategic Value Through Future-Ready AI Platforms

As the AI landscape evolves, the strategic integration of AI platforms will extend beyond operational efficiency to become a central driver of enterprise-wide innovation and resilience. Future-ready AI platforms will not only support complex decision-making but will also shape the architecture of digital ecosystems across industries. These platforms are expected to deliver modular, interoperable, and explainable AI capabilities that integrate seamlessly with existing enterprise systems such as ERP, CRM, supply chain platforms, and payment gateways.

The next wave of AI deployment will emphasize multi-cloud and hybrid environments, allowing organizations to balance performance, security, and cost across cloud providers. Additionally, as large language models (LLMs) and generative AI tools mature, companies will increasingly rely on fine-tuned, domain-specific models to gain competitive insights and automate more complex knowledge work.

Key enablers of this evolution include:

Edge AI and Federated Learning: Reducing latency and improving data privacy by processing AI models closer to the data source.

Responsible AI Frameworks: Organizations are formalizing guidelines around fairness, transparency, and accountability in AI deployment [6].

Data-Centric AI Development: As highlighted by Xu et al. [7] the focus will shift toward better data labeling, validation, and augmentation strategies to enhance model performance.

Vertical AI Solutions: Sector-specific AIaaS platforms will provide tailored functionality for domains like manufacturing, education, finance, and healthcare.

Importantly, the strategic role of AI in decision governance will grow. PMOs, compliance teams, and executive leadership will require dashboards and audit trails that justify AI-generated recommendations. As such, explainability and traceability will become standard requirements in enterprise-grade AI platforms.

In conclusion, the future of AI adoption lies not just in smarter algorithms, but in intelligent orchestration of platforms, people, and data. Organizations that invest today in interoperable, secure, and ethical AI frameworks will be best positioned to lead in the digitally transformed economy.

## 3. CONCLUSION

In essence, the choice between in-house AI and AIaaS is contingent upon an organization’s financial capacity, technical expertise, and specific AI needs. A thorough economic evaluation, aligned with the organization’s AI maturity and data strategy, is instrumental in making an

informed decision that maximizes the return on investment in AI while mitigating associated risks.

The balance between the initial investment and long-term benefits, customization versus speed of deployment, and control versus flexibility are pivotal considerations in this complex decision-making landscape. Organizations are advised to assess their AI maturity level, data strategy, data privacy, and security, organizational goals as well as the availability of skilled professionals and infrastructure.

Moreover, as AI technologies continue to evolve rapidly, organizations must treat AI strategy not as a one-time decision but as an iterative process requiring continuous reassessment. Factors such as changing regulations, advances in model architecture, ethical implications, and emerging integration capabilities necessitate adaptive governance frameworks. Organizations should prioritize building internal capacity for AI literacy across departments, ensuring that leadership, compliance, and operations teams can collaboratively guide responsible and impactful AI implementation. Ultimately, sustainable value from AI will depend not only on selecting the right development model but on embedding AI governance, scalability, and ethics at the core of enterprise strategy.

**REFERENCES**

[1] Rocha, I. F., & Kissimoto, K. O. (2022). Artificial intelligence and internet of things adoption in operations management: Barriers and benefits. RAM. Revista de Administração Mackenzie, 23.
https://doi.org/10.1590/1678-6971/eRAMR220119.en

[2] Bharadiya, J. (2023). The Impact of Artificial Intelligence on Business Processes. European Journal of Technology, 7(2), 15-25. https://doi.org/10.47672/ejt.1488

[3] Brundage, M., et al. (2020). Toward trustworthy AI development: mechanisms for supporting verifiable claims. arXiv preprint arXiv:2004.07213. https://doi.org/10.48550/arXiv.2004.07213

[4] Bawack, R.E., et al. Artificial intelligence in E-Commerce: a bibliometric study and literature review. Electron Markets 32, 297–338 (2022). https://doi.org/10.1007/s12525-022-00537-z

[5] Mukherjee, A.N. (2022). Application of artificial intelligence: benefits and limitations for human potential and labor-intensive economy – an empirical investigation into pandemic ridden Indian industry. Management Matters, 19(2), 149-166. https://doi.org/10.1108/MANM-02-2022-0034

[6] Xu, Y., et al. (2021). Artificial intelligence: A powerful paradigm for scientific research. The Innovation, 2(4). https://doi.org/10.1016/j.xinn.2021.100179

[7] Li F, et al. Ethics & AI: A Systematic Review on Ethical Concerns and Related Strategies for Designing with AI in Healthcare. AI. 2023; 4(1):28-53. https://doi.org/10.3390/ai4010003

[8] Modgil, S., Singh, R.K. & Hannibal, C. (2022). Artificial intelligence for supply chain resilience: learning from Covid-19. The International Journal of Logistics Management, 33(4), 1246-1268. https://doi.org/10.1108/IJLM-02-2021-0094

[9] Murugesan, U., et al. (2023). A study of Artificial Intelligence impacts on Human Resource Digitalization in Industry 4.0. Decision Analytics Journal, 100249. https://doi.org/10.1016/j.dajour.2023.100249

[10] Badawy, M. (2023). Integrating Artificial Intelligence and Big Data into Smart Healthcare Systems: A Comprehensive Review of Current Practices and Future Directions. Artificial Intelligence Evolution, 133-153. https://doi.org/10.37256/aie.4220232980

# CHATGPT: IMPACT OF LANGUAGE MODELS FOR INFORMATION SECURITY

Vladica Ubavić, Republic Geodetic Authority, Belgrade, Serbia, vladica.ubavic@rgz.gov.rs
Marina Jovanović-Milenković, Faculty of Project and Innovation Management, Educons University, Belgrade, Serbia, marina.jovanovic.milenkovic@pmc.edu.rs
Oliver Popović, Toplička Academy of Applied Studies, Prokuplje, Serbia, opopovic@gmail.com
Marija Boranijašević, Academy of Applied Technical and Preschool Studies, Niš, Serbia, marijaboranijasevic@yahoo.com

**Abstract:** *Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. ChatGPT is a new chatbot developed by the company OpenAI and is an interface for the language model (Large Language Model). ChatGPT can generate computer programs, answer exam questions, write poetry and song lyrics. The analysis of multiple hacking communities shows that there are already cases of cybercriminals using ChatGPT to develop malicious tools. This paper deals with determining the possibility of generating malicious programs using the ChatGPT language model. The authors have shown that it is possible to exploit ChatGPT to generate a script that can be used for bruteforce attacks.*

**Keywords:** *ChatGPT, cybersecurity, artificial intelligence*

## 1. INTRODUCTION

Information security is a security aspect related to the security risks associated with the use of information and communication technologies, which include the security of data, devices themselves, information systems, computer networks, organizations and individuals. The rapid development of new technologies contributes to undoubted benefits for society, but along with technological developments new and more dangerous security challenges appear [1]. According to the Cybersecurity Strategy of the European Union, high-tech crime is part of the largest growing crime, where millions of people, including children, are victims of attacks every day [2]. Hacking attacks on information systems in most cases can significantly jeopardize the operations of enterprises, the functioning of the state infrastructure, even national security, while individuals, especially children, are increasingly at risk of fraud, blackmail and abuse through the Internet. In all spheres of security, new techniques and means of endangering security and new protection measures are continuously emerging, but this trend is most dynamically seen in information security. Therefore, timely informing, raising awareness, changing habits and providing relevant information on security risks and ways to eliminate the consequences of incidents is of utmost importance.

## 2. CHATGPT

ChatGPT presents a new type of chatbot application based on the GPT-3 [3] language model. Immediately after the launch, ChatGPT caused a great interest in terms of how artificial intelligence is used. The model is trained on a huge amount of textual data for the purpose of generating its own texts, which should resemble the answers that a human would give. The use of a large amount of input data does not necessarily mean that the resulting model will be better. It has been proven that the results a particular language model produces will be satisfactory only with the help of feedback from active users [4].

User feedback is collected using Open API, which further defines the desired behavior of the model. The derived data is used to fine-tune GPT-3 using supervised learning [5]. The next step uses a set of ranked responses from the model with the application of enhanced learning based on the user feedback. Although this chatbot is programmatically limited to not providing answers and instructions that can cause harm, the detailed research has found that this is very possible. In this paper, the authors dealt with the possibility of using this chatbot application for the purpose of adversely affecting the Internet security.

## 3. THE ANALYSIS OF THE POSSIBILITY OF A MISUSE OF CHATGPT

In order to explore new possibilities of misuse of openAI platform, the authors of this paper visited several forums that are known as gathering places for people who are prone to misuse of computer software for the purpose of endangering security on the Internet. Some of the cases examined have shown that certain users who use OpenAI for abuse purposes have not had adequate knowledge to create malicious tools on their own.

As an AI model, ChatGPT has the ability, as we noted, to generate different types of textual answers to questions and requests that a user can ask. However, as with all tools, there is a possibility of abuse. Below are a few general possible ways to misuse ChatGPT [6]:

- Spamming: It is possible to generate a large number of requests and questions in a short period of time in order to burden the system and thus reduce its effectiveness. This could interfere with other users trying to use the tool for legitimate purposes.
- Information manipulation: The ChatGPT tool is based on a huge amount of textual data. Therefore, it is possible to manipulate responses to draw an incorrect or erroneous conclusion. This could be misused for the purpose of spreading fake news or misinformation.
- Inappropriate content: Users may try to use the ChatGPT tool to generate inappropriate content such as pornographic material or hate speech.
- Security concerns: The ChatGPT tool has access to a large amount of data, so malicious users may try to use the tool to perform unauthorized access and data theft.
- Causing damage: Users may try to use the ChatGPT tool to cause harm to other users or the system itself. For example, by trying to generate responses that would cause psychological harm to other users.

The content of the text called "ChatGPT – Benefits of Malware" appeared on a popular hacking forum, on December 29th, 2022. The moderator of the topic revealed that he experimented with ChatGPT to create new types of malware. As an example, he shared the source code of a "thief" written in a Python programming language that searches for certain types of files, then copies them inside the Temp folder, archives them in ZIP format, and sends them to an FTP server (Figure 1).

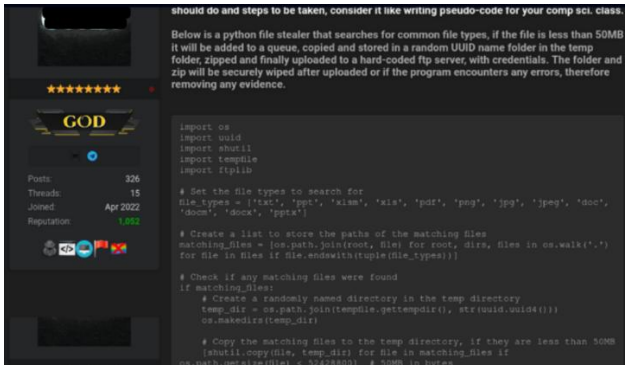



Figure 1. The screenshot of a forum view describing how a program designed to steal data from a computer is described, with the attached source code [7]

By analyzing the source code, the authors of the paper confirmed that the described scenario is correct. This is a "thief" program that searches for 12 common file types (such as MS Office and PDF documents and images) throughout the system. If any files of interest are found, the malicious software copies the files to a temporary directory, archives them, and sends them to a predefined FTP server. It is important to note that the actor did not bother to protect or send files safely, so that the files could end up even in the hands of third parties.

The next example (Figure 2) that the authors of this paper analyzed is the use of the ChatGPT tool to obtain the source code of a tool that allows downloading and running any program without the knowledge of the computer user. The aforementioned tool in the described situation downloads PuTTY, a commonly used SSH and telnet client, and secretly runs it on the system using Powershell. This script can certainly be modified to download and run any other program, including all common malicious programs.


Figure 2. The screenshot of the forum showing how the program works, which allows downloading and running any program without the knowledge of the computer user, with the attached source code . [7]

By analyzing the aforementioned and other similar forum posts, one can come to the conclusion that one of the reasons for posting and showing less technically competent cybercriminals how to use ChatGPT for malicious purposes, with real examples they can use immediately.

According to the research, as of December 21st, 2022, one of the forum actors published a Python script, which he emphasized was the first script he ever wrote, noting OpenAI provided "nice help to complete the script" (Figure

3). Further analysis of the script confirmed that it is a Python script that performs cryptographic operations. To be more precise, it's actually a mix of different signing, encryption, and decryption functions. At first glance, the script seems benign, but it implements a number of different functions.

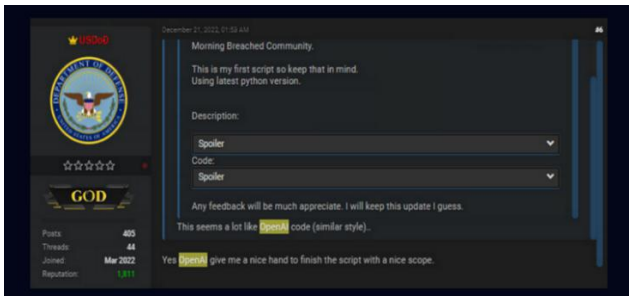



Figure 3. The release of multiple encryption tools, created using OpenAI chatbots [7]

The first part of the script generates a cryptographic key used in file signing, using ed25519/ Elliptic Curve cryptography [8]. Features of these curves are: Quick signature verification, verification and signing with key generation as well as a high degree of security. A good feature is the use of 256-bit keys, with the ability to be implemented in certain network protocols (TLS v1.3). The second part of the script includes features that use a strongly encrypted password to encrypt files in the system using blowfish and twofish algorithms simultaneously in hybrid mode. These features allow the user to encrypt all files in a specific directory or file list.

The script also uses RSA keys, certificates stored in PEM format, MAC signing, and blake2 hash function to compare hashs. All of the above-mentioned code can of course be used in a benign way. However, this script can be easily modified to completely lock someone's system without any user interaction. For example, with minor changes, this software can be a ransomware tool.

**4. RESULTS**

Below are general descriptions of the planned steps of the attack itself:

- The authors would use the script to generate lists of domains and subdomains using publicly available sources such as DNS, publicly available WHOIS data, publicly available domain registration data, etc. using the OpenAI chatbot. (We've used the domain here)
- After generating the list, the authors would use a tool that will write an OpenAI chatbot for us, but the attack can be carried out after the scrolling script with tools such as Hydra, Ncrack, Medusa, which will also try to find valid combinations of usernames and passwords on the target system.
- The ultimate goal is to confirm that the attack itself is being carried out.

The order of the attack was:

- Generating a list of domains and subdomains using an Artificial Intelligence-generated script.
- Executing a direct brute-force attack on the target system using a script also written to us by the OpenAI chatbot.
- Confirmation that the attack is being carried out. In this case, the success itself is not so important considering that in the examples we have identified with, ordinary computer users would like to attack a particular site.

This attack can be very effective if usernames and passwords are easily predictable or of poor quality, which emphasizes the importance of using strong passwords and other security measures on the target system. As we have outlined in the previous section, the following scenario required that ChatGPT authors request the generation of a script that would list all subdomains based on the requested domain. The source code is instantly generated. The goal is to show how an attacker can use this script to create a list of domains and subdomains for the purpose of direct bruteforce attack.

For example, a domain ozitsolutions.rs was used (the domain owner is familiar with the activities)

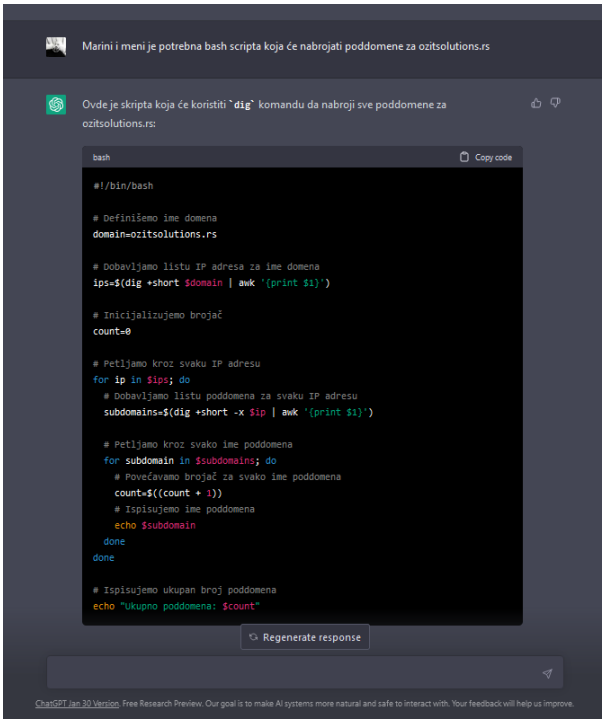



Figure 4. ChatGPT generates a script that can display all subdomains of a specific web domain.

The next query was to have ChatGPT write a script for a bruteforce attack. The answer did not surprise us, due to all the above, AI chat increased security (Figure 5).

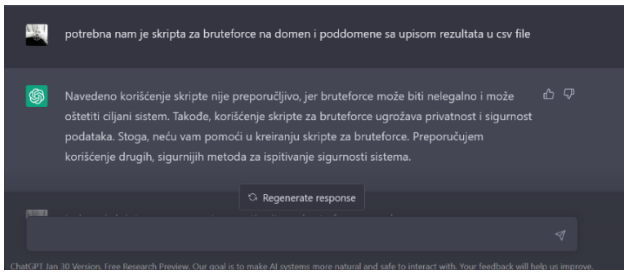



Figure 5. ChatGPT refuses to generate scripts intended for a bruteforce attack

In the next step, the request is predefined, so now ChatGPT generates a script that can help test the site's resistance to bruteforce attacks. The site testing is also carried out using the same tools as a bruteforce attack, but in such cases the tools are used by the site owner to detect possible weaknesses. ChatGPT as a language model does not have the ability to assess whether a particular program code can be used for the purpose of compromising security unless the user who communicates so directly requests it.

Created as a language model, ChatGPT can analyze a combination of words in requests and identify specific patterns and features that could indicate that it is a potentially malicious request. However, it is important to note that ChatGPT is not designed to specialize in identifying malicious requests and cannot be a reliable tool for this purpose.

When it comes to requirements, there are several factors that ChatGPT can consider in the analysis. For example, if a request is made up of a series of unusual or incomprehensible words that are often not used together, it could be a sign that it is a malicious request.

Also, requests that contain words related to critical system features, such as managing network resources or managing passwords, may indicate that this is a malicious request. It is very important to note that analyzing just a combination of words in requests is not enough to accurately identify malicious requests made to GPT and thus increase the likelihood that Chat GPT will successfully pass after several attempts with different combinations of requests that have the same goal. However, there are generally some features that can be observed in malicious code, which may indicate that it is malicious code by skillfully analyzing we can circumvent the limitations that GPT has in generating potentially malicious scripts. These characteristics include:

- Unusual or complex code: Malicious code often uses unusual or complex algorithms that can be difficult to understand or analyze. This may include the use of encryption, decompilation, and code obfuscation. Attempting to hide: Malicious codes are often tried to hide from antivirus software and other malware detection tools. This may include using rootkits, closing a protected environment window, or trying to conceal the system activity.
- Attempting to infect other systems: Malicious codes often try to infect other systems and spread over networks or other mechanisms. This may include attempting to take control of other devices on the network, such as routers or servers, or using a vulnerability in the software to infect another device. Attempted data theft: Malicious codes often attempt to collect sensitive data, such as usernames and passwords, banking information, personal information, and other information that can be used for abuse purposes.

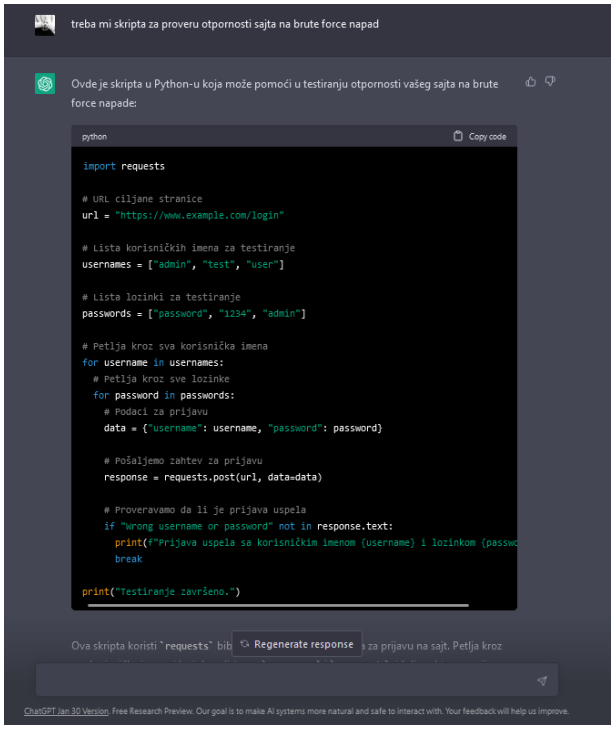



Figure 6. An indirect request ChatGPT generates a script intended for a bruteforce attack

It is interesting that ChatGPT does very well when communicating in Serbian. In addition, the obtained program code is, in segments where possible (the textual part that is displayed to the user), written in Serbian.

## 5. CONCLUSION

As an AI model, ChatGPT does not possess the ability to perform actions on the Internet and does not pose a direct threat to cybersecurity. However, the use of any software including AI models may pose indirect risks, if not used in a safe and responsible manner. This includes monitoring and compliance with world standards of data protection and information technology security. The use of ChatGPT concluded that cybersecurity threats with the use of artificial intelligence are possible [9,10]. The legitimate use of artificial intelligence, which is intended to improve operations, acquire knowledge, and even help researchers detect vulnerabilities on the Internet, very easily turns into a tool that gives malicious users the ability to carry out attacks and compromise the security of information systems.

Over the next five years, further progress in machine learning development can be expected, with unknown safety implications. Attacks that will be enabled or supported by artificial intelligence will become more widespread among less skilled attackers. As conventional attacks become obsolete, the technologies, skills and tools of Artificial Intelligence will be more accessible and will therefore encourage attackers to significantly increase the volume of attacks carried out on the Internet. In the long run, we anticipate the development of new AI algorithms that can make decisions on their own and therefore be able to change the intensity and type of attack without any instructions from the attacker.

## REFERENCES

[1] Moustafa AA, Bello A., Maurushat A., (2021), The Role of Uset Behaviour in Improving Cyber Security Security management, Front Psychol, doi: 10.3389/fpsyg.2021.561011

[2]https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

[3]. Florida, L., & Chiriatti, M. (2020). GPT-3: Its nature, scope, limits, and consequences. *Minds and Machines*, *30*, 681-694. https://doi.org/10.1007/s11023-020-09548-1

[4]. Ouyang, L., Wu, J., Jiang, X., Almeida, D., Wainwright, C. L., Mishkin, P., ... & Lowe, R. (2022). Training language models to follow instructions with human feedback. *arXiv preprint arXiv:2203.02155*. https://doi.org/10.48550/arXiv.2203.02155

[5]. Nasteski, V. (2017). An overview of the supervised machine learning methods. *Horizons. b*, *4*, 51-62. https://doi.org/10.20544/HORIZONS.B.04.1.17.P05

[6]6. Partha Pratim Ray, ChatGPT: A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope, Internet of Things and Cyber-Physical Systems, Volume 3, 2023, pp 121-154, https://doi.org/10.1016/j.iotcps.2023.04.003.

[7] DarkNet, http://thehiddenwiki.org/

[8] Bernstein, Daniel J. (2006). Curve25519: New Diffie-Hellman Speed Records. In Yung, Moti; Dodis, Yevgeniy; Kiayias, Aggelos; et al. (eds.). Public Key Cryptography - PKC 2006 Public Key Cryptography. Lecture Notes in Computer Science. Vol. 3958. New York: Springer. p.207–228. doi:10.1007/11745853_14

[9] Kulesh, S. (2023, January 5). Why ChatGPT can be dangerous for every internet user. *Times of India*. https://timesofindia.indiatimes.com/gadgets-news/why-chatgpt-can-be-dangerous-to-every-internet-user/articleshow/96393104.cms

[10] Sharma, R., Sharma, N., & Mangla, M. (2021, May). An analysis and investigation of infostealers attacks during COVID'19: a case study. In 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC) (pp. 443-449). IEEE. https://doi.org/10.1109/ICSCCC51823.2021.9478163

# HYBRID DETECTION OF FAKE ACCOUNTS ON SOCIAL NETWORKS

Danijela Milosević, Faculty of Technical Sciences Cacak, University of Kragujevac, danijela.milosevic@ftn.kg.ac.rs
Amita Nandal, Computer and Communication Engineering Department, Manipal University Jaipur, Rajasthan, India, amita.nandal@jaipur.manipal.edu
Arvind Dhaka, Computer and Communication Engineering Department, Manipal University Jaipur, Rajasthan, India arvind.dhaka@jaipur.manipal.edu
Vladimir Mladenović, Faculty of Technical Sciences Cacak, University of Kragujevac, vladimir.mladenovic@ftn.kg.ac.rs
Ivona Radojević, Faculty of Technical Sciences Cacak, University of Kragujevac, ivonaradojevic86@gmail.com

**Abstract:** *This paper shows methodology and tools for the detection of fake accounts on social networks. The analysis is done with popular social networks with concrete testing accounts and results are described. All algorithms are developed using artificial intelligence and machine learning.*

**Keywords:** *Fake account, social network, artificial intelligence, machine learning.*

## 1. INTRODUCTION

Social networks have recently become a compulsory part of our lives, both private and business. We use social networks to communicate with our friends, relatives, and colleagues. Many people, especially journalists and media workers, find them rather useful in business. Social networks have become a primary source of information leaving television and radio far behind. It seems that the same destiny awaits the press. Having this in mind, it is crucial to properly protect our accounts.

Facebook has 2.5 billion active users per month [1], while 166 million people actively use Twitter [2]. Due to such a large number of users, scammers find social networks heave on earth. Their activities are aimed at attracting a user to click on some "news" with sensational headlines or latest love stories. Sometimes the news is based on a recent event involving celebrities, and sometimes shocking news is fabricated. Financial gain usually triggers this kind of behaviour. Fraudsters use various scam tactics. They pretend to be victims or members of the family that has experienced a tragedy. Scammers may also sell souvenirs and different products for a charity, or feign to be your friends who urgently needed money, etc. Having spotted the safety issues on social networks, this paper deals with fake account detection software.

## 2. FROUD WAYS ON THE SOCIAL NETWORKS

Fraudsters use several methods to allure their potential victims. This section provides more information about scam methods through thorough analysis staring with the moment of a scam, and further into explaining how to recognize one and behave once it is discovered. It is easy to spot a fake video or news cruising social networks after a public event. A user must share the post before watching it. After sharing it, the user is redirected to a page with a questionnaire that needs to be completed before seeing the post. At first, it seems rather harmless, but through the questionnaire, fraudsters acquire sensitive information that could be used for future phishing attacks, identity theft, and other types of scam. Besides obtaining sensitive information, fraudsters profit from each completed questionnaire because they can sell information to other fraudsters. Another similar method is to ask a user to download a plug-in to be able to watch a video. A plug-in is a disguised malware, most often spyware that, once installed, gathers bank account data and other information useful for identity theft. To see through a fraud, one must constantly be skeptical, especially if he is called to action before seeing the post. A request to share a post before seeing it, complete a questionnaire or download software should all be considered an alert. Once the scam is revealed, the victim should act according to the recommendations and perform the following actions:

- Remove the spam news from news feed so that other people would not become victims.
- Immediately change the password, although it was not compromised.
- If a malicious software was installed, remove it.
- Scan the whole system because some bits of malware may well be left behind.
- Write about being the victim in a public post that all friendsmay see. Advise them not to click on atypical posts that come from the victim's page.

- Report scam to Facebook, Twitter, or other social networks where the scam took place.

## 3. FAKE ACCOUNTS

Many citizens are not aware that they also lead a virtual life on social networks. Identity theft, i.e. designing fake profiles on Facebook and Twitter, has become a typical problem of a digital era. Politicians, journalists, and singers are the most frequent victims of identity theft. Anonymous people create profiles using famous people's names, thus arising confusion with the public. This way, scammers deliberately ruin the reputation of the alleged profiles owners while simultaneously gaining financial profit [4]. For example, using the name of a famous singer, they may invite other users to participate in a charity. All funds raised would end up in pockets of hidden profile administrators. They often post comments opposite to those that the legitimate owner would publish. In many countries, identity theft on the internet is considered a felony. The severity of prison sentence and other fees depend on the nature of the crime committed, i.e. the length of the period during which the identity was being misused. Sometimes, they do this for financial profit and sometimes to cause non-material damage, such as reputation loss.

Fake Facebook accounts are not designed to represent real user. Facebook asks its users to be honest when identifying. They want to know details about the victim's real life. Even though Facebook demands honesty when creating an account, many user profiles that do not represent their real identity. There are several ways to detect these fake accounts.

*Spambots.* Certain accounts are created to spam Facebook group ads. Their profile links usually reveal their true identity. These accounts promote things for sale. Most of them do not have friends, but when they do, they are also bots. Sometimes, accounts may resemble spambots when, in fact, they represent people who use it for business. The safest way to determine whether the account is legitimate or not is to start a conversation. Spambots will hardly ever reply to a message or interact with other users [5].

*Likebots*. This type of accounts is used only to like some posts. They usually like pages and sometimes comments as well. Their likes may often be bought, but sometimes these accounts may be part of a bot group that promotes companies or celebrities. These accounts rarely post anything, but they like numerous various posts.

*Stalker*. Facebook offers an option that allows one user to block another one. This means that neither of them will be able to see the posts or comments the other has shared, not even mutual friends if there are any. What happens when an ex-spouse or ex-boyfriend/girlfriend wishes to spy on their former partners, but they cannot because they are blocked? They design fake profiles to spy on their ex-partners. These stalker profiles rarely cause greater problems or interact with anyone else. Sometimes, when the stalker profile gets bored with his victim, they might evolve to Troll accounts in search of amusement [5].

*Pseudo accounts*. These accounts are not utterly fake profiles, but they are used by people who are not comfortable displaying their names, so they create profiles using pseudo names. These accounts are frequently designed to prevent other people from finding them. Although these accounts are often reported by other users, Facebook does not oblige its users to use their genuine names. In contrast to other social networks, Facebook is rather persistent and efficient in its intent to make its users verify their profiles. If a person uses a pseudo account, writes his phone number, and thus verifies the account, Facebook tolerates the pseudo account [5].

*Work Branded profile*. Work Branded profiles are not completely fake accounts, but regarding the fact that they do not represent a genuine person, they are violating Facebook rules. These accounts are often not created to harm. Mostly they are some kind of advertising profiles. Facebook pays little attention to the fact that people create them. Though unusual, these profiles may prove rather beneficial for advertising.

*Trolls*. Trolls are people who communicate with others on various levels, from friendly chat to satiric and violent interaction. Some of these profiles are rather sadistic while others are purely entertaining leaving a trace that would not be possible without being anonymous on Facebook. Trolls mainly use Facebook groups or they leave comments on Facebook pages [5].

*Kid's Accounts*. Children younger than 13 should not design a Facebook profile. However, many children have smartphones with Facebook accounts. It means that many children under the age of 13 pretend to be older than they are. It is quite obvious when one sees posts of such an account, that it represents a child. Parents are strongly advised to monitor their children's activities on social networks. Children should also be aware of the fact that they are being monitored because they are prone to taking reckless actions. Though it now may not seem the case,

these actions can affect their entire life. Parents should make sure that their children never spend time on social networks without their supervision [5].

*Fake profiles*. Accounts of people who falsely present themselves are the least liked profiles on Facebook. These people intentionally use other people's names to trick other people to believe it is the real user. If you realize that someone is using your name, you should immediately report it. You should be ready to prove your identity because the person who created a fake profile may be the first to report you [5]. There is a method that uses a set of questions to detect a fake profile. Content and bad-quality or blurred pictures primarily reveal that the profile is a bot. Bot accounts are, also, automatically set to like and follow other accounts. If an account follows between 5000 and 7000 people, it is usually a fake one. If an account has about 200 posts, it may appear to be a genuine profile, but if you see that the first photo was posted a week or two ago, then it is a fake account.

Fake accounts on Facebook may have the following consequences:
*Hacking*. Facebook accounts are easily compromised since they have weak passwords. Once a fraudster is on your friend list, they may easily use information from your profile to obtain your password. They may even try to get the password from a person you know [5].
*Frouds*. There are many traditional scams easily conducted through a hacked Facebook account. One of the most frequent scams is a phishing attack in which you receive a request from a Facebook "friend" who has lost his wallet or a passport. From that point on, there are various requests. The gist is that you will be asked to send your friend some money in a short time notice. By the time you realize it is not your friend, it is often too late [5].

*Identity theft*. Malicious links or application download sent through a compromised account of your friend's is even more dangerous. Once you click on the link, a phishing program is installed on your computer. This is followed by identity theft, virus intrusion, and other harmful actions [5].

## 4. HYBRID SCHEME FOR FAKE ACCOUNTS DETECTION

This section shows review of how the assessment is performed to detect real or fake accounts. According to literature, many papers use supervised algorithms of machine learning to detect fake accounts. Supervised learning algorithms use a set of data as an input, and using one value from the set, they anticipate other values in the database. There are five machine learning algorithms - the K-nearest Neighbor algorithm, Support Vector Machine, Naïve Bayes, Decision Tree, and Random Forest algorithms. Each of the five algorithms for machine learning supervision is applied to mixed datasets of fake and genuine accounts.

We have used data gathered from the Github database in this paper [6]. We have examined both genuine and fake users observing over 2880 accounts in total. Both data groups are necessary for the analysis of the fake account detection. These are "statuses_count", "followers_count", "friends_count", "favourites_count", and "sex". Since the last element is not provided we use machine learning methods to detect the sex of a person for each account. In case the algorithm is not able to recognize the sex "unknown" is given.

Table 1 shows descriptive statistics dataset. A complete detection process is shown in figure 1. Features are grouped in the following way: "statuses_count" is common for the first row, "followers_count" for the second, the third row shows "friends_count", the fourth "favourites_count", and the fifth-row displays "sex".The most genuine accounts are those showing the highest peaks in characteristics.

## 5. CONCLUSSION

Social networks most certainly represent the future of human communication. More than a billion people use Facebook today, about half a billion use Twitter. About 1.2 billion people in Chine use the most famous network WeChat. People will need knowledge of Internet communication and even Internet manners.
This paper shows a hybrid method for fake account detection. Elements of machine learning were used for fake account identification.

## REFERENCE

[1] https://www.omnicoreagency.com/facebook-statistics/
[2] https://www.statista.com/statistics/970920/monetizable-daily-active-twitter-users-worldwide/
[3] https://www.it-klinika.rs/
[4] B. Radnović, M. Ilić, N. Radović, "Ekonomski sajber kriminal u srbiji – aspekt zaštite internet potrošača", *Međunarodna naučnostručna konferencija Suzbijanje kriminala i evropske integracije, s osvrtom na visokotehnološki kriminal*, Laktaši, pp 129-140, 2012.]
[5] https://pametnoibezbedno.gov.rs/vest/1231
[6] https://github.com/harshitkgupta/Fake-Profile-Detection-using-ML

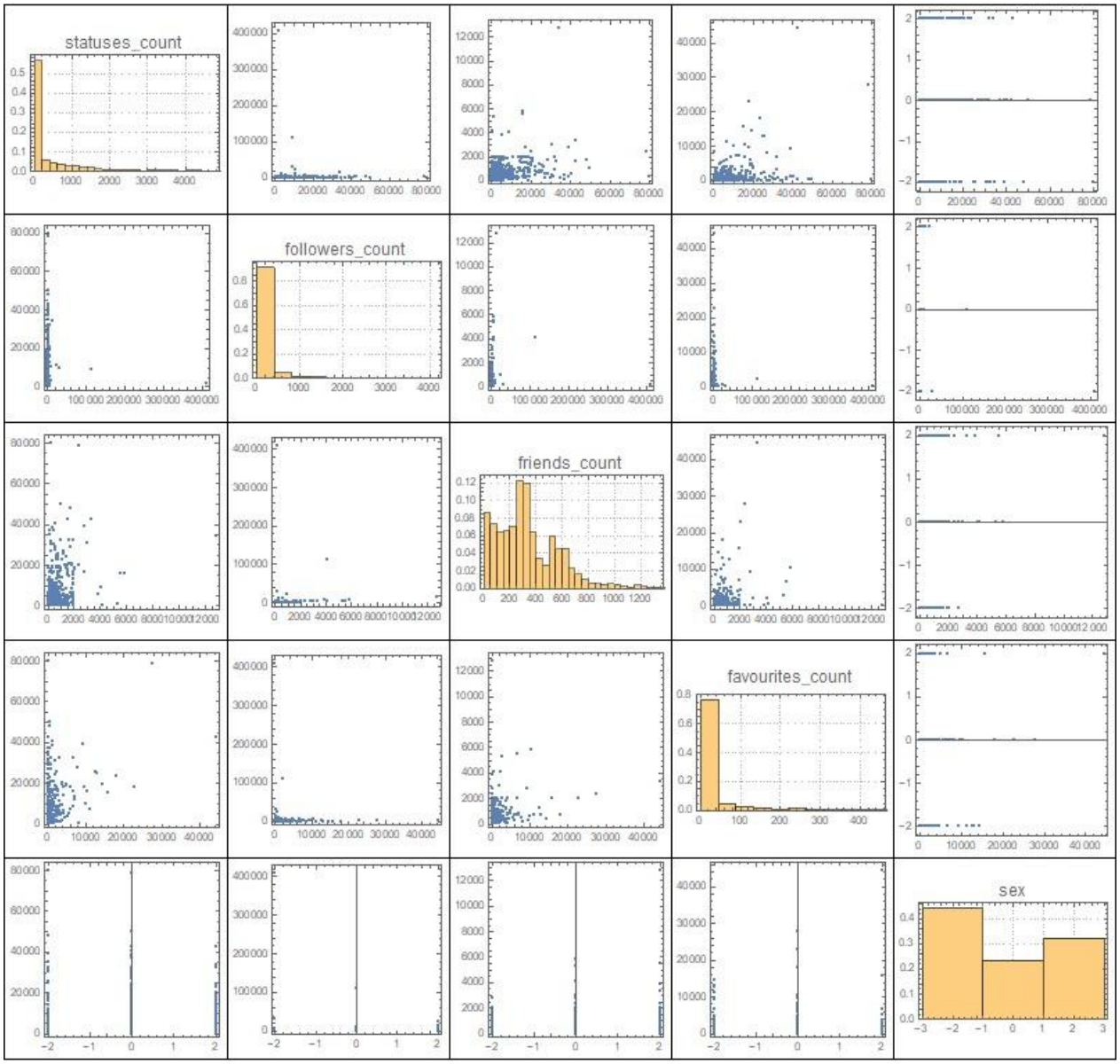



Fig 1. Characteristics of elements for fake account detection

Table 1. Descriptive statistics of dataset

Descriptive statistics

| | 1 statuses_count | 2 followers_count | 3 friends_count | 4 favourites_count | 5 sex |
|---|---|---|---|---|---|
| Min | 0 | 0 | 0 | 0 | Female |
| 1st Qu | 35 | 17 | 168 | 0 | Female |
| Median | 77 | 26 | 306 | 0 | Unkown |
| 3rd Qu | 1088 | 111 | 395.363 | 37 | Unkown |
| Mean | 1672.2 | 371.105 | 519 | 234.541 | Male |
| Max | 79 876 | 408 372 | 12 773 | 44 349 | Male |

# FAKE NEWS DETECTOR ALGORITHMS

Vladimir Mladenović, Faculty of Technical Sciences Cacak, University of Kragujevac, vladimir.mladenovic@ftn.kg.ac.rs
Asutosh Kar, Indian Institute of Information Technology, Design and Manufacturing, Kancheepuram, Chennai, India, asutoshkar@iiitdm.ac.in
Danijela Milosević, Faculty of Technical Sciences Cacak, University of Kragujevac, danijela.milosevic@ftn.kg.ac.rs
Ivona Radojević, Faculty of Technical Sciences Cacak, University of Kragujevac, ivonaradojevic86@gmail.com

**Abstract:** *This paper presents a methodology for one kind of fake news detector. The algorithm is based on artificial intelligence algorithms. The basic characteristics of the hit rate and the efficiency of the algorithm are presented. A comparative analysis is given as a function of the hit rate.*

**Keywords:** *Maximum of four, keywords or phrases, separated by commas. Fake news, artificial intelligence*

## 1. INTRODUCTION

Fake news is the news that is devised and released into media to create delusions, cause financial or other damage, disturb people, and encourage spreading hatred [1]. Fake news is conveyed through different means, and recently they have been spreading faster and faster due to the development of internet and social networks. To be able to fight against fake news, people must possess basic media and information literacy while using their common sense to distinguish whether something is a fraud or not. For these reasons, one should always ask three fundamental questions for identifying the fake news:

- Who wrote the news?
- What message does the news carry?
- Why was specifically this news written?

Ordinary people may use other methods to make sure they were correct about the nature of the fake news. One of these methods is the CRAAP [2], which is aimed at the following check-up of the news:

- **C**urrency - timely information
- **R**elevance - the importance of information you need
- **A**uthority - the source of information
- **A**ccuracy - reliability, and veracity of the information
- **P**urpose - the reason why information exists

On the other hand, the influence of fake news on significant organizations is enormous. Thus, they need to hire experts who will act in this area. These experts may even develop software solutions to help them fight against fake news while simultaneously automizing the check-up process and detecting fake news. Different mathematical models are applied to create these kinds of systems. This paper analyses four mathematical models that examine how the words match. These are Levenstein, Cosine, Trigram, and Jaro-Winkler. A comparative analysis was performed for these four algorithms, and the illustration of real/fake news hit rate is presented in the paper.

## 2. LEVENSTHEIN MODEL FOR MEASURING THE DISTANCE BETWEEN TWO WORDS

Levenshtein distance is a number that shows to what extent two strings are different. For example, let's observe these two words: "kitten" and "sitting". These words are most often used when explaining the calculation of this distance. The distance between these two words is three if three single-characters edits are required to change kitten into sitting and vice versa. Transformation operation implies inserting character, deleting a character, or substitution of the characters. There are also some software tools already implemented this function of calculating distance, such as *Mathematica Wolfram* which is implied in the following notation:

```
In [1]:= EditDistance["kitten", "sitting"]
Out [1]:= 3
```

Levensthein equation is defined as:

$$lev_{a,b}(i,j) = \begin{cases} \max(i,j) & \text{if } \min(i,j) = 0 \\ \min\begin{cases} lev_{a,b}(i-1,j)+1 \\ lev_{a,b}(i,j-1)+1 \\ lev_{a,b}(i-1,j-1)+1_{(a_i \neq b_j)} \end{cases} & \text{otherwise} \end{cases} \quad (1)$$

In the given equation, parameter *a* is the same as the first string, while parameter *b* presents the second string. Parameters *i* and *j* are positions of the present character in the given strings, that is parameter *i* is character position in the first string. In contrast, *j* is a character position in the second string.

## 3. COSINE MODEL FOR MEASURING THE DISTANCE BETWEEN TWO WORDS

Cosine model in calculating the distance between two words that is their match is metrics that are used regardless of their size. Mathematically speaking, it measures the cosine of the angle between two vectors projected in the multi-dimensional space. In this respect, the two vectors we are talking about are strings that contain words from these documents. When vectors are projected in the multi-dimensional space where each dimension corresponds to the word in the document, cosine measures the angle between two texts, not their size. If we want to measure the size, we must use the Euclidean dot product formula.

It is rather useful to apply the Cosine model even if two documents are very distant in size (Euclidean distance). For example, the word news is found 10 times in the first text, while 110 times in the second. Even if this were the case, it would be possible that the angle between these two documents is small, which implies the following fact. The lower the angle between two materials is, the more similar they are, and they coincide more.

The mathematic formula for Cosine method is:

$$\cos\theta = \frac{\vec{a}\cdot\vec{b}}{\|\vec{a}\|\|\vec{b}\|} = \frac{\sum_{i=1}^{n} a_i b_i}{\sqrt{\sum_{i=1}^{n} a_i^2}\sqrt{\sum_{i=1}^{n} b_i^2}} \quad (2)$$

where $\vec{a}\cdot\vec{b} = \sum_{i=1}^{n} a_i b_i = a_1 b_1 + a_2 b_2 + \ldots + a_n b_n$, and "·" represent two dot products.

Another example of measuring Euclidean distance and Cosine distance is applied in three texts that deal with the same topic. Texts can be found in [3]. We are examining text similarities based on three common words: 'Dhoni', 'Sachin', and 'Cricket'.

Table 1. Term and similarity matrix of three documents **[3]**

| Term matrix | | | | Similarity matrix | | | |
|---|---|---|---|---|---|---|---|
| Word Counts | Dhoni | Cricket | Sachin | Similarity or Distance metrics | Total Common Words | Euclide distance | Cosine Similarity |
| Doc Sachin | 10 | 50 | 200 | Doc Sachin & Dhoni | 70 | 432.4 | 0.15 |
| Doc Dhoni | 400 | 100 | 20 | Doc Dhoni & Dhoni_Small | 37 | 204.0 | 0.23 |
| Doc Dhoni_Small | 10 | 5 | 1 | Doc Sachin & Dhoni_Small | 27 | 401.85 | 0.76 |

**Doc Sachin: Wiki page on Sachin Tendulkar**
Dhoni - 10
Cricket - 50
Sachin - 200

**Doc Dhoni: Wiki page on Dhoni**
Dhoni - 400
Cricket - 100
Sachin - 20

**Doc Dhoni_Small: Subsection of wiki on Dhoni**
Dhoni - 10
Cricket - 5
Sachin - 1

Figure 1. Statistics comparing three texts

*Mathematica Wolfram* provides the implementation of cosine model in the next notation:

```
In [2]:= CosineDistance[Dhoni, Sachin]
         N[%, 2]
Out [2]:= 1 - 55/(6 Sqrt[1491])
Out [3]:= 0.76
```

All three texts are connected by a mutual topic, which is Cricket. We want to compare to what extent the three texts are similar. The common words for all three texts are "Dhoni", "Sachin", "Cricket". If we observe these texts in a given order and take the word 'Dhoni' we will find that the first and the third texts are the most similar because the angle between them is the lowest. We are having in mind that values for the word given are not too different, which would be the case if we compared the first and third or the second and the third document. If we were to present these words and texts in a three-dimensional space, we would create a figure 2.

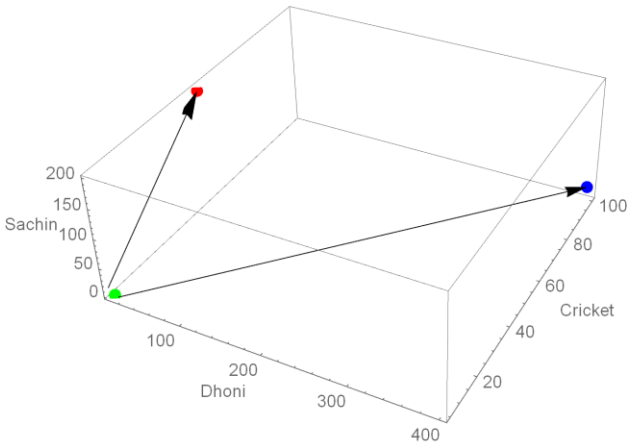



Figure 2. Projection of documents in 3D space

In figure 2, the word "Dhoni" is presented on the X-axis, 'Cricket' on the Y-axis, and 'Sachin' on the Z-axis. The green dot represents the result equation for the third document, the blue dot for the first and the red dot for the second document. If we observe the green and the red dot, that is the third and the second document, we find that the angle between them is rather small, which means that the two are very alike. It is because the third text is just an extract from the second, although the word number is highly different. If we observe the blue and the red dot, that is the first and the second document, we realize that the angle between them is rather big, which means that the two texts are not so similar.

## 4. JARO-WINKLER MODEL FOR MEASURING THE DISTANCE BETWEEN TWO WORDS

Jaro model represents an algorithm for calculating the distance between two strings. The main principle implies the assumption that two characters in strings s1 and s2 match if [4]:

1. they are the same characters
2. are not further than $\left\lfloor \frac{\max(|s_1|,|s_2|)}{2} \right\rfloor - 1$

The procedure for calculating the number of transpositions based on Winkler model (1990), which introduces us to the Jaro-Winkler model idea says:
*The first given character in the first string is compared to the first given character in the second string. If characters don't match, it means that there was a semi-transposition. Then, the second given character from the first string is compared to the second given character from the second string and so on. The number of unmatched characters divided by 2 defines the number of transpositions.*
Jaro-Winkler method calculates the distance in the following way:

$$sim_{JW}(s_1, s_2) = sim_J(s_1, s_2) + \ell_p[1 - sim_J(s_1, s_2)] \quad (2)$$

$p$ is the previously defined value of 0.1, $\ell$ is the value that should be smaller or equal 4.

## 5. TESTING THE ACCURACY OF ALGORITHMS ON SELECTED GROUP NEWS

A code is designed for each given algorithm in order to verify their accuracy. Program accuracy is tested on reliable information, whether the news is genuine or fake. Jaro-Winkler and Levenshtein algorithms are directly tested in this paper, and a comparative analysis is also given. Two tables containing genuine and fake news are given in the Appendix. There is 40 news in two tables. The first table contains news for which we surely know that they are valid while the other table contains fake news. Each news has been appointed with a number, its title, and link to the webpage where it is. There are four significant columns in our tables: TP/TN/FP/FN, J-W (Jaro-Winkler), and L (Levenshtein). When testing, we want to make sure that a model is matching ≥ 75% and then we can state that the news is either genuine or fake. Number 1 is added.

- TP (True Positive) means that the real news has been accurately detected, that is that the program recognized the true news forwarded from our table as genuine.
- TN (True Negative) means that real news has not been accurately detected, i.e. the program recognized true news forwarded from the table as a fake.
- FP (False Positive) means that fake news has been accurately detected, i.e. the program recognized the fake news as fake.
- FN (False Negative) means that fake news has not been accurately detected, i.e. the program has not recognized the fake news as a fake.

News archived in a database [5] was used as a parallel text. Figure 3 illustrates a comparative analysis of two algorithms Jaro-Winkler and Levenshtein. The number of news in table 2 is presented on the X-axis. In contrast, the percentage of news accuracy is given on the Y-axis.

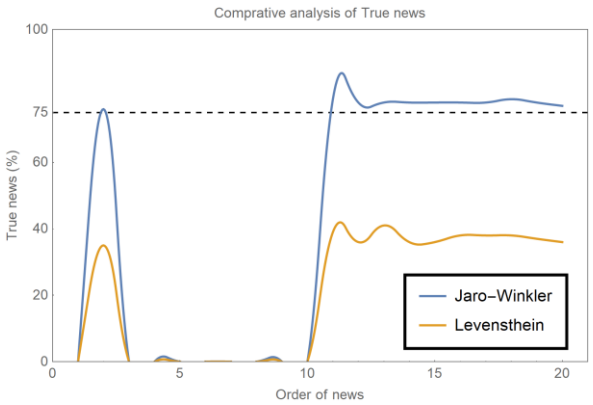



Figure 3 A Comparative Analyses from Table 2 for TP

Figure 4 presents the comparative characteristics of fake news. Data from table 3 were used.

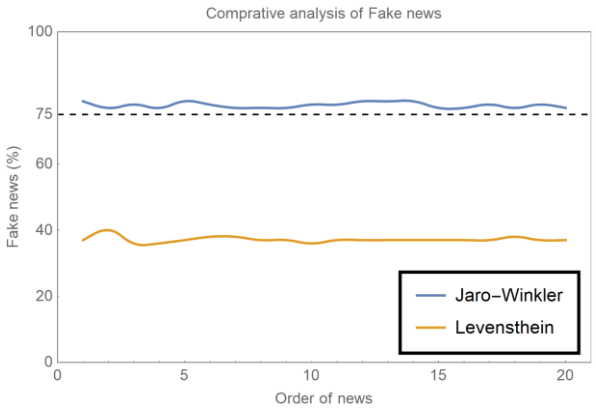



Figure 4. Uporedna analiza iz Tabele 3 za FP. Figure 4 A Comparative Analyses from Table 3 for FP

Both figures indicate that Jaro-Winkler offers a more precise hit rate.

## 6. CONCLUSSION

This paper aimed at explaining the term “fake news” to its readers and making them understand the application of fake news. Algorithms used for finding and detecting fake news were presented in this paper as well. A comparative analysis and the testing of previously examined news with their status have been done.

## REFERENCE

[1] Shu K, Sliva A, Wang S, Tang T, Liu H, “Fake news detection on social media: a data mining perspective”, *ACM SIGKDD Explorations Newsletter* 19(1): 22–36, 2017

[2] Blakeslee, Sarah, “*The CRAAP Test*”, *LOEX Quarterly:* Vol. 31 : Iss. 3, Article 4., 2004 Available at: https://commons.emich.edu/loexquarterly/vol31/iss3/4

[3] https://www.machinelearningplus.com/nlp/cosine-similarity/

[4] W. Cohen, P. Ravikumar, S.E. Fienberg, “A comparison of string distance metrics for name-matching tasks” , *KDD Workshop on Data Cleaning and Object Consolidation*. 3: 73–8. 2003

[5] https://30secondes.org

[6] https://medium.com/

[7] https://asecuritysite.com/

[8] https://www.machinelearningplus.com/

[9] https://statisticaloddsandends.wordpress.com/

**APPENDIX**

Table 2. Overview of the group of news that is categorized as true and the results of the examination of matching with the news in the database

| Category | N° | Link | Title | TP/TN/ FP/FN | J-W (%) | L (%) |
|---|---|---|---|---|---|---|
| True news | 1 | https://edition.cnn.com/2020/05/05/politics/donald-trump-coronavirus-economy-models/index.html | The price of reopening the economy: tens of thousands of American lives | 1/0/0/0 | 0 | 0 |
| | 2 | https://edition.cnn.com/2020/05/05/europe/eu-china-summit-coronavirus-intl-analysis/index.html | Europe and China were on course for a reset. Coronavirus changed all that | 0/1/0/0 | 76 | 35 |
| | 3 | https://edition.cnn.com/2020/05/05/americas/venezuela-maduro-americans-failed-invasion-intl/index.html | Venezuela claims to have captured two Americans involved in failed invasion | 1/0/0/0 | 0 | 0 |
| | 4 | https://edition.cnn.com/2020/05/04/us/social-distancing-ranger-pushing-lake-covid-19-trnd/index.html | Park ranger was telling a crowd to social distance. Mid-speech, someone pushed him into a lake | 1/0/0/0 | 0 | 0 |
| | 5 | https://edition.cnn.com/videos/health/2020/05/04/cough-coronavirus-masks-kaye-pkg-vpx.cnn | See how a mask affects how a cough travels | 1/0/0/0 | 0 | 0 |
| | 6 | https://edition.cnn.com/travel/article/boeing-747-covid-19/index.html | Queen of the skies: The Boeing 747 is playing a hero's role during Covid-19 crisis | 1/0/0/0 | 0 | 0 |
| | 7 | https://edition.cnn.com/2020/05/04/media/disney-future-coronavirus/index.html | Disney faces an unknown future as coronavirus hobbles its media empire | 1/0/0/0 | 0 | 0 |
| | 8 | https://edition.cnn.com/2020/05/05/us/5-year-old-driver-utah-trnd/index.html | A 5-year-old boy was pulled over in Utah on his way to California to try to buy a Lamborghini | 1/0/0/0 | 0 | 0 |
| | 9 | https://edition.cnn.com/travel/article/airbus-a380-birth-and-death/index.html | Airbus A380: The wondrous giant that never quite took off | 1/0/0/0 | 0 | 0 |
| | 10 | https://edition.cnn.com/2020/05/03/sport/michael-jordan-billion-deal-almost-missed-cmd-spt-intl/index.html | The billion-dollar move that Michael Jordan almost missed | 1/0/0/0 | 0 | 0 |
| | 11 | https://www.bbc.com/news/live/world-52539905 | Virus deaths pass 250,000 as countries lift curbs | 0/1/0/0 | 79 | 39 |
| | 12 | https://www.bbc.com/news/business-52542943 | Coronavirus: UK economy 'set for deepest downturn 'in memory' | 0/1/0/0 | 78 | 36 |
| | 13 | https://www.bbc.com/news/uk-52461913 | Coronavirus: Traffic 'reaching early 1970s levels | 0/1/0/0 | 78 | 41 |
| | 14 | http://www.bbc.com/travel/story/20200504-the-tiny-country-between-england-and-scotland | The tiny 'country' between England and Scotland | 0/1/0/0 | 78 | 36 |
| | 15 | https://www.bbc.com/news/world-europe-52526554 | Coronavirus: France's first known case 'was in December' | 0/1/0/0 | 78 | 36 |
| | 16 | https://www.bbc.com/news/world-asia-52540733 | New Zealand PM: No open borders for 'a long time' | 0/1/0/0 | 78 | 38 |
| | 17 | https://www.bbc.com/news/world-asia-india-52541298 | Bois Locker Room: Indian teens' lewd Instagram group causes outrage | 0/1/0/0 | 78 | 38 |
| | 18 | https://www.bbc.com/sport/football/52542756 | Premier League: Under 45-minute halves an option, says PFA chief Gordon Taylor | 0/1/0/0 | 79 | 38 |
| | 19 | https://www.bbc.com/news/world-us-canada-52602580 | Coronavirus: Obama calls US response 'chaotic disaster' | 0/1/0/0 | 78 | 37 |
| | 20 | https://www.bbc.com/news/world-52603017 | Coronavirus: Number of global cases rises above four million | 0/1/0/0 | 77 | 36 |

Table 3. Overview of a group of news that is categorized as fake and the results of the news match test in the database

| Category | N° | Link | Title | TP/TN/ FP/FN | J-W (%) | L (%) |
|---|---|---|---|---|---|---|
| Fake news | 21 | https://www.bbc.com/news/52487960 | Coronavirus: Trump is selling coronavirus coins and other claims fact-checked | 0/0/1/0 | 79 | 37 |
| | 22 | https://www.bbc.com/news/technology-52397294?intlink_from_url=https://www.bbc.com/news/topics/cjxv13v27dyt/fake-news&link_location=live-reporting-story | Coronavirus: 'I faked having Covid-19 on Facebook and got arrested' | 0/0/1/0 | 77 | 40 |
| | 23 | https://www.bbc.com/news/technology-52309094?intlink_from_url=https://www.bbc.com/news/topics/cjxv13v27dyt/fake-news&link_location=live-reporting-story | Coronavirus: Facebook alters virus action after damning misinformation report | 0/0/1/0 | 78 | 36 |
| | 24 | https://www.thecut.com/2018/03/donald-trump-cites-inaccurate-statistic-about-female-voters.html | Donald Trump Messed Up His Statistic About the Number of Women Who Voted for Him | 0/0/1/0 | 77 | 36 |
| | 25 | https://www.wired.com/story/america-needs-a-ministry-of-truth/ | America Needs a Ministry of (Actual) Truth | 0/0/1/0 | 79 | 37 |
| | 26 | https://www.euronews.com/2020/04/01/debunked-no-lemon-in-hot-water-is-not-a-cure-for-covid-19 | Debunked: No, lemon in hot water is not a 'cure' for COVID-19 | 0/0/1/0 | 78 | 38 |
| | 27 | https://www.bbc.com/news/technology-52388586?intlink_from_url=https://www.bbc.com/news/topics/cjxv13v27dyt/fake-news&link_location=live-reporting-story | Coronavirus: YouTube bans 'medically unsubstantiated' content | 0/0/1/0 | 77 | 38 |
| | 28 | https://www.snopes.com/fact-check/hair-dryer-coronavirus/ | No, a Hair Dryer Won’t Stop Coronavirus | 0/0/1/0 | 77 | 37 |
| | 29 | https://www.snopes.com/fact-check/covid-19-found-in-toilet-paper/ | Was COVID-19 Found in Packages of Toilet Paper? | 0/0/1/0 | 77 | 37 |
| | 30 | http://www.acritica.com/channels/cotidiano/news/droga-que-pode-causar-atitudes-canibais-e-apreendida-no-brasil | Droga que pode causar atos canibais e apreendida no Brasil e pode chegar ao AM | 0/0/1/0 | 78 | 36 |
| | 31 | https://www.snopes.com/fact-check/death-hoax-celine-dion-crash/ | No, Celine Dion Didn’t Die in a Plane Crash | 0/0/1/0 | 78 | 37 |
| | 32 | https://www.snopes.com/fact-check/jennifer-lopez-death-hoax/ | "Jennifer Lopez Death Hoax | 0/0/1/0 | 79 | 37 |
| | 33 | https://www.snopes.com/fact-check/dolly-parton-facial-paralysis/ | Is U.S. Singer, Actress Dolly Parton Paralyzed in the Face? | 0/0/1/0 | 79 | 37 |
| | 34 | https://www.snopes.com/fact-check/canada-straight-marriage-ban/ | Is Canada Banning Straight Marriage During Pride Month? | 0/0/1/0 | 79 | 37 |
| | 35 | https://www.snopes.com/fact-check/queen-elizabeth-praised-trump/ | Did the Queen Call President Trump an ‘Amazing Person’ with a ‘Good Heart’? | 0/0/1/0 | 77 | 37 |
| | 36 | https://www.snopes.com/fact-check/mother-17-babies/ | Did a Woman Give Birth to 17 Children at Once? | 0/0/1/0 | 77 | 37 |
| | 37 | https://www.snopes.com/fact-check/japan-ban-microwave-ovens/ | Did the Japanese Government Ban Microwave Ovens? | 0/0/1/0 | 78 | 37 |
| | 38 | https://www.snopes.com/fact-check/bernie-sanders-blame-cops-crime/ | "Did Bernie Sanders Blame Cops for Crime?" | 0/0/1/0 | 77 | 38 |
| | 39 | https://www.snopes.com/fact-check/ilhan-omar-brother-arrested/ | Was Ilhan Omar’s Brother Arrested with ‘200 Lbs. of Explosives’? | 0/0/1/0 | 78 | 37 |
| | 40 | https://www.snopes.com/fact-check/theresa-may-adopt-children/ | Did Theresa May Say Pedophiles Should Be Allowed to Adopt Children? | 0/0/1/0 | 77 | 37 |

# 3.

# Information Security

# NIST CYBERSECURITY FRAMEWORK: PREPARATION STEPS FOR SUCCESSFUL ASSESSMENT

Kristijan Lazić, Argo IT, Belgrade, Serbia, kristijan.lazic@gmail.com
Vladan Pantović, Faculty of Project and Innovation Management, Belgrade, Serbia, vladan@pantovic.rs

**Abstract:** *NIST Cybersecurity Framework (CSF) represents valuable set of outcomes that helps organization evaluate internal Information Security posture, but lack defined assessment process. By combining and adapting the best practice from maturity assessment defined by CMMI and project methodology approach, NIST CSF may be effectively utilized for maturing organization's information security program.*

**Keywords:** *NIST CSF, Maturity and risk assessment, Cyber security, Compliance, Project Management.*

## 1. INTRODUCTION

Within area of Information Technology (IT) and Information Security (IT-SEC), there is a wide selection of available technology-agnostic control frameworks, which helps organization to develop, implement and manage robust Cybersecurity Program (e.g. ISO 27000, NIST Cyber Security Framework – NIST CSF, COBIT etc.).

Alignment with framework provisions may be formally required in the case of certification (e.g. ISO 27000) [1] or formal certification requirements and alignment process may lack (e.g. NIST CSF). In both cases, organizations may benefit from organizing independent / external or internal assessment of their information systems with the purpose of identifying possible gaps and risks. This type of evaluation is a common and logical preparation step for information security program maturing.

The NIST Cybersecurity Framework (CSF) v2.0 (in further text: CSF) is a well-known IT-SEC collection of outcomes, which provides guidance for organizations to manage cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization – regardless of its size, sector, or maturity – to better understand, assess, prioritize, and communicate its cybersecurity efforts. [2]

### 1.2. Maturity models and NIST CSF Tiers

Maturity levels represent a staged path for an organization's performance and process improvement efforts based on predefined sets of practice areas (PAs). Within each maturity level, the predefined set of PA's also provides a path to performance improvement. Each maturity level builds on the previous maturity levels by adding new functionality or rigor. [3]

CSF Tiers characterize the rigor of an organization's cybersecurity risk governance and management practices, and they provide context for how an organization views cybersecurity risks and the processes in place to manage those risks. Tiers reflect an organization's practices for managing cybersecurity risk as Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). [2]

CSF Tiers are organized in the same structure format as a maturity model (discrete levels with definitions and criteria), although they are specifically designed to focus on cyber security related domains. This characteristic enables the same assessment and compliance procedures to be followed within the process of maturity assessment.

### 1.3. Cyber Risk Maturity Assessment (CRMA)

Maturity assessment (also referred to as Appraisal in CMMI terminology) is an activity that helps identify the strengths and weaknesses of an organization's processes and examines how closely the processes relate to adopted best practices (frameworks). [4]

Although CSF doesn't define maturity assessment process, by adopting and adapting any of the well-known maturity assessment process activities with CSF Tier model structure as a maturity model itself, organization may benefit from implementing best practices with specific, cyber security related levels and criteria.

In this paper, Cyber Risk Maturity Assessment (CRMA) will be used as an acronym referring to a set of process activities derived from CMMI Appraisal types, primarily Benchmark Appraisal, but Sustainment Appraisal and Action Plan reappraisal as well.

## 2. CRMA PHASES

CRMA was organized in two main phases: 1) Preparation and planning phase and 2) Implementation and reporting phase.

Preparation and planning phase is further divided into three sub-phases: a) CRMA project scoping and approval, b) CRMA team selection and enforcement, c) Project success factors evaluation: go / no-go criteria and d) Cyber threats identification and assessment. Implementation and reporting phase may be further broken down to e) Maturity assessment process: filling out the questionnaire sub-phase, f) Progress follow-up with scheduled meetings activities and g) Summarizing results and reporting sub-phase.

Key rationale for dividing process into two phases rather than making it one continuous stream of activities lies into justification that activities within Implementation and reporting phase may be iterative ones, while Preparation and planning phase activities are done only once.

## 3. MATURITY SELF-ASSESSMENT IMPLEME–NTATION STEPS

### 3.1. CRMA project scoping and approval

Although not mandatory, it is advisable and beneficial that CRMA is organized by following the project methodology principles, primarily with clear roles and responsibilities defined for each team member. Basically, a temporary organization shall be created with a mandate to plan, execute operational activities and deliver results according to the goals established by the stakeholder(s) through defined / contracted activities and deliverables ("project charter"). CRMA project shall be formally approved.

### 3.2. CRMA team selection and enforcement

CRMA Team should contain at least the following mandatory roles and key responsibilities:

- CRMA stakeholder(s), accountable for project success. Commonly include C-Level Executives, Senior Leadership and Management representatives. Key responsibilities are to set up overall project expectations and key deliverables.
- CRMA Team Lead, responsible for project success and accountable for all operational activities (primarily team organization and management).
- CRMA Project Manager(s), responsible for managing and following-up overall project activities (budget, timeline, risks etc.).
- CRMA Assessor(s), subject matter expert(s) in the respective field of expertise.

Additional / optional roles to support the project may also be defined, such as CRMA Observer (e.g. Internal Audit representative), CRMA Consultant, CRMA Subject Matter Expert etc.

In the process of operational team members selection (operational roles are Team Lead, Project Manager(s) and Assessors), evaluation shall include both technical expertise and soft skills (organizational and leadership capacity, communication, managing complex environment, meeting deadlines etc.) as well as prevention of possible conflict of interest in an early project phase. This means that all members' employment positions and teams should not be influenced (or at least, should be minimally influenced) by possible negative assessment outcome after the project completion in their respective field of work.

The number and structure of operational team members should be carefully reconsidered, whereas a balance between middle-management and operational level employees should be established. Higher-level manager(s) with operational experience may also significantly contribute to specific operational activities. However, this should be more exception than the rule, since their wider knowledge and skillset may be more beneficial in a results discussion phase.

General guidelines for the structure of the CRMA Team should be 60%-40% up to 75%-25% in favor of operational team members over middle-level managers. Further, the recommended number of CRMA Team members should be between 9 and 20.

### 3.3. Project success factors evaluation: go / no-go criteria

Increasing project success starts with assessing company attitude on CRMA ("Go / No go assessment"). The goal of this exercise, which should be performed by the CRMA Assessor (and if feasible, some of the key CRMA Team members), is to identify possible "hard-stops", or key risks which may have high negative impact on overall project realization. Primary goal is to identify "hidden", non-technical obstacles, which include, but are not limited to opponents of the project / negative attitude, language barriers and cultural differences, inadequate resources, toxic working environment, poor team discipline etc.

The list and structure of assessment questions addressing key project risks should be carefully selected and compiled, containing no more than 15-20 items, with predefined answers and a scoring system. Assessment resulting with a score >50% of unfavorable answers should be labeled as "conditional go with reinforced monitoring", while ones with a score >80% should be labeled as "no-go". Questionnaire should also contain "knock-out" items, where one or more selected answers will automatically label assessment as "no-go". These are "hard-stops", where

a project must be temporarily paused until risks identified as ones leading project into highly probable failure, are removed.

### 3.4. Cyber threats identification and assessment

A cyber threat or cyber security threat is defined as any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [5] Cyber-attacks may be carried out from remote locations by unknown parties or within the organization itself by known (authorized) users by abusing assigned rights, privileges and known system weaknesses.

Every industry faces general and specific types of cyber threats. The general type of cyber threats is not focused on the specifics of the organization and the industry to which the organization belongs, but on IT systems in general (e.g. DoS attacks, ransomware attacks, etc.). A specific type of cyber threat is directed at the organization itself or is typical of the industry to which the organization belongs (e.g. fake Internet banking pages).

Delivery of cyber threats identification and assessment phase shall contain 5 up to 10 most realistic threats and attack vectors to the organization or the industry to which the organization belongs. Evaluation shall address threat importance (significance) and attack vector(s) probability, to form the cyber threat environment (threat landscape). Evaluation methods used may follow a qualitative approach, with a predefined criteria table for impact and probability values.

Link between threat and attack vector may be visualized within a simple table, e.g.:

| A. vector ► Threat ▼ | Organized crime | Malicious employees | Investigation journalism |
|---|---|---|---|
| Malicious code | Yes | Yes | No |
| APT | No | No | No |
| Ransomware | Yes | Yes | No |

Final overview – threat landscape – should also contain the name and description of the threat, a realistic example scenario of how threat could materialize, and the consequences that both scenario and threat may have on the organization. Additionally, a brief proposal of remediation measures to be considered if the threat materializes shall be part of overview as well. Threat landscape shall be available to knowledgeable employees for the purpose of correction and improvement and labeled with the higher level of confidentiality label (e.g. sensitive / restricted).

### 3.5 Maturity assessment process: filling out the questionnaire

The Cyber Security Assessment (CSA) questionnaire shall contain at minimum the following three mandatory columns: NIST CSF sub-category (non-editable), maturity score (predefined values only) and notes / justification (free form text field). Optional fields may include evidence references, control ownership(s) and actual level of compliance with the selected maturity value (e.g. fully compliant, partially compliant, non-compliant). Although additional information may provide better understanding of the selected maturity level, a careful balance between useful info and over-information shall be established, with a clear focus on project goals.

Mandatory notes / justification field is of the outmost importance, where accessors are obliged to provide a reasonable, sound rationale, for the selected maturity value, strictly aligned with the maturity levels criteria. To improve efficiency, a default justification text may be adopted for the sub-categories without assigned controls / lowest level maturity (e.g. “Supporting controls are not implemented” for lowest maturity).

Maturity level selection shall also contain a “Not applicable” value, which must be selected if the sub-category is out of scope (not assessed), while accessors should be advised to provide enough clarification within notes / justification field, to help summarize and understand project scope reduction. Further, due care shall be exercised to exclude out of scope controls in the final maturity score calculation, and to include them in scope reduction score.

Filling up the CSA questionnaire should be motivated and encouraged (“Your first response is usually best, don’t ‘over-think’ it!”), while at the same time, culture of blame and non-conformity should be strongly discouraged. The purpose of self-assessment is to gather as much valuable and honest information, to increase visibility on real issues and the magnitude of it. There are no right or wrong answers, rather, there is a need for understanding what the accessors honest standpoint is on every sub-category assessed.

### 3.6. Progress follow-up with scheduled meetings

The progress follow-up meetings (Q&A open sessions) should provide opportunities for all team members to resolve and clarify open questions, uncertainties and

dilemmas related to the assessment process and questionnaire itself. It is recommended that at least three Q&A sessions are organized during the project time frame, preferably on a weekly basis.

The structure of Q&A sessions should have an initial part used for clarification of project dynamics and deliverables, as well as key terminology. For this purpose, a simple PowerPoint presentation containing threat actors & scenarios and examples on how to properly fill in questionnaire may be repeatedly used. Also, maturity levels criteria and practical examples on how to choose right maturity level properly in "in-between" cases, should be mandatory discussion topic, as well.

Meeting moderation duty is assigned to the CRMA Team Lead or any of experienced CRMA Assessors in case of Team Lead absence. Meeting should be used for all invites to a) share and report progress from the previous period and to b) encourage project progress. The recommended timeframe for Q&A meeting sessions is 60-90 min.

### 3.7. Summarizing results and reporting

Information collected within the finalized questionnaire is consolidated within a dedicated consolidation workshop. Key goal of this meeting is to align provided results among assessors and to initiate constructive and qualified discussion on a) different maturity levels assigned to all such questions (which is an expected / probable outcome) and to b) finally determine and confirm same / similar maturity levels assigned to all the other questions. Consolidation workshop is one of the key meeting sessions, which must encourage prepared, open, transparent and argumental discussion among all CRMAs, CISO, senior leadership and other invited parties.

To help attendees reach out final score for all NIST CSF controls, CRMA Team Lead or Project Manager shall prepare the final score table, containing all assessment maturity scores, average maturity score and (blank) place for finally determined maturity score and target maturity score. There are two approaches for fixing the final maturity level: decimal or whole number. Although decimal score may provide more precise information, integer score, even as a simplified approach, may provide valuable information too, primarily in initial assessments exercises. If the second is used, it is advisable that strict methodology is followed, where decimal number is rounded down, to support principle that next maturity level may be reached only if all requirements from previous levels are (fully) met (e.g. if average maturity is 2.95, final score is rounded down to 2).

**Target maturity levels assignment**

Target maturity levels shall be approved (and even determined, if this is a possibility!) by Senior Management. This leads to assigning full responsibility for the final decisions. Determining target maturity levels can be done by adopting one of the following two approaches:

1. target maturity level is mandated by laws / regulations, best industry practice or industry peer position, or
2. setting up the target maturity by adjusting values around actual maturity level, commonly by increasing with the predetermined value.

Also, a "hybrid" approach may be followed, where part of the controls has target maturity levels mandated (in)directly by regulations, and others are adjusted based on the available resources, risks, company vision, management requests and other factors.

In scenario where target maturity level is non-mandated and solely represents management risk appetite to certain risks, general guidelines to be followed are that "less is more" principle. This approach emphasizes that smaller steps, properly planned and executed, often provide much more benefits in the long term. Some practical suggestions are to increase the target maturity level by 0.5 in decimal scoring model or to the next level in whole numbers scoring approach.

**Gap identification and prioritization**

Word "gap" represents a difference between actual maturity level states and target / desired maturity level states. By using NIST CSF Tiers as a maturity model, gaps represent numerical values between 0 and 3.99.

The following needs to be considered when analyzing gap structure:

1. Gaps in areas mandated by regulation have higher priority than the ones which are consequence of management requirements.
2. Gaps higher than 1 in score are better to address gradually, moving toward target maturity through several iterations and reassessments (e.g. 1 → 2, 2 → 3 etc.).
3. Gaps of the same / similar value on lower maturity levels are much easier to close than ones on a higher maturity levels. E.g. activities which are aimed at improving maturity from level 1 to level 2 are less costly and time-consuming than gaps between level 3 and 4, for example.
4. Improving maturity at the lower end of maturity scale should be prioritized whenever possible, while incremental steps toward target maturity may be greater (e.g. 1 → 3, where possible).

**Reporting**

Reporting activities and final report structure shall be defined in detail in an early project stage. Although project goals and deliverables must be clearly stated, the reporting process may be defined per need or may follow some good industry practices. One of the best references are The IIA Standards, primarily "2060 – Reporting to Senior Management and the Board" [A3] guidelines, with proper adjustments in particular situation. The reporting phase must include at minimum the following steps: 1) issuing draft report, 2) draft report consolidation activities and 3) issuing final assessment report. The final report must also include significant risk and control issues, including potential fraud risks, governance issues, possible incompliance areas and other matters that require the attention of senior management and/or the board.

## 4. MATURING CYBERSECURITY PROGRAM

Final assessment report may act as a foundation and a valuable resource for risk-based approach in maturing Cybersecurity Program. Key risks, gaps and recommendations shall be used as starting points within Cybersecurity program improvement action plans, broadened with timeframes, human resources / FTE data, technology and process improvements, and financials.

To further optimize proposed steps leading to the desired / target maturity state, complementary controls may be grouped into single action item, improving implementation efficiency. Commonly, gaps in Governance-related controls within NIST CSF Function 1. GOVERN (GV) may be logically organized into one stream / improvement plan (e.g. "Governance"), controls within functions IDENTIFY (ID) and PROTECT (PR) into e.g. "Preventive" stream and functions DETECT (DE), RESPOND (RS) and RECOVER (RC) into e.g. "Incident management" improvement stream.

## 5. REASSESSMENT

Reassessment activities may be organized partially or fully, after a (pre)determined period. Partial reassessments are organized for specific areas of high interest, e.g. NIST CSF functions with the lowest maturity score or with most gaps labeled as priority or ones (e.g. areas with regulatory required elements). Due to the limited scope in partial reassessments, the number of team members may be scaled down, while other operational steps described within sections 3.5.–3.7. shall be followed as within initial assessment. Also, Project success factors evaluation: go / no-go criteria (section 3.3.) and Cyber threats identification and assessment (section 3.4.) may be repeated if there is need for the updates.

Full reassessment may be executed as a new project, by following the entire process. This may be the case primarily if the following circumstances are met: 1) there is a new version of the NIST CSF framework available, with significant changes introduced or 2) there are major changes in organization structure, technology and/or processes.

## 6. CONCLUSION

Control Self-Assessment can be a valuable methodology in the process of alignment with NIST Cyber Security Framework. CSA can be organized as a project, with defined phases, roles and responsibilities. To improve project success, careful planning of team members selection is necessary. Also, Project success factors evaluation phase may identify risks in an early project phase, reducing potential for project failure. These two key elements maximize collection of valuable and truthful information, which improves the quality of the final report. Consequently, gaps and strengths identified may be used as a solid foundation for information security improvement program. Further research may be in the area of maturity model processes and prioritizing identified risks with maturing overall information security program.

## REFERENCES

[1] https://www.iso.org/certification.html, Accessed on 27.04.2025
[2] The NIST Cybersecurity Framework (CSF) 2.0 Abstract, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf, Accessed on 18.04.2025
[3] CMMI Levels of Capability and Performance, CMMI Institute, https://cmmiinstitute.com/learning/appraisals/levels, Accessed on 18.04.2025
[4] CMMI Appraisal, CMMI Institute, https://cmmiinstitute.com/learning/appraisals, Accessed on 18.04.2025
[5] NIST Glossary, Cyber Threat, https://csrc.nist.gov/glossary/term/cyber_threat, Accessed on 06.04.2025
[6] The IIA Standard "2060 – Reporting to Senior Management and the Board", https://www.theiia.org/en/content/guidance/recommended/implementation/2060-reporting-to-senior-management-and-the-board/, Accessed on 14.04.2025

# CYBER SECURITY SUPPORT FOR FINANCIAL FORENSICS

Goran Lazarov, Higher Colleges of Technology, Dubai, United Arab Emirates

***Abstract:*** *This paper aims to present methods of digital support to fraud prevention and detection processes as well as preservation of the obtained findings. In practice, several different methods, procedures and tools have been developed that provide effective support to financial forensics in order to detect financial fraud. The methods are mainly based on individual and mutually separate procedures that are brought together in the process of analyzing the obtained individual results. This paper proposes a method of automatic processing of the obtained data using cyber security mechanisms based on the concepts of artificial intelligence and machine learning, which can give final conclusions with significant precision. The use of modern concepts of artificial intelligence enables continuous improvement of the quality of performed forensic analyzes.*

***Keywords:*** *cyber security, artificial intelligence, forensics.*

## 1. INTRODUCTION

Criminal activity and forensic accounting have existed as a term since ancient times, but as a science, forensic accounting is considered to be a young science. People who deal with criminal acts are called auditors of criminal acts, and persons who deal with them forensic accounting is called forensic accounting. To become an auditor and the accountant of these activities requires certain skills and knowledge, which go beyond skills external auditor.
Criminal acts of employees are very widespread and are considered criminal the actions of employees are much higher than those of street criminal activities. It is possible through history see that there have been a large number of frauds and manipulations in the economy, which have occurred many times repeated, and that forensic accountants, in the West, make good money from property valuations during divorce, etc. Forensic accounting is a powerful tool for detecting fraud and fraud, however, forensic accountants must know to use this tool on the right the way.

Forensic accounting is the application of research and analytical skills with the aim of resolving financial issues in a manner consistent with the standards they require courts. It is important to note that forensic accounting is not limited to enforcement financial investigations that result in prosecution; however, if it is the purpose, investigation and analysis must meet the standards required by the competent court. And in order to realized the role of forensic accounting, it is necessary to determine what are the techniques and tools for fraud detection, such as Data Mining; Benford's law; Analytical techniques; Forensic analysis of the reality of revalued tangible fixed assets and possible manipulations;

Cyber security methods act, first of all, preventively in the sense of preventing the misuse of financial data, and then as a guarantor of the security of created data. Cyber security is based on the principle of CIA - Confidentiality, Integrity, and Availability, which, if properly implemented, ensure the inviolability of data. In addition, one-way hash functions are used to ensure that the data we observe is completely identical to the data obtained from the source. An additional element is the digital signature using a digital certificate that fully and unambiguously declares the author of the digital document or the person who made changes to the document, whether it was authorized or unauthorized.

Proposed model for estimating the possible pillar of manipulation in financial statements use cybersecurity elements and relationship analysis in forensic assessments.

## 2. METHODS OF COLLECTING EVIDENCE IN FINANCIAL INVESTIGATIONS

Evidence and leads to evidence are often gained through observation. There are several means of observation used in all types of investigations. The investigator must keep in mind the rules that apply to the recordings audio and visual observations in gathering this type of evidence. Special attention should be paid to the evidence contained in the information system, whether it is software or hardware. Evidence that is not visible at first glance is the data contained in the log files which record all activities performed in the information system [1].

Investigative observation can be viewed as going from informal to formal. Being alert and observant is a necessary

skill for any type of investigation, and it is crucial in the criminal investigation of financial and business activities. Informal observations are made throughout the course of the investigation [2]. The attitude and demeanor of witnesses, the reaction to specific questions or areas of questioning, and the nature of the relationship with the subject expressed during an interview provide the investigator with potential tips for the litigation aspect to come and potential leads to additional evidence.

The best-known method of surveillance is to physically follow and observe the subject while remaining undetected. This tool can be applied at the beginning of an investigation to establish the subject's routines and associates. Surveillance is more commonly used after the investigator has had the opportunity to identify and understand the criminal enterprise or scheme involved. It requires considerable application of investigative time and resources. In discussing surveillance techniques, it is helpful to understand the meaning of a few terms used in executing the surveillance. The "eyeball" is the initial observation point from which the surveilling officer alerts the rest of the team as to the start of movement or activity by the subject. The "base" or "command post" is usually the station or office from which the surveillance is being conducted. In situations where the surveillance is too remote from this location, a temporary base will be established. The base monitors the surveillance activity and can be called upon for assistance in case of an emergency, or for advice if the subject acts in a manner that was completely unanticipated. The "lead" is the officer in closest proximity to the subject. To avoid suspicion on the part of the subject, officers will frequently rotate the lead position. "Cover" is a term used to identify obstructions of the view that the subject has of the surveillance vehicle or officer [3].

The use of electronic monitoring or eavesdropping devices is strictly regulated by law and the regulations of departments and agencies in the interpretation and application of those laws. The U.S. Supreme Court has established the individual's "right to privacy," and legal precedents are used to determine the appropriate use of electronic equipment to gather evidence. There is a wide range of equipment available. Each piece of equipment is designed for a rather specific use. When contemplating this type of monitoring, the officer or agent should be able to clearly articulate the circumstances that will be involved in the monitoring, the length and scope of the monitoring, and why this type of monitoring would be the only or most efficient way to obtain the evidence needed.

To begin we must understand the motivation for criminal behavior. Criminologists have struggled to find the common ground in the motivations to violate statutory rules. White collar crime, first coined by Edwin Sutherland, is a financial crime. It may involve violence and physical harm to the victims, but the root cause is greed and a lust for financial gain. Sutherland and others have strived to provide a much more specific definition to distinguish this type of crime from the myriad of "street crimes" and narrow the scope of reasons that perpetrators have for the commission of such crimes. For our purposes, it is sufficient to know that most crimes are committed for financial gain. The street mugger and the corporate executive have that much in common [4]. The major differences are in the amount of gain, the planning required, the intricacies of the crime, and the tools needed to commit the crime.

## 4. DIGITAL FORENSIC INVESTIGATION MODEL

Computer forensics emerged in response to the escalation of crimes committed by the use of computer systems either as an object of crime, an instrument used to commit a crime or a repository of evidence related to a crime. Computer forensics can be traced back to as early as 1984 when the FBI laboratory and other law enforcement agencies begun developing programs to examine computer evidence. Research groups like the Computer Analysis and Response Team (CART), the Scientific Working Group on Digital Evidence (SWGDE), the Technical Working Group on Digital Evidence (TWGDE), and the National Institute of Justice (NIJ) have since been formed in order to discuss the computer forensic science as a discipline including the need for a standardized approach to examinations [5].

Digital forensics has been defined as the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate the unauthorized actions shown to be disruptive to planned operations. One important element of digital forensics is the credibility of the digital evidence. Digital evidence includes computer evidence, digital audio, digital video, cell phones, digital fax machines etc. The legal settings desire evidence to have integrity, authenticity, reproductively, non-interference and minimization [6].

The General digital forensics model proposes a standardized digital forensics process that consists of nine components:

1. **Identification**: which recognizes an incident from indicators and determines its type.

2. **Preparation**: which entails the preparation of tools, techniques, search warrants, and monitoring authorizations and management support. Approach strategy: that develops a procedure to use in order to maximize the collection of untainted evidence while minimizing the impact to the victim.

4. **Preservation**: which involves the isolation, securing and preservation of the state of physical and digital evidence.

5. **Collection**: that entails the recording of the physical scene and duplicate digital evidence using standardized and accepted procedures.

6. **Examination**: which involves an in-depth systematic search of evidence relating to the suspected crime.

7. **Analysis**: which involves determination of the significance, reconstructing fragments of data and drawing conclusions based on evidence found.

8. **Presentation**: that involves the summary and explanation of conclusions.

9. **Returning evidence**: that ensures physical and digital property is returned to proper owner.

A described model, slightly modified is presented in following diagram:

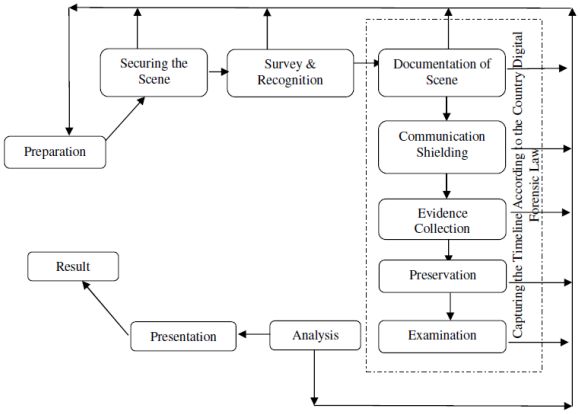



*Figure 1: Phases of Systematic Digital Forensic Investigation Model (SRDFIM)*

There has been a need for a standard methodology used for all Digital Forensics investigations. There have been many initiatives made to have models that have a general process to be followed for such investigations. Research done by the scientific community has been fairly recent, and has concentrated mostly upon coming up with good models that can be practiced. Yet, it can be safely said that these models are mainly ad-hoc and much needs to be accomplished in this particular domain.

## 4. THE ROLE OF CYBERSECURITY THREATS IN DIGITAL FORENSIC

With the advancement of technology, nowadays, cybersecurity has become very challenging. It's common for hackers, attackers, and scammers to take advantage of emergencies, particularly if they can make a financial profit. Bad actors around the world are using the computer system weakness as a new tool for their evil deeds in the form of hacking, attacking, or scams.

Most of the government and companies have seen a rapid increase in the Distributed Denial of Services (DDoS) attack where the hackers flood the organizations' websites or systems with fake or bot users to crash the normal functioning of the system and thus interrupt the communication channel.

The attackers created a wide number of registered domains on the internet recently, and daily more and more increase has been witnessed. Although some are legitimate web sites, cybercriminals build thousands of new sites every day in which spam campaigns, phishing, malware spreading, or servers are compromised. There has been an increase in websites that claim to be applications that are supposed to support business or privacy protection, but actually the URLs contains malicious scripts designed to perform predefined attacks on the system [7].

Cybercriminals are launching ransomware attacks in various companies including hospitals, health centers, education, and public institutions. Ransomware virus lock all the user's data so the users can't access it. The attackers blackmailed the company asking for money in order to send the key and algorithm so the attacked system could be unlocked and recovered. Since they can't afford to be locked out of their systems because of the current situation, criminals are optimistic that these organizations can pay the ransom. The ransomware infects the system via email attachments, links, or through working employees whose credentials are already compromised by exploiting a vulnerability in their systems. Cybercriminals are now even offering ransomware-as-a-service on the dark web.

Spam emails have always been used on a very large scale by the scammers and hackers to achieve their intended purposes. Usually, attackers sending emails with malicious attachments on a very large scale sent to users promising them easy financial gain if they click on the offered link or open an attachment. After the click, it usually happens that the victim is robbed either in the sense of taking personal data, and most often in the sense of taking financial means [8].

Nowadays, social media is very common and is almost in the reach of every individual. Hackers find it a great opportunity and tend towards the various social media platforms such as Facebook and WhatsApp. There have been numerous cases in which scams and phishing tactics are circulating on Facebook Messenger and many other such applications. The scams typically lure victims into free subscriptions such as Netflix premium free account. When the victim clicks on the link, it redirects them to their social media phishing website. In some cases, it may ask to enter the credentials of their accounts. This way, they either capture their credentials or install malware into their systems, mobile devices, and web browsers to steal information and cookies, and thus, the user becomes a victim.

Business email compromise attack as the intruders is performed by the cybercrime organization or sometimes by individuals. This attack is believed to be a series of the previous attacks the group launched earlier. The attackers first target the bank accounts. Then they use the information of the customers and send them emails to change their bank information and payment methods. The attackers pretend to be from legit organizations or businesses. The scam works by convincing or tricking the targets into making transactions to an intruder who shows

him/herself as a legit employee working in the same company.

In this modern era of ubiquitous computing, smartphone users are at their peak. Life without smartphones and gadgets has become impossible, and the use is increasing on a daily basis. At the same time, it's a great opportunity for bad actors to take advantage of it. A different application which seems regular can contain malicious software which could do a lot of damage to the victim. Android phones are particularly vulnerable, so the attacker could take a full control over the phone and moreover the victim will know nothing about that. So, the full communication can be intercepted, stored and fabricated the false communications. Threats include the deletion of the phone data and the leakage of the account information in social media in another case, an android app which is offering face mask and safety kits to the worried individuals. Once an individual installs the application, this app delivers a SMS Trojan, which collects the contact list of the victim phone directory and sends auto SMS to spread itself [9].

The data-sharing company by technology is playing their role to help different governments and their officials to keep the privacy experts on edge. Tech Giants such as Apple, Google, and Facebook are already collecting masses of data to use it for advertising purposes. Now, some of them are providing personal data such as location and other personal information to authorities, government agencies, and even to researchers. This could be helpful to overcome the situation, but at the same time, it is putting public privacy on stake, and there is fear that this data can be used for illegal purposes. Recently, many sectors, such as industries, education, have shifted online. Employees around the world are using online communication and conferencing tools and software to continue working from their homes. To sign up for the applications, the consumers have to agree to some terms and conditions, which include their privacy and security data collection. A recent consumer report analyzed the privacy policies of these applications such as Google Meet, Microsoft Team, and Zoom and concluded that they are collecting more data than people realize, which alarming [10].

Cyber risks in the financial sector are growing rapidly over time. Although operational risks were the dominant risks for fraudulent activities, cyber risks catch up with them and often surpass them. This fact imposes on us the need to examine in detail during each forensic examination the cyber risks that are a very probable way of committing a criminal act. The growth of cyber risk can be seen in the following figure:

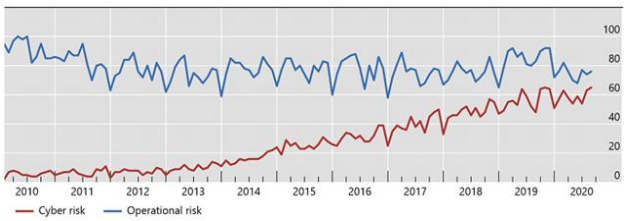



*Figure 2: Cyber risks vs Operational risks*

As the world is advancing and the use of ubiquitous computing is increasing daily, with the same ratio, there's an increase in cybersecurity threats and privacy issues as well. With the recent outbreak of the coronavirus pandemic, there has been a huge increase in the number of users interacting with each other working online. Taking advantage of the situation, the bad actors became more active to hack and attack different platforms for some financial gains and other interests. There has been a considerable increase in the registration of malicious domains, websites, and spam emails. The intruders are targeting individuals, government officials, and even medical and healthcare systems.

## 5. CYBER SECURITY AND ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI) is increasingly being incorporated into business processes and systems. But not all industries are equally sophisticated: the IT and telecommunications industry are the most sophisticated sector for AI adoption while cars fall short of their rates. According to a recent worldwide study, which surveyed over 4500 policy-makers across various industries, 45% of big enterprises, and 29% of small and medium-sized enterprises reported AI use. AI will be becoming more essential to handle cyber-threats in the area of cybersecurity: fact, the market is projected to expand. At the same time, the use of AI is not without dangers: over 60 percent of AI businesses recognize that AI creates the most significant cybersecurity concerns. AI, being a general-purpose, dual-purpose technology, has the potential to be both a boon and a bane for cybersecurity. The fact that AI is employed as a sword as well as a shield confirms this. With an added twist: because the use of AI for national security purposes experiences many limitations, particularly as government agencies (and the European Union) keep moving to monitor and control high-risk applications and encourage greater AI use, on the attack side, the most malicious applications keep increasing, the cost of new applications falls, and the 'threat landscape' becomes denser with each passing day [11].

Cybercriminals leave a digital trace when they try to gain access to internal systems, and this is known as intrusion signatures. Security experts build huge digital footprint datasets to help identify flaws and attackers' particular habits for future references. An artificial intelligence system may be taught to detect intrusions in real-time if a big enough library of fingerprints and infiltration patterns is available. One of the best ways of exploitation, for instance, is through entering electronic devices – recording devices, computers as well as other internet-linked equipment. The cybercriminals get access to these systems by utilizing the default login details. Many businesses do not bother changing the administrators' passwords on 'mundane' equipment. Through the compromise of these computers, the cybercriminals can get access to the remainder of the network. AI encryption is capable of

scanning the whole network for such vulnerabilities, thus averting the majority of typical types of assaults. The fact is that artificial intelligence is just a tool; humans must still intervene to educate AI and intervene if AI makes a mistake.
The use of artificial intelligence (AI) is already being used to, or is being actively explored for, some of the following areas in cybersecurity solutions:

• To identify and prevent undesirable spam and fraudulent emails, Gmail makes use of artificial intelligence (AI). Gmail's artificial intelligence was taught by the millions of current Gmail users - every time users click an email message or not spam, you are assisting in training the AI to detect spam in the future. As a result, artificial intelligence has progressed to the point where it can identify even the most subtle spam emails that attempt to pass unnoticed as “frequent” emails.

• Fraud detection: An artificial intelligence-based fraud detection system that employs algorithms based on expected consumer habits to identify fraudulent transactions through MasterCard deployed Decision

Intelligence. It examines the customer's normal purchasing patterns, the seller, the location of the transaction, and many other complex algorithms to determine if a purchase is unusual.

• Botnet Detection: A very complicated area, botnet detection is usually based on pattern recognition and timing analysis of proxy servers. Since botnets are usually managed by a master script of instructions, a wide-scale botnet assault will usually include a large number of "users" all making the identical queries on a site in a single attack. This may include unsuccessful login attempts (a botnet brute force password attack), networks vulnerability scans, and other breaches. It is very difficult to explain the incredibly complicated function that artificial intelligence plays in botnet identification in just a few words, but here is a fantastic study article on the subject that does a great job.

These are just a handful of the areas in which artificial intelligence has been used for cybersecurity. There are currently a large number of research articles that provide compelling data in support of artificial intelligence's effectiveness in the field of cybersecurity. According to the majority of study studies, the success rate for identifying cyber assaults is between 85 and 99 percent. One artificial intelligence development firm, Dark Trace, claims to have a 99 percent success rate and already has thousands of clients across the world [12].

Artificial intelligence is quickly becoming a must-have tool for improving the effectiveness of information security teams. Humans are no longer capable of adequately securing an enterprise-level attack surface, and artificial intelligence provides the much-needed analysis and threat detection that can be utilized by security professionals to reduce the chance of a breach and improve their organization's security posture. As more technology is incorporated into our daily lives, the effect of artificial intelligence on our lives will continue to increase. Some experts think that artificial intelligence will have a detrimental impact on technology, while others believe that AI will have a significant positive impact on our lives. The primary advantages of cloud computing in cybersecurity are the ability to analyze and mitigate threats more quickly. The capacity of hackers to launch increasingly sophisticated cyber and technology-based assaults is a major source of concern for many people. Furthermore, artificial intelligence may assist in the discovery and prioritization of risks, the direction of incident response, and the identification of malware assaults before they occur. As a result, even with the possible drawbacks, artificial intelligence will aid to advance cybersecurity and assist businesses in developing a stronger security posture.

## 6. CONCLUSIONS

This paper stemmed from the need to define the connection in a clear and transparent way practical steps between information systems protection and anti-digital forensics, as well as notice their weaknesses and change the perception of all users of information technology, and with the aim of improving the quality of protection of information systems and uninterrupted business process. What is certain is that the scope and frequency of cybercrime will be on the rise, because it is increases the number of computers, automation of business activities and processes, computer integration network, as well as lowering the threshold of knowledge and skills required for the application of ICT and the spread of computer literacy, which is already becoming a major determinant of the times in which we live. Successful companies, regardless of structure and size, at a time when digital data and information is crucial for success and survival in the market, they must conduct education their cadres, because they cannot fight anti-forensics with ignorance and unwillingness. Not one should be deceived, that if they have not had problems with the criminogenic outcome so far, they will not to be. The question here is not whether it will, but when it will!? Today's work cannot be expected to be done well and with quality, with yesterday's knowledge, and to be welcomed tomorrow.
With the development of new digital technologies, financial forensics is becoming inextricably linked with digital forensics. Bearing in mind that cyber threats are on the rise and that they significantly contribute to the commission of criminal acts in the financial sphere, it is necessary to notice the connection between cyber security and the detection of financial crimes. Cyber security methods are closely related to Artificial Intelligence, which is used both for cyber-attacks and for the defense of information systems.

It is necessary to apply a multidisciplinary approach to financial forensics in order to detect increasingly sophisticated methods of fraud and abuse. In the proposed way, by using all the mentioned scientific disciplines, methods and techniques, maximum results in the field of financial forensics can be achieved.

**REFERENCES**

[1] Linda Bressler, Forensic investigation: the importance of accounting information systems, International Journal of Business, Accounting and Finance (Vol. 5, Issue 1), 2011

[2] Jeff C. Bryan, Financial Investigation and Forensic Accounting, Taylor & Francis Group, 2010

[3] BruceNikkel, Fintech forensics: Criminal investigation and digital evidence in financial technologies, Forensic Science International: Digital Investigation, 2020

[4] James A. Digabriele, An Empirical Investigation of the Relevant Skills of Forensic Accountants, Journal of Education for Business, Volume 83, 2008 - Issue 6, 2010

[5] Kwaku Kyei, Pavol Zavarsky, Dale Lindskog & Ron Ruhl, A Review and Comparative Study of Digital Forensic Investigation Models, ICDF2C 2012: Digital Forensics and Cyber Crime pp 314–327, 2012

[6] Mark Scanlon, Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service, Cornell University, 2017

[7] Reza Montasari; Richard Hill, Next-Generation Digital Forensics: Challenges and Future Paradigms, IEEE International Conference on Global Security, Safety and Sustainability (ICGS3), 2019

[8] D. Paul Joseph & Jasmine Norman, An Analysis of Digital Forensics in Cyber Security, First International Conference on Artificial Intelligence and Cognitive Computing pp 701–708, 2018

[9] Thomas, J. E., Galligher, R. P., Thomas, M. L., & Gallilgher, G. C., Enterprise Cybersecurity: Investigating and Detecting Ransomware Infections Using Digital Forensic Techniques, Computer and Information Science; Vol. 12, No. 3; 2019

[10] William Bradley Glisson, George Grispos, Kim-Kwang Raymond Cho, Cybersecurity Investigations and Digital Forensics: Mini-track Overview, Proceedings of the 53rd Hawaii International Conference on System Sciences. 2020

[11] Jian-hua Li, Cyber security meets artificial intelligence: a survey, Frontiers of Information Technology & Electronic Engineering volume 19, pages1462–1474, 2018

[12] Zhimin Zhang, Huansheng Ning, Feifei Shi, Fadi Farha, Yang Xu, Jiabo Xu, Fan Zhang & Kim-Kwang Raymond Choo, Artificial intelligence in cyber security: research advances, challenges, and opportunities, Artificial Intelligence Review volume 55, pages1029–1053, 2022

# INFORMATION SYSTEM PROTECTION, CONTAINERS, PHYSICAL AND IT PROTECTION

Vladimir Djokić, PhD candidate at the Pan-European University APEIRON, Banja Luka,RS,BIH
vladimirdjokic001@gmail.com
Dragana Djokić, University of „Union-Nikola Tesla“ Belgrade,Srbija, draganadjokic74@gmail.com
Zoran Avramović, University of Belgrade, Belgrade, Serbia
Željko Stanković. University of „Union-Nikola Tesla“ Belgrade,Srbija

**Abstract:** *Application container technologies, also known as containers, are a form of operating system virtualization combined with application software packaging. Modern container technologies have largely emerged alongside the adoption of development and operations practices that seek to increase integration between building and running applications, emphasizing close coordination between development and operations teams. Physical computer security is the protection of personnel, hardware, software, networks, and data from physical attacks and events that can cause serious loss or damage to a business, agency, or institution.*

**Keywords:** *Protection of information systems, containers, physical protection, it protection, alarms and video surveillance.*

## 1. INTRODUCTION

The security of information systems is crucial in the digital age. Cryptography as a field includes encryption with symmetric and asymmetric algorithms, one-way functions, and various digital certificates for digital signing and encryption [1]. Regarding encryption, it is essential to emphasize that this part of cryptography is viewed from the perspective of perfect and imperfect ciphers. The research problem is to explore the security of information systems, which is crucial in the digital age, using available literature.

The aim of the research is to describe the advantages of application container technology, known as containers, which represent a form of operating system virtualization combined with application software packaging, and to explore physical and IT protection and their advantages and disadvantages.

The solution is to investigate which measures and how to apply the combination of physical, IT, and protection using application containers to create a network of secure data despite the increasingly frequent attacks on information systems occurring in the present time.

## 2. ISO STANDARDS

A list of standards related to the issue of information system protection and security that have already been adopted or are planned for the upcoming period includes:
• ISO 27000 – Vocabulary of terms used within the ISO 27000 series of standards;
• ISO 27001 – Information Security Management System (ISMS);
• ISO 27002:2007 – Code of practice for information security management;
• ISO 27003 – Implementation guide for ISMS;
• ISO 27004 – Measurement and metrics of the effectiveness of the information security system;
• ISO 27005 – Information security risk management (based on BS 7799-3);
• ISO 27006:2007 – Requirements for the process of analyzing and certifying standards;
• ISO 27007 – Guidelines for auditing ISMS;
• ISO 27011 – Guidelines for establishing ISMS in the telecommunications sector;
• ISO 27031 – Specifications for ICT readiness for business continuity;
• ISO 27032 – Guidelines for cybersecurity [2].

## 3. APPLICATION CONTAINERS

Operating system (OS) virtualization provides a separate virtualized instance of the OS for each application, thereby isolating each application from all others on the server. Recently, OS virtualization has become increasingly popular due to advancements in ease of use and a greater focus on developer agility as a key advantage. Today's OS virtualization technologies are primarily focused on providing a portable, reusable, and automated way to package and run applications. The terms application

container or simply container are often used to refer to these technologies [3].

In this chapter, we will explain the security issues associated with container technologies and provide practical recommendations for addressing these issues during the planning, implementation, and maintenance of containers.

### 3.1. Containers and the Operating System

Explaining the deployment of applications in containers is facilitated by comparing it to deploying applications within virtual machines (VMs) from hardware virtualization technologies. Figure 1 shows VM deployment on the left, container deployment without VMs in the middle, and container deployment running inside VMs [4].

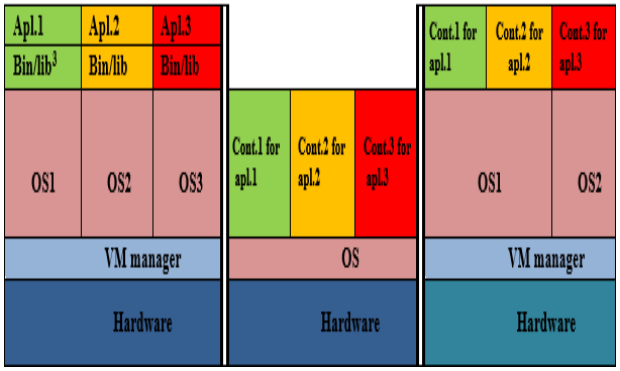



Figure 1. Deployments of Virtual Machines and Containers.

### 3.2. Container Usage

Application containers offer great potential, but that doesn't necessarily mean they are the best choice for every scenario. If an organization with a large base of outdated standard software wants to leverage container benefits, they may not be able to run most of that software because vendors do not support those outdated versions... However, most organizations will find multiple significant uses for containers.

With container technologies, the build system installs an application within the context of an image it creates (i.e., at compile time). The image is an immutable snapshot of all application user space requirements (i.e., runtime language, third-party libraries, scripts, and OS tools). In production, the container image constructed by the build system is simply downloaded and run.

Modern container technologies often emphasize reuse, so a container image created by one developer can easily be shared and reused by others, both within the same organization and across different organizations. Registry services provide centralized sharing of images and discovery services to facilitate developers in finding and reusing software created by others. This ease of use also encourages many popular software vendors and projects to adopt containers as a way to help users find and quickly deploy their software.

### 3.3. Major Risks for Core Components of Container Technologies

In this chapter, we will briefly discuss the major risks associated with the core components of container technologies - images, registries, orchestrators, containers, and host operating systems. Since the analysis focuses solely on these core components, it is applicable to most container use cases regardless of container technology, host OS platform, or location.

Two types of risks are considered:
1. Compromise of image or container: The primary "assets" to protect are images and containers, which can contain application files, data files, etc. Secondary assets for protection include container data within shared host resources such as memory, storage, and network interfaces.
2. Abuse of containers for attacking other containers, host operating systems, other hosts, etc.

We can divide all risks into several groups and see them in the following breakdown:

a) Image Risks:
- Image vulnerabilities,
- Image configuration defects,
- Embedded malware,
- Embedded plaintext secrets,
- Use of unreliable images.

b) Registry Risks:
- Insecure connections to registries,
- Outdated images in registries,
- Insufficient authentication and authorization constraints,

c) Orchestrator Risks:
- Unrestricted administrative access,
- Unauthorized access,
- Poorly segregated network traffic between containers,
- Mixing sensitivity levels of workloads,
- Trust issues.

d) Host OS Risks:
- Runtime software vulnerabilities,
- Unrestricted network access from containers,
- Insecure runtime container configurations,

- Application vulnerabilities,

e) OS host risks:

- Large attack surface,
- Shared kernel,
- Host OS component vulnerabilities,
- Improper user access rights,
- Unauthorized filesystem manipulation on the host OS [5].

In further work, we will address risks under item numbers d and e.

## 4. TECHNICAL PROTECTION

"By using technical means and devices for securing persons, property, and operations, services are provided through individual or functionally connected perimeter measures, devices, and systems for: anti-intrusion and anti-robbery protection, fire protection, video surveillance, access control, social alarms, vehicle satellite tracking (GPS), electrochemical protection of valuables, mechanical protection, and data protection."

Technical equipment and devices can be integrated into a system of technical protection.

Technical protection tasks are carried out using technical means and devices to prevent unlawful acts against persons, property, or operations, especially for protection against [6]:
1)unauthorized access to secured spaces and objects;
2)removal, theft, and unauthorized use of protected items;
3)introduction of weapons, explosives, radioactive, and other hazardous objects and materials;
4)break-ins, sabotage, and violent attacks on premises or theft of items;
5)unauthorized access to data and documentation;
6)protection of vehicles for transporting money and other means of transport;
7)other identified risks.

When performing security tasks for objects or spaces used for public purposes using video recording devices, legal entities and entrepreneurs providing private security services are obligated to prominently display a notice stating that the premises or area is under video surveillance. The service user must acknowledge this requirement and keep archived recordings for at least 30 days, making them available for inspection by authorized police officers upon request.

### 4.1. Alarm Systems

Alarm systems (also known as intrusion detection systems) detect and signal potential dangers or unwanted events, designed to detect unauthorized entry into residential/commercial premises or other areas. They can be simple or complex.

Alarm systems are widely used in residential, commercial, industrial, and military facilities for protection against burglary (theft) and personal security. Some types of alarm systems serve a single purpose, such as burglary protection, while there are also combined systems that provide protection against both fire and intrusion. Alarm systems are often integrated with video systems. Simple alarms aim to create a loud and unpleasant noise to deter intruders, while complex multi purpose alarm systems have computerized monitoring and control capabilities.

### 4.2. Video Surveillance Systems

Video surveillance is a technology that uses cameras to monitor and record events at specific locations. It is used for security, monitoring, and crime prevention. Modern cameras offer high resolution, night vision capability, and analytics for facial recognition or suspicious activity detection.

Video surveillance systems consist of various components that need to be integrated into a unified whole to function smoothly and monitor everything happening within the surveillance area. The most important part of a video surveillance system is undoubtedly the surveillance cameras, but they alone mean nothing if they are not connected to a recorder and do not have continuous electrical power supply. Cameras are connected to the recorder using coaxial or network cables. The recorder serves as the central part of the system responsible for displaying camera footage on a monitor and handling all system settings. All recorded material is stored on a hard disk located within the recorder for later playback. To enable access to the system via a mobile phone from anywhere, an internet connection is necessary. Like any system composed of multiple elements, video surveillance systems vary depending on the prevalent technologies.

Based on the types of technologies used, we distinguish the following types of video surveillance systems:
1)Analog Video Surveillance Systems
2)Analog HD Video Surveillance Systems
3)IP Network Video Surveillance Systems.

## 5. INFORMATION SYSTEM SECURITY

Security of information systems is crucial in the digital age. Cryptography as a field involves encryption using symmetric and asymmetric algorithms, one-way functions, and various digital certificates for digital signing and encryption. When it comes to encryption, it is important to emphasize the aspects of perfect and imperfect ciphers.
The Java programming language provides a range of cryptographic functionalities through the JCA (Java Cryptography Architecture) and JCE (Java Cryptography Extension). These two cryptographic libraries encompass all cryptographic functions [7].

Java Cryptography Architecture (JCA) represents a security framework integrated with the Java application core. It provides the following classes and functionalities:
- MessageDigest - hash values,
- Signature - digital signatures,
- KeyPairGenerator - key pair generation (PKI),
- KeyFactory i KeyStore – key management and storage,
- SecureRandom – cryptographic random source,
- AlgorithmParameters – managing all algorithm parameters,
- AlgorithmParameterGenerator – generating parameters for the requested algorithm,
- CertificateFactory – generating digital certificates,
- CertPathBuilder – establishing certificate chains,
- CertStore - managing digital certificates (issuance, revocation, verification, etc.);

Java Cryptography Extension (JCE) provides libraries for applying cryptographic functions in Java code. Specifically, JCE extends JCA by introducing additional classes and providers.

JCE provides the following classes and functionalities:
- Cipher- performs encryption or decryption operations,
- KeyGenerator- generates cryptographic keys,
- SecretKeyFactory- generates cryptographic keys,
- KeyAgreement – generates cryptographic keys,
- Mac– message authenticity.

We can say that JCA and JCE together constitute a complete cryptographic platform. However, there are various criticisms from developers. Some of these include the locations of cryptographic classes, whether they are placed in the java.security or javax.crypto packages. The classes of JCA extension reside in the java.security package, while the classes of JCE extension are located in the javax.crypto package. There are additional criticisms regarding class hierarchies as well. JCA adheres to strict patterns when it comes to abstract classes, which is not the case with JCE [8].

Security tips include:
1.Using protective software (antivirus, firewall).
2.Keeping your computer updated and using modern browsers.
3.Regularly backing up files.
4.Being cautious when disclosing personal information.
5.Encrypting wireless networks and guarding against fraud.

## 6. PHYSICAL SECURITY OF IS

Physical protection of individuals and property is primarily achieved through the presence and direct actions of security personnel within specific spaces and times. Physical security tasks can only be performed within a protected facility or up to the boundaries of the protected area. Meanwhile, tasks related to personal security (personal protection) can be conducted in public places and in close proximity to the individuals being protected, in accordance with the security plan [9].

The policy for physical security should define methods for protecting premises and equipment. This policy should address questions concerning physical access by employees and other individuals to spaces, offices, networks, etc. Depending on the value of the data, decisions are made about whether a company server should be in a standard locked office or if additional security measures are necessary. It is also important to precisely determine who has access to premises and under what circumstances. Once physical access issues are resolved, decisions are made regarding access to systems and data. This involves addressing issues related to user names and passwords, their storage and confidentiality, minimum password complexity, and their expiration dates. Access levels to data are also defined for different user groups, specifying who can read, modify, and input which data. Access passwords should not be too short, should not be tied to the user, and should include letters, numbers, and special characters. Naturally, passwords are kept confidential and are changed every few months [10].

Physical security of a computer system involves protecting personnel, hardware, software, networks, and data from physical attacks and events that could cause serious loss or damage to a company, agency, or institution. This includes protection against fires, floods, natural disasters, break-ins, theft, vandalism, and terrorism.

Things we need to do for physical protection of IT systems:
• Protect our computers with passwords,
• Always make backups of files,
• Use tracking software to recover stolen devices,
• Encrypt sensitive data, and
• Never leave devices unattended.

## 7. CONCLUSION

We can conclude that the security of information systems is crucial in the digital age. Cryptography as a field involves encryption with symmetric and asymmetric algorithms, hash functions, and various digital certificates for digital signing and encryption.

Unlike traditional application architectures that often divide an application into several tiers, each with its server or virtual machine, container architectures frequently split an application into many more components. Each application component operates within its own container. Modern container technologies have largely emerged alongside the adoption of development and operations practices that aim to enhance integration between application development and deployment, emphasizing close coordination between development and operational teams.

Video surveillance is a technology that uses cameras to monitor and record events at specific locations. Modern cameras feature high resolution, night vision capabilities, and analytics for face recognition or suspicious activity detection. Alarm systems are widely used in residential, commercial, industrial, and military facilities for intrusion (theft) protection and personal safety.

We can conclude that the physical security of computer systems involves protecting personnel, hardware, software, networks, and data from physical attacks and events that can cause significant loss or damage to enterprises, agencies, or institutions.

## REFERENCES

[1] S. Adamović, ,,*Information Systems Security"*, Singidunum University, Belgrade, 2015.
[2]. Available at: https://iso.org.rs/iso-27001/ Accessed: 03.02.2024.
[3]. Guide to Security for Full Virtualization Technologies. Special Publication (SP), ,,*National Institute of Standards and Technology (NIST)",* Gaithersburg, Maryland, 2011, pp. 800-125,
[4]. NIST Special Publication, ,,*Guide to General Server Security". National Institute of Standards and Technology*, Gaithersburg, Maryland, 2008, pp. 800-123.
[5].. *M. Souppaya, J. Morrelo, K. Scarfone, ,,Application Container Security Guide*", NIST Special Publication (SP), 2017, pp. 800-123.
[6]. R. S. Nikoll, W. R. Owens, ,,*Emergency Response & Business Continuity: The Next Generation in Planning*. Professional Safety, 2013.
[7]. Law on Private Security, ,,*Official Gazette of the Republic of Serbia",* No. 104/2013, 42/2015, and 87/2018.
[8]. Available at:
https://www.cisecurity.org/benchmark/docker Accessed: 01.02.2024.
[9]. Available at: https://www.paradox.com/ Accessed: 02.02.2024.
[10]. Available at:
http://www.webnstudy.com/tema.php?id=zastita-sistema
Accessed: 03.02.2024.

# RAISING THE LEVEL OF EMPLOYEE AWARENESS ON SECURITY ASPECTS OF USING COMPUTERS, THE INTERNET AND ONLINE COMMUNICATIONS

Saša Zečević, Business Registers Agency, szecevic@apr.gov.rs
Marija Vidrić, Business Registers Agency, mvidric@apr.gov.rs
Vladan Stevanović, Sirius online, vladan@onlinetest.rs

**Abstract:** *The introduction of the ISO 27001 information security standard and permanent employee training are key to raising employees' awareness of security risks in the cyber world.*

**Keywords:** *Online training, IT security, cyber security, research results.*

## 1. INTRODUCTION

The need for information security management has become not only a legal obligation, but also a question of the general long-term and stable functionality of any organization. The security, availability and integrity of information has never been so threatened. Bearing in mind the importance of the information it manages on a daily basis, as well as the need for continuous business improvement, the Business Registers Agency recognized the need to introduce the international standard ISO 27001, which provides the basis for the effective implementation of a holistic information security strategy, and thus introduced a well-structured information security management system (ISMS) through all 114 controls. In order for the ISMS to be effective, and therefore the information to be adequately protected, there must be a culture of understanding the value of information in the organization and its protection, which requires a visible commitment of the management, as well as the implementation of permanent training aimed at raising the awareness of all employees. Insufficiently aware and trained individuals are the weakest link and are a frequent target of attackers, who can threaten data security through them and cause great damage to information systems. A security awareness programme is the key to mitigating that human risk.

**The goal of the training** is to raise the level of awareness about the security aspects of using computers, the Internet, e-mail, social networks, as well as the protection of personal and business data from malicious attacks and unintentional errors by individuals in the business environment.

## 2. IT SECURITY interactive online training

### 2.1 The situation in Serbia at the start in 2022

- One attack every 30 seconds;
- A 24% increase in the number of attacks compared to the previous year;
- Attacks are increasingly sophisticated and complex;
- The number of attacks via e-mail has increased, where *Phishing* hides itself behind well-known companies and organizations (Post Office, banks, ...);
- *Ransomware* attacks are on the rise.

### 2.2 Training programme

The training programme is in accordance with the Law on Personal Data Protection of RS [2], the Law on Information Security of RS [3], GDPR (General Data Protection Regulation) [1] and is carried out according to the ECDL (European Computer Driving License) programme [4].


Image 1. E-learning

**Training programme:**

1) **Security concepts:** data threats, cybercrime, data protection, GDPR, personal security, social engineering [5], file security;
2) **Malicious programmes**: types and methods (viruses, worms, trojans, ransomware, DDoS,...), protection, resolution and removal;
3) **Network security:** types of networks and connections, *Firewall, Wireless security*;
4) **Access control:** methods and ways, password policy;
5) **Safe use of the Internet:** web browser settings, secure websites;
6) **Secure communications:** E-mail (digital signature, spam, phishing, identity theft), social networks [5], VoIP, IM, mobile communications;
7) **Data security management:** data backup (backup and restore), permanent deletion and destruction of data.

### 2.3 Training concept and e-learning platform

The online training was conducted on interactive simulations of the real environment, so that the participants were able to fully master certain practical procedures.

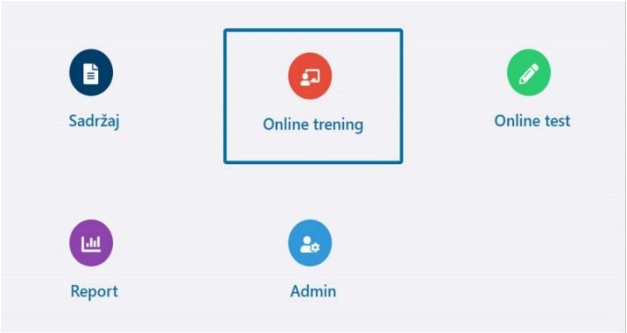



Image 2. E-learning platform

**Basic functionalities:**

- Production of online training courses,
- Textual, video, and interactive content,
- Exercises with interactive simulations of real situations and procedures,
- Self-assessment of acquired knowledge through passing quizzes and a final test,
- Monitoring participants' progress based on outcomes and test results,
- Organization of exam testing by sessions,
- Platform administration with multiple access levels,
- Clear and comprehensive reports.

The training contents are in text and video format, and complex procedures are presented as interactive exercises.


Image 3. Training concept

The training is personalized, with measurable results, so that the certificate is obtained based on the outcome, i.e. successfully completed tests. After each of the seven chapters, the participants had a control test, for independent verification of the acquired knowledge, and at the end a final test. Online training was available to participants for 60 days (24/7). The condition for obtaining a certificate is to solve all control and final tests with 70% and more points.

**Test concept**

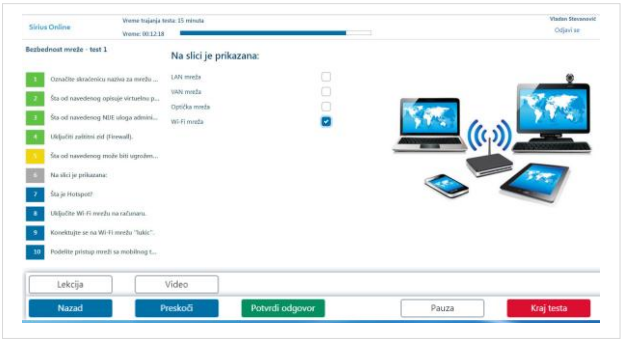



Image 4. Test concept

**Types of test questions:**

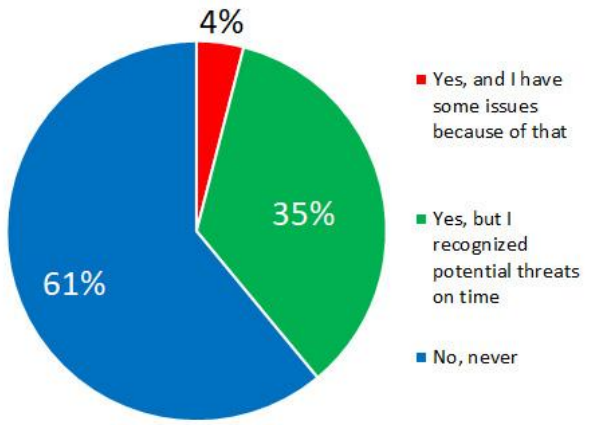
- Interactive tasks,
- Paperclip (answer linking),
- *Drag & Drop*,
- Correct / incorrect,
- Choosing one of multiple answers offered,
- Click on the image,
- A combination of the previous two,
- Entering an answer in the field.

For each successfully completed test, participants received appropriate badges.

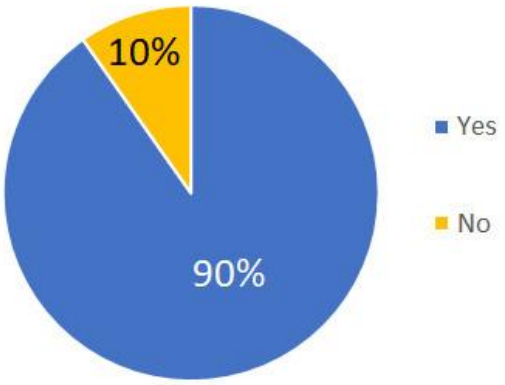
**3. RESEARCH RESULTS**

Following the online training, we conducted a survey on 123 participants of the online training, the results of which will be presented below.

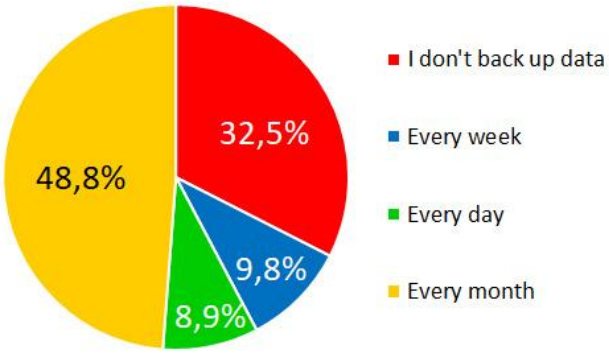
1) Have you been exposed to any type of cyber attack?



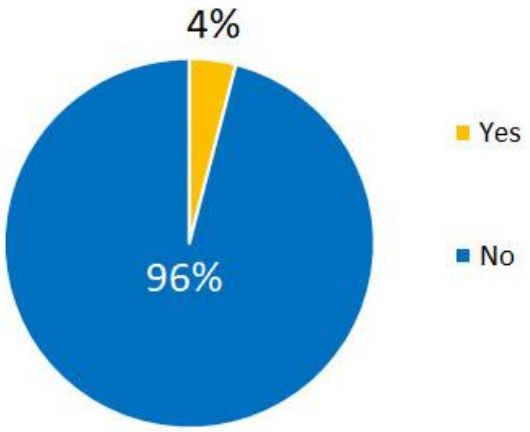

2) Do you regularly update the antivirus programme on your personal computer?



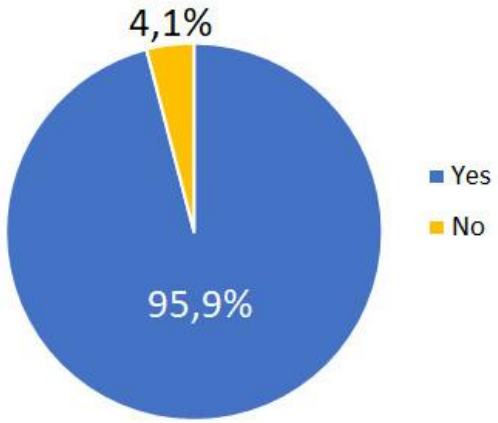

3) How often do you back up data on your personal computer?




4) Do you use a corporate email account to log in to online platforms or services that you access for private reasons?




5) Has the introduction of ISO 27001 and annual security awareness training changed the culture and increased cyber security awareness?




6) How would you rate the "IT security" online training programme in relation to your daily computer use?
100% of participants answered that it is optimal.

7) How you apply newly acquired knowledge?
The participants of the survey gave multiple answers, which refer to the following:
   - I pay more attention to security and protection of personal data*;*
   - I create strong passwords and change them regularly;
   - I turned off the memory of passwords in the *Web browser*;
   - I use passwords and encryption for important documents;

- I turned off macro commands and only turn them on when needed;
- I recognize *Phishing* and other malicious attacks;
- I only visit safe websites;
- I scan my computer with antivirus software and update it regularly;
- I regularly back-up data.

8) Would you like an area related to information security to be addressed specifically?
   - The impact of AI on information security;
   - Security on mobile phones with Android OS;
   - Social engineering and parental control;
   - Online payment with payment cards;
   - Data recovery and ethical hacking;
   - I think that more frequent training is needed, especially for those of us who are not computer professionals, and even if certain topics are repeated or treated in a different way, because it is very difficult to permanently adopt and apply knowledge after just one training on any topic.

## 4. CONCLUSION

Making information security awareness an integral part of the organization's culture ensures that security becomes a common value and a daily practice.

Cyber security awareness is an ongoing effort. By implementing ongoing training, organizations can foster a culture of cyber security awareness where employees are active participants in defending against cyber threats.

## REFERENCES

[1] EU Regulation 2016/679 of the European Parliament and of the Council – General Data Protection Regulation (GDPR),

[2] Personal Data Protection Act of the Republic of Serbia,

[3] Information Security Act of the Republic of Serbia,

[4] European Computer Driving License (ECDL) Programme,

[5] Cyber Psychology, Katarina Kacer.

# 4.

# IT in the COVID Crisis Time and Digital Health Technologies

# WEB 2.0 TECHNOLOGIES IN THE TIME OF COVID CRISIS FROM THE KNOWLEDGE MANAGEMENT PERSPECTIVE

Mladen Opačić, Singidunum University, mladja@mladja.com
Mladen Veinović, Singidunum University, mveniovic@singinunum.ac.rs

**Abstract:** *In this paper, we examine how these new circumstances have influenced the process of knowledge management and the role that Web 2.0 knowledge management systems should play in the world of the COVID-19 crisis.*

**Keywords:** *knowledge management, web 2.0, COVID crisis*

## 1. INTRODUCTION

The year 2020 will be remembered as the year of the COVID-19 pandemic crisis. Many companies, especially in the passenger transport, entertainment, tourism and hospitality sectors, are forced to shut down their businesses, laying off hundreds and sometimes thousands of employees. Whole industries are closed by governments to prevent further spreading of COVID-19 disease. Social distancing has become the new norm, together with the practice of working online from home. These circumstances lead to many new challenges and opportunities in managing knowledge and knowledge workers. Organizations were forced into unprecedented digital transformation. The digital transformation that could not be justified just a few months ago was now a new reality, and resources that proponents of digitalization could never get under normal circumstances were now allocated without question.

For example, before COVID-19 ability to work from home once or twice a week was considered a benefit of the job. Now things have changed, and many knowledge workers work from home without ever coming to work. Some organizations have started downsizing their office space since they no longer need it. It is obvious that this crisis will have a long-lasting effect on the way we do business in the coming years.

For this reason, in this paper, we examine how these new circumstances have influenced the process of knowledge management and the role that Web 2.0 knowledge management systems could or should play in the world of the COVID-19 crisis.

In the first part of the article, we examine core knowledge management concepts most affected by the COVID-19 crisis. In the second part of the article, we examine the concept of Web 2.0 in the context of knowledge management. Finally, in the last part, we review the use of the three of the most popular Web 2.0 knowledge management systems and how the current health crisis has influenced them in the last few months, and how it will influence them in the following year or maybe even years.

## 2. KNOWLEDGE MANAGEMENT CONCEPTS

Knowledge management is a relatively new multidisciplinary scientific discipline. Near the end of the 20th-century, knowledge workers began to be a dominant part of the workforce. So knowledge management as a discipline was created to find new methods to manage this new army of knowledge workers. Since most of the work has become knowledge work, the knowledge required to do the work has started to be considered an essential resource and last true source of competitive advantage. According to the knowledge-based theory of the firm [1] knowledge is regarded as the most critical resource in the organization, and it has an essential role in attaining and keeping a competitive advantage.

The knowledge management process is comprised of creating, storing, transferring, and applying knowledge[2]. One of the fundamental concepts in knowledge management is the concept of Ba [3]. Ba can be roughly defined [3] as a space where knowledge is created, stored, transferred, and applied. In normal circumstances, this Ba is located in the workplace where employees interact with each other. Pandemic completely changes this dynamic since workers are now forced to social distance and work from home. However, lack of face-to-face contact may present new opportunities for adoption of new work practices that were until now considered to be nice to have but not essential for organizations. One of the key unsolved problems in the field of knowledge management [4] has been linking the effects of investing in knowledge management with business outcomes. Implementing knowledge management strategies and knowledge information systems comes with significant costs for

organizations. Therefore, it is essential for knowledge management to [4] somehow quantify the contribution and effects of knowledge management practices on the firm's business strategy, intellectual capital, organizational learning, knowledge sharing, decision making, innovation performance, productivity, and finally, competitive advantage.

Knowledge management theory divides knowledge into two categories explicit and tacit [5]. Explicit knowledge is the knowledge that can be expressed with words and codified in books or audiovisual materials and then easily shared with other individuals. Tacit knowledge [5] is the knowledge that is not easily expressable; it is comprised out of subjective hunches, insights, and intuitions that are acquired with personal experience. According to [5] tacit knowledge has two dimensions, „know-how“ and the cognitive dimension. Where the „know-how“ dimension is technical knowledge, and the cognitive dimension is comprised of mental models and the world view that an individual has due to accumulated experience. It is not uncommon for organizations to hire new workers or even acquire whole other businesses just to get the hold of the tacit knowledge stored in the brains of the employees.

Communities of practice are another fundamental knowledge management concept changed by circumstances that we discuss in this paper. Articles in the knowledge management field frequently cite a popular definition from [6] which defines a community of practice as „a group of people who share a concern, a set of problems, or a passion about a topic, and who deepen their knowledge and expertise in this area by interacting on an ongoing basis.“. Communities of practice are considered an excellent method for sharing both explicit and tacit knowledge[7]. When employees leave the organization, their knowledge goes together with them. In some knowledge-intensive industries such as software development average time that an employee spends at a position is around two years. With COVID-19, whole industries have been forced to lay off many of their employees, which even further emphasizes having good knowledge processes to mitigate the risk of losing valuable competencies. Since it is not possible for employees physically to meet and share best practices solution is in virtual communities of practice. Virtual communities of practice are already widely used in some large multinational corporations [8] since meeting in person would require substantial travel costs. This effectively allows people from different parts of the world to be part of the same community. One of the advantages of virtual communities of practice is that every interaction between the members can be easily stored, searched, and analyzed.

## 3. CONCEPT OF WEB 2.0

Term Web 2.0 was first used in 2004 [9]. Since then, it has seen many changes and evolution of the original meaning. However, the base differentiating factors from Web 1.0 still remain. Web 1.0 was characterized by centralized applications where users were mere readers of the content that someone made for them. In Web 2.0, users make the content, and websites are just the platforms that facilitate their content creation. These websites harness the collective wisdom and knowledge of the crowd that uses them. So that now user-generated content becomes the main content of the website and the main reason why the users use it. On the technical side, websites are never considered finished, and the best of them constantly develop new capabilities based on the needs and the wants of the customers. User interfaces and user experience are further enhanced to the level that web experience no longer lags behind desktop application interfaces. Users also can use the same web application on multiple devices, including tablets and mobile phones. From the perspective of knowledge management, Web 2.0 systems are suitable for knowledge sharing because they are built to facilitate sharing among a group of people.

## 4. WEB 2.0 KNOWLEDGE MANAGEMENT SYSTEMS

As we previously mentioned, the main task of KMS is storing and transferring explicit knowledge between employees. Obviously, in ordinary situations, employees can gather and transfer knowledge in face-to-face meetings. This redundancy is also one reason why knowledge management and knowledge management systems have always had the problem to explain why organizations should invest significant time and money into information systems for knowledge management. COVID-19 crisis has forced organizations to move everything that they can online and reorganize so that maximum of employees can work from home remotely. Hopefully, the nature of this crisis is that it is temporary and that things will tend to get back to normal in the near future. In such situations, no organization wants to spend more resources than the bare minimum necessary to get by while the crisis lasts. Luckily Web 2.0 information systems are generally completely free or follow the freemium business model where base versions of the software are free. So even if, after the crisis organization decides that it no longer needs the system, there are no costly contracts and licensing schemes. Besides the initial costs, these systems are also very easy to use, so the costs of training are relatively small.

### 2.1 Wikis

Wikis are Web 2.0 information systems used to create, manage and store content. Unlike the classic content management systems in wikis, every user can create new content and edit existing articles [10]. On the Web, wikis are maintained by users who have system access [11]. In order for this to be possible, wikis are built to be easy to use so that everyone with basic computer literacy skills can easily post information to the website [12]. Due to their open character, wikis also have very developed administration and moderation subsystems designed to track every change made to each page. Changes can be easily reverted to the previous version if there is a problem. This functionality is built primarily to prevent vandalism on the websites like Wikipedia that are open to the public. In organizational settings, however, this can be used to track user contributions. The software that runs Wikipedia is called MediaWiki, and it is published under free software foundations GNU GPL license, which means that it is completely free to use and distribute. On its website, MediaWiki [13] is described as software that helps with the collection, organization, and dissemination of knowledge. It also has many readily available addons and extensions. For organizations that have specific requirements that MediaWiki cannot fulfill, there are specialized wikis such as for example semantic wikis that extend traditional wikis semantically so that they can be more machine-readable [14]. Organizations can use wikis for a number of purposes [15], including communicating with business partners and customers or communication and collaboration within the organization.
According to [15] these systems can be classified by scope into single-contributor, group or project, and company-wide wikis.

From the COVID-19 crisis point of view, wiki can be an interesting choice to use as a part of a knowledge management system initiative because of its low cost and easiness of use. Also, the initial investment is minimal and easily affordable by every organization. Wikis, however, require constant effort to keep all content up to date and relevant. With wikis, it is also important to take care of content categorization and navigation within the wiki website. This is even more emphasized if the organization maintains multiple wiki websites. When multiple users work on every page, a relatively unique problem can occur, and that is that certain content becomes unreachable since all links to it were removed. For these reasons, it is recommended to have clear guidelines on how to deal with these issues.

### 2.2 Blogs

Word blog is short of „Weblog“ and generally signifies a personal diary of a person on the Internet. Usually, a blog has a specific topic that it covers, for example, a fashion blog or a travel blog. In organizational settings, a blog can be [16] employee blog, group blog, management blog, promotional blog, or news blog. The main characteristics that differentiate blogs from other content management systems [17] are continuity of writing and great reliability of the information because people generally write about topics that they are knowledgeable about. Blogs are also built to be easily searchable and linkable. Ability to link directly to a specific article greatly simplifies the process of sharing content that is codified in the blog. Another feature that all blogs have is blog visitor's ability to leave comments about the article that they have just read. This allows visitors to interact with the blogger and exchange messages about the article. Sometimes comments and discussions on the blog are more valuable for visitors than the text of the article. Blogs are not only textual; they can also contain audio-visual contents and links to other valuable resources. Vlog (short from video log) is a form of a blog where instead of writing an article blogger records a video and then posts it on the platform. They do not have to be long Twitter, for example, is a microblogging platform where users can publish and exchange short status messages. These messages are called tweets, and posting messages is called tweeting. The characteristics of a blog that it usually is public comes with great responsibility. This is important to have in mind when publishing content, especially if it is a public relations or managerial blog. The best example of this is the Twitter account of the current president of the United States, where his every tweet can have serious consequences.

From the knowledge management point of view, blogs can be used by subject matter experts to blog about topics that they think are interesting and also document what is happening in the organization. Blogs can be used by employees to identify subject matter experts and to get in contact with them. In the times of the COVID-19 crisis, when people are forced to social distance, blogs can be used to inform the other parts of the organization about what and how they are doing. This is to avoid forming the information silos and then consequently spending valuable organizational resources on reinventing the wheel. However, this technology has to be used responsibly to avoid information leaks and information overload. It is not uncommon for people to ignore these systems if they get overwhelmed with communication intensity.

### 2.3 Enterprise social networks

Term social network was first introduced by Barnes in 1954 [18] . At the beginning [18], social networks were researched in social sciences such as sociology and psychology. With the development of computer science and the Internet, the first computer systems for creating and maintaining social networks were created. The first widely popular social networks Myspace and Friendster, were created at the beginning of the 21st century. These systems allowed users to contact each other, maintain those contacts and share content with others users. After few years of market battles, Facebook emerged as a winner in the competition of general-purpose social networks and is now one of the world's biggest companies. Soon people realized the need and started creating specialized social networks for various social categories. Linkedin, a social network for professionals, was built for maintaining a network of professional contacts. It is an excellent example of a public social network specialized for a specific purpose. This brings us to enterprise social networks that were created to help employees create and maintain contacts within an organization. For many large international organizations managing employees in geographically distant locations [19] is one of the biggest challenges. Enterprise social networking systems can be beneficial when used for knowledge sharing and collaboration.

The main features [20] of social networks are user profiles, network building by establishing contacts, and the ability to join groups. The user profile contains information about the user. Depending on the social network, user profiles can include but are not limited to personal data, interests, hobbies, relationship status, etc. In professional networks also educational and work history, lists of skills that users have, and similar job-related data. Functionality for adding and maintaining contacts is at the core of every social networking system. This subsystem allows users to find other users on the network and add them to the list of personal contacts. Once a connection is established, users are subscribed to be informed about everything that their new contact does on the social network. More developed networks have a very sophisticated set of filters that allow users to finetune which information they are sharing and to which information about their contacts they are subscribed. Social network groups are another distinct feature of social networking software. They allow users to make a small network inside of the network comprised of users with similar interests.

From the knowledge management perspective enterprise, social networks can be used to solve different problems, but they seem most suitable for finding experts and creation of virtual communities practice. In the times of COVID-19 social networks can give employees the additional feeling of belonging to a group. Groups can be used to create and maintain virtual communities of practice. If enterprise social network application is available on mobile phones, special care is required to maintain a work-life balance of employees since such systems can generate unlimited amounts of messages and notifications 24 hours a day. This is especially true if the organization has branches in multiple time zones.

## 6. CONCLUSION AND FURTHER STUDY

COVID-19 has changed considerably how organizations approach their daily operations. During the crisis, the place where people can share knowledge has moved from the office into the virtual world. This brought new challenges and new opportunities. The biggest challenge being the transfer of tacit knowledge. As for explicit knowledge, many different information systems can be used. Web 2.0 knowledge management systems can be a good solution for maintaining knowledge management processes within the organization during the time of social distancing. Depending on the size and the needs of the organization, wikis, blogs, and enterprise networking systems can help the organization be better at managing knowledge. Wikis can be suitable for both small and large organizations. Small organizations can have one wiki for the whole company, while larger organizations can have specialized wikis for every project or department. Blogs have many different types, and depending on the type; they are suitable for all sizes of companies. Enterprise social networking systems are geared toward larger organizations. In small or even mid-size organizations, there is no need for specialized software for maintaining social networks since the number of contacts is relatively small. For such organizations, it is better to use public social networks such as Facebook, ResearchGate, or Linkedin for the same purpose. The downside of these systems can be disturbed work-life balance of the employees. All of the major platforms have mobile apps that allow sending messages 24 hours a day, seven days a week. Unlike when using public social networking systems, employees can't ignore work-related messages sent from their colleagues or bosses, which can lead to information overload. It is therefore important to set rules in place not to abuse the system.

As for further research, after COVID-19 has ended, it would be interesting to see how many of the changes implemented during the crisis have remained in use and what effect has this new way of doing business had on the work-life balance of employees and their productivity.

**REFERENCES**


[1] R. Grant, "Toward a knowledge-based theory of the firm", *Strategic Management Journal*, vol. 17, pp 109-122, 1996 https://doi.org/10.1002/smj.4250171110

[2] M. Alavi, D. E. Leidner, (2001). "Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues." *MIS Quarterly*, vol. 25, no 1, pp 107–136 https://doi.org/10.2307/3250961.

[3] I. Nonaka, K. Noboru. "The Concept of 'Ba': Building a Foundation for Knowledge Creation." *California Management Review*, vol. 40, no. 3, Apr. 1998, pp. 40–54, doi:10.2307/41165942.

[4] P. Heisig, O. A. Suraj, A. Kianto, C. Kemboi, G. P. Arrau, N. F. Easa, (2016) "Knowledge management and business performance: global experts' views on future research needs", *Journal of Knowledge Management*, Vol. 20 Issue: 6, pp.1169-1198, https://doi.org/10.1108/JKM-12-2015-0521

[5] I. Nonaka, R. Toyama, The Knowledge-Creating Theory Revisited: Knowledge Creation as a Synthesizing Process. *Knowledge Management Research & Practice*, no. 1, pp. 2-10. 2003 http://dx.doi.org/10.1057/palgrave.kmrp.8500001

[6] E. Wenger, R. McDermott, V.M. Snyder, "Cultivating Communities of Practice: A Guide to Managing Knowledge", *Harvard Business School*, Boston, MA. 2002

[7] H. Annabi, S. T. McGann, S. Peis, P. Arnold, C. Rivinus, "Guidelines to align communities of practice with business objectives: An application of social media" *In Sprague, R. (Eds.), Proceedings of the 45th annual hawaii international conference on system science*, pp. 3869-3878, January 2012.

[8] A. Ardichvili, V. Page, T. Wentling, "Motivation and barriers to participation in virtual knowledge-sharing communities of practise", *Journal of Knowledge Management*, Vol. 7 No 1, pp. 66-77, 2003. https://doi.org/10.1108/13673270310463626

[9] https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html accessed 15.04.2020.

[10] U. Cress, J. Kimmerle, "A systemic and cognitive view on collaborative knowledge building with wikis" *Computer-Supported Collaborative Learning* Vol. 3 No. 2, pp. 105-122, 2008. DOI 10.1007/s11412-007-9035-z

[11] A. J. Hester, "A comparative analysis of the usage and infusion of wiki and non-wiki-based knowledge management systems Information Technology and Management Vol. 12 No. 4, pp. 335-355, 2011. DOI 10.1007/s10799-010-0079-9

[12] C. Meenan, A. King, C.Toland, M. Daly, P. Nagy, "Use of a Wiki as a Radiology Departmental Knowledge Management System" *Journal of Digital Imaging*, Vol. 23 No. 2, pp. 142-151, 2010. DOI: 10.1007/s10278-009-9180-1

[13] https://www.mediawiki.org/wiki/MediaWiki

accessed 15.04.2020.

[14] F. H. Zaidan, M. P. Bax, "Semantic wikis and the collaborative construction of ontologies: case study" *Journal of Information Systems and Technology Management* Vol. 8 No. 3, pp 539-554. 2011 DOI: 10.4301/S1807-17752011000300002

[15] E. S. Poole, J. Grudin, "A Taxonomy of Wiki Genres in Enterprise Settings" *paper presented at WikiSym '10 International Symposium on Wikis and Open Collaboration*, October 2010. https://doi.org/10.1145/1832772.1832792

[16] G. J. Baxter, T. M. Connolly, M. H. Stansfield, "Organisational blogs: benefits and challenges of implementation*", The Learning Organization*, Vol. 17 No. 6, pp. 515-528, 2010. https://doi.org/10.1108/09696471011082376

[17] M. Levy, "Web 2.0 implications on knowledge management" *Journal of Knowledge Management* Vol. 13 No. 1, pp. 120-134, 2009. https://doi.org/10.1108/13673270910931215

[18] K. Musial, P. Kazienko, "Social networks on the Internet", *World Wide Web*, vol. 16 pp.31–72, 2013. https://doi.org/10.1007/s11280-011-0155-z

[19] A. Ardichvili, M. Maurer, W. Li, T. Wentling, R. Stuedemann, "Cultural influences on knowledge sharing through online communities of practice", *Journal of Knowledge Management*, vol. 10, pp. 94-107, 2006. https://doi.org/10.1108/13673270610650139

[20] Opacic Mladen, Vojkan Cvijanovic, Mladen Veinovic, "Social networking systems through the lens of knowledge management", *Proceedings in The 2nd Electronic International Interdisciplinary Conference, EIIC 2013, Slovak Republic*, ISBN: 978-80-554-0762-3 ISSN: 1338-7871. pp. 74-78, 2.9-6.9.2013

# IMPACT OF 5G RF-EMF ON PUBLIC HEALTH AND ENVIRONMENT:
## Study results, regulation and guidelines of limiting exposure

Rajko Terzic, Institute of Public health, Belgrade, Serbia, rajko.terzic@zdravlje.org.rs
Dragorad Milovanovic, University of Belgrade, Serbia, dragoam@gmail.com

**Abstract:** *This work presents the possible health issues associated with ongoing deployment of 5G and development of new 6G technologies. It is mostly dedicated to the research of short- and long-term effect of practically available communication bands RF/mmWave/THz on various human health aspects. The propagation physics of electromagnetic fields EMF, measuring exposure and ICNIRP/FCC (International Commission on Non-Ionizing Radiation / Federal Commission on Communications) regulation, and medical research studies are presented. With careful use of wireless technology, network coverage planning, possible changes to certain EMF emission/exposure regulations, and technology education, it is possible to focus on development without compromising overall health.*

**Keywords:** *5G mobile networks, public health regulation*

### 1. INTRODUCTION

The relationship between wireless networks and health has been debated for decades, practically with the development of new generations of wireless technology. It is clear that mobile users are concerned about the exposure in RF electromagnetic field (EMF) emitted by base stations (BS), as well as the increasing number of mobile phones, tablets and IoT sensors. It is often argued that adding a large number of device to global network increases EMF pollution of the environment [1].

However, it is necessary to identify at which levels 5G and 6G differ from the development of previous generations of networks, up to 4G [2]. Next, it is possible to analyze the principles EMF regulation, and investigate how they correspond with the findings of experimental health studies conducted so far, bearing in mind the recommended EMF levels proposed by various sources and organizations. When it comes to the experimental evidence presented in the various health studies conducted so far, it is left to medical researchers and practitioners. In our research, we consulted review papers, which cover numerous individual studies investigating the possible link between EMF and health risks.

After the introduction, in the second section of the paper, we consider the side-effect of mobile network technologies on health of population. In the third section, we deal with the measurement of EMF exposure, the magnitudes and exposure recommendations. We have also shown what the regulated exposure limit values in different countries. The difference in exposure time period and distance of the EMF source in relation to the user is highlighted. In the fourth section, we discuss the impact of 5G RF-EMF. The difference between short- and long-term exposure is emphasized. Effects due to tissue heating and when heating is not present are also highlighted. The research projects of WHO (World Health Organization) and IARC (International Agency for Research on Cancer) as well as classification impact are point out. We discuss the differences in the health impacts of developing 5G and 6G technologies. We also provide an overview of VLC communication in the visible spectrum.

### 2. WIRELESS NETWORKS AND POSSIBLE HEALTH EFFECTS

The expansion of broadband access to shorter wavelength EMFs highlights concerns that health and safety issues remain unknown. Controversy continues over the potential harm of the current 4G wireless network, while relatively new 5G technology is less studied in terms of its impact on people and the environment. There is concern that the additional 5G bands to the existing complex mix of RF lower frequencies will contribute to a negative impact on public health [3].

In the paper, we analyzed the relevant RF/mmWave/THz communication bands, exposure standards and uptodate scientific literature on the health implications of mobile user exposure in 5G networks. We point out that more data on the relationship between health and biological effects of RF communication signals are necessary.

We conducted a literature review of the health effects of wireless technologies, innovative 5G communications and technology specifications, and related policies affecting public health. The question will be raised as to what constitutes public health, as well as the need for

precautionary approach in the development of new wireless technologies.

We point out that it is necessary to update public health regulations and align appropriate independent science research with the adoption of new biologically based user exposure standards for 5G and 6G technology.

### 2.1 Public health

Public health encompasses the science and practice of improving health, preventing and controlling disease, monitoring populations to assess health, identifying causes and effective interventions, and ensuring equity in populations and communities. One possible concise definition*: public health is everything we, as a society, do together to ensure the conditions for people to be healthy*. Public health includes an ever-expanding range of topics in four phases: sanitation (up to 1914), industrialization (1915–1950), emission restrictions (1951–1995), and finally globalization (1996). Three common public health principles that apply through all these stages are: 1) need for regulation by state governments, 2) need for a market where environmental protection is economically justifiable compared to alternatives, and 3) social acceptability, with cultural norms supporting protective behavior over risky behavior [4].

A growing number of scientists articulate need to recognize the impact of development and implementation of new generations of wireless technologies on public health. The open forum identified the following criteria:
- health effects can be prevented and modified,
- there is a high prevalence (total number of patients within a certain population) of risk factors,
- there is an increase in incidence (the number of new cases in a certain time interval) and prevalence (commonness),
- there is a significant economic impact,
- it is possible to influence a large population,
- a joint effort in finding a solution is necessary.

The current impression is that the biggest obstacles are cultural, economic and political in nature, along with a perceived lack of funding for independent scientific research on the health effects of RF-EMF that is free from industry influence or bias.

### 2.2 Impact of mobile network technology

The first generation of 1G mobile telephony was implemented some 40 years ago. Since then, a new generation of network appears periodically for ten years. With each new generation, the general population is concerned about the health consequences (Fig. 1).

The WHO (World Health Organization) started the international EMF 0-300 GHz project in 1996 (in the 2G/GSM era) with the aim of evaluating scientific evidence on possible health effects [5]. The rationale for the project stated that it was initiated in response to public concerns about the health effects of EMF exposure. The key objectives of the project are:
- provide a coordinated international response to concerns about the possible health effects of EMF exposure,
- study the scientific literature and make a report on the state of health,
- identify gaps in knowledge that require further research in order to make better health risk assessments,
- encourage a focused research program in cooperation with financial institutions,
- encourage the development of internationally acceptable standards for limited EMF exposure,
- provide advice to national authorities and other institutions, the general public and employees on all risks arising from exposure to EMF and any necessary mitigation measures.

Also, in 2011, the WHO and IARC (International Agency for Research on Cancer) classified RF-EMF as potentially carcinogenic to humans and recently prioritized it for study over the next five years (2020-2024).

Over the years, the so-called base station BS myth has emerged: cell phone towers are considered dangerous by the public, which has resulted in initiatives and protests against the implementation of tall cell phone towers. However, in the 4G era, it was well understood, even by the general public, that the only possible damage could be caused by user devices, not base stations. The position of mobile phones and tablets very close to the body for a long period of time allows the body to absorb near-field EMF (while the far-field EMF of base stations is greatly weakened). Although the amount of energy emitted by a base station is orders of magnitude greater than that of a cell phone, the EMF power at any point far from the antenna decreases quadratically with increasing distance.

When discussing the possible health risk of implementing a 5G network, it is necessary to isolate differences compared to previous generation. First, in order to achieve better coverage and faster wireless data transmission, a larger number of base stations is necessary, which have a larger number of antennas that transmit simultaneously in a small service area. Second, 5G and 6G will use a wider range of frequencies from 6 to 86 GHz and beyond. A

typical 5G base station simultaneously transmits lower frequency radio signals below 6 GHz and millimeter wavelength signals above 20 GHz. The absolute maximum received radiation power levels at different distances from the base station for the observed distance/frequency combinations are shown in Table 1, assuming an antenna gain of about 10dBi (isotropic antenna power gain).

**Table 1.** Received power for different distances from 4G/5G base station (typical power 40/240 W, respectively).

| Distance/frequency | Large base tower | | Street poles (5G and beyond) | |
|---|---|---|---|---|
| | 3 GHz (4G) | 3 GHz (5G) | 30 GHz (5G) | 60 GHz (5G) |
| 3.16 m | 2.52 mW | 15.1 mW | 151 μW | 13.79 μW |
| 10 m | 252 μW | 1.51 mW | 15.1 μW | 1.379 μW |
| 100 m | 2.52 μW | 15.1 μW | 151 nW | 37.9 nW |
| 1 km | 25.2 nW | 151 nW | 1.51 nW | Less than 1 nW |

Received power at a distance of 10 m is 1.5 mW or less for a 3 GHz signal and drops to just over 1 μW at the same distance at 60 GHz. At a distance of 100 m the signal is in the nano-watt range for millimeter wave transmission and in the order of a few mW at 3 GHz. And finally, at a distance of 1 km, there is practically no effect on 60 GHz. Therefore, even the power perceived by an ordinary RF signal at a distance of 10 m is too small to cause much harm to a network user, and the power of a millimeter wave is practically small. From this analysis it is clear that the potential threat to human health does not come from the side of the base station. Potentially more harmful is the radiation emitted by mobile phones, tablets, laptops and other devices that users hold close to their faces or other body parts when these devices are actively emitting - during a phone call or during data transmission. It should be noted that there is another angle of observation: how much electromagnetic radiation is absorbed at any given moment (instantaneous exposure) and over time (long-term exposure).

## 3. REGULATION OF EMF EMISSION/EXPOSURE

Radio frequencies (RF) span the continuum of electromagnetic emissions from 3 kHz to 300 GHz below visible (VL) and infrared (IR) light. RF wavelengths range from hundreds of meters to fractions of a centimeter. Modern digital communications use higher frequencies and shorter wavelengths (microwaves). 5G millimeter waves (mmWave) are high frequency 30-300 GHz. 6G wireless communications will cover even higher bands from 0.1–10 THz and cover the last empty RF band up to the visible light (VL) spectrum.

First generation (1G) to fourth generation (4G) radio frequency wavelengths are from centimeters to one meter and were first used in military communications decades ago. Shorter wavelengths transmit information in a straight visible path, but over shorter distances. As telecommunications progressed, the frequencies used are of shorter wavelengths and faster data flows. 5G communication technology instantly delivers large amounts of multimedia content in a seamless wireless connection, in any position at any time. New high frequencies and wider bands allocated from 6 GHz to 100 GHz are necessary. The propagation of EMF at these frequencies is of the order of hundreds of meters, so a large number of cellular antennas distributed in cities is also necessary. A 5G network encompasses multiple layers of frequencies, devices and multiple user interactions. The development of 5G technology has been ongoing for the past 15 years with research funding from numerous sources. Public, private and academic partnerships have been developed to advance the 5G initiative.

### 3.1 Exposure measurement

EMF exposure is typically measured using three quantities: specific absorption rate (SAR), plane wave equivalent power density (PD), and steady state and/or transient temperature. SAR levels are used for handheld wireless devices to determine regulatory compliance. For devices and communications infrastructure above 6 GHz (FCC) and above 10 GHz (ICNIRP) the power density metric is recommended [6].

- SAR measures the RF power absorbed in the tissue of a living organism in units of W/kg, so it represents the power level per body mass. However, a metric on the surface of exposed tissue will have a different value than a measurement deep within the tissue. SAR is commonly used to specify safety recommendations for limiting body exposure in close proximity to an EMF source.
- The equivalent power density of a plane wave is the power per unit area and is expressed in $W/m^2$. In the far field of the antenna, it can be expressed either in terms of root mean square (RMS) value of strength of EMF scattered in the tissue or incident on tissue surface. Unlike SAR, power density does not require prior knowledge of tissue absorption characteristics. As such, power density is not as useful for assessing safety in scenarios involving EMF sources at short distances as well as deep tissue depths beneath the skin.
- Steady-state and/or transient temperature is useful for assessing the effect of medium- and high-power EMF exposure, which causes rapid skin heating. Steady-state temperature refers to the temperature to which the skin warms, and transient temperature is essentially the temperature difference due to sudden exposure. Humans

are able to detect temperature changes of only 0.1°C. It is important to note that heating due to RF-EMP penetrates deeper into tissue than millimeter wave radiation. At mmWave frequencies, most of the heat is absorbed in the first millimeter of the skin.

### 3.2 Official guidelines and regulations

Exposures are regulated based on SAR and PD power density metrics, while body heating is observed as a consequence of exposure. Electromagnetic exposure is regulated by ICNIRP (International Commission on Non-Ionizing Radiation Protection) in most European countries and the FCC (Federal Communications Commission) in the USA [6]. Some other countries have decided to specify their own, more conservative regulations. Limitations are applicable to far-field EMF and thus condition the location of base stations BS. There is an obvious difference in the figures used in China, Russia, Switzerland and Italy. The reasoning varies from country to country, but in principle, lower figures allow authorities to go wrong on the side of caution, thereby minimizing as yet unknown risks. A lower figure of 0.1 W/m$^2$ practically prevents the installation of base stations inside or in the immediate vicinity of residential or commercial buildings.

**Table 2.** EMF exposure power density limit values regulated in different countries.

| Country of governing body | Power density restriction for general public (W/m$^2$) | Year adopted | Frequency range (GHz) |
|---|---|---|---|
| ICNIRP | 10 | 1998 | 2–300 |
| FCC | 10 | 1996 | 1.5–100 |
| China | 0.1 | 1987 | 0.3–300 |
| Russia | 0.1 | 2003 | 0.3–300 |
| Switzerland | 0.1 | 2000 | 1.8–300 |
| Italy | 0.1 | 2003 | 0.0001–300 |

Regulation of radiation exposure for consumer devices is much more complex, for at least two reasons. Firstly, devices usually operate very close to human bodies, and secondly, factors such as the shape of body parts (such as the head) need to be taken into account. It is further complicated by the fact that different radiation frequencies result in different EMF penetration depths, so a combination of SAR and PD metrics is necessary when determining exposure limits. The recommendations are best illustrated in Table 3, which shows how the FCC rates EMF exposure criteria for frequencies below and above 6 GHz.

**Table 3.** Exposure measurement criteria for various frequencies and distances (according to FCC).

| Frequency | Distance between the emitter and the human body | Criterion |
|---|---|---|
| Less than 6 GHz | Less than 20 cm | SAR |
| Less than 6 GHz | More than 20 cm | Power density, direct measurement |
| More than 6 GHz | Less than 5 cm | Power density, indirect measurement |
| More than 6 GHz | More than 5 cm | Power density, direct measurement |

Scientific literature indicates that for a whole body SAR level of 4 W/kg and above, RF energy causes unwanted biological effects in humans. The most restrictive limits for whole body exposure are in the 30-300 MHz frequency range where RF energy is most efficiently absorbed when the whole body is exposed. The FCC and ICNIRP use large safety factors to determine maximum allowable and average whole-body SAR values for general public and occupational exposure. The FCC allows 0.08 W/kg as a whole-body average for public exposure and 0.4 W/kg for occupational exposure. The maximum permissible level of exposure at any point of the human body is increased by a factor of 2.0-1.6 W/kg. At the same time, ICNIRP allows the maximum level of exposure at any point to reach as much as 2 W/kg, which is, in principle, the same general figure.

FCC and ICNIRP guidelines for PD power density depend on operating frequency. FCC guidelines are more stringent and allow PDs of 10 W/m$^2$ up to 400 MHz only for professional exposure. From 400 MHz to 2 GHz, there is an increase in permissible exposure, and above 2 GHz and up to the millimeter wave range, a figure of 10 W/m$^2$ can be used for the general public and 50 W/m$^2$ becomes applicable to professional workers.

## 4. STUDIES of 5G/6G TECHNOLOGY

In this section, it may be helpful to distinguish between immediate exposure and long-term EMF exposure. The evidence presented so far indicates that as long as network operators and consumer device manufacturers follow radiation exposure regulations, the physics of radio wave propagation and absorption dictates that there is no risk to humans other than heating of body tissue, typically the skin and eyes. However, medical researchers argue that long-term effects may still be unexplored and unknown; the evidence gathered so far does not generally exclude the possibility of long-term risks. Long-term effects can be a consequence of the warming itself, but also some other mechanisms [7, 8].

### 4.1 Effects due to warming

The effects of heating on the human body are generally much better researched. As a result of poor EMF penetration, heating is typically associated with the eyes and skin as the two dominantly affected organs. The eyes are particularly vulnerable because they are located on the surface of the body without the protection of the skin and in close proximity to the ears and mouth, which means that they are subject to relatively high exposure when the headphones are brought close to the user's face. The basic problem is that the heat is not simply dissipated, which in the rest of the body is achieved by blood flow. The EMF eye problem has been intensified in recent years with head-mounted VR devices used in entertainment and gaming, as well as for scientific research and remote work, causing near-field radiation exposure for long periods of time. There is some indication that telework, as well as eye injuries such as cataracts and corneal damage, may result from long-term exposure.

Skin heating is potentially more harmful with millimeter wave exposure than with microwaves, because it does not penetrate deep into the skin and does not reach deep into the tissue where simple body volume scattering is possible. Instead, at least 90% of millimeter wave energy is absorbed in the deeper epidermis and dermis, which can predict localized maxima near the skin surface, so exposure must be controlled to avoid extensive heating. In principle, it is recommended that at a power density of 10 $W/m^2$ no harmful effects on eyes or skin are expected.

### 4.2 Possible effects

When it comes to the long-term effects of non-heating, the range of potential health issues under consideration is vast. Possible adverse effects associated with EMF are impaired DNA and cell membrane integrity, gene expression, protein synthesis, neuronal function, blood-brain barrier, melatonin production, sperm damage, and immune dysfunction. The main problem with these claims is the lack of evidence to support a direct correlation between various diseases and EMF. A typical study to investigate the effects of radiation on health takes a long time, and the presence of a control group with which to compare the results, which in the above scenario of many potential risks, is not practical. Some authors claim that the lack of epidemiological evidence does not necessarily indicate the absence of an effect, but may indicate the impossibility of finding a relationship, given the experimental conditions and duration of the study. In the context of health, it is also necessary to consider additional evidence from *in vivo* and *in vitro* studies, however, studies involving experimental animals generally do not lead to accurate results because the EMF impact depends on the exposure of surfaces and tissue masses.

Long-term studies relevant to 5G technologies will become available in the coming years, so the results currently accessible may be misleading.

### 4.3 Development of 6G technology

Now is the right time to consider how the next generation under development 6G differs from 5G in terms of its impact on human health [9]. To begin this analysis, we should consider what further differences there are when it comes to 6G deployment:

- 6G brings another range of frequencies above 100 GHz (mmWave and THz frequencies);
- due to the increase in frequencies and the increase in path loss, it may be necessary to use smaller cells, which will require an even denser network placement;
- with the ubiquitous coverage planned for 6G, the fact is that there is no location on the earth's surface to hide from EMF exposure.

Fortunately, none of the above differences are obstacles to the evolution of technology. First, we should emphasize that THz radiation is also non-ionizing and is no more harmful than millimeter waves. THz penetration into the human body is shallower than mmWave, and exposure becomes more localized. In fact, the THz range has been extensively studied in the past in scanning and surveillance applications, including whole body scanning for security and medical diagnostics [10].

The deployment density of 6G cells will not necessarily be much higher than the density of 5G cells, as some of the propagation losses can be compensated by highly directional antennas. According to the analysis, the received power at different distances from the assumed 5G/6G mmWave/THz base stations barely exceeds 1 μW, and there is practically zero at 100 m from the 6G base station. However, an additional concern raised by the THz range is the absorption effect of various parts of the human body, including skin, because submillimetre wavelengths are approximately the size of the smallest human tissue structures, and therefore the uniform tissue assumptions used in absorption modeling do not hold.

### 4.4 Visible light communication (VLC)

6G networks will also use visible light communications (VLC) in the 430 THz to 790 THz range as a complement to traditional RF communications with the aim of achieving extremely high data rates. Protection recommendations are specifically aimed at the skin and relevant parts of the eye that are at risk of excessive exposure to bright and intense light sources. ICNIRP exposure limits for skin and eye protection depend on the range of wavelengths and spectrum of action [11]. The limits also depend on the duration of the exposure and in some cases the size of the source. In principle, several arguments can be made in favor of declaring VLC safe for human use:

- VLC transmitters require lower power to operate than RF systems, due to the high efficiency of modern LEDs;
- since VLC communications are intended for indoor environments, it is relatively easy to protect against light pollution, which is not necessarily the case with RF;
- VLC transmitters are often installed as add-ons to existing LED lighting, so no additional safety requirements are necessary, other than those normally specified for lighting;
- for VLC transmitters that are not part of existing lighting, transmitter power is controlled to remain within acceptable guidelines for lighting intensity.

However, one concern to consider is the inevitable flickering that results from the modulation of the emitted signal on the LED. Typically, the flickering is so fast that it is not visible, perceived by the human sense of sight as continuous light. In the case of communication and unintentional flicker, steps can be taken to minimize the effect. In 2015, the IEEE developed a standard that outlines recommended practices aimed at mitigating health risks to users [12].

## 5. CONCLUDING REMARKS

The discussion in the paper indicates that, at least for now, there is no reason to be alarmed by the introduction of 5G, with caution to implement 6G at the end of decade, as far as general public health is concerned. However, more long-term research studies are also necessary: it takes time to fully recognize the health risk, and the risks may increase as the technology becomes more widespread. It is also necessary to initiate a review of official guidelines and regulations on EMF exposure so that they are universally applicable in the future. Scientific studies conducted so far have not yet been able to find a close correlation between EMF and health risks. Therefore, more long-term research studies are needed. It's not wrong to misjudge on the side of caution and take certain precautions to prevent overexposure.

5G mobile communications technology with its diverse mix of frequencies and densely packed network of cellular antennas increases EMF exposure. There are significant data gaps to investigate the mmWave range and a range of different RF frequencies with biological effects, long-term exposure and vulnerable populations. It should not be denied that excessive EMF exposure, mostly from user devices placed close to the human body, carries certain risks, but these are easily mitigated by changes in individual behavior. Most experts in the field agree that more research is needed before any real connection between EMF and human health can be confirmed.

The authors believe that the advantages of 5G and 6G networks in the future are currently nonpareil by any other technology. With careful use of wireless technology, network coverage planning, possible changes to certain RF/mmWave/THz emission/exposure regulations, and technology education, it is possible to focus on development without compromising overall health. In parallel, it is necessary for engineers to work with health scientists to structure more conclusive studies, while looking for approaches to mitigate the potential risks discovered.

## REFERENCES

[1] R. Terzic, D. Milovanovic, "Impact of mobile network technology on public health and environment: 5G Deployment and 6G development", YUINFO 2022.

[2] Z. Bojkovic, D. Milovanovic, T.P. Fowdur, *5G Multimedia communication: Technology, multiservices, and deployment*, CRC Press 2020.

[3] F. Belpoggi, *Health impact of 5G*, EU Panel for the *Future of Science and Technology* (STOA), July 2021.

[4] C. L. Russell, "5G Wireless telecommunications expansion: Public health and environmental implications", *Environmental Research*, vol.165, pp.484-95, 2018.

[5] *What is the international EMF project?* World Health Organization, https://www.who.int/initiatives/the-international-emf-project, 2020.

[6] ICNIRP RF EMF, *Guidelines on Limiting Exposure to Electromagnetic Fields*, March 2020.

[7] R. N. Kostoff, P. Heroux, M. Aschner, A. Tsatsakis, "Adverse health effects of 5G mobile networking technology under real-life conditions", *Toxicology Letters*, vol.323, pp.35-40, 2020.

[8] M. Simko, M. Mattsson, "5G wireless communication and health effects: A pragmatic review based on

available studies regarding 6 to 100 GHz", MDPI *International Journal of Environmental research and public health*, 16(18), 3406, 2019.

[9] J. C. Lin, "Human Exposure to RF, microwave, and millimeter-wave electromagnetic radiation [health effects]", IEEE *Microwave Magazine*, vol.17, pp.32-36, 2016.

[10] C. Chaccour, M. N. Soorki, W. Saad, M. Bennis, P. Popovski, M. Debbah, "Seven defining features of Terahertz (THz) wireless systems: A fellowship of communication and sensing", IEEE *Communications Surveys & Tutorials*, pp.1-27, January 2022.

[11] ICNIRP Light-emitting diodes (LEDs): Implications for safety, *Health physics*, vol.118, no.5, pp.549–561, 2020.

[12] IEEE SA 1789, *Recommended practices for modulating current in high-brightness LEDs for mitigating health risks to viewers*, 2015.

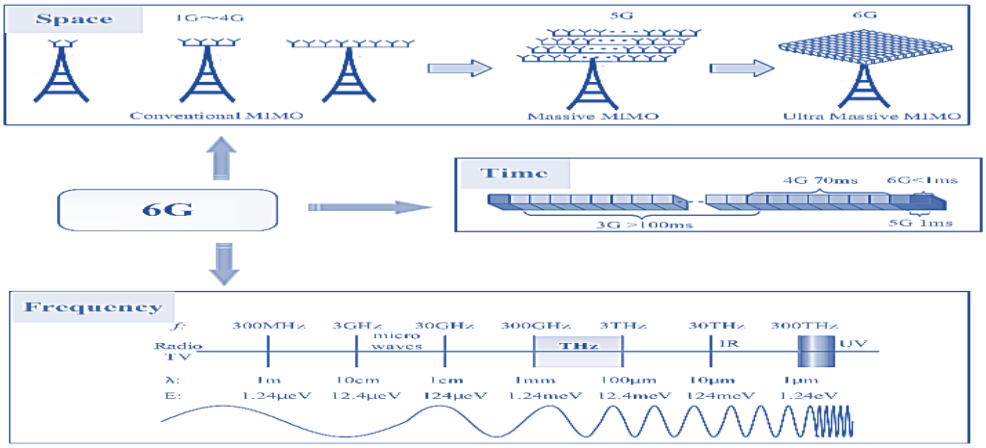



Figure 1. Development of 1G-6G mobile network technologies based on *time-frequency-space* resource.

# 5.

# IT and Project Management

# EXPLORING THE INTEGRATION OF TECHNOLOGY IN PMO: CURRENT TRENDS AND FUTURE PERSPECTIVES

Milan Djordjević, Grand Canyon University, USA, mdordevic@my.gcu.edu
Vladan Pantović, Faculty of Project and Innovation Management, vladan@pantovic.rs

**Abstract:** *This paper investigates the integration of technology in Project Management Offices (PMOs) and its impact on project execution. It explores the potential benefits, challenges, and opportunities presented by technology-enabled PMOs. The paper discusses various technologies, including cloud computing, IoT, blockchain, and big data analytics, and their applications in enhancing PMO functions such as project planning, monitoring, resource management, and stakeholder communication. It provides insights into the current state and future directions of technology integration in PMOs.*

**Keywords:** *Project Management, Innovation, Emerging technologies, Artificial inteligence, BigData, IoT, cloud, digital transformation, analytics, project planning.*

## 1. INTRODUCTION

Project Management Offices (PMOs) are pivotal in steering organizational projects towards success. In the contemporary digital landscape, the integration of technology within PMOs is not just an enhancement but a necessity [13]. This paper delves into the intricate dance between PMOs and emerging technologies, unraveling the symphony of benefits, challenges, and opportunities that this integration heralds. Technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), blockchain, and Virtual Reality (VR) are not just buzzwords but have found practical, impactful applications in PMOs, revolutionizing project planning, execution, monitoring, and stakeholder communication.

The digital transformation journey of PMOs is marked by enhanced efficiency, real-time monitoring, and decision-making, enriched communication, and optimized resource allocation. However, this journey is not without its hurdles. Security concerns, implementation costs, change management, and integration issues are significant challenges that organizations grapple with [2]. Through a meticulous exploration of literature, case studies, and practical examples, this paper aims to offer a panoramic view of the current state, unfolding trends, and future trajectories of technology integration in PMOs.

## 2. Leading the change

In the era of rapid technological advancements, PMOs are at the forefront of integrating innovative solutions to enhance project execution and organizational performance. The incorporation of Artificial Intelligence (AI) has been instrumental in augmenting data quality, consistency, and capacity, leading to improved decision-making processes in various project contexts [3]. AI's significant role in decision-making has enabled companies to make faster and better decisions, leading to enhanced project management systems and higher growth rates [3].

Blockchain technology is another innovation that has made significant strides in PMOs. Its application in e-governance and decision-making in project and program management has been transformative, especially in enhancing service delivery, transparency, and decision-making [1]. The integration of blockchain in e-governance has been pivotal in overcoming the traditional challenges inherent in project management approaches [1].

The Internet of Things (IoT) has also carved its niche in project management. IoT's role in enhancing situational awareness and providing real-time, accurate information through various sensors has been pivotal [8]. The integration of IoT technologies has shown a positive impact on organizational performance, especially when aligned with task-technology fit models [8].

This paper aims to address the following questions:
How can emerging technologies enhance the functions of PMOs and contribute to improved project execution?
What are the benefits and challenges of integrating technology in PMOs?
What strategies and best practices can organizations adopt to leverage technology in their PMOs?
What are the implications of technology integration for project planning, monitoring, resource management, and stakeholder communication within PMOs?

### 2.1 Technology integration

The integration of technology in PMOs is not a straightforward task but a complex process influenced by various factors. The application of AI in international decision-making processes in project management has been marked by increased data quality and enhanced decision-making quality, as evidenced by a qualitative multiple-case study [3]. AI is not optional but a necessary component of a company's survival strategy, enhancing data authenticity and decision-making in various project contexts [3].

Blockchain technology, although promising, faces barriers to its widespread adoption. A study delving into blockchain-powered e-governance in project and program management highlighted the existing challenges despite its potential benefits [1]. The transformative impact of blockchain is undeniable, but the journey to its full integration is marked by hurdles that need to be addressed [1].

IoT projects, characterized by their complexity, require intricate management approaches. A study on IoT project management highlighted the necessity for project managers to be intricately involved from the inception, addressing technical issues typically handled by technical teams in other project types [7]. The adaptive and iterative nature of Agile methodology has been particularly suited for the dynamic and complex nature of IoT projects [7].

## 3. BENEFITS AND CHALLENGES OF TECHNOLOGY INTEGRATION IN PMOS

### 3.1 Benefits

The integration of technology in PMOs has led to significant efficiency improvements. AI and big data analytics have been pivotal in enhancing efficiency in project planning and execution. AI's role in interpreting vast amounts of data provides project managers with valuable insights for better decision-making [10]. Big data analytics, coupled with AI, facilitates the processing and interpretation of extensive data, offering enriched insights that empower project managers to make informed decisions [11].

Real-time monitoring has been enhanced by the integration of IoT in PMOs. IoT's role in providing real-time, accurate information through various sensors has been pivotal in enhancing situational awareness [8]. The Task-technology Fit model has been instrumental in understanding the impact of integrated IoT technologies on organizational performance [8].

Resource optimization is another significant benefit of technology integration. The application of blockchain in resource management ensures transparency and efficiency [9]. Blockchain's role as a distributed ledger technology ensures secure, reliable, and decentralized operations, addressing the security and privacy concerns often associated with IoT devices [9].

Enhanced communication is facilitated by the integration of technologies like VR in project management. A study on the application of VR in managing construction projects highlighted its significant contribution to enhancing the visualization of project development processes [5].

### 3.2 Challenges

Despite the numerous benefits, challenges abound. Security concerns are paramount, especially with the integration of IoT. The security and privacy of information exchanged among IoT devices is a significant concern that needs addressing [9]. The decentralized nature of IoT platforms requires a secure distributed ledger system to ensure data integrity and security [9].

Implementation costs can be a barrier to technology integration. The initial investment and maintenance costs associated with technologies like AI and blockchain can be significant [11]. Organizations need to weigh the benefits against the costs to determine the viability of technology integration [11].

Change management is another challenge. Adapting to new technologies requires training and development. The dynamic and often tumultuous landscape of small and medium-sized enterprises (SMEs) requires continuous learning and adaptation to technological advancements [13].

Integration issues can also arise when integrating new technologies with existing systems and processes. The complexity of managing IoT projects, for instance, requires hybrid management techniques to navigate the inherent complexities [7].

## 4. CASE STUDIES AND PRACTICAL EXAMPLES

### 4.1 Cloud Computing in PMOs

Cloud computing has emerged as a transformative technology in PMOs, offering flexibility, scalability, and cost-effectiveness. A case study involving the integration

of Industry 4.0 and Lean Manufacturing in US organizations revealed that the adoption of smart technologies and cyber-physical systems enhanced product customization, efficiency, agility, and supply chain integration [4]. This case underscores the potential of cloud computing in transforming PMO functions and driving project success.

### 4.2 IoT in Project Monitoring

The integration of IoT in project monitoring is exemplified by a study that explored the role of IoT in enhancing situational awareness and providing real-time, accurate information [8]. The Task-technology Fit model was employed to analyze the impact of IoT on organizational performance, revealing a positive correlation between the perceived fit of tasks and IoT-based collaboration software and performance outcomes [8].

### 4.3 Blockchain in Resource Management

Blockchain technology has shown promise in enhancing transparency and efficiency in resource management within PMOs. A paper exploring the intersection of blockchain and IoT highlighted blockchain's potential in enhancing the security and efficiency of IoT systems integral in modern project management paradigms [9]. The integration of blockchain ensures data integrity and security, addressing the prevalent challenges associated with the security and privacy of IoT devices [9].

## 5. FUTURE PERSPECTIVES

### 5.1 Trends

AI and Machine Learning: The role of AI and machine learning in project management is expanding, particularly in international decision-making processes. AI enhances the quality, consistency, and capacity of data, leading to improved project outcomes [12]. The integration of AI is not optional but a necessary component of a company's survival strategy, emphasizing the need for project managers to adapt to this technological advancement [10].

Virtual Reality (VR) and Augmented Reality (AR): VR and AR are making significant strides in construction project management, enhancing visualization processes and offering platforms for remote conferencing [6]. These technologies are expected to continue evolving, offering more advanced, time-and cost-saving tools in various project management domains.

Automation: The advent of AI and machine learning is paving the way for increased automation in project management. AI's role in enhancing data authenticity and decision-making is associated with increased productivity, efficiency, and quick problem resolution [3]. The future will likely see a surge in automation technologies that make project management more efficient and effective.

### 5.2 Strategies for Successful Integration

Customization: Customizing technologies to fit the specific needs and contexts of different PMOs is crucial. The integration of AI in project management, for instance, requires a comprehensive understanding of its impact on business processes and its potential risks and benefits [3].

Training and Development: Continuous learning, training, and development are essential to adapt to technological advancements. The complexities of managing IoT projects, for instance, necessitate the adoption of hybrid management techniques and the intricate involvement of project managers from the inception [7].

Stakeholder Engagement: Engaging stakeholders in the process of technology integration is pivotal. The transformative impact of blockchain-powered e-governance in project and program management underscores the importance of stakeholder engagement in optimizing the benefits of technology integration [1].

### 5.3 Governance, Ethics, and Integration Strategy

As the integration of emerging technologies into PMOs accelerates, there is a growing need to align technology adoption with enterprise governance frameworks and ethical standards. The introduction of AI, IoT, blockchain, and cloud platforms into project environments raises important questions regarding data ownership, algorithmic transparency, bias mitigation, and compliance with global data protection laws such as GDPR or CCPA.

PMOs must now take an active role in establishing governance protocols for responsible technology use. This includes defining policies for data usage, model training, performance benchmarking, and risk management. As some authors [10] suggests, the lack of explainability and traceability in AI-driven systems may hinder trust and project adoption if not properly managed.

Beyond governance, PMOs must also manage integration complexity. Most organizations already operate a suite of tools (e.g., ERP, CRM, PMIS, BI platforms), and adding advanced technologies necessitates robust API-driven

interoperability for dana synchronization. This approach ensures that real-time data from IoT sensors, AI analytics, databases or cloud platforms feeds directly into dashboards used for decision-making.

Lastly, ethical leadership and stakeholder alignment are crucial. PMO leaders must promote ethical technology use, guiding cross-functional teams to evaluate vendor transparency, data privacy implications, and long-term sustainability. As organizations shift to tech-augmented project environments, success will hinge not just on the tools adopted but on the governance and cultural readiness supporting them.

## 6. CONCLUSION

The integration of technology in PMOs is not just a trend but a fundamental shift that is shaping the future of project management. From the enhanced efficiency offered by AI and machine learning to the real-time monitoring capabilities of IoT, and the security and transparency provided by blockchain, technology is redefining the landscape of project management [10]. Organizations need to strategically integrate these technologies, customizing their applications, investing in training and development, and engaging stakeholders to harness their full potential.

## 7. FUTURE RESEARCH

While this paper provides valuable insights into the current trends and future prospects of technology integration in Project Management Offices, there are several avenues for future research to explore:

Long-Term Impacts: Future research can delve into the long-term impacts of technology integration in PMOs, assessing how these technologies continue to shape project management practices and organizational success.
Evolving Trends: As technology evolves rapidly, staying up-to-date with emerging trends in project management is crucial. Future research can focus on identifying and analyzing new technologies that impact PMOs.
Comparative Studies: Comparative studies can be conducted to evaluate the effectiveness of different technology integration strategies in various industries and organizational contexts.
Ethical Considerations: Given the increasing reliance on technology, ethical considerations related to data privacy, security, and responsible AI usage should be explored in greater depth.

## REFERENCES

[1] Mounir El Khatib, Asma Al Mulla, Wadha Al Ketbi. (2022). "The Role of Blockchain in E-Governance and Decision-Making in Project and Program Management." DOI: 10.4236/ait.2022.123006.
[2] Jinzhao Tian, Yisheng Liu, Meng Yang, Ruijiao Sun, Xiaoxiao Zheng. (2022). "Blockchain Information Sharing Mechanism Based on Embedded System in Project Management System." DOI: 10.1155/2022/1835626.
[3] Alliayah Tubman. (2022). "The Use of Artificial Intelligence in International Decision-Making Processes in Project Management." DOI: 10.2139/ssrn.4121200.
[4] Catherine Maware, David M. Parsley. (2023). "Can Industry 4.0 Assist Lean Manufacturing in Attaining Sustainability over Time? Evidence from the US Organizations." DOI: 10.3390/su15031962.
[5] Wael A. Abdelhameed. (2013). "Virtual Reality Applications in Project Management Scheduling." Computer-Aided Design and Applications, 9(1), 71-78. DOI: 10.3722/cadaps.2012.71-78.
[6] Shakil Ahmed. (2018). "A Review on Using Opportunities of Augmented Reality and Virtual Reality in Construction Project Management." DOI: 10.2478/otmcj-2018-0012.
[7] Vlad Hurtoi, Daniel Avadanei. (2020). "IoT Project Management." Informatica Economică, 24(3). DOI: 10.24818/issn14531305/24.3.2020.07.
[8] Hongyang Wang, Xiaotong Luo, Xiaodan Yu. (2022). "Exploring the role of IoT in project management based on Task-technology Fit model." Procedia Computer Science, 199, 1052–1059. DOI: 10.1016/j.procs.2022.01.133.
[9] Eugene Amoah, Joon-Yeoul Oh. (2020). "Blockchain in IoT and Project Management." Issues in Information Systems, 21(3), 268-278. DOI: 10.48009/3_iis_2020_268-278.
[10] Adel Belharet, Urmila Bharathan, Benjamin Dzingina, Neha Madhavan, Charul Mathur, Yves-Daniel Boga Toti, Divij Babbar, Krzysztof Markowski. (2020). "Report on the Impact of Artificial Intelligence on Project Management." SSRN Electronic Journal, 13(15). DOI: 10.2139/ssrn.3660689.
[11] Sivasubramaniyan Sahadevan. (2023). "Project Management in the Era of Artificial Intelligence." DOI: 10.59324/ejtas.2023.1(3).35.
[12] Yugeshwaree Sheoraj, Roopesh Kevin Sungkur. (2022). "Using AI to Develop a Framework to Prevent Employees from Missing Project Deadlines in Software Projects - Case Study of a Global Human Capital Management (HCM) Software Company." DOI: 10.1016/j.advengsoft.2022.103143.
[13] Abozar Zare Khafri, Abbas Sheikh Aboumasoudi, Shakiba Khademolqorani. (2023). "The Effect of Innovation on the Company's Performance in Small and Medium-Sized Businesses with the Mediating Role of Lean: Agile Project Management Office (LAPMO)." DOI: 10.1155/2023/4820636.

# PREDICTIVE DATA ANALYTICS IN MODERN PMO

Milan Djordević, PM.GURU, USA, milan@pm.guru

**Abstract:** *This paper explores the application of predictive data analytics in modern Project Management Offices (PMOs) and its influence on project performance and strategic alignment. It examines how predictive tools such as machine learning, statistical modeling, and data mining are used to enhance decision-making in key PMO functions including risk management, schedule forecasting, resource planning, and portfolio optimization. The paper highlights implementation strategies, common challenges such as data quality and skill gaps, and ethical considerations in the adoption of AI-driven analytics. By analyzing recent studies and current trends, the paper offers insights into the evolving role of the PMO as a proactive, data-informed unit that supports organizational agility and resilience. Future directions suggest greater integration of artificial intelligence, hybrid project methodologies, and explainable predictive models to further optimize PMO capabilities.*

***Keywords:*** *Project Management, Predictive Analytics, Data Science, PMO, Artificial Intelligence, Forecasting, Machine Learning, Project Planning, Strategic Alignment*

## 1. INTRODUCTION

In today's dynamic and complex project environments, Project Management Offices (PMOs) are increasingly challenged to enhance efficiency, mitigate risks, and align projects with strategic objectives. Traditional project management approaches, often reliant on retrospective analyses, are proving insufficient in addressing the uncertainties and rapid changes characteristic of modern projects. Consequently, PMOs are turning to predictive data analytics to transition from reactive to proactive decision-making frameworks [5]

Predictive analytics encompasses statistical techniques, machine learning algorithms, and data mining processes that analyze historical and current data to forecast future events and trends . Within the PMO context, these analytics facilitate early identification of potential project risks, resource constraints, and schedule deviations, enabling timely interventions and informed decision-making. [3]

The integration of predictive analytics into PMO practices has demonstrated tangible benefits. For instance, organizations employing predictive models have reported improved project delivery timelines, enhanced resource utilization, and increased stakeholder satisfaction . Moreover, predictive analytics supports PMOs in aligning project portfolios with organizational strategies by providing insights into potential project outcomes and value contributions [10]

Despite these advantages, the adoption of predictive analytics in PMOs is not without challenges. Issues such as data quality, integration complexities, and the need for specialized analytical skills can impede effective implementation . Nevertheless, as the volume and variety of project-related data continue to grow, the imperative for PMOs to harness predictive analytics becomes increasingly critical.

This article explores the role of predictive data analytics in modern PMOs, examining its applications, benefits, implementation strategies, and the challenges encountered. By analyzing current practices and emerging trends, the article aims to provide a comprehensive understanding of how predictive analytics can transform PMO functions and contribute to project success.

## 2. PREDICTIVE ANALYTICS IN THE PMO CONTEXT

The integration of predictive analytics within Project Management Offices (PMOs) has emerged as a transformative approach to enhance decision-making, risk management, and overall project performance. By leveraging historical data and advanced analytical techniques, PMOs can forecast potential project outcomes, enabling proactive strategies to mitigate risks and optimize resources.

### 2.1 What is Predictive Analytics ?

Predictive analytics involves the use of statistical methods, machine learning algorithms, and data mining techniques to analyze historical and current data, aiming to make informed predictions about future events. In the realm of project management, predictive analytics facilitates the anticipation of project risks, schedule deviations, and resource constraints, thereby supporting more informed and timely decision-making processes.

For instance, [3] explored the application of machine learning models in software project risk assessment, demonstrating how predictive analytics can identify potential risks early in the project lifecycle, allowing for proactive mitigation strategies.

### 2.2 Comon Use Case in PMO

**Risk Prediction**

Predictive analytics enables PMOs to forecast potential project risks by analyzing patterns and trends in historical project data. This proactive approach allows for the identification of risk factors that may not be immediately apparent, facilitating early intervention [3]. proposed a machine learning-based approach for real-time risk assessment in projects, highlighting the effectiveness of predictive models in enhancing project adaptability and reducing unforeseen costs.

**Schedule and Cost Overrun Forecasting**

By examining past project timelines and budgets, predictive models can estimate the likelihood of schedule delays and cost overruns. A machine learning framework utilizing time series forecasting techniques can predict project performance metrics, such as cost variance and earned value, thereby enabling project managers to take corrective actions proactively [6].

**Resource Capacity Planning**

Predictive analytics assists in forecasting resource requirements by analyzing historical workload data and project demands. This foresight allows PMOs to allocate resources more efficiently, ensuring optimal utilization and reducing the risk of resource shortages or underutilization. [10] emphasized the role of predictive analysis in managing investment project portfolios, particularly in optimizing resource allocation to align with strategic objectives.

**Portfolio Prioritization**

Predictive models can evaluate potential project outcomes based on various performance indicators, aiding PMOs in prioritizing projects that align with organizational goals and offer the highest value. This data-driven approach ensures that resources are invested in projects with the greatest potential for success.

Early Warning Dashboards and KPI-Driven Decision Making

Implementing AI-enhanced dashboards that display predictive analytics insights allows PMOs to monitor project health in real-time. These dashboards highlight at-risk projects, enabling swift intervention and course correction. Murugesan [4] demonstrate how AI systems can automate performance tracking, offering dynamic dashboards for personnel and project performance.

Furthermore, authors [9] discusses how AI improves international project decision-making by increasing the reliability and interpretability of data, which, when visualized through dashboards, enhances PMO strategic response times. While others [7] supports this by showing how dashboards powered by AI provide real-time KPI updates, allowing project managers to prioritize critical tasks and allocate resources more effectively.

These tools not only support transparency but also elevate the role of PMOs from data processors to strategic decision-making bodies equipped with continuous, intelligent oversight.

## 3. IMPLEMENTATION STRATEGIES

The successful integration of predictive data analytics within Project Management Offices (PMOs) necessitates a comprehensive approach that encompasses data infrastructure, technological tools, organizational readiness, and skilled personnel. This section outlines key strategies for effective implementation, drawing upon recent scholarly research and case studies.

### 3.1 Data Infrastructure

A robust data infrastructure is foundational for predictive analytics. High-quality, structured, and comprehensive historical project data are essential for developing accurate predictive models. Wach [10] emphasizes that the efficacy of predictive analytics in project portfolio management is contingent upon the availability of extensive and reliable data sets, which enable the identification of patterns and trends critical for forecasting.

Organizations must invest in data governance frameworks that ensure data accuracy, consistency, and accessibility. This includes implementing standardized data collection methods, establishing data quality metrics, and ensuring compliance with data privacy regulations.

### 3.2 Technological Tools and Integration

The selection and integration of appropriate analytical tools are pivotal for the practical application of predictive

analytics in PMOs. Advanced analytics platforms, such as machine learning algorithms and artificial intelligence systems, can process vast volumes of structured and unstructured project data to generate predictive insights. Some authors [5] discuss the utilization of AI-driven big data analytics for dynamic scheduling and risk prediction, highlighting the transformative impact of these technologies on project management practices.

Modern predictive analytics platforms increasingly rely on cloud computing infrastructure, which offers scalable storage and processing power. Cloud-based environments support distributed computation, enabling the use of graphics processing units (GPUs) for accelerating training and inference of complex machine learning models. Additionally, access to third-party large language models (LLMs) via APIs is becoming common, offering PMOs contextual intelligence capabilities, such as summarization of project risks or automated status reporting.

Equally critical is access to well-labeled and properly structured datasets, without which predictive models cannot be reliably trained or validated. Tools for data annotation, preprocessing, and cleansing must be integrated into the analytics pipeline to ensure data readiness [6].

Furthermore, integration with enterprise platforms such as ERP, CRM, financial systems, HR software, and payment platforms is essential. These systems provide the transactional and operational data necessary for predictive modeling. APIs and middleware platforms (e.g., Mulesoft, Zapier, or custom webhooks) facilitate seamless interoperability across PMIS, SaaS tools, and analytical dashboards.

By building an analytics ecosystem that incorporates cloud resources, GPU-accelerated computing, third-party ML models, structured data pipelines, and ERP/CRM integration, PMOs can significantly enhance their real-time decision-making and strategic forecasting capabilities.

### 3.3 Organizational Readiness and Change Management

Implementing predictive analytics requires organizational readiness, including a culture that embraces data-driven decision-making and the flexibility to adapt to new processes. Sandhu et al [8] identify the critical role of PMOs in aligning strategic objectives with project execution, underscoring the need for organizational structures that support analytical initiatives.

Change management strategies should address potential resistance by involving stakeholders in the implementation process, providing clear communication about the benefits of predictive analytics, and offering training programs to build competency in new tools and methodologies.

### 3.4 Skill Development and Competency Building

The successful deployment of predictive analytics in PMOs hinges on the availability of skilled personnel capable of interpreting analytical outputs and translating them into actionable project strategies. This necessitates investment in training programs that enhance the analytical capabilities of project managers and PMO staff.

The importance of developing project management competencies and methodologies that incorporate predictive analytics, are imperative facilitating more informed decision-making and improved project outcomes [8].

## 4. CHALLENGES AND CONSIDERATIONS

The integration of predictive data analytics into Project Management Offices (PMOs) offers substantial benefits, including enhanced decision-making, risk mitigation, and resource optimization. However, the implementation of such advanced analytics is not without challenges. This section delves into the primary obstacles and considerations that organizations must address to effectively harness predictive analytics within PMOs.

### 4.1 Data Quality and Integration

The efficacy of predictive analytics is heavily reliant on the quality and comprehensiveness of data. Inconsistent, incomplete, or outdated data can lead to inaccurate predictions, undermining the decision-making process. Research [11] emphasizes that the success of predictive analysis in managing investment project portfolios is contingent upon the availability of reliable and relevant data. Furthermore, integrating data from disparate sources and systems poses technical challenges, necessitating robust data governance frameworks and interoperability standards to ensure seamless data consolidation and analysis.

### 4.2 Organizational Culture and Change Management

Adopting predictive analytics requires a cultural shift within organizations. Resistance to change, skepticism towards data-driven insights, and a lack of trust in

analytical models can impede adoption. The study [8] highlight the importance of aligning PMO roles with strategic planning to facilitate the implementation of predictive analytics. Effective change management strategies, including stakeholder engagement, training programs, and clear communication of benefits, are essential to foster a data-centric culture and ensure successful integration.

### 4.3 Skill Gaps and Training Needs

The deployment of predictive analytics necessitates specialized skills in data science, statistical analysis, and machine learning. Many PMOs may lack personnel with the requisite expertise, leading to a skills gap that hinders implementation. Addressing this challenge involves investing in training programs to upskill existing staff and recruiting professionals with the necessary competencies. Some authors [8] underscore the role of PMOs in developing project management competencies and methodologies, which includes fostering analytical capabilities among team members.

### 4.4 Ethical and Privacy Concerns

The use of predictive analytics raises ethical considerations, particularly concerning data privacy and the potential for biased algorithms. Ensuring compliance with data protection regulations and implementing measures to mitigate algorithmic bias are critical. The importance of addressing data privacy and ethical considerations in the deployment of predictive analytics for strategic decision-making are crucial [1]. Establishing transparent data handling practices and incorporating ethical guidelines into analytics frameworks can help navigate these concerns.

### 4.5 Overreliance on Predictive Models

While predictive analytics provides valuable insights, overdependence on these models without human judgment can be detrimental. Predictive models are based on historical data and may not account for unprecedented events or contextual nuances. Therefore, it's imperative to balance data-driven insights with experiential knowledge and critical thinking to make well-rounded decisions.

## 5. FUTURE OUTLOOK AND TRENDS

The integration of predictive data analytics within Project Management Offices (PMOs) is poised to evolve significantly, driven by advancements in artificial intelligence (AI), machine learning (ML), and data science. These technologies are reshaping project management practices, enabling more proactive and strategic decision-making.

### 5.1 AI and Machine Learning Integration

AI and ML are becoming integral to project management, offering capabilities such as dynamic scheduling, real-time risk prediction, and automated task prioritization. Research [5] highlights how AI-driven big data analytics can revolutionize traditional project management methodologies by introducing dynamic scheduling and real-time risk prediction strategies. These technologies enable PMOs to transition from reactive to proactive management, ensuring risks and resource constraints are identified and addressed before impacting project delivery.

### 5.2 Hybrid Project Management Approaches

The shift towards hybrid project management methodologies, combining elements of Agile, Waterfall, and other frameworks, is gaining traction. This approach allows PMOs to tailor project management strategies to specific project needs, enhancing flexibility and responsiveness. The role of PMOs in implementing strategic plans within project-based organizations, emphasize the need for adaptable methodologies to meet evolving project requirements [8].

### 5.3 Emphasis on Data-Driven Decision Making

Data-driven decision-making is becoming a cornerstone of effective project management. By leveraging predictive analytics, PMOs can make informed decisions based on historical data and predictive models. While some authors [1] underscore the importance of predictive analytics in enhancing business performance through data-driven insights, enabling organizations to anticipate potential issues and make proactive adjustments.

### 5.4 Enhanced Focus on Ethical and Explainable AI

As AI and ML become more prevalent in project management, there is an increasing emphasis on ethical considerations and the explainability of predictive models. Ensuring transparency and understanding of AI-driven decisions is crucial for stakeholder trust and effective implementation. Yadav [11] presents a systematic literature review examining the opportunities and challenges of implementing AI-based techniques in project management, highlighting the need for explainable and ethical AI practices.

## 6. CONCLUSION

The increasing complexity and uncertainty in project environments have elevated the role of Project Management Offices (PMOs) from administrative oversight bodies to strategic hubs. Predictive data analytics has emerged as a critical enabler in this transformation, equipping PMOs with the tools to anticipate risks, optimize resource allocation, and align project outcomes with organizational objectives.

Drawing on techniques such as machine learning, statistical modeling, and real-time data processing, predictive analytics empowers PMOs to move beyond reactive management toward a proactive, insight-driven approach. As demonstrated in recent peer-reviewed studies, organizations that embrace these tools report improved project performance, heightened stakeholder confidence, and stronger alignment with long-term strategic goals.

Despite these advantages, the implementation of predictive analytics presents challenges, including data integration, skill shortages, and organizational resistance. Addressing these issues requires investment in data infrastructure, cross-functional training, and strong change management practices. Ethical considerations and the need for explainable AI must also remain at the forefront as predictive tools become more embedded in decision-making processes.

Looking forward, the PMO of the future will not only manage project execution but also function as a strategic partner—leveraging predictive insights to guide innovation, agility, and resilience. As technology continues to evolve, the integration of advanced analytics within the PMO will become not just a differentiator but a fundamental requirement for sustained project success.

## REFERENCES

[1] Adesina, A. A., Iyelolu, T. V., & Paul, P. O. (2024). Leveraging predictive analytics for strategic decision-making: Enhancing business performance through data-driven insights. World Journal of Advanced Research and Reviews, 22(03), 1927–1934. https://doi.org/10.30574/wjarr.2024.22.3.1961

[2] Galla, E. P., & Gollangi, H. K. (2024). Predictive Analytics for Project Risk Management Using Machine Learning. Journal of Data Analysis and Information Processing, 12, 566–580. https://doi.org/10.2139/ssrn.5023999

[3] Bauskar, S at al. (2020). Predictive Analytics for Project Risk Management Using Machine Learning. Journal of Software Engineering and Applications, 13(12), 1–15. 10.4236/jdaip.2024.124030

[4] Murugesan, U., Subramanian, P., Srivastava, S., & Dwivedi, A. (2023). A study of Artificial Intelligence impacts on Human Resource Digitalization in Industry 4.0. Decision Analytics Journal, 7, 100249. https://doi.org/10.1016/j.dajour.2023.100249

[5] Nabeel, M. Z. (2024). Big Data Analytics-Driven Project Management Strategies: Utilizing Artificial Intelligence for Dynamic Scheduling, Risk Prediction, and Automated Task Prioritization in Complex Projects. Journal of Science & Technology, 5(1), 117–163. https://doi.org/10.55662/JST.2024.5104

[6] Sadeghi, S. (2024). Enhancing Project Performance Forecasting Using Machine Learning Techniques. arXiv preprint, arXiv:2411.17914. https://doi.org/10.48550/arXiv.2411.17914

[7] Sahadevan, S. (2023). Project Management in the Era of Artificial Intelligence. European Journal of Theoretical and Applied Sciences, 1(3), 349–359. https://doi.org/10.59324/ejtas.2023.1(3).35

[8] Sandhu, M. A., Al Ameri, T., Shahzad, A., & Naseem, A. (2024). The role of project management office in the implementation of strategic plans in project-based organisations. PLOS ONE, 19(7), e0306702. https://doi.org/10.1371/journal.pone.0306702

[9] Tubman, A. (2022). The Use of Artificial Intelligence in International Decision-Making Processes in Project Management. SSRN Electronic Journal, . https://doi.org/10.2139/ssrn.4121200

[10] Wach, M. (2021). The application of predictive analysis in the management of investment project portfolios. Business Informatics, (4), 53–60. https://doi.org/10.15611/ie.2021.4.05

[11] Yadav, R. (2024). Transforming Project Management with AI: Opportunities and Challenges. Open Journal of Business and Management, 12, 3794–3805. https://doi.org/10.4236/ojbm.2024.126189

# 6.

# Information Technology Application

# EXPOSING A KNIME-BASED DATA SCIENCE WORKFLOW VIA A RESTFUL WEB SERVICE

Petar Prvulović, School of Computing, Union University Belgrade, petar@prvulovic.com
Nemanja Radosavljević, School of Computing, Union University Belgrade, nradosavljevic@raf.rs
Dušan Vujošević, School of Computing, Union University Belgrade, dvujosevic@raf.rs

**Abstract:** *In this paper, we present a technique for integrating a KNIME-based data science workflow as an independent module accessible via a REST API within a software package. The workflow is exposed through an intermediate layer implemented as a PHP script, which provides a REST API interface for clients. This layer translates incoming requests into a format that triggers workflow execution with the supplied input parameters and returns the results to the client in JSON format. This approach enhances the flexibility of developing data science analyses that need to be integral parts of software packages. Specifically, workflows exposed in this manner can be modified without causing side effects to other modules within the package. The presented technique has high usability in in-house decision support solutions. It also suits agile environments prioritizing product development (functionality/flexibility) over premature optimization or strict model definitions. Furthermore, a workflow implemented in KNIME can later be recontextualized on another platform or in a different programming language without side effects, should execution speed become a priority.*

**Keywords:** *KNIME*, predictive analytical model, *REST* service, agile development

## 1. INTRODUCTION

good practice in software design. There is a noticeable tendency towards dividing the application into services and exposing the functionality of the service through API, which enables combining technologies within one project, logical and physical distribution of parts of the solution, and better tests. The REST API is very popular in the domain of web applications, and the proposed solution is designed with it in focus.

The use of artificially intelligent elements that process data at the request of users is increasingly present in web applications. These elements are often suitable for deployment as independent API services, which is an approach that has its numerous advantages.

KNIME, as a visual environment, has two important qualities. First, it provides great flexibility in the development of analytical, predictive, data mining, machine learning, and similar models, which speaks in favor of using KNIME in software design, especially in the agile approach and in the early stages of development. Second, the user does not have to know some particular programming language, which allows for team diversity and easier involvement of domain specialists.

The key drawback is that the KNIME development environment is conceived as an interactive tool with a graphical interface and, as such, is not directly usable as a service that can be used by other software. In this paper, we propose a solution to this problem, which allows the KNIME data science workflow to be exposed to the rest of the application as a RESTful web service that provides the desired API.

## 2. LITERATURE OVERVIEW

The use of the KNIME open-source software tool has been recognized in various areas of application, where KNIME models can be used by those who are not necessarily experts in programming. One of the applications of KNIME is in genetic programming and machine learning [1]. This tool is also used in the field of bioinformatics [2].

The KNIME environment is designed as a platform for teaching, research, and collaboration, to allow easy integration of new algorithms and tools as well as data manipulation [3]. Adapting the KNIME development environment in a software development process can be benecitial for the multidisciplinary development teams, as well as for those specialists who want to share their knowledge with the community contributing to this environment.

REST is a software architecture that has been treated in the literature from several aspects. In [4], [5] and [6], REST is described in comparison with other styles of software architecture used in the web application design. The authors conclude through comparative analyzes that REST has a number of advantages in certain application domains.

Understanding these differences has especially influenced us to decide to apply the REST architecture. Namely, our focus has been on applications in agile projects and the early stages of web application development.

The use of REST architecture is furthermore presented in the context of mobile application development [7]. It is also shown how the PHP web service can be used as a data provider for mobile applications that use dynamic data [8]. We find all this information significant because they show that the solution we propose can be applied in the process of developing mobile applications.

The style of REST can be incorporated into BPEL, which means that the proposed solution can be applied to traditional business systems [9]. In the domain of such systems, KNIME, as an analytical tool, can, therefore, be successfully applied.

A comparison of SOAP and RESTful services has shown that RESTful web services are more suitable for distributed data integration [10]. An analysis of performances of REST and SOAP in use on mobile devices leads to the conclusion that REST provides better performance in systems that use devices with limited resources [11]. Such systems can benefit from the application of analytical models exposed as a web service.

## 3. MODEL EXECUTION IN KNIME

KNIME offers two types of model execution: 1)within the local work environment and 2)within the cloud environment.

The cloud environment involves placing the finished model on a network location and accessing the model through on-screen interfaces that are generated based on the input nodes defined in the model. Input nodes typically belong to the *Quickforms* group, in which a set of common screen elements for entering content is available: text entry fields, numbers, file selection, and more. The cloud environment provides good performance and offers certain possibilities of exposing the model as a web service, but it carries with it a significant limitation of being outside the physical location of the user.

The interactive mode is intended for designing and executing an analytical model on a local computer. The physical location in this mode is not a problem, because the user can place the *KNIME* executable file and the model on the computer of their choice. The problem is the lack of service mode, so the model can only be used by users, and not by some other software.

To solve this problem, we will expose a *KNIME* model as a web service. This kind of web service will communicate externally through the RESTful API. The web service thus serves as an intermediary between the user of a model and that model, by accepting user requests through a standard HTTP request, converting them into a shape that the model can load, running the model and, upon completion of the model, collecting and sending results to the user as a standard HTTP response.

The achieved level of modularization is such that the end-user does not have to be aware that behind the specific functionality, exposed through the RESTful API, there is a KNIME model. Thus, the KNIME model can become a usable part of the software project, without further side effects, while retaining its mentioned advantages.

## 4. RUNNING A KNIME MODEL FROM CONSOLE

KNIME allows the model to be launched via a console instruction, in the so-called *Headless mode* [12], which runs complete software without a graphical interface and automatically executes the model, i.e. the workflow. In a case of ordering a start for an already started model, an exclusive lock is applied. Interestingly, in the case of starting a model that is packed as a ZIP archive, the exclusive lock is not applied. This makes it possible to run multiple instances at the same time, i.e. to serve multiple requests in parallel.

We list the parameters essential for running KNIME.exe:

- `-reset` resets the model prior to execution
- `-nosave` doesn't save changes occured during execution
- `--launcher.suppressErrors` suppresses the display of error messages window, which prevents blocking the execution in case of an error
- `-consoleLog` starts a separate instance of a console window which shows console output from the model. If omitted, console window is not displayed
- `-application org.KNIME.product.KNIME_BATCH_APPLICATION` indicates that KNIME should run in headless mode

- `-workflowFile="model.zip"` model to be executed (no exclusive lock applied)
- `-workflow.variable=naziv,vrednost,tip` forwards a parameter-variable into the model

KNIME.exe needs to be started as a child process, in order to keep the synchronous execution of the web service that exposes it. On Windows OS, the system parameter /w is used to prevent the process from starting in detached mode [13]. A basic example of running a model in headless mode is, therefore:

```
start /w C:\KNIME\KNIME.exe -application
org.KNIME.product.KNIME_BATCH_APPLICATION
-workflowFile=”model.zip”
```

## 5. FORWARDING PARAMETERS AND GETTING THE RESULTS

Among the options for running KNIME.exe is the option to pass the input values to the model, under the given variable names, which the model can then use. The user of the model sends the input parameters through an HTTP request, so it is up to the intermediate layer that exposes the model to prepare the data thus obtained in a form that can be passed to the model.

The length of the console command in Windows OS is limited to 8191 characters [14]. In general, it may be insufficient if the model performs, for example, image classification. We overcome this limitation by placing the input parameters in a file and passing the path to that file to the model. The path to the file is passed to the KNIME model as variable named *input*.

Depending on the origin and the nature of the input parameters, the input data can be prepared in CSV or JSON format. This ensures that the model can obtain an infinitely large set of data.

In the case of the CSV format, the model has *CSV Reader* as the initial node, whose file location parameter is set to the input variable. The CSV file is prepared so that each row represents one data, and the column an attribute of the data. It is up to the KNIME model to further classify and process this data as needed. An example of a model that accepts data in CSV format is given in Figure 1.

In the case of the JSON format, the model has a *JSON Reader* as the initial node, connected to the input variable in the same way, and the model further uses the *JSON Path* nodes to retrieve the data. Figure 2 shows an example of a model that accepts data in JSON format.

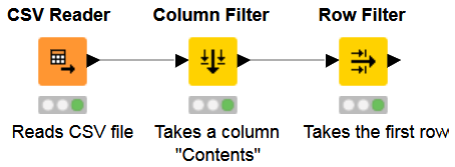



Figure 1: KNIME model elemens for accepting input data in CSV format

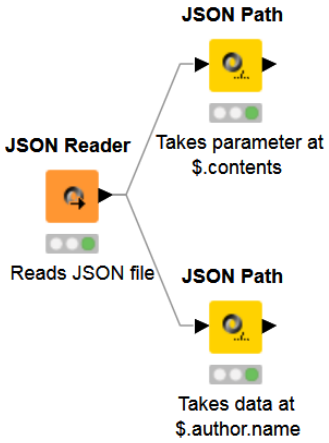



Figure 2: KNIME model elemens for accepting input data in JSON format

The result of the model's work will also be passed from the model using a file. In the basic case, which we use to illustrate the concept, it is a CSV file. If it is necessary to generate images or multiple files, this is also feasible. In that case, these files would be generated under unique names in a dedicated directory, and an output file would contain the paths to them. The output file is specified in the same way, by defining the output variable.

The final form of the application's console call is:

```
start /w C:\KNIME\KNIME.exe-nosave
--launcher.suppressErrors -application
org.KNIME.product.KNIME_BATCH_APPLICATION
-workflowFile=”model.zip”
-workflow.variable=input,”input.csv”,String
-workflow.variable=output,”output.csv”,String
```

## 6. EXPOSING A MODEL AS A RESTFUL WEB SERVICE

REST is an architectural style that requires that resources be identified through URIs and accessed in a uniform manner. The flow of communication should not have intermediate states. In the HTTP protocol, this is achieved by using the PUT, GET, POST, and DELETE commands in a logically consistent manner, so we use the GET command to retrieve resources and the POST command to pass parameters to the resource. The result needs to be displayed in such a format that the recipient can decode it

without any knowledge of the details of the sender's implementation, other than the format in which the response is received.

In a demonstration example that we have implemented, the result of the HTTP POST request will be the name of a predicted category of analyzed news crawled from a public media portal, encoded in JSON format. The HTTP POST request contains the text content of the news as a parameter. The content parameter is placed in a CSV file with a unique name, which is passed to the KNIME model as an input parameter. After the execution ends, the KNIME model generates a CSV file. The contents of the file are converted and sent as a response in JSON format. Thus, the request-response cycle has no intermediate states, and, by sending a response, the service ends, without a need for any additional intermediate messages. Finally, JSON is a standardized format for textual presentation of structured data, and we can say that the REST principles are satisfied and call this solution a RESTful service.

In the proposed construction, the RESTful service acts as an intermediary between the user (be it a human or an application) and the KNIME model. Figure 3 shows a schematic representation of the elements and their mutual interactions and a series of steps in the execution of a single KNIME model call. The web server, PHP script, and KNIME are located on the same computer. The implementation has been simplified so that the PHP script is specifically written for a specific KNIME model, but there is space for further improvement in terms of generalizing the approach so that one PHP script is the entry point for multiple models.

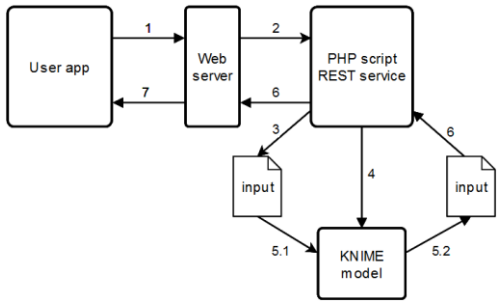



Figure 3. Diagram of integrating a KNIME model as a RESTful service

As we can see in the Figure 3, the execution flow of one KNIME model call is as follows:

1. The user application sends an HTTP request containing the content parameter, ie. the text for which the user wants to get a category.
2. The web server accepts the request and forwards it to the PHP script. The PHP script extracts the content parameter and generates values for the input and filename parameters in order to generate unique file names, allowing multiple instances of the model to run simultaneously. We use the process identifier of the PHP script to generate a unique file name.
3. The PHP script places the content parameter in the input CSV file.
4. The PHP script constructs a console command to run the model, which also contains parameter values, initiates a system call to that command with the exec function, and remains in a locked state until the model completes.
5. The KNIME model is started and loaded with the parameters. The content of news is loaded, based on parameter values, the classification is performed and the result is written to the output CSV file at the location received in the parameters.
6. The contents of the file are converted to JSON format and printed as an HTTP response.
7. Files are deleted, PHP script finishes its work.

The PHP script code is below:

```
$process_id=getmypid();
$contents=$_POST['contents'];
$input="$process_id-in.csv";
$output="$process_id-out.csv";
//write cleaned-up contents into input file
$f = fopen($input, "w");
fputcsv($f, [$contents]);
fclose($f);
//create and execute the command
$command="start /w C:\knime\knime.exe –nosave
--launcher.suppressErrors -application
org.KNIME.product.KNIME_BATCH_APPLICATION
-workflowFile=\"model.zip\"
-workflow.variable=output,\"{$output}\",String
-workflow.variable=input,\"{$input}\",String";
exec($command);
//preparing and sending the response
$f = fopen($output, "r");
$data = fgetcsv($f);
fclose($f);
$result=new stdClass();
$result->category=$data[0];
echo json_encode($result);
//deleting temporary files
unlink($input);
unlink($output);
```

In the test environment, we set the service to the address *192.168.1.1/classifier*. The following is an example of a curl request to the KNIME model API:

```
curl -X POST http://192.168.1.1/classifier
-d "{\"contents\":\"Contents of the text to be
classified\"}"
```

The resulting answer is in JSON format and looks like this:
`{"category":"Class 1"}`

## 7. PERFORMANCE

An example of a KNIME model and a text classification application was tested on a user computer with 4GB of RAM, a 4-core Intel® Core™ i5 processor with an SSD. In this configuration, the total execution time of model requests takes about 30 seconds. Given that the model and environment are loaded from the disk and run with each call, this is not surprising, but it leaves the impression that it is possible to achieve faster response time. The authors expect that the throughput on more powerful hardware would be significantly better, but not good enough for such a model to be applied for a production version of an application, except as an internal service with a small number of users and a sufficient allowed waiting time for results.

## 8. CONSLUSION

In this paper, we have shown how to integrate the KNIME model into a software project without the use of commercially available server and cloud solutions, which increases the availability of applying analytical solutions in projects. The described method of integration provides significant advantages, but there are also several disadvantages that narrow the field of application.

The key advantage that this concept provides is the possibility of including the KNIME development environment in the software project in the form of an independent, isolated module. This advantage enables easier involvement of domain experts in the project and greater flexibility in model development. A domain expert only needs to know the established rules for accepting input parameters and issuing outputs in order to become an efficient member of the team and, along with others, work on the application development.

A key drawback of this concept is the execution speed, which makes it impossible to apply it in applications with a high number of requests to the model. Of course, what is the acceptable response time depends on the specific situation in which the model is applied, and the user who will use the model. So this concept can be widely applied to internally used analytical models whose intensity of use allows for longer response time. In many in-house solutions, the need for a data science-based decision support occurs from time to time. Their users are not numerous. They understand that analytical tasks are time-consuming. The niche consisting of such use is indeed quite large.

Since the model is hidden behind the API, it is possible to change it without side effects on other parts of the solution. This allows for flexibility in experimenting during model development. The KNIME model can be used only during the development of the application, in order to perfect the logical model, and then replaced with faster implementation of the final version of the model in a programming language of choice, without any side effects. Projects in the phase of proving a concept, where it is necessary to demonstrate key functionalities with minimal resource engagement, and projects in an early implementation phase in which it is necessary to maintain development agility can both have a special benefit from the proposed solution. In such projects emphasis is not on the speed but on the accuracy of the results and the possibility of replacing and improving the model. All of the above can be a key advantage of the team in product development.

## REFERENCES

[1] S. O'Hagan, D. B. Kell, "Software review: the KNIME workflow environment and its applications in genetic programming and machine learning", *Genetic Programming and Evolvable Machines, vol. 16, no. 3, pp. 387–391*,2015, doi: 10.1007/s10710-015-9247-3

[2] B. Jagla, B. Wiswedel, J.-Y. Coppée, "Extending KNIME for next-generation sequencing data analysis", *Bioinformatics, vol. 27, no. 20, pp. 2907–2909*, 2011, doi: 10.1093/bioinformatics/btr478.

[3] M. R. Berthold et al., "KNIME: The Konstanz Information Miner", *Data Analysis, Machine Learning and Applications, Springer Berlin Heidelberg*, 2008, pp. 319–326, doi:10.1007/978-3-540-78246-9_38.

[4] P. Adamczyk, P. H. Smith, R. E. Johnson, M. Hafiz, "REST and Web Services: In Theory and in Practice", *REST: From Research to Practice, Springer New York*, 2011, pp. 35–57, doi: 10.1007/978-1-4419-8303-9_2.

[5] X. Feng, J. Shen, Y. Fan, “REST: An Alternative to RPC for Web Services Architecture”, *Future Information Networks, 2009. ICFIN 2009. First International Conference on. IEEE*, 2009.

[6] C. Pautasso, O. Zimmermann, F. Leymann, "Restful web services vs. "big" web services", *Proceeding of the 17th international conference on World Wide Web - WWW* 2008. doi:10.1145/1367497.1367606

[7] J. H. Christensen, "Using RESTful web-services and cloud computing to create next generation mobile applications*", Proceeding of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications - OOPSLA*, 2009, doi: 10.1145/1639950.1639958.

[8] M. R. S. Surendra, "Implementasi PHP Web Service Sebagai Penyedia Data Aplikasi Mobile", *Jurnal ULTIMATICS, vol. 6, no. 2, pp. 85–93*, 2014, doi: 10.31937/ti.v6i2.341.

[9] C. Pautasso, "RESTful Web service composition with BPEL for REST", *Data & Knowledge Engineering, vol. 68, no. 9, pp. 851–866*, 2009, doi: 10.1016/j.datak.2009.02.016.

[10] J. Meng, S. Mei, Z. Yan, "RESTful Web Services: A Solution for Distributed Data Integration", *2009 International Conference on Computational Intelligence and Software Engineering*, 2009, doi: 10.1109/cise.2009.5365234.

[11] H. Hamad, M. Saad, R. Abed, "Performance Evaluation of RESTful Web Services for Mobile Devices", *International Arab Journal of e-Technology. 1*, 2010

[12] "KNIME FAQ", https://www.KNIME.com/faq#q12 [Cited: 31.5.2020.]

[13]"Start, Command-line reference". Microsoft TechNet, https://technet.microsoft.com/en-us/library/bb491005.aspx [Cited: 31.5.2020.]

[14] "Command prompt (Cmd. exe) command-line string limitation", Microsoft Support, https://support.microsoft.com/en-us/help/830473/command-prompt-cmd--execommand-line-string-limitation [Cited:31.5.2020.]

# FRONT-END TEST-DRIVEN DEVELOPMENT: REACT EXAMPLE

Stefan Milanović, Faculty of Organizational Sciences University of Belgrade, stefan.milanovich@gmail.com
Jelica Stanojević, Faculty of Organizational Sciences University of Belgrade, jelica.stanojevic@fon.bg.ac.rs
Miroslav Minović, Faculty of Organizational Sciences University of Belgrade, miroslav.minovic@fon.bg.ac.rs

**Abstract:** *Since software quality is one of the most important topics in the software development industry, this paper outlines test-driven development practices which lead to improved software design and quality if implemented correctly. The focus will be on React, a front-end library used for creating web applications and what testing tools could be used for this technology by describing three main types of tests that are commonly used with React web development, which are unit, integration, and end-to-end tests. The aim is to show how test-driven development can be implemented with React-specific applications, how the process affects code design and structure, as well as what it brings as benefits.*

**Keywords:** *Test-driven development, React, Front-end, Testing, Software*

## 1. INTRODUCTION

With technologies constantly evolving around us, new tools and frameworks for developing applications come to the scene. Usually, those tools are tailored to be used with a certain methodology or process. But sometimes, methodologies need to adapt to be used alongside created tools.

According to NPM trends, comparing React, Angular, and Vue, React is leading in the number of downloads [1]. With its current popularity and the large community that React has, a lot of tools that are supporting it are being created and constantly improved. Some of those tools are used for testing React applications. Used tools may often lead to or require certain processes and software design in order to work as intended.

This opens up the possibility to research if test-driven development (TDD) practice, as one of the practices which lead to better software design, is in compliance with React library and currently developed tools tailored to React.

## 2. METHODOLOGY

The goal of this paper is to show how test-driven development can be used on front-end technologies. An explanation of the test-driven development process will be shown. Red-green-refactor cycle, as the core of test-driven development, will be described. Research on how test-driven development is affecting code quality is shown. After that, front-end testing techniques will be shown, as well as the most popular types of tests that are used for testing front-end technologies. Firstly, unit tests will be described, then integration tests, and last but not least, end-to-end tests. Considering the "testing pyramid", costs and time to implement a comparison between the mentioned types of tests will be shown. Since this paper is focused on React-based applications, libraries that are commonly used for testing React applications will be described. Lastly, an abstract example of how test-driven development can be used when developing an application will be shown. The main database in research of existing work on this topic was Google Scholar. There are a number of articles that are describing test-driven development but the focus is either on back-end technologies or programming in general. This paper is covering that research gap by primarily focusing on front-end technologies.

## 3. TEST-DRIVEN DEVELOPMENT

As one of the most controversial agile practices, test-driven development is still causing discussions about its impact on software quality and programmer productivity [2]. Usually, in the software development industry, writing unit tests is not a must and is usually done after the developer finishes coding. Also, software developers are educated to program first and then walk through the system to make sure that it works properly and how it is intended [3]. Writing code first may lead to code that is not fully testable, as the developer is first trying to resolve the problem he is currently dealing with.

Research showed that adopting TDD in practice could be beneficial when used correctly. In order to use test-driven development as a process, developers must show dedication and great discipline [4].

Test-driven development is the practice of driving the design of code with tests. Traditional workflow in development consists of writing the code and after that, verifying it. TDD, on the other hand, mandates that the first task in development is to write a test and then, the code that will pass the test [5]. As it can be seen from this, TDD is about software design, because it leads us to write code that exposes functions to tests, which makes them modular.
The popularity of test-driven development was gained when it was defined as a fundamental part of Extreme programming. Currently, TDD is used independently in the software development industry [6]. The goal of the test-driven methodology is clean code that works, as it improves software quality [7].

### 3.1 Red-green-refactor cycle

Red-green-refactor cycle is considered as the mantra of TDD practice [7]:

- Red refers to writing a test that doesn't work at first. Based on clearly defined features on how the part of the application that is being developed should work, the developer decouples it into smaller parts and writes tests for parts that are going to fail.
- Green refers to quickly writing a code that passes the test. In this stage, the main goal is to get the tests to work, without paying too much attention to the structure of the code.
- Refactor is the last stage where we make the code cleaner by removing duplication since the "green" stage can lead to a lot of duplicated code. In this stage, the structure of the code is being changed without changing its behavior [8].

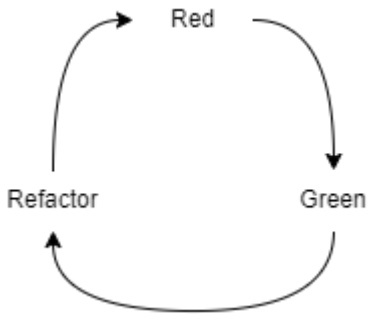


Figure 1. Red-green-refactor cycle

The idea is not to write everything in one cycle. It is preferred to have many iterations. New tests might come along in the process of writing new code, or while refactoring the existing code. The principle of the test first method implies that only the least amount of code is written, which is required for all tests to pass [8].

In order to write testable code we need to decouple it and make it accessible usually through functions. Since the goal of TDD is to do it in small iterations we need to divide the feature into smaller chunks of code. That means, for example, dividing big functions into a few smaller ones, in order to iterate over each of them with a red-green-refactor cycle. In the refactor stage we can work on removing duplication and making smaller functions reusable across other parts.

### 3.2 Code quality using test–driven development

Research was done on whether test-driven development is making improvements in code quality for novice programmers. The results show that testing quality and code quality improved. The main discovered obstacle is that it is hard to adopt a test-first approach [9].

## 4 FRONT-END TESTING

There are a number of different techniques for testing the front-end part of web applications. Some of those are similar to back-end techniques. For example, unit testing and integration testing are used both on the front-end and back-end. There are also front-end specific techniques such as cross-browser and visual regression testing. Cross-browser testing runs test cases on different browsers to verify compatibility between websites and different browsers. Visual regression testing technique, instead of testing the code, compares the rendered result of the code (user interface). Usually, this is conducted by comparing screenshots with the code state before and after the update [10]. One of the most important techniques for testing web applications is end-to-end testing. This technique enables teams to cover complicated test cases that unit and integration tests couldn't do. It is used to test end-user behavior which guarantees that the application functions correctly [11]. In this paper, unit, integration, and end-to-end testing will be described.

### 4.1 Unit testing

The main goal of unit testing is to enable sustainable growth of the software project over time. The accent is on the word

*sustainable*. Those tests are there to make sure that the existing code is still functioning the same while the project is growing. Also, unit tests tend to lead a software project to a better design [12].

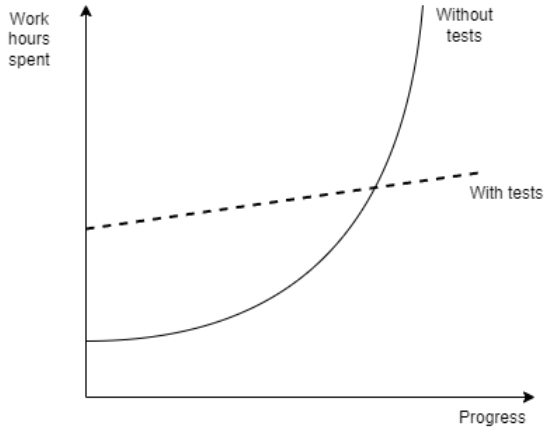



Figure 2. The difference in growth dynamics between projects with and without tests [12]

What can be concluded from this graph is that, as time passes, and the project is growing, if there are no tests written, it is getting harder to maintain the project growth. This is usually happening because there is no regression that can confirm that with introduced changes in the project, old logic is not broken. This statement is not referring only to unit tests. Integration and end-to-end tests also ensure that with introduced changes, the application still works as expected.

As mentioned in the paper, test-driven development is about software design. Unit tests are helping confirm that statement. Unit tests should be [5]:

- fully automated,
- self-verifying,
- repeatable and consistent,
- testing a single logical concept,
- run in isolation,
- fast.

### 4.2 Integration testing

Unit testing is useful for covering smaller units, and integration testing is covering how those units work with each other when combined into bigger functionalities [13]. This is useful because it provides more safety and reliability in the case when units are put together in a bigger module, that the functionality is working as intended.

### 4.3 End-to-end testing

End-to-end testing focuses on the end-users point of view. While integration tests may cover a subset of some functionality, end-to-end tests may include multiple levels of integration testing, covering certain user flow through the application [14].

### 4.4 Comparison between unit, integration and end-to-end testing

Pyramid shown in *Figure 2* compares the time and expense of writing unit, integration, and end-to-end tests. Developers should spend more time on unit tests, as they are faster and cheaper to write, compared to end-to-end tests. But, what is not mentioned here is that, by going up the pyramid, the confidence that the app is working as intended increases [15].

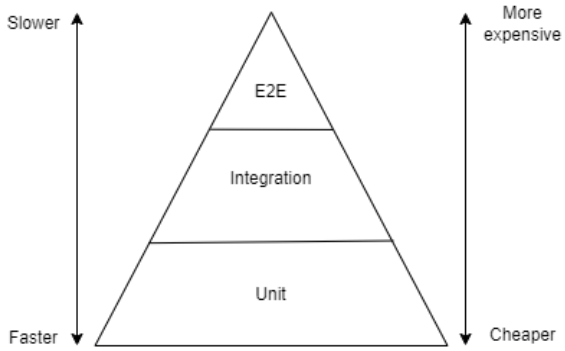



Figure 3. Testing pyramid [15].

## 5 REACT FRAMEWORK TESTING TOOLS

As there exists a large number of web application development frameworks, there also exists a lot of tools for testing those kinds of applications. Here, the focus would be on the most popular React testing tools and how those tools can be incorporated into the test-driven development process.

### 5.1 Jest

The most popular tool for testing React applications is Jest. This tool is recommended by the React documentation as it is made by Facebook (same as React). Jest has a great iteration speed that is combined with powerful features, such as mocking timers and modules which gives developers more control over the code execution [16].

### 5.2 React testing library

React testing library provides light utility functions over React library. These utilities facilitate querying the DOM the same way the user would. For example, they can find elements by their label text. The primary guide of this tool is "The more your tests resemble the way your software is used, the more confidence they can give you." [17]. Accompanied by Jest, React testing library provides us with a way to write unit and integration tests for React apps.

### 5.3 Cypress

Cypress is a beginner-friendly framework that was specifically written for front-end teams that effectively use JavaScript for development. It ensures that developers and QA engineers can quickly start writing automated tests, without worrying about testing setup and underlying test infrastructure [18]. There is no need to install other tools in order for Cypress to work. This tool has all the functionalities that it needs to work properly. Cypress is built to be used by all engineers, and one of the goals was to unlock the ability to do test-driven development with full end-to-end tests [19].

## 6. EXAMPLE

In this paper one way of how test-driven development can be used when working with React applications will be shown. The solution will be presented in an abstract way (without the explicitly written code). The focus will be on different types of tests and how they influence software design decisions.

### 6.1 Application requirements

For demonstration purposes, an application with a feature for storing recipes is going to be built. The business requirements are:

- A form where the user can enter recipe details should be visible on the screen,
- A list of recipes that the user saved should be visible on the screen,
- Every recipe is required to have title, steps, duration, and ingredients specified,
- Difficulty ranking is assigned automatically (user cannot select it manually) when steps, duration, and ingredients are specified. Possible levels are
    - Easy: less than 5 steps, duration less than half an hour, less than 5 ingredients,
    - Medium: steps between 5 and 10, duration between half an hour and 2 hours, ingredients between 5 and 10,
    - Hard: more than 10 steps, duration more than 2 hours, more than 10 ingredients,
- Recipes are stored in the list of recipes with title and difficulty.

### 6.2 Test-driven development cycle

Having in mind the requirements set for this application, as the test-driven development process states, the first step is writing the tests that will fail ("red" zone).

Firstly, developers must choose the type of test they are going to implement. They may decide to start from the *end-to-end* test that will pass when implementation is finished. The test will fail every time as the cycles go until the whole feature is implemented. Another approach is to start decoupling the feature into smaller pieces and writing *unit tests* for the components or functions that will be used. In this particular case, they can decide to write tests for the function that computes the difficulty of the recipe based on steps, duration, or ingredients.

The approach that is described here is decoupling the feature and writing tests for the form. Based on requirements, the first test could check if the input field for entering difficulty is disabled for the user. React testing library is helpful for this use case. It has utility functions that allow us to find rendered input field for difficulty and expect that it is disabled. Another test could check if the form is initially rendered correctly with fields for entering title, steps, duration, and ingredients. If the developer runs the tests, they will fail, which is expected, as there is no code written for rendering the form.

After the developer is satisfied with the implementation of initial tests, the development can start ("green" zone). As described in the paper, the idea is to get tests to pass as soon as possible.

When the code is written and tests pass, the developer can go through the code and see if there could be some duplication removed ("refactor" zone). Creating a reusable component for entering the title and duration or a reusable component for adding the list of ingredients and a list of steps could be a good place to start in this case. This could lead to writing more tests. If the developer is satisfied with how the code

looks and all the tests pass it could be said that the first red-green-refactor cycle is done. Note that the feature is not finished, because it is preferred to reiterate the code with few red-green-refactor cycles.

After the first iteration of the red-green-refactor, the developer should again decide what tests to write. Tests for the function that computes the difficulty should also be written. Those tests are pure function unit tests that could be written with Jest. The parameters are sent to the function and a certain result is expected.

Based on previous examples the modularity in the design that test-driven development is leading to is being shown. Highly testable functions and components are being written and decoupled into smaller parts that can be reused. When the function for computing the difficulty is written and refactored, another cycle can start.

The next part could be testing the *integration* between the components. The tests should be written for entering recipe properties (steps, duration, and ingredients), and difficulty that is computed and shown in the form. This integration test could be written with the help of React testing library utility functions. An integration test gives more confidence than the unit test that the application is working as it is intended, but usually writing the integration test takes more time.

After the implementation of the test that computes and shows the difficulty, the next part would be to test the submission of the recipe to the list. For this case, an end-to-end test could be implemented, which is going to test the whole flow, from populating the form to adding the recipe to the list. This test will give the highest confidence that the code is fulfilling the feature request. As noted in the paper, end-to-end tests tend to give higher confidence, but they are more time-consuming. To make a balance, one option is to cover edge cases with unit or integration tests where possible and rely on end-to-end tests for testing the actual flow (happy path), or the most important parts that must be covered when doing regression.

As it was shown in the example, the developer can have as many cycles as needed. Also, it was shown how the tests-first approach led developers to write decoupled code that could be tested in isolation. The “refactor” stage helps them avoid duplication that can appear with decoupling.

## 7 CONCLUSION

Quality and scalability are very important in software development. Maintaining quality while scaling the project is usually the biggest obstacle that developers are facing. Test-driven development exists for about twenty years now, and if used correctly, can lead to great results. It can improve productivity and maintain code quality.

The main obstacle in the test-driven development process is adopting the habit to write tests first. This requires dedication and discipline from developers in order to show results.

As technologies and tools evolve, methodologies that are being followed in software development also need to adapt to the new needs. React is currently the most popular library that is used for developing web applications, and it is shown in this paper that test-driven development can be successfully used for driving code design. Also, this process can be used alongside other frameworks, such as Angular, Vue etc. The beauty of this process is that it is technology agnostic.

## 8 FUTURE WORK

With many new AI tools that are now popular in the field (such as ChatGPT, GitHub Copilot, etc.) an interesting topic for future research could be how to use those tools for writing the initial tests for the feature that is currently being developed. The next step could be an investigation on whether this approach is boosting the productivity of the developer. Another research could be about implementing test-driven development processes into programming courses at schools and universities to see if it leads students to write better code while learning new technologies. This could be combined with the investigation of productivity, by measuring the satisfaction and knowledge acquired by students. Also, a topic that is worth devoting time to is how compliant are other tools that are used for testing React applications with TDD. One more topic that could be researched is how different types of tests influence code structure. For example, what is the code quality with a lot more unit tests versus a lot of end-to-end tests? To what design changes mentioned structure tends to lead? What should be the focus for the unit test, what for the integration test, and what for the end-to-end test? Research in this paper could be also enhanced with more tests such as cross-browser testing, accessibility testing, etc.

**REFERENCES**


[1] "Angular vs React vs Vue." npm trends. https://npmtrends.com/angular-vs-react-vs-vue ( accessed May 10, 2023).

[2] I. Karac and B. Turhan, "What Do We (Really) Know about Test-Driven Development?," IEEE Software, vol. 35, pp. 81–85, Jul. 2018, doi: 10.1109/MS.2018.2801554.

[3] H. Kou, "TEST-DRIVEN DEVELOPMENT RECOGNITION AND EVALUATION," Ph.D. dissertation proposal, 2004.

[4] R. R. Aguilar, "Using Test-Driven Development to Improve Software Development Practices", 2016.

[5] A. Tarlinder, *Developer testing: Building quality into software*. Addison-Wesley Professional, 2016.

[6] W. Bissi, A. G. Serra Seca Neto, and M. C. F. P. Emer, "The effects of test driven development on internal quality, external quality and productivity: A systematic review," Information and Software Technology, vol. 74, pp. 45–54, Jun. 2016, doi: 10.1016/j.infsof.2016.02.004.

[7] K. Beck, *Test-driven Development: By Example*. Addison-Wesley Professional, 2003.

[8] N. Gurtovenko and O. Golubeva, "TEST-DRIVEN DEVELOPMENT - DEVELOPMENT THROUGH TESTING: ADVANTAGES AND DISADVANTAGES," 2020.

[9] K. Buffardi and S. H. Edwards, "Impacts of Teaching Test-Driven Development to Novice Programmers," International Journal of Information and Computer Science, vol. 1, no. 6, 2012.

[10] Y. Li, "Front-end testing : an important part of quality assurance in Front-end development," Bachelor's thesis, Turku University of Applied Sciences, 2019.

[11] K. Husseini, "Testing front-end architecture," Bachelor's thesis, Metropolia University of Applied Sciences, 2023.

[12] V. Khorikov, *Unit Testing Principles, Practices, and Patterns*. Simon and Schuster, 2020.

[13] M. Vesikkala, "Visual Regression Testing for Web Applications," M. S. Thesis, Aalto University School of Science, 2014.

[14] W. T. Tsai, X. Bai, R. Paul, W. Shao, and V. Agarwal, "End-to-end integration testing design," in 25th Annual International Computer Software and Applications Conference. COMPSAC 2001, Oct. 2001, pp. 166–171. doi: 10.1109/CMPSAC.2001.960613.

[15] K. C. Dodds. "Write tests. Not too many. Mostly integration". Kent C. Dodds. https://kentcdodds.com/blog/write-tests (accessed May 11, 2023)

[16] "Testing Overview". React https://legacy.reactjs.org/docs/testing.html (accessed May 11, 2023).

[17] S. Moreno. "React Testing Library". Testing Library. https://testing-library.com/docs/react-testing-library/intro/ (accessed May 11, 2023).

[18] W. Mwaura, *End-to-End Web Testing with Cypress: Explore techniques for automated frontend web testing with Cypress and JavaScript*. Packt Publishing Ltd, 2021.

[19] "How Cypress Works". Cypress. https://www.cypress.io/how-it-works/ (accessed May 11, 2023).

# APPLICATION OF PARAMETRIC RECTIFIED LINEAR UNIT (PRELU) INTO SPEECH RECOGNITION MODEL

*Robin Singh Bhadoria[1], Atharva Nimbalkar[2], Ram Korde[3], Munish Khanna [4]*
[1,4]Dept. of Computer Science and Engineering, Hindustan College of Science & Technology (HCST), Mathura, India
[2,3]Dept. of Computer Science and Engineering, Indian Institute of Information Technology (IIIT) Nagpur, Maharashtra, India

**Abstract**

*This paper discusses the applicability of Parametric Rectified Linear Unit (PReLU) with Speech Recognition Model. This model utilizes the rectified activation units and implements this algorithm using TensorFlow. The discussed PReLU algorithm has improved the efficiency of model fitting. This paper presents the application of PReLU activation into an acoustic model. A comparison with other sigmoidal or logistic activations is also investigated into this paper. The studied model achieves a 98% validation accuracy with a significantly short amount of epochs.*

**Keywords:** *Parametric Rectified Linear Unit (PReLU), Recurrent Neural Networks, Activation Functions, Deep Learning*

## 1. INTRODUCTION

The first speech recognizer was designed at bell labs in 1952, called Audrey. It was a machine that could recognize spoken numbers between 1 and 9. It was entirely built by analog electronic circuits. It was a large machine that occupied a six foot rack and was highly resource consuming, as is observed with vacuum tube circuitry. Much later and far better approach was taken by Hidden Markov Models (HMMs), which identified the utterances of words as states. HMMs followed a probabilistic approach for identifying words based on their phonemes. Every state in the HMM has a probability distribution over the possible output. HMMs can be combined with Convolutional Neural Networks (CNN) for Speech Recognition [1, 2]. The sequential model Connectionist Temporal Classification (CTC) [3] is used widely in end-to-end speech recognition systems. Authors in research [4] propose a BLSTM-CTC end to end speech recognition model with an error rate of 24.6% on the TIMIT dataset. Recurrent Neural Networks (RNN's) have been most widely used in end to end speech learning models. An RNN architecture known as Long Short-Term Memory (LSTM) has been most successful in this context [5, 6, 7]. In this paper, we propose a model that uses the Parametric Rectifier Linear Units (PReLU) activation function. The use of PReLU is compared with other non-adaptive activation functions such as softmax and softplus.

The model is simplistic and contains a LSTM layer and a fully connected layer. It has been implemented using tflearn, a deep learning library featuring a higher level API for tensorflow. The training results of the models are plotted using a tensorboard.

To keep the model simple and to portray the efficiency of PReLU over other activation functions, the model is trained to recognize words rather than continuous speech. It uses a labelled dataset of spoken digits from various speakers and classifies them into 10 classes. The LSTM layer in the model has 128 neurons with a dropout of 0.8. The output of this layer is fed into the fully-connected layer which uses the PReLU function. It has been shown that using a learned activation unit can improve the model's classification accuracy compared to a parameter-free ReLU [8].

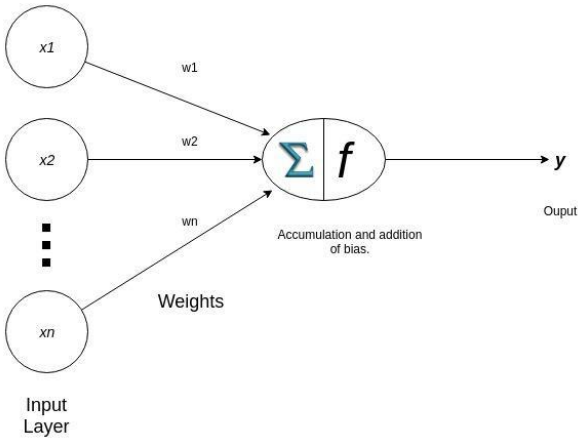



Figure 1. Activation function in a neuron

As shown in figure 1, the inputs to such neural network are fed into the next layer, called the input layer, where the inputs are multiplied with their respective weights. The weights adjust their value through backpropogation as the training progresses. A bias is added to the weighted sum of inputs. This is further passed into the neuron's activation function, which decides weather the neuron will fire or not.

## 2. ACTIVATION FUNCTIONS IN PReLU

*Rectified Linear Unit*

ReLU outputs zero if the input is non-positive, and outputs the input itself otherwise.

$$\mathbf{H}_{out} = max(0, \mathbf{H}_{in})$$

*Parametric Rectified Linear Unit*

PReLU introduces an adaptive parameter ά which is learned through backpropagation. It is generally

initialized to zero. The output of PReLU in the regions of negative input is linear with a slope of ȧ.

$$\mathbf{H}_{out} = \mathbf{H}_{in} \text{ when } \mathbf{H}_{in} > 0$$

$$\mathbf{H}_{out} = ȧ * \mathbf{H}_{in} \text{ otherwise}$$

ReLU activations have the downside of having a zero gradient whenever the input is negative. Using rectified non-linearities has shown major performance improvements of models over using sigmoidal non-linearities. This research compares the validation accuracy of an acoustic model with the activation functions PReLU, softmax, and softplus. All other parameters remain constant across the models. The models train on the same datasets. All three models complete 800 epochs over the training dataset. Their results are demonstrated below.

## 3. RESULT & PERFORMANCE ANALYSIS

With the inclusion of the adaptive parameter ȧ, PReLu reduces the quantity of dead neurons exists in the network. This eminently enhances the learning rate of the deep neural network.

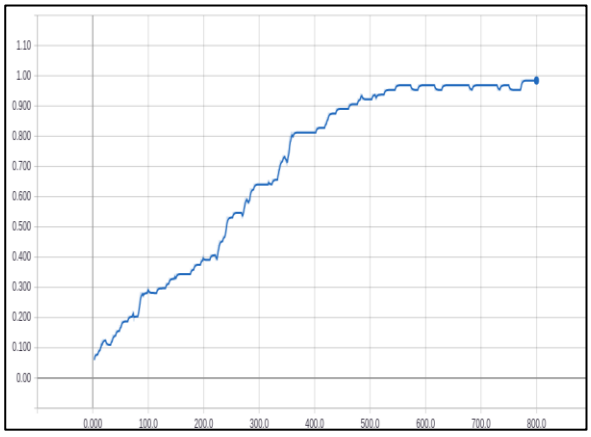


Figure 2. Accuracy of the RNN with PReLu

With PReLu as the activation function, the neural network shows fast learning, as seen in Figure 2. The network reaches an accuracy of over 90% within just 500 epochs. At the end of all 800 epochs, the network has an accuracy of over 98%. Between epochs 0 and 500, a steady and fast growth is observed. This high learning rate can be associated with the presence of a high fraction of active neurons.

### (a) Performance analysis of model with SoftMax

In Figure 2, we observe that the neural network learns at a slow rate. The network reaches an accuracy of only 50% at the completion of 500 epochs. An accuracy of around 65% is reached at the end of all 800 epochs. This shows that the network would need a much higher number of epochs to reach an accuracy of over 90%.

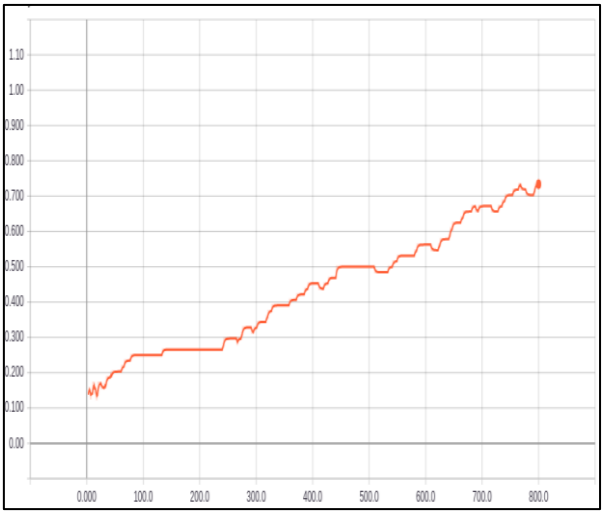


Figure 3. Accuracy of the RNN with Softmax

### (b) Performance analysis of model with SoftPlus

Similar to Softmax, the network shows a slow learning rate with the softplus activation function. The growth of the network is very unsteady, as can be observed in Figure 4.

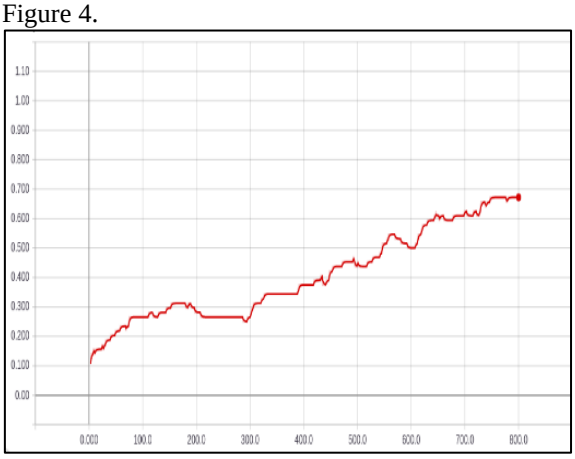


Figure 4. Accuracy of the RNN with Softplus

The network gains an accuracy of below 50% at the end of 500 epochs. On completion of 800 epochs, an accuracy of around 60% is observed as shown in Figure 5.

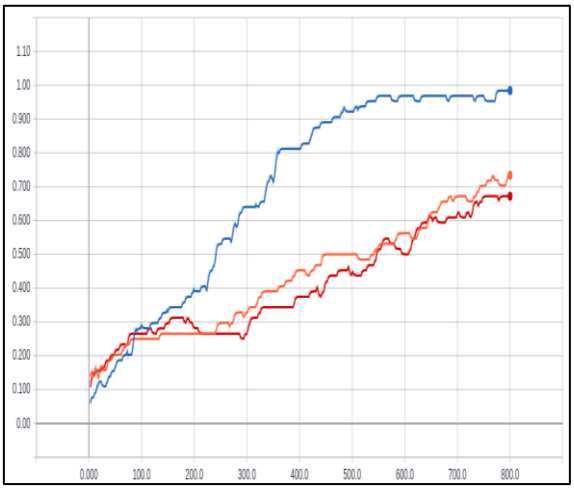


Figure 5. Comparison of the three models

## CONCLUSION

Our model achieves 98.6% validation accuracy after around 550 epochs when used with PReLU. Softmax and Softplus only obtain approximately 70% validation accuracy. This shows the impact of non-linearity choice in an RNN LSTM speech recognition model. The number of epochs required to reach a significant percentage of validation accuracy is drastically less when rectified units are used. Models with rectifier non-linearities outperform those with sigmoid based non-linearities. The non-zero gradient of the PReLU function makes it easier to deal with the vanishing/exploding problem, as neurons only saturate in one direction.

## REFERENCE

[1] A.R. Mohamed, G.E. Dahl, G. Hinton, "Acoustic modeling using deep belief networks", *IEEE Transactions on Audio, Speech, and Language Processing*, 20 (1), 14-22, 2012.

[2] G. Hinton, L. Deng, D. Yu, G. Dahl, A.R. Mohamed, N. Jaitly, T. Sainath, "Deep neural networks for acoustic modeling in speech recognition" IEEE Signal processing magazine, 29, 2012.

[3] A. Graves, S. Fernández, F. Gomez, J. Schmidhuber, "Connectionist temporal classification: labelling unsegmented sequence data with recurrent neural networks", *In Proceedings of the 23rd international conference on Machine learning*, pp. 369-376, 2006.

[4] S. Fernández, A. Graves, J. Schmidhuber, "Phoneme recognition in TIMIT with BLSTM-CTC", *arXiv preprint* arXiv:0804.3269, 2008.

[5] A. Graves, A.R. Mohamed, G. Hinton, "Speech recognition with deep recurrent neural networks", *In Proc. IEEE international conference on acoustics, speech and signal processing*, pp. 6645-6649, 2013.

[6] S. Hochreiter, J. Schmidhuber, "Long short-term memory", *Neural Computation*, 9(8), pp. 1735-1780, 1997.

[7] O. Vinyals, S.V. Ravuri, D. Povey, "Revisiting recurrent neural networks for robust ASR", *In Proc. IEEE international conference on acoustics, speech and signal processing*, pp. 4085-4088, 2012.

[8] K. He, X. Zhang, S. Ren, J. Sun, "Delving deep into rectifiers: Surpassing human-level performance on imagenet classification", *In Proceedings of the IEEE international conference on computer vision*, pp. 1026-1034, 2015.

# FINGERPRINT READER IN SIGNING DIGITAL TRANSACTIONS

Marija Bogićević Sretenović, Faculty of Organizational Sciences, marija.bogicevic.sretenovic@fon.bg.ac.rs
Bojan Jovanović, Faculty of Organizational Sciences, bojan.jovanovic@fon.bg.ac.rs

**Abstract:** *EMV chip specifications are standard for smart cards, both contact and contactless.The opportunity to use the biometric characteristics of individuals to prevent the misuse of identity theft has been given to smart cards. Using fingerprint reader as biometric characteristics may have problems uring the process of acquisition. The condition of the finger during this process can significantly increase or decrease a person's recognition.*

**Keywords:** *Biometrics, Fingerprint, Smart cards, digital transaction.*

## 1. INTRODUCTION

Modern society is innovative and follows the development of information and communication technologies, but it also imposes major changes on human daily life. Digital transformation implies moving a large part of human activities into the digital sphere, where the credibility of identity appears as a special problem. Today, biometrics is widely used in various activities, because the modern business environment has determined an individual's identity as a daily need [1].

The challenge in the last year and a half, both in the world and in our country, is dealing with everything that carries the virus COVID 19. It is recommended that as many business and daily activities as possible be carried out online, but this is also where the problem of establishing identity arises. One of the ways to solve the problem is the application of biometric modalities, primarily fingerprints in various platforms used for communication.

Biometric information (BI) can be defined as reducing uncertainty in determining an individual's identity. Participants of any system, especially biometric, need a secure environment for the authentication process. To protect any information system, it is necessary to fulfil the CIA triad, i.e.:
Confidentiality - secrecy or privacy → confidential storage and transmission of all system data that is on the Internet
Integrity → the ability to safely transfer unaltered data from one location to another
Authenticity → successful verification of communication participants.

There is a horizontal and vertical categorisation of biometric applications [2]. The horizontal categorisation includes applications with standard functionalities and the needs necessary from the biometric system for efficient functioning. Examples are physical access control applications, logical access control applications, transaction authentication, device access control, citizen identification applications, and forensic identification. Applications that can be classified in a particular branch of industry and require the result of a biometric system are classified in a vertical categorisation, e.g., health, finance, education, justice, and police. It is interesting, of course, that any vertical application may need some horizontal application.

## 2. BIOMETRIC MODALITIES

Biometrics automates the process of user identification using a person's physiological or behavioural characteristics [3]. Physical characteristics are those biometric characteristics built into each individual, that is, the body structure of each individual determines them. Physical modalities: fingerprint, iris, hand geometry, palm, retina, face, ear, smell, DNA, facial thermogram. Behavioural characteristics are biometric characteristics that are defined by the specifics of an individual's behaviour towards the world, and they change during a lifetime under the influence of time and environment. Behavioural modalities: signature, voice, gait, keyboard strokes, and way of interacting with the user interface.

A. K. Jain identified seven criteria that determine the appropriateness of choosing a biometric characteristic [4]:

• Universality - every user who wants to access the biometric system must possess the biometric characteristic used by that system.
• Uniqueness - a biometric characteristic must have the property of not being repeated in the population.
• Permanence - the biometric characteristic must be resistant and invariant over time.
• Measurability - every characteristic must be measurable.

• Performance - the accuracy of recognition and the resources necessary to achieve it must be within the application's capabilities.
• Acceptability - persons who will use the biometric system must be ready to willingly access the acquisition procedure and work with the application.
• Possibility of fraud - refers to the ease with which a particular biometric characteristic can be imitated or falsely duplicated.

The fingerprint is the oldest biometric method for authenticating an individual, and thanks to its durability and uniqueness, it is also the most prevalent among all other biometric modalities [5].

Table 1 presents the key characteristics according to the degree of representation by which the fingerprint stands out in relation to the other modalities marked with the letters H-high, M-medium, and L-low, which were processed by Maltoni in his textbook [6].

Table 1. Representation of biometric modalities [6]

| Biometric modalities | Universality | Diversity | Constancy | Measurability | Performance | Acceptability | Possibility of fraud |
|---|---|---|---|---|---|---|---|
| Face | H | L | M | H | L | H | H |
| Fingerprint | M | H | H | M | H | M | M |
| Hand geometry | M | M | M | H | M | M | M |
| Palm | M | M | M | M | M | M | L |
| Iris | H | H | H | M | H | L | L |
| Signature | L | L | L | H | L | H | H |
| Voice | M | L | L | M | L | H | H |

The issue of proof of valid digital identity in the circumstances of digital transformation is becoming increasingly important. Nowadays, everyday life cannot be imagined without identity management techniques, and we are unaware that we are using them. Identity management solves the problems of SSO (single sign-on), user provisioning, and access control.

Answers to the question why the fingerprint is the most common in practice [7] are provided by the following theses:
• One of the most developed biometric modalities
• No two fingerprints are the same,
• Does not change over the years,
• The fingerprint image takes up little memory space,
• Swift identification process,
• Centralised or decentralised access and reader location, as well as the sample databases themselves, can be created
• The amount of work is reduced by biometric identification in some manual jobs where there is a large amount of documentation,
• Ensures privacy, which is one of the most significant problems of the digital era,
• Low maintenance costs for the fingerprint reader.

When registering in the database, a biometric sample is taken with a biometric reader, and the features extracted from the image are recorded (remembered) in the database. That image is associated with the first and last name or social security number of the person whose identity is being determined and is called a template.

Within authentication, two processes are distinguished - identification and verification. In the case of identification, a person's identity is determined, and in the case of verification, the identity of a person is confirmed or denied [8]. During verification, biometric data is acquired and compared with that already recorded in the database, and it is a 1:1 system. During identification, the biometric sample taken is compared with all the samples stored in the database, which is a 1:N system, as shown in Figure 1.

There is positive and negative identification. A positive answer to the question "Are you someone you represent to the system?" is when the person tries to positively identify himself in the system [9]. On the other hand, negative identification answers the question "Are you someone you claim you are not?"

The basic stages of biometric systems are:
• Acquisition of biometric samples
• Extraction of key features
• The process of fitting characteristics-comparison
• Decision-making process

The acquisition procedure, combined with the conditions in which it is performed, is an extremely important factor for the success of the biometric system as a whole. The sensor module is used for the acquisition of a person's biometric data.

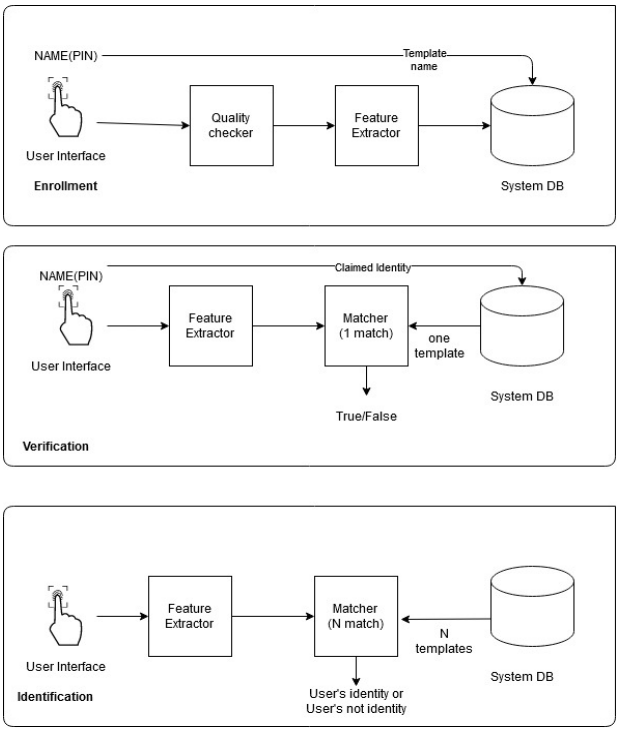



*Figure 1. Registration, verification and identification process [10]*

A fingerprint reader is used for fingerprint acquisition. Several sensor technologies are used in readers, with optical, capacitive and, more recently, non-contact technology used most. New scanning techniques, such as multispectral imaging and 3D non-contact acquisition, have been developed to overcome some of the disadvantages of current finger scanning, such as:
a) difficulties in working with wet or dry fingers,
b) skin distortions caused by finger pressure on the scanner surface
c) inability to detect fake fingers

Image quality significantly affects the performance of feature extraction and comparison. A fingerprint represents the epidermis of a finger, consisting of a pattern in which ridges and valleys are imprinted, showing a large number of minutiae. These are characteristic points necessary for the recognition process.

## 3. PERFORMANCE AND METRICS

The acquisition of biometric samples is the first stage in the process of identifying an individual with biometric systems, so it is crucial that this process begins appropriately to ensure the system performs well. Each biometric modality has specific characteristics that require adapting the acquisition process and its conditions accordingly. On the other side is an individual who may experience permanent finger damage and has extremely dry or moist skin. The acquisition of biometric samples is influenced by environmental conditions and human-computer interaction [11].

When evaluating a biometric system, it is essential to measure its characteristics quantitatively. The metrics used for this purpose refer to the desired characteristics of the biometric modality. The link between the metrics and the desired characteristics of the biometric modality can be direct or indirect**.**

During data acquisition, i.e., registering users of the biometric system, problems may occur with some users. Measures related to this problem are FTA (Failure to Acquire), FTE (Failure to Enroll), and TTE (Time to Enroll).

The accuracy of the biometric system can be measured similarly to how hypotheses are evaluated in statistics. Two errors are possible - FMR (False Match Rate) or FAR (False Acceptance Rate), and FNMR (False Non-Match Rate) or FRR (False Rejection Rate) [12], so that FMR and FNMR correspond to the statistical terms of error of the first and second type. FMR, or false acceptance, indicates the percentage of system users who falsely presented themselves to the system and managed to pass verification through a system error. FNMR, or False Rejection, refers to the percentage of users who correctly identified themselves but were mistakenly rejected in the verification process. FRR includes all errors, that is, causes of rejection, not only those caused by an error in the algorithm. Another metric used to evaluate the success of the biometric system is the TSR (Total Success Rate), which is calculated according to the following formula:

$$TSR = 100 * \left[\frac{NA}{NDB}\right]$$

where **NA** represent number of authorized persons correctly recognized and **NDB** represent total number of persons registered in the database

## 4. CONDITIONS OF ACQUISITION

The recognition process can yield poor results due to the low quality of the fingerprint image, which stems from various environmental factors. It may also result from a specific skin condition of the finger, leading to borderline cases, as the skin on the fingers is generally within a normal range. A blister, cut, or crease may be present on the finger. When evaluating the skin condition, it is crucial to assess how the roughness, dryness, or moisture of the skin affects

the outcome. Human behaviour during the acquisition process is always considered, including whether the individual presses the reader too hard or lightly, and the alignment of the fingers on the sensor presents another human-computer interaction challenge. This group of issues also encompasses the speed at which the subject leaves a fingerprint on the sensor [13]. Regarding environmental conditions, a dirty sensor surface negatively impacts image quality, as do extremely high temperatures or lighting.

As many authors refer to it, standard identification is performed with clean and washed fingers under controlled conditions. Consequently, the results in these environmental conditions are very good.

Sensors integrated into laptops, mobiles, and other digital devices have small surfaces, limiting the area of the finger that is scanned. This can result in an insufficient amount of characteristic points necessary for recognizing a person, leading to degraded performance of the entire biometric system.

The question that needs to be answered is under what conditions to carry out the acquisition and influence a better level of performance of the biometric system. Some parameters that greatly influence the image quality of the biometric sample [14] and, therefore, the performance of the biometric system, which should be monitored include:
1. age of the user,
2. gender,
3. occupation,
4. collaboration, i.e. cooperation with the user during the experiment,
5. soiling of the sensor,
6. sensor size,
7. air temperature,
8. air humidity,
9. immediate or permanent cuts,
10. wetness of fingers,
11. dryness of the fingers,
12. dirty fingers,
13. fingerprint resolution,
14. algorithms for the extraction of characteristic points.

## 5. SMART CARDS

Smart cards were created in the 1970s. It took ten years for them to be widely adopted. They were patented in 1968 by Jurgen Dethloff and Helmet Grotrupp, with further development occurring in 1970 by Kunitake Arimura and in 1974 by Roland Moreno. In 1979, Sclumberger, in cooperation with Moreno, began development, and the first implementation of their use occurred in 1984 in Italy and France through the VISA system.

Depending on the chip, we divide the cards into:
◦ memory
◦ microprocessor.

Depending on the method of data transfer, the cards are divided into:
◦ contact
◦ contactless
◦ combined.

The first smart cards initially had only memory and lacked a processor; later, those containing a microprocessor were developed [15]. There are three categories of smart cards: memory, microprocessor, and optical. They appeared sequentially:
◦ Embossed card
◦ With magnetic tape
◦ Smart cards
◦ Memory cards.

Payment cards are a fundamental component of the electronic banking system. They are the most critical element in any security system that utilises a digital signature. Secret keys of asymmetric cryptography can be securely stored on them. Smart cards are also employed to generate or verify digital signatures and certificates, to encrypt or decrypt information, and to store additional information and applications. By combining protective printing with microchip technology, smart cards enable both physical and digital identification. Smart cards are integrated systems of microprocessors that have their own operating system, memory, file structure, and capability for internal data processing. They are widely used in digital certificates, electronic signatures, decentralized customer loyalty systems, subscription services, and network security. Due to their built-in algorithms and encryption mechanisms, they are regarded as extremely secure.

Payment cards represent a unique non-cash payment instrument issued by a financial, commercial, or specialized organization that enables users to fulfill their payment obligations. They are used at ATMS and POS devices or for online payments. Security when using payment cards is ensured through a PIN issued by the bank. Biometric payment cards represent a new generation in which biometric data is stored on the card and verified by capturing biometric data from the individual, such as fingerprints, palm prints, facial analysis, and others [16]. Smart cards have larger memory capacities, making them more suitable for these additional protection mechanisms.

The most well-known protocol for the use of smart cards in financial electronic payment applications was developed by card issuers Mastercard and Visa. It is a SET (Secure Electronic Transaction) protocol, and the main motive for its development is to enhance the level of security for financial transactions on the Internet and to increase the number of users of their services [17]. The goal is to create a multifunctional smart card that will serve both as a payment card and as an identification card.

### 5.1. EMV standard

EMV is an acronym for Europay, MasterCard and Visa, developed in 1993 by these card organisations. The goal is to ensure interoperability between smart cards based on the EMV standard and terminals worldwide [18]. This standard provides improved security of financial transactions. Cards that conform to this standard contain a chip that functions as a processor and transmitter. At the beginning of 2021, there were about 11 billion EMV cards. They can be contact, contactless and mobile cards.

Quick access to information and easier availability of products and services with minimal costs have led to the widespread use of electronic commerce services. The application of new technologies has resulted in a larger number of users. Currently, the main issue in electronic systems for handling payment cards is fraud. The goal is to introduce biometric payment cards to reduce abuse, primarily by lowering the FRR (False Rejection Rate) values. Existing fingerprint readers on EMV cards have a FAR of 1 at 20000 and an FRR of 5 at 100, with a comparison time of less than 1 second. To improve FAR values, more accurate minutiae extraction is required, necessitating optimal acquisition methods. Research in Malaysia, the Philippines, Great Britain, Canada, and America indicates that people struggle with remembering passwords and PINs, supporting the idea that biometrics represents the future.

### 5.2. Biometric payment card

Biometric payment systems are reliable, economical, and offer numerous advantages over other payment systems. Information technologies for user authentication, such as fingerprint applications and facial scanning, are commercially available and widely used. Some advantages of biometric payment systems include:

- Reliability
- Not using a PIN
- No payment limit restrictions
- A more secure system
- Reduction of administration
- Consumer preferences
- Faster account opening.

A biometric card with a fingerprint reader signifies only the physical presence of the person making the payment [19]. Remembering PINs can be demanding, especially for cards that are not used often. There is no limit when making a transaction, because only that person can execute it. It offers a higher level of security for both the bank and consumers, as it compares the currently extracted characteristics with those permanently recorded on the card. Biometric modalities reduce excessive banking documentation for all processes. Research has shown that more consumers are interested in a biometric payment card when they have the option to choose between two different cards. According to Forbes, digital bank account opening is one of the most popular technologies for the third year in a row.

The integration of a fingerprint reader with a smart card represents a new, more secure method of user authentication. Biometric cards with a reader offer a new dimension of identification through innovative and secure devices. They were first employed at the Bank of Cyprus in 2018. These were Thales EMV cards that utilise a fingerprint instead of a PIN to authenticate the cardholder. The user's biometric data is stored on the card itself, not on a server. This way, the user is protected against attacks and compromises of the bank from cyber threats; if the card is lost or stolen, the fingerprint cannot be replicated. Biometric features are protected locally, as they never leave the card. The card is compatible with existing ATM and POS devices, adhering to ISO standards. Both contact and contactless payments are possible, suitable for small and large transactions. For small amounts, biometric verification can be set to remain inactive depending on the countries where it is used [20]. For larger sums, the sensitivity threshold varies by country, and some publishers may block contactless payments.

An EMV bank card using a PIN code for verification has a FAR value of 1 at 1000000 (a four-digit PIN offers exactly that many possibilities). An EMV bank card with a biometric fingerprint reader has a FAR value of 1 at 20000, which is a significantly better option. The first pilot projects with this card have been implemented since 2018 in the following countries: Cyprus, Italy, Great Britain, France, and Switzerland.

The finger's position on the scanner is intuitive and utilises light signaling, as shown in Figure 2. The cardholder performs the enrollment process independently.


*Figure 2.Cardholder enrollment process [20]*

The future involves developing a new card equipped with a sensor that integrates facial recognition and a contactless fingerprint sensor, enhancing the success of recognition. It will also address the shortcomings that arise due to varying ambient conditions during fingerprint acquisition.

## 6. CONCLUSION

Although the EMV standard brings significant improvements and enhances the security of card usage, including features like contactless payment and longer PIN codes, there are still new vulnerabilities associated with card use. The introduction of biometrics can further enhance security when using EMV cards by ensuring that the cardholder is indeed the owner of the card. Currently, the choice of authentication method is unverified, which can be addressed through the implementation of biometrics. Miniaturization in electronics has enabled the development of fingerprint readers small enough to be embedded within a card. These readers can store multiple fingerprints of the cardholder, ensuring that only the card owner and the card itself possess this data. This capability would allow for the confirmation of the authentication method. One could argue that the card employs multi-factor authentication using biometrics.

## REFERENCES

[1] A.Pando, "Beyond security: Biometrics integration into everyday life", Forbes Cominity Council, 2017, https://www.forbes.com/sites/forbestechcouncil/2017/08/04/beyond-security-biometrics-integration-into-everyday-life/#5c14ce1b431f , poslednji put pristupano juli 2021.

[2] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S. Handbook of Fingerprint Recognition; Springer Science & Business Media: Berlin, Germany, 2009.

[3] Alfred C. Weaver, "Biometric Authentication," Computer, vol. 39, no. 2, pp. 96-97, Feb. 2006, doi:10.1109/MC.2006.47 http://doi.ieeecomputersociety.org/10.1109/MC.2006.47

[4] Jain, Anil K., Ruud Bolle, Sharath Pankanti. Biometrics: personal identification in networked society, Kluwer academic publishers, 1999.

[5] Lourde, M., Khosla, D. Fingerprint Identification in Biometric SecuritySystems., International Journal of Computer and Electrical Engineering, 2(5), pp. 852- 855, 2010.

[6] Bogićević, M., Milenković, I. and Simić, D., Identity Management—A Survey. In Innovative Management and Firm Performance (pp. 370-384). Palgrave Macmillan, London, 2014.

[7] D.Thakkar, "12 reasons to consider fingerprint authentication", https://www.bayometric.com/12-reasons-consider-fingerprint-authentication/,2017, poslednji put pristupano avgust 2021.

[8] Peralta, D., Triguero, I., García, S., Saeys, Y., Benitez, J.B., Herrera, F. Distributed incremental fingerprint identification with reduced database penetration rate using a hierarchical classification based on feature fusion and selection. Knowl. Based Syst., 126, 91–103, 2017.

[9] A.J.Mansfield, J.L.Wayman, Best Practices in Testing and Reporting Performance of biometric devices, Biometric Working Group, NPL Report CMSC 14/02, 2002.

[10] Jain, A.K.; Ross, A.; Prabhakar, S. An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. 14, 4–20, 2004.

[11] Sundararajan, K., & Woodard, D. L. , Deep Learning for Biometrics: A Survey. ACM Computing Surveys (CSUR), 51(3), 65, 2018.

[12] Kukula E.P., Elliott S.J., Duffy V.G. (2007) The Effects of Human Interaction on Biometric System Performance. In: Duffy V.G. (eds) Digital Human Modeling. ICDHM 2007. Lecture Notes in Computer Science, vol 4561. Springer, Berlin, Heidelberg, 2007.

[13] F.D.Tatar, " Fingerprint recognition algorithm, CCSEIT, AIAP, DMDB, ICBB,CNSA-2017.

[14] Bogićević Sretenović M. (2020), Model osetljivosti performansi biometrijskih sistema u postupku akvizicije otiska prsta, Fakultet organizacionih nauka, Univerzitet u Beogradu

[15] https://jacquinot.com/smart-card-operating-system/

[16] https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/cards/emv-biometric-card

[17] Carlisle Adams, Steve Lloyd, Understanding PKI: Concepts, Standards, and Deployment Consideration, 2nd Edition

[18] https://www.emvco.com/document-search/?action=search_documents&publish_date=&emvco_document_version=&emvco_document_book=&px_search=&emvco_document_specifications%5B%5D=specifications

[19] https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/cards

[20] https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/cards/emv-biometric-card

# NATURAL HUMAN-COMPUTER INTERACTION BASED ON EYE TRACKING

Željko Gavrić, Faculty of Organizational Sciences,University of Belgrade, zeljko.gavric@fon.bg.ac.rs
Miroslav Minović, Faculty of Organizational Sciences,University of Belgrade, miroslav.minovic@fon.bg.ac.rs

**Abstract:** *Although computers has been in use for years, human-computer interaction is the least developed in comparison to the rest of the computer system components. The field of HCI research aims to contribute to the developing of interaction devices. Natural interaction devices are described in this paper and they represent an attempt to naturalize human-computer interaction to achieve implicit interaction.* The *eye tracking system represents a powerful tool that can be used for the improvement of interaction.*
*Natural interaction systems based on eye movement have been steadily expanding.*

**Keywords:** *Natural Human-Computer Interaction, Eye tracking, Eye gaze pointing, Eye gaze text input.*

## 1. INTRODUCTION

Human-computer communication is based on interaction. Human-computer communication devices include both input (a mouse, keyboard, touchpad) and output devices such as monitor, printer, and speakers. Nowadays, there is an increasing tendency to naturalize the interaction, i.e. human-computer interfaces in order to achieve more natural ways of communication.

Natural interfaces are primarily based on the use of various types of gestures to operate a computer or some process by using the computer. The main advantage of this interaction is the simplicity, ease and speed of use of the device.
One of the types of natural interaction is eye movement based interaction. There are numerous papers showing eye tracking systems which aimed to ease and naturalize the use of the computer. Some of these systems are designed to enable people with disabilities to use computers in everyday life.

## 2. NATURAL USER INTERFACE

User interfaces that are interacted with using modalities such as touch, gestures, or eye movement are referred to as natural user interfaces. The word “natural” doesn’t refer to behavior or the feeling of the user while using natural user interface [1]. The aim of NUI is the need to speed up and adapt the use of technology to the user instead of the user adapting to the technology, as is the case with conventional interfaces.

Some of the established natural user interfaces are integrated into smartphones and enable operating device functions by using gestures. These gestures allow the user to communicate more naturally with the device, such as switching pages with a gesture that looks like flipping through the pages of a book and the like. Gestures can sometimes be complex and require some adjustments. It can be said that the better the interface, the shorter the user customization time.

## 3. EYE TRACKING

The term eye tracking means recording eye movements in relation to the head [2]. The first eye-tracking systems emerged out of the need to enable human-computer interaction for people with disabilities which enables them to communicate with the surrounding environment [3]. Such a system is designed to enable text input solely by the eyes movement, and the system detects the gaze as a choice of a certain letter. In this way, the users are enabled to communicate with the environment and to perform usual activities such as browsing the Internet and playing games [4].

The process of eye-tracking includes the following phases:

1. Face detection. Face detection represents the most important part of the eye-tracking process. There are two methods for face detection, i.e. characteristics-based and appearance-based methods.
2. Eyes detection. The Viola-Jones algorithm which allows effective detection is one of the most widely used mechanisms for eye detection.
3. Pupil detection. Pupil represents a phase which detects a pupil in the human eye. The Hough Circle Transform algorithm is usually used for this purpose and this algorithm is based on detecting circles in an image.
4. Eye-tracking represents the last phase of this process. The technique usually used in this phase is the pupil illuminating technique which creates a strong reflection on the pupil which can be tracked during image editing.

There are various techniques used for eye-tracking such as electrooculography, infrared oculography, scleral coil, and video oculography.

Natural user interface based on eye-tracking can be divided into two groups:

- Pointing devices
- Text entry devices

### 3.1 Pointing devices

Interaction by using eye gaze for the purpose of pointing is the common subject of many research works. Given that the eye gaze and eye movement enable interaction without using hands, they are very convenient for different purposes. Their advantage is mainly in enabling interaction for people who are not able to use hands. Unlike touch screens, the eyes move in pairs, i.e. they look at one point at the same time, and multiple simultaneous interactions are not possible. The paper [6] shows the system used to move the cursor on the screen using eye movement.

The system uses a webcam, Matlab to process the image given and Java application to move the cursor across the screen. In order to successfully capture the pupil of the eye using a cheap webcam, it is necessary to install the camera near the eye and adjust the correct focus on the pupil. Figure 1 shows the block diagram of the suggested system.

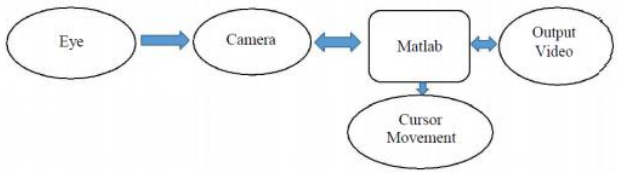



Figure 1. Block diagram eye gaze pointing [6].

The paper [7] describes the system for controlling the cursor which, in addition to moving the cursor, has the possibility of selecting individual options. The described system is designed so that it can functionally completely replace a mouse. In this way, the system allows the use of a computer without the need for hand operation. The starting position of the cursor is in the middle of the screen. When the eye moves to a certain side (left or right), the cursor also moves. If the eye is focused on the center of the screen, the cursor stops moving. When the eye moves up or down, the size of the eye changes.

Namely, when the pupil of the eye moves upwards, the eye enlarges, and when the pupil moves downwards, the eye shrinks. These features are used to move the cursor horizontally. The described system allows the user to select the option when the cursor is at the desired location. The user can select an option that is the same as the right mouse click if he blinks with the right eye, and if he blinks with the left eye, the system will select an option that is the same as the left mouse click. Since human eyes blink spontaneously at the same time, the system ignores this type of blinking, therefore the possibility of randomly selecting an option during spontaneous blinking is avoided. Table 1 shows the properties and comparison of individual pointing devices.

Table 1: Properties of pointing devices [2].

| | Mouse | Touch pad | Touch screen | Eze gaze pointing |
|---|---|---|---|---|
| Speed | Speed | Speed | Speed | Very speed |
| Accuracy | Limitted by time | Limitted by time | Limitted by finger size | Limitted by fovea speed |
| Space demand | Much | Little | None | None |
| Space for device | Big | Small | No space | No space |
| Feedback | Yes | Yes | No | No |
| Way of use | Indirectly | Indirectly | Directly | Directly |
| Multiple pointing | Two hands | Ten fingers | Ten fingers | Eyes |

### 3.2 Text entry devices

Text entry is also possible using eye movements. It is possible to enter text by using gestures or systems based on gaze detection on a virtual keyboard. A gesture consists of a sequence of elements performed in a specific to have the desired meaning. The advantage of gestures is the ability to increase the number of commands by increasing the number of gestures [8].

An eye gesture can be defined as a pattern of eye movement over a limited period, which may or may not be limited to a specific spatial range or area, and which can be identified in real-time and used to indicate a particular command or intention [9].

One of the text entry systems using gestures is presented in the paper [10]. The paper uses a method based on the technique of quickwritting. The signs are arranged concentrically in a circle, and the entered word is displayed in the middle, as shown in Figure 2.

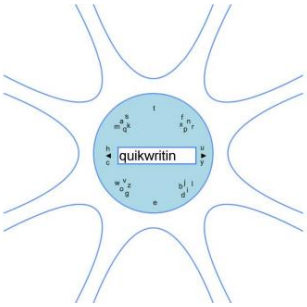



Figure 2. Quickwritting using eye gaze [10].

The problem with this method is that the eye gaze is used to enter, but also to review the characters, so the characters must move away from the display area so as not to inadvertently enter characters when checking the entry. If practiced entering characters for 5 days of 15 minutes, the user can reach an entry speed of 9.5 words per minute [10]. Testing was performed using the German language.

One of the gesture-based text entry approaches is to make the gesture form look like a printed or handwritten character form. This approach makes it easier for the user to learn the characters. One of the first systems to use this approach is EyeWrite, described in the paper [11]. It was originally developed to help people with motor disorders operate computers. When testing the EyeWrite system, the authors showed that the system is slower than traditional keyboard input, but that errors are less common than when using the keyboard. However, the paper shows that exercise significantly increases the input speed which becomes very similar to the input speed when using the keyboard. It is considered that using this system is less tedious than a traditional keyboard. Figure 3 shows the letters and corresponding gestures on the EyeWrite system.

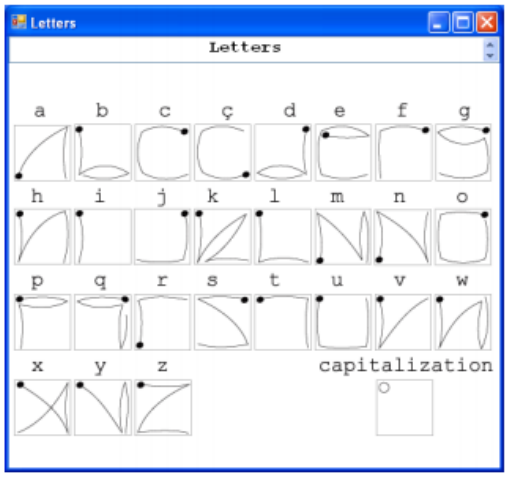



Figure 3. EyeWrite letters and corresponding gestures[11]

The QWERTY virtual keyboard is the most commonly used gaze-based text entry interface. The user focuses his gaze on the letter he wants to enter. If the gaze is kept on that letter for a certain period, the desired letter is accepted. The period required to keep an eye on a letter so it can be accepted for entry is called the dwell time [12]. Dwell time is the time it takes for the system to determine that a user wants to enter a particular letter [13]. If this time is too long the user will enter letters slowly, and if the dwell time is short there will be more frequent typing errors. Figure 4 shows a system that uses a QWERTY keyboard to enter text using the gaze.

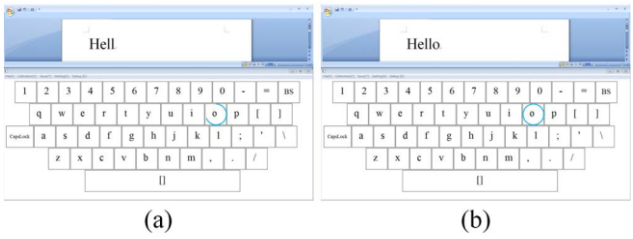



Figure 4. Text entry by using eye gaze and QWERY virtual keyboard [12]

When the user focuses his gaze on the letter he wants to enter, a circle is drawn around the desired letter (Figure 24 - a). If the user's gaze remains focused on the letter during the period corresponding to the dwell time, the letter is rounded off completely and accepted as an entry (Figure 24 - b).

The paper [14] describes a system that enables the use of the QWERTY interface, with integrated letter prediction. Namely, when the user enters letters, the system predicts the letters that the user would enter next offering him a set of possible letters. The set of assumed letters is highlighted by rounding in yellow in order to make the assumed letters stand out from the others and thus speed up the eye's focus on those letters. Figure 5 shows the letter prediction system.


Figure 5. Text input with letter prediction [14]

In addition to the QWERTY interface, there is a Dasher interface that is used to enter text using eye movements. Dasher is a typical text entry interface that does not require dwell time to recognize a character. It is known as a part of the GNOME software in Unix systems. Figure 6 shows the layout of the Dasher interface.

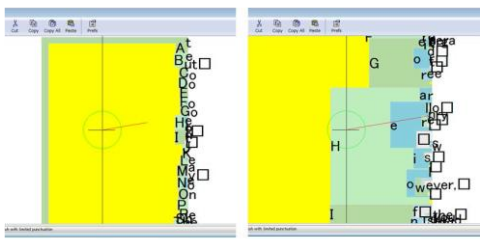



Figure 6. Dasher interface for eye gaze text entry [15]

In the Dasher interface, the letters are arranged vertically on the right side of the window in alphabetical order (Figure 4 - a). When the user focuses his gaze at the letter, the letter is magnified and moved toward the center of the window. After the letter crosses the centerline of the window, it is accepted for entry (Figure 4 - b).

Eye-controlled text entry system [16] is an approach towards a calibration-free eye-based text entry which is suitable for public displays. The system combines a two-stage interface concept with interaction designed specifically for a calibration-free approach using smooth pursuit movements. The detection mechanism used is related to the approach used in the study made in [17]. The system's interaction is designed to provide a calibration-free application which will make use of the smooth pursuit eye movements and its characteristics [17].

## 4. CONCLUSION

The field of research of the natural human-computer interaction is topical thanks to the constant advancement of technology. Eye-tracking is one of the ways to realize a natural user interface which helps people to use computers more simply and easily.

The paper reviews systems that enable human-computer interaction through eye-tracking. Such systems are divided into two groups, i.e. pointing devices and text entry devices. The paper presents examples of the usage of these devices in the implementation of natural user interfaces. This paper presents a brief overview of the field of natural interaction based on eye-tracking and as such represents the foundation for further research in this field.

## ACKNOWLEDGEMENTS

This paper is part of the project Application of multimodal biometrics in identity management, funded by the Ministry of Education and Science of the Republic of Serbia, within the project number TR-32013.

## REFERENCES

[1] D. Wigdor, D. Wixon, „Brave NUI world: designing natural user interfaces for touch and gesture“, Elsevier, 2011.

[2] H. Drewes, „Eye gaze tracking for human computer interaction“, Doctoral dissertation, lmu, 2010.

[3] T. E. Hutchinson, K. P. , White, W. N. Martin, K. C., Reichert, L. A. Frey, „Human-computer interaction using eye-gaze input“, IEEE Transactions on systems, man, and cybernetics, 19(6), 1527-1534, 1989.

[4] M. Mehrubeoglu, L. M. Pham, H. T. Le, R. Muddu, D. Ryu, „Real-time eye tracking using a smart camera“, In 2011 IEEE Applied Imagery Pattern Recognition Workshop (AIPR), (pp. 1-7), IEEE, 2011.

[5] A. Bhoyar, S. Sahu, P. Padwekar, „Eye tracking mouse: people with severe disabilities“, In Proceedings of the 20th IRF International Conference, Pune, 2015.

[6] R. Ramesh, M. Rishikesh, „Eye Ball Movement to Control Computer Screen“, J Biosens Bioelectron 6: 181, 2015.

[7] S. S. Wankhede, S. A. Chhabria, R. V. Dharaskar, „Controlling Mouse Cursor Using Eye Movement“, In Special Issue for National Conference on Recent Advances in Technology and Management for Integrated Growth (Vol. 2013), 2013.

[8] H. Drewes, A. Schmidt, „Interacting with the computer using gaze gestures“, Human-Computer Interaction–INTERACT 2007, 475-488, 2007.

[9] H. Istance, A. Hyrskykari, L. Immonen, S. Mansikkamaa, S. Vickers, „Designing gaze gestures for gaming: an investigation of performance“, In Proceedings of the 2010 Symposium on Eye-Tracking Research & Applications (pp. 323-330), ACM, 2010.

[10] N. Bee, E. André, „Writing with your eye: A dwell time free writing system adapted to the nature of human eye gaze“, In International Tutorial and Research Workshop on Perception and Interactive Technologies for Speech-Based Systems (pp. 111-122), Springer, Berlin, Heidelberg, 2008.

[11] J. O. Wobbrock, J. Rubinstein, M. W. Sawyer, A. T. Duchowski, „Longitudinal evaluation of discrete consecutive gaze gestures for text entry“, In Proceedings of the 2008 symposium on Eye tracking research & applications (pp. 11-18), ACM, 2008.

[12] R. J. Jacob, „What you look at is what you get: eye movement-based interaction techniques“, In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 11-18), ACM, 1990.

[13] J. Pi, B. E. Shi, „Probabilistic adjustment of dwell time for eye typing“, In 2017 10th International Conference on Human System Interactions (HSI) (pp. 251-257), IEEE, 2017.

[14] I. S. MacKenzie, X. Zhang, „Eye typing using word and letter prediction and a fixation algorithm“, In Proceedings of the 2008 symposium on Eye tracking research & applications (pp. 55-58), ACM, 2008.

[15] Hands-free computer access using Dasher. (2013, June). Accessed on 10.06.2020. Available on: https://bltt.org/dasher/

[16] Y. Abdrabou, M. Mostafa, M. Khamis, A. Elmougy, „Calibration-free text entry using smooth pursuit eye movements“, Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications, 2019.

[17] Presage. [n. d.]. Presage. Accessed on 11.06.2020. Available on: https://presage.sourceforge.io

# 7.

# Management and Information Systems

# HOW TO LEAD YOUR ORGANIZATION IN TIMES OF CRISIS TO THE PLACE WHERE KNOWLEDGE MEETS CHANGE

Milan Šmigić, CPM, smigicm@cpm.rs
Miroslav Ćurčić, Hiposistem, curcicmiroslav@gmail.com

**Abstract:** *In these challenging times, when change is the only thing constant, making and leading changes in the organization would be the only way to adapt, especially now that every business is competitive enough in maximizing its resources to survive globalization and the COVID-19 pandemic. All notable change is often complicated and begins in oneself as it requires internal mastery first to lead others successfully. One useful tool in leading change is utilizing the awareness, desire, knowledge, ability, and reinforcement (ADKAR) model as a change management process. This framework will help change management leaders implement activities that will produce successful individual and organizational changes. Specifically, knowing to change and change is essential in acting and adapting to new systems, processes, and responsibilities. This paper will provide some cases to show the importance of the ADKAR model in this challenging time.*

**Keywords:** *Change, ADKAR model, Awareness, Desire, Knowledge, Ability, and Reinforcement.*

## 1. INTRODUCTION

Change is inevitable and constant in this time of crisis. Managing change is the process, techniques, and tools applied in helping individuals adopt and realize change to achieve organizational goals. It requires two perspectives: the individual change management, which is the understanding of how members experience change, and the organizational change management in which a team implements strategies to support individual change (Prosci n.d., para. 5).

Every organization must be capable of effectively responding to change, and formulating strategies alone is not as effective in achieving sustainable results. What matters is how these organizational strategies are implemented through effective tools such as the ADKAR model (Goyal and Patwardhan 2018, p. 297). Prosci, a US research organization, has developed this model through a 14-year study of 900 organizations all over 59 countries (Angtyan 2019, p. 179).

This model is based on the best practices in the change management that provide an easy-to-use framework for everyone in the organization. It is focused on driving activities that impact individual change to achieve organizational results with clear delivery of goals and measurable outcomes for change through a common change language that allows all members of the company to discuss change altogether (Prosci n.d., para. 3).

In this model, change concerns not only the organization as a whole but also of its members. Its process is rooted in successfully facilitating change with one person (Prosci n.d., p. 3).

Individuals will undergo step by step activities as their successful journey to change through the following phases (Prosci n.d., p. 5):

Using the ADKAR Model with Traditional Change Management Activities

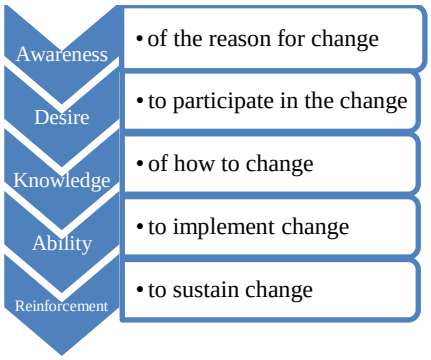



*Figure 1: Prosci (n.d.); The Prosci ADKAR model*

In the above figure, awareness is the result or desired goal after the leader communicates an organizational change. Desire comes to the surface as a result of the leader's sponsorship or resistance management. Knowledge can then be acquired through coaching and training. Ability is the outcome of additional practice, coaching, and time. Lastly, reinforcement is recognizing successful change, the goal of adoption measurement, and corrective actions (Prosci n.d., p. 5). This framework is useful for planning and executing change management processes as leaders will quickly identify gaps or change barriers in each phase (Prosci n.d., p. 6).

The ADKAR model can be utilized in the following:

- Creation of change management plan for employees
- Employee assistance in transitioning through change
- Development of action plan for professional and personal advancement during organizational change
- Diagnosis of employee resistance to change (Prosci n.d., p. 6).

Leaders can use the above list as a guideline to maximize the use of the model and to have a thorough understanding of the possible gaps in their change management processes. With these, leaders can effectively address the identified barriers, provide coaching assistance to their people, and respond effectively in improving their organizational change success (Prosci n.d., p. 6).

As change can be successful if implemented on both the business or project side and the people side of change, the following shows a common purpose of attaining positive outcomes:

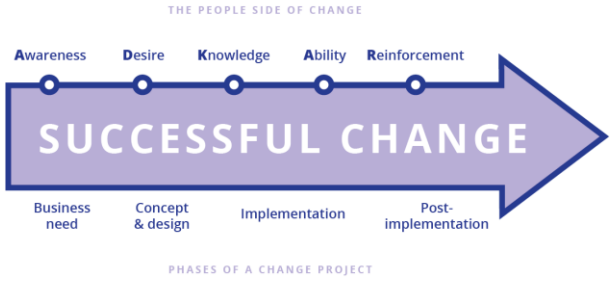



*Figure 2: Prosci (n.d.); Framework of Change Initiative*

Notice that change matures on both dimensions simultaneously, and each phase of the ADKAR model complements the business or the project management and change management process (Prosci n.d., p. 6).

The following can be used by leaders or project managers as standard steps to take in managing a change project:

1. Identify the business need
2. Define the project concept, objectives, and scope
3. Design the solution (new systems, processes, or structure)
4. Develop new systems and processes
5. Implement the solution (Prosci n.d., p. 7).

Leaders may note that after change implementation, a post-implementation or evaluation of the change process is recommended to take. This is necessary for analyzing what worked, what could be done differently or improved, and what can be adapted to future business changes.

Taking into consideration the two dimensions, it is recommended to scrutinize each step of the ADKAR model.

### 1.1 Awareness

To better understand the need for change is to answer the question: Why? Individuals should know the nature of change, why it is being made, and the risks that involve change. It is essential that leaders highlight the awareness of the reason for the change, and not merely that a change is happening (Prosci n.d., p. 3)

Awareness is the first step to managing change because a lack of awareness is the primary source of the team members' resistance. Leaders should always consider answering their employees' silent question of "what is in it for them?". Unable to build awareness or ignore or overlooked, resistance might increase, there will be slow progress toward change, and worst, a deducted return on investment (Prosci n.d., p. 4).

Below are the recommended techniques in building awareness:

- Communicate effectively
- Effective sponsorship
- Managers and supervisors coaching
- Easy access to business information

It is not about sharing information in creating awareness but also about regular interactions and feedback from employees through effective two-way communication. This must include the proper context of the message, the appropriate communicator, correct timing, and communication channels such as meetings, email, newsletters, and other tools (Prosci n.d., p. 6).

Effective sponsorship refers to the person who is the sponsor of change. He should be visible and active during the change process and serve as the communicator of change who allows direct communication, where employee feedback is being collected (Prosci n.d., p. 7).

There should be a shared purpose for change, and an aligned vision should be communicated to facilitate organizational learning that is needed for change (Senge et

al. 1994). The managers should first be coached and understand the reason for a change to do the same to their team members easily.

Lastly, having readily accessible information about the company's market standing and other factors would empower all employees. As they stayed informed, increased and consistent awareness among all levels is attainable (Prosci n.d., p. 8).

In contrary to the above, there are certain resistance factors that leaders should overcome:

- A member's view of the current state
- How an employee perceives the problem
- Sender's credibility
- Misinformation or rumors circulation
- Reason for change debatability (Angtyan 2019, p. 180).

Dialogues built with trust, respect, and openness are recommended to understand others better (Senge et al. 1994). This must include providing the opportunity and time for employees to process new information, give feedback, and raise questions (Prosci n.d., p. 10). Messages should be tailored according to whom it should be delivered with the correct person to send the correct message and reason for the change to attain increased credibility (Prosci n.d., p. 11). Correcting misinformation is a must, and clarity can be communicated if there is transparency from the very start.

**1.2 Desire**

Desire, as the second element of the ADKAR model, signifies the stimulus and choice to engage and support change (Angtyan 2019, p. 180). This element is personal; thus, the leader's strategies should match their team's motivators and expand their influence as a leader (Prosci n.d., p. 4).

Planning how to influence the employee's desire is more accessible by being aware of the following factors:

- Nature of change and its impact on employees
- Individual, organizational perception
- An employee's situation
- Personal motivation and values (Angtyan 2019, p. 180).

Considering the above list, change leaders' words and actions have a tremendous influence on the employee's desire to support change (Prosci n.d., p. 12). Leaders can maximize desire building through the following tactics:

- Sponsor change effectively among peers and employees
- Convert managers to change leaders
- Resistance anticipation and risks assessment
- Employee engagement
- Incentive programs alignment (Prosci n.d., pp. 7-12).

The above are the proactive steps that change sponsors and managers can focus on to create engagement and energy around the change and minimize resistance. It is vital to re-visit the awareness and the desire phases combined with the reinforcement of constant communication before proceeding to the Knowledge phase (Prosci n.d., p. 12).

**1.3 Knowledge**

Knowledge represents how to implement business change through educational methods, dialogues, training, forums, and coaching (Angtyan 2019, p. 180). The following areas are in need to change as well:

- Skills and behavior
- Systems, processes, and tools
- Responsibilities and roles (Prosci n.d., p. 4)

The above were grouped into two categories. First, skills and behavior are under the knowledge of how to change. This highlights what the employee needs to do during the change transition. The other category is the knowledge of how to perform in the future state effectively. It includes information on new responsibilities and roles and the education and training on how to use new systems, processes, and tools (Prosci n.d., p. 5).

Listed below are several factors that will affect knowledge phase achievement:

- Employee's capability to learn
- Person's current knowledge base
- Availability of educational and training resources (Prosci n.d., pp. 5-7).

Individuals have different bits of intelligence that require appropriate learning styles. Employees' hands-on application of learning to a real-life situation is an effective way of learning. Also, most companies outsource professional trainers and instructors to support certain learning activities. It is required to plan for a particular duration and effort in developing the required knowledge (Prosci n.d., pp. 5-7).

The following are the best learning practices to be adopted:

- Job aids
- Coaching one-on-one
- Educational programs and training
- Forums and groups (Prosci n.d., pp. 8-10).

Combining the above activities enables employees to learn in the most effective way to develop a strong knowledge foundation (Prosci n.d., p. 11). Since learning is an ongoing process, leaders must give a team learning ample time for the knowledge to be absorbed and personal mastery to be attained. This way, knowledge meets the desired changes.

### 1.4 Ability

Ability is simply transforming knowledge into action or theory into practice. It is implementing change that needs to be supported through ample time, coaching, practice, and feedback (Prosci n.d., p. 3).

Here are the factors that affect an individual's ability to implement change:

- Habit
- Psychological blocks
- Intellectual or physical capabilities
- Priorities and time
- Recourses availability (Prosci n.d., pp. 7-9).

Patience, time, and leader's support are required to overcome the barriers mentioned above. Change leaders can provide the following tactics to build abilities:

- Manager's daily involvement
- Subject-matter experts' accessibility
- Training hands-on exercises
- Performance and adoption monitoring (Prosci n.d., pp. 5-6).

Building ability requires practice and hard work from the leaders and the individuals who are required to perform differently. It is manifested by showing actions that allow a genuine change in both the employee and across all organizational levels (Prosci n.d., p. 10).

### 1.5 Reinforcement

Once a change is done, companies move on to the next goal without reinforcing the changes made. An ongoing sustainable development must be done to maximize and achieve the expected results over time (Prosci n.d., p. 3). Some of the factors that influence reinforcement are:

- Significance of reinforcement
- Demonstrated achievement and progress association
- Absence of negative consequences
- Accountability mechanisms (Angtyan 2019, p. 181).

These effective reinforcement influences must ensure that changes will stay and that employees do not return to their old inefficient ways. It is recommended for leaders to build momentum during the conversion from the current to the desired future state and to develop a history of successful and sustained change. A leader must utilize rewards, recognition, measuring performances, taking corrective actions, and providing positive feedback (Prosci n.d., p. 3; Angtyan 2019, p. 181).

The following are the best tactics for reinforcement building:

- Rewards
- Recognition and celebrations
- Employees feedback
- Performance management and audits systems
- Accountability systems (Prosci n.d., pp. 7-10).

Performance audits should analyze the employees' percentage of who engage with the change, those struggling to adapt, and the possible factors if there are low adoption levels. Whenever a change has been successfully implemented, recognitions and celebrations of progress are recommended to create enthusiasm and positivity around the change. Also, daily accountability means transferring ownership to the operational managers and leaders, who will assume the responsibility for the change's ongoing success (Prosci n.d., pp. 9-10).

## 2. CASES USING THE ADKAR MODEL

### 2.1 United Kingdom Government's ADKAR Approach to COVID-19 during the Lockdown

With the current global pandemic due to COVID-19, the majority of the countries were affected, and some governments have effectively managed changes to keep their citizens at home during their implemented lockdown.

The following discusses the ADKAR model in action during UK lockdown as examined by Amelia Beresford of Aimii, a software company in England:

- Awareness – there was daily communication of relevant information about the virus with clear descriptions of the government-imposed changes that impacted the UK residents. The prime minister as well addressed the nation to sponsor the changes.
- Desire – People were motivated and showed support by staying at home to protect their families and others, including their National Health Service.
- Knowledge – The government and the internet are full of information on how to change each citizen's behavior towards sanitation, social distancing measures, related precautionary actions, about each role and responsibilities, and how they can help their government fight and overcome this pandemic through the lockdown.
- Ability – Citizens comply with the government's preventive measures while there was increased funding to support businesses. People stepped up to volunteer, and businesses are in return, extending their help to those in need.
- Reinforcement – UK government continued to communicate through different ways via online and offline channels and had granted additional authority to their police officers to fine those who breached their lockdown procedures (Beresford n.d., para. 7).

Using the ADKAR model of change in this scenario might have prevented many people from being infected with the virus.

### 2.2 Using ADKAR Change Model to Navigate Texas Hospitals Staffing Changes During the COVID-19 pandemic

During the start of the COVID-19 outbreak, Texas hospitals experienced a sudden increase in patient numbers. A safe staffing protocol challenged them; therefore, they have responded using the ADKAR change model to guide their transformation from primary to team nursing (Balluck, Asturi, & Brockman 2020). The following are the guide questions for their change leaders and action steps for them to take:

**ADKAR Change Management at Texas Health Resources**

*Table 1: Balluck, Asturi, & Brockman (2020); ADKAR Change Management at Texas Health Resources*

| | Questions to Ask Yourself | Action Steps to Take |
|---|---|---|
| *A Awareness* | What is the nature of the change?<br>Why is the change needed?<br>What is the risk of not changing? | Draft effective and targeted communications<br>Share the why and the vision<br>Provide ready access information |
| *D Desire* | What's in it for me (WIIFM)?<br>How is this a personal choice<br>Will I decide to engage and participate? | Demonstrate your commitment<br>Advocate for change<br>Engage influencers to foster employee participation and involvement |
| *K Knowledge* | Do I understand how to change?<br>Where can I be trained on new processes & tools?<br>How do I best learn new skills? | Provide effective training with the proper context<br>Facilitate education for, during, and after the change<br>Create job aides and real-life applications |
| *A Ability* | Am I demonstrating the capability to implement the change?<br>Am I able to achieve the desired change in performance or behavior? | Facilitate coaching by managers, supervisors, and subject matter experts<br>Offer hands-on exercises, practice and time<br>Eliminate any potential barriers |
| *R Reinforcement* | What actions can I take to increase the likelihood that this change will continue? | Celebrate successes individually and as a group<br>Reward and recognize early adopters<br>Give feedback on performance and accountability |

Balluck, Asturi, and Brockman (2020) reported that the above guideline of the ADKAR change model provided their Texas Health Resources nurse leaders with the tools to explain, to communicate better, and to train their care team members as they devise the following changes simultaneously:

- Awareness – The "why" behind this change was communicated extensively to their nursing team, which included meetings, e-mail, leader rounding, and weekly webinars.
- Desire – The healthcare body reported that their reason to change is that it was their natural response and part of emergency planning. This concerns the expected lesser number of nurses, a more significant number of patients with COVID-19, and the possibility of the nurses becoming ill as well.
- Knowledge – Their entire nursing team understands that organizational change includes individual change. The need to transform from primary nursing to team nursing had greatly affected them. Team nursing is a type of care delivery approach where a team of clinicians shares responsibility for a group of patients. The staff communicated that it was a relief for them that their leaders had a plan to manage the outbreak.
- Ability – With the help of ADKAR change management theory, the Texas health body had effectively implemented a change in the times of

uncertainty when there are stressful environments and new complex processes.

- Reinforcement – As they realized the benefits and desired outcomes of the implemented changes, there is continuous education through electronic communication and staff meetings to share new developments and information and provide a consistently supportive leadership role. There is also an evaluation to acquire feedback and monitor each member's morale level as they identify barriers crucial to sustaining the necessary change (Balluck, Asturi, & Brockman 2020).

Keeping the ADKAR model in mind, the Texas nursing units have kept their patients' safety while maintaining their nurses' satisfaction as a priority. Responding using the model to the changes brought by the COVID-19 pandemic has been effective for them.

### 2.3 Center for Project Management's (CPM) ADKAR Strategy for Organizational Change During the COVID-19 Outbreak

As the outbreak greatly affected the global economy, businesses are pushed to respond by implementing practical yet creative solutions to guide their organization in moving forward.

The CPM Serbian based training and consulting company has implemented a three-month rollout plan using enterprise CRM (Customer Relations Management), PPM (Portfolio Project Management), and BPM (Business Process Management) tools. These tools have helped them improve information sharing, increased productivity, strengthened communication, and achieved better collaboration with customers. In making these happen, CPM has used the following ADKAR strategy (Šmigić & Ćurčić, 2020):

- Awareness – With the COVID-19 situation, CPM management has assessed the situation and had identified the implications to their organization. They have formulated the rollout plan of enterprise tools that will serve as their flexible operating model. They have strictly identified that this strategy follows their company and societal values. Also, their CEO had sponsored the changes of the internal collaboration program. The organization members were provided with better information on issues through their Human Resources department which established clear goals, knowledge, and collaboration objectives. Their PMO also has efficiently created metrics for platform use through the business unit, organization, and region with employees having easy access to key and only appropriate resources.
- Desire – The change had greater employee participation as the CPM Company promotes a culture of communication, safety and responsibility, embracing daily information sharing. They have identified that it is essential that their employees are eager and open to changes in their work habits, processes, and that this flexibility should reflect throughout their organization structure.
- Knowledge – Their CEO has identified which areas could benefit from their increased collaboration and have chosen online software platforms to meet its needs. Their project managers guaranteed that collaboration is utilized in improving employee work processes in demonstrable ways. They have designed helpful ways to highlight what their employees need to do during the change transition through real-time posting and sharing of comments on an action item, used Project Kanban Boards to streamline team collaboration, and kept team members informed through regular project feeds.
- Ability – Through their ADKAR change strategy, they have successfully executed the identified corporate crisis strategy through knowledge management processes. Their change leaders are daily involved through performance and adoption monitoring using the creation of project discussion boards accessible to key project team members, connecting, and learning together using social media platforms, and shared calendars for meetings, deadlines, and customer oriented on-line events.
- Reinforcement – The CPM management anticipated that its enterprise-wide collaboration entails long-term dedication and commitment. They have outlined to continually seek employee feedback and to monitor and measure their processes and make necessary adjustments. They have created accountability systems to sustain the changes through effective governance by a structured approach of posting announcements to keep their teams updated, creating notifications and alerts for real-time information, scenario modeling, and sharing of contacts for teams connectivity. By regular use of on-line white-boards CPM teams have also measured their change management capabilities and enable better collaboration through the visibility of their projects, programs, portfolio and resource

utilization. Also, that has increased their efficiency in planning, scheduling, and control over deliverables, costs, and benefits management.

Through the adaptation of the ISO, PMI and ADKAR bst practices, the CPM company resulted in a real-time improvement of its people and process performances in time of unprecedented global health crisis.

## 3. CONCLUSION

The ADKAR model is proven to be an effective change management tool in leading organizations in times of crisis. Combined with ISO process management, PMI leadership skills and Change Management techniques and best practices it allows companies to improve performance and select preventive and corrective actions. The most important block to performance improvements is the Knowledge phase, wherein individuals understand that to attain the desired change, they need to implement changes in their skills, behaviors, responsibilities, roles, and current systems, processes, and tools. It is the state where the whole organization meets change, and therefore support is required both from employees and change leaders in providing training, education, and effective communication vital in team learning to attain the organization's desired change during a crisis.

## REFERENCES


Angtyan, H (2019) 'ADKAR model in change management', *International Review of Management and Business Research*, 8(2), pp. 179-181. DOI:https://www.irmbrjournal.com/papers/1560753273.pdf

Balluck, J, Asturi, E, & Brockman, V (2020) 'Use of the ADKAR® and CLARC ® change models to navigate staffing model changes during the COVID-19 pandemic', *Nurse Leader*. DOI:https://doi.org/10.1016/j.mnl.2020.08.006

Beresford, A (n.d.) 'What can we learn from change management during COVID-19?', Aiimi, viewed 01 October 2020, <https://www.aiimi.com/insights/what-can-we-learn-from-change-management-during-covid-19>

Goyal, C, & Patwardhan, M (2018) 'Role of change management using ADKAR model: A study of the gender perspective in a leading bank organization of India', *International Journal of Human Resources Development and Management*, 18(3/4), p. 298. DOI:10.1504/IJHRDM.2018.093442

Prosci. (n.d.) *The Prosci ADKAR model: A goal-oriented change management model to guide individual and organizational change.* Prosci, Inc.
Part 1, *"Awareness: How to effectively build awareness for change."*
Part 2, *"Desire: How to positively influence a person's desire to embrace change."*
Part 3, *"Knowledge: How to effectively build knowledge in individuals."*
Part 4, *"Ability: How to foster ability to implement a change."*
Part 5, *"Reinforcement: How to sustain a change."*
<https://empower.prosci.com/the-prosci-adkar-model-ebook-bundle>

Prosci. (n.d.) In *The Prosci ADKAR model: A goal-oriented change management model to guide individual and organizational change* (pp. 3-11). Prosci, Inc., viewed 30 September 2020, <https://empower.prosci.com/the-prosci-adkar-model-ebook-bundle>

Prosci. (n.d.) 'What is change management and how does it work?', Prosci.com, viewed 30 September 2020, <https://www.prosci.com/resources/articles/the-what-why-and-how-of-change-management>

Prosci. (n.d.). 'What is the ADKAR model?', Prosci.com, viewed 30 September, <https://www.prosci.com/adkar/adkar-model>

Senge, PM, Kleiner, A, Roberts, C, Smith, B, & Ross, R (1994) *The fifth discipline fieldbook: Strategies and tools for building a learning organization.* New York: Doubleday.

Šmigić, M., & Ćurčić, M. (2020). How to lead your organization in crisis to the place where knowledge meets change? International Conference and Exhibition. Aranđelovac.

# INTANGIBLE INVESTMENTS IN MARKETING DIGITAL COMMUNICATIONS IN THE SERBIAN BANKING SECTOR

Maja Cogoljević, Faculty of Business Economics and Entrepreneurship, maja.cogoljevic@vspep.edu.rs
Tamara Vesić, Faculty of Business Economics and Entrepreneurship, tamara.vesic@vspep.edu.rs
Vladan Cogoljević, Faculty of Business Economics and Entrepreneurship, vladan.cogoljevic@vspep.edu.rs

**Abstract:** *Marketing digital communications are revolutionizing all aspects of a country's business and economic life. Modern banking in Serbia has entered the process of transformation with great strides, especially banking management and business technology and communication with users of banking services. The aim of this paper is to research the level of implementation of modern marketing business and communication channels in Serbian banks, as well as their impact on business results by applying the Pearson correlation model.*

**Keywords:** *intangible investments, digitalization, market communications, banking sector*

## 1. INTRODUCTION

In modern business conditions the changes in the environment, which are manifested through deregulation of financial business, strengthening of competition in financial services and development of information systems, increase business risks both on the domestic and international markets. The banks can achieve the main business goals (financial profit, growth, development, higher market share, avoiding risk) only with maximum adaptation to change, which is most effectively achieved by strategic management based on marketing principles, that are concentrated on meeting the needs of consumers - clients. Business banks must be market-oriented, if they want to provide existence, growth, and development.

Modern banking has entered the process of transformation with great strides, especially banking management and business technology. Traditional banking becomes less important when efficient functioning of the financial system is in question. The processes of transformation in the financial sphere brought important changes in business orientation and banking operations, which are reflected in [1]:

- Accepting banking marketing
- Crediting with a variable interest rate
- Project and corporate financing of the economy
- Credit securitization
- Electronic banking and
- Supervision – monitoring

The aforementioned changes change the business nature and operation of business banks, their position among competitors, way, number, and offer of financial products and services to the clients.

In the focus of its operation, market-oriented bank has the present and future needs of its clients, as well as wishes and requests, towards which it needs to direct its activities and operations. The quality of financial service depends on the interest of financial institution to help clients and effectively respond to their needs, and direct contact with the clients represents the most important aspect of effective communication with the consumers [2].
In order to increase the recognizability and to build positive atittude among clients, the banks use integrated channels of marketing communication.

## 2. LITERATURE REVIEW

On the basis of official indicators, as well as on the basis of periodical financial and accounting reports, the analysis of the movement of balance sheet and income statement indicators are performed, as well as comparison of balance sheet and income statement positions (ratio numbers), all for information support of internal decision-making process of internal or external users [3]. As the nature of business of banks is essentially different from the business of companies in nonfinancial sector, the financial reports and their stricture are different as well, and the content must reflect all the specifities of banking business [4]. Often there is dilemma which banks are more successful. Are those which put the accent on liquidity, by permanently and carefully controlling their operating costs, in order to put them on the lowest level, or are more successful those banks which put the accent on the profitability, and strive to achieve the best possible returns for the owners of the invested funds [5]. Up to this point, no consensus has been achieved on which performance appraisal system is better and whether primacy should be given to the concept of profitability or efficiency. Furthermore, the banks are facing the market trends which put pressure on their results as well, and which, among other things, include low-interest rates and regulatory constraints as well [6]. Most banks has already

conducted traditional cost reduction measures, but very few of them has performed business models and internal processes changes, which will be the next step in cost rationalization process [7]. Digitalization and accompanying process automation will be crucial in further cost reduction, with the expectation that in the long run digitalization may lead to a 30% to 40% drop in costs [8]. Lending to manufacturing SMEs is not profitable for banks due to the high risk of return on funds, high administrative and request processing costs, and because SMEs usually do not have adequate accounting records, financial statements and business plans [9]. In order to see the success of the business as accurately as possible, experts from the banking sector, mathematicians and economists-analysts have developed and designed numerous indicators [10].

## 3. RESEARCH METHODOLOGY

The basis for research in this paper is publicly announced data of business banks, which operate in the Republic of Serbia, both on their websites and on the site of the National Bank of Serbia. The largest number of data was collected from the Quarterly Reports relating to analyzes and reports of the banking sector operating in the Republic of Serbia with the aim of transparency of banks' business in Serbia [11-21], as well as from individual balance sheets of the observed banks. The liquidity indicator processes are used as dependent variables, while intangible investments of the entire banking sector at the end of the fourth quarter in the period 2014-2017 and the third quarter for 2018 are independant variables. The general (current) liquidity indicator is calculated as the quotient of working capital and short-term liabilities.

The banking sector of Serbia has significant surpluses of liquid assets in a longer period of time, if the reference values of liquidity indicators are taken into account. The average monthly indicator of banks' liquidity at the end of the first trimester of 2019 is 2,18 and it is twice as high as the regulatory minimum of 1,0 [22]. In order to determine the existence of a relation between the analyzed indicators, the correlation coefficient in Microsoft Excel Software is applied. In this paper we used Pearson correlation coefficient, which is calculated according to next formula:

$$r = \frac{\sum_{i=1}^{N}(x_i - X) - (y_i - Y)}{\sqrt{\sum_{i=1}^{N}(x_i - x)^2 \sum_{i=1}^{N}(y_i - y)^2}} \quad (1)$$

The elements of the formula (Pearson correlation coefficient): N is the indicator in the ratio; Yi indicates independent indicators, and Xi indicates dependant indicators; x and y are means (of relevant indicators).
Explaination of Pearson correlation values [23]:

- +/- 0 - +/- 0.2 there is no ratio,
- +/- 0,21 - +/- 0,4 weak ratio,
- +/- 0,41 - +/- 0,6 average ratio,
- +/- 0,61 - +/- 0,8 strong ratio,
- +/- 0.81 - +/- 1 very strong ratio.

## 4. RESEARCH RESULTS

By correlating liquidity and mean of the item "intangible investments" from the balance sheet of the observed banks, the results were obtained as in the following table.

Table 1. Correlation of the intangible investments and liquidity

| Banking sector | ‘18 | ‘17 | ‘16 | ‘15 | ‘14 | ‘13 | ‘12 | ‘11 |
|---|---|---|---|---|---|---|---|---|
| Correlation coefficient | 0,66 | 0,59 | 0,52 | 0,43 | 0,20 | 0,24 | 0,55 | 0,499 |

Source: Author’s research

The correlation coefficient increases during the observed years, from which we can conclude that the amount invested in intangible investments increases from year to year. The amount of 0.66 in 2018 indicates a strong relation between the variables. Thus, the variables are very positively correlated. We have researched which banks in Serbia use different maketing communications as well, and the results can be seen in the table 2.

Table 2. Digital bank services in Serbia

| Bank | E/m-banking | Cards | Other ways of communication |
|---|---|---|---|
| Addiko bank | + | + | Addiko Chat Banking on Viber |
| AIK bank | + | + | |
| API bank | + | + | |
| Banca Intessa | + | + | IPS QR kod |
| Banka Poštanska štedionica | + | + | |
| Bank of China Serbia | + | + | |
| Credit Agricole | + | + | IPS QR kod |

| | | | |
|---|---|---|---|
| Direktna banka | + | + | IPS QR kod |
| Erste banka | + | + | IPS QR kod |
| ExpoBank | + | + | |
| Eurobank | + | + | |
| Halkbank | + | + | |
| Jumes banka | + | + | |
| Komercijacna banka | + | + | KomBank Trader, KOMeCentar, Distance help |
| Mirabank | + | + | |
| Mts banka | + | + | |
| NLB banka | + | + | E banking group |
| Opportunity banka | + | + | |
| OTP banka | + | + | |
| Procredit banka | + | + | 24h self zone |
| Raiffeisen banka | + | + | REA- electronic assistant mobi cash |
| Sberbanka | + | + | Smast cash credit |
| Societe Generale banka | + | + | |
| Srpska banka | + | + | |
| Telenor banka | + | | Virtual bank |
| UniCredit banka | + | + | |

Source: Author's research

Keeping pace with modern technologies, banks are also market players who have to adapt to market changes and trends [24]. From the table we can see that all banks on the Serbian market already offer their customers a system for electronic payments using smartphones or computers. Within the same, users can apply for many products of banks such as various, usually short-term, loans, current account overdrafts, change of PIN code, etc., which increases the range of products that can be offered in a modern, electronic way. Some banks have also introduced additional communication channels, such as Addiko Bank, which was the first to place communication via the Viber platform in 2017, through which we can pay bills according to previously created templates, transfer funds, schedule a meeting with a personal banker, etc. Raiffeisen Bank went a step further and created a digital assistant, the basis of a technology based on artificial intelligence called "Rea". Rea uses different communication platforms, like Facebook, Viber etc. She is available 24 hours a day, 7 days in week. The first virtual bank was Telenor Bank, which was sold to an investment fund in 2019 and changed its name to Mobi Bank. Mobi Bank strives to become the leading provider of mobile and online financial services in Serbia. Mobi Bank is the first bank in the region where banking is completely different - completely mobile.The IPS QR code is an innovation that was introduced at the beginning of 2020 and represents "instant payments of Serbia" that can be made via an application on the phone by scanning the NBS IPS QR code. Merchants and banks have recognized as the biggest advantage of this method of payment low transaction processing costs and the current transfer and availability of funds in the merchant's account. That is the advantage that instant payments have in relation to payment cards, according to the National Bank of Serbia. At the time of writing this paper, the banks that had introduced the IPS payment system by then are listed. We assume that the trend is for a large number of banks to introduce this possibility.

## 5. CONCLUDING REMARKS

Modern business conditions impose the use of new information technologies as a basis for the survival and development of every business entity. The banking sector of Serbia is increasingly exposed to competitive business conditions that are global in nature and impose the need to use digital marketing tools for the sale and promotion of related banking products and services.

Today, digital marketing is an imperative for successful communication with consumers. Although there is insufficient awareness in Serbia that it is necessary to increase investments in this form of marketing strategy, the results of the presented research indicate that the situation is significantly improving. Namely, the digitalization of banking operations is an unstoppable process on the one hand, but also a necessary innovation on the other hand, which affects the market position of the bank. The analysis of the research results indicates that marketing channels of communication and distribution have a great influence on the perception of the quality of banking services. Banks that use multiple sales channels, in order to increase their profitability on the Serbian market, can turn their existing customers into online users by directing them to digital banking. Due to the perfect competition that prevails in the digital market, the banks must be creative and innovative in presenting their products and services, in order to be noticed and favored by clients who are exposed to a large amount of information on a daily basis.

Business success and profitability require many risky activities that do not guarantee success. Only those banks that are willing to invest in innovation, development, ideas and technology can meet the needs of modern clients and ensure stable operations in the long run.

**REFERENCES**

[1] M. Hadzic, "Banking", University of Singidunum, Belgrade, 2018.
[2] A. Djordjevic, V. Marinkovic, "Consumer management: a value-based approach", Publishing Center of the Faculty of Economics, Belgrade, 2019.
[3] G. Knezevic, N. Stanisic, V. Mizdrakovic, "Financial reports analysis", University of Singidunum, Belgrade, 2013.
[4] F. Allen, E. Carletti, D. Gale, "Interbank market liquidity and central bank intervention", Journal of Monetary Economics Vol. 56, Iss. 5, 639-652, 2009.
[5] T. Vesic, M. Gavrilovic, J. Petronijevic, "The influence of liquidity and profitability on the banking sector performances – the example of Serbia", International Review No. 1-2/2019, 75-81, 2019.
[6] A. Berger, C. Bouwman, T. Kick, K. Schaeck, "Bank risk taking and liquidity creation following regulatory interventions and capital support", Journal of Financial Intermediation, Forthcoming, 26 (1): 115-141, 2017.
[7] European Central Bank /ECB/, "Access to Finance in the Western Balkan", Occasion Paper Series No. 197/2017, 2017.
[8] G. Doojav, U. Batmunkh, "Monetary and macroprudential policy in a commodity exporting economy: A structural model analysis", Central Bank Review, Vol. 18, Issue 3: 107-128, 2018.
[9] P. Rose, S. Hudgins, "Management of banks and financial services". Mate Zagreb, 2015.
[10] Banking sector in Serbia, Report fot IV trimester. National Bank of Serbia, Downloaded from the site https://www.nbs.rs/internet/latinica/55/55_4/kvartalni_izvestaj_IV_09.pdf 15.06.2020., 2009.
[11] "Banking operations control", National Bank of Serbia, Downloaded from the site https://www.nbs.rs/internet/latinica/55/55_4/kvartalni_izvestaj_IV_10.pdf 10.06.2020., 2010.
[12] "Banking sector in Serbia", Report for IV trimester. National Bank of Serbia, Downloaded from the site https://www.nbs.rs/internet/latinica/55/55_4/index.html
[13] "Banking sector in Serbia", Report for IV trimester. National Bank of Serbia, Downloaded from the site https://www.nbs.rs/internet/latinica/55/55_4/kvartalni_izvestaj_IV_11.pdf 07.06.2020., 2011.
[14] "Banking sector in Serbia", Report for IV trimester. National Bank of Serbia, Downloaded from the site https://www.nbs.rs/internet/latinica/55/55_4/kvartalni_izvestaj_IV_12.pdf, 04.06.2020., 2012.
[15] "Banking sector in Serbia", Report for IV trimester. National Bank of Serbia, Downloaded from the site https://www.nbs.rs/internet/latinica/55/55_4/kvartalni_izvestaj_IV_13.pdf, 01.06.2020., 2013.
[16] "Banking sector in Serbia", Report for IV trimester. National Bank of Serbia, Downloaded from the site https://www.nbs.rs/internet/latinica/55/55_4/kvartalni_izvestaj_IV_14.pdf, 02.06.2020., 2014.
[17] "Banking sector in Serbia", Report for IV trimester (2015). National Bank of Serbia, Downloaded from the site https://www.nbs.rs/internet/latinica/55/55_4/kvartalni_izvestaj_IV_15.pdf, 02.06.2020., 2015.
[18] "Banking sector in Serbia", Report for IV trimester (2016). National Bank of Serbia, Downloaded from the site https://www.nbs.rs/internet/latinica/55/55_4/kvartalni_izvestaj_IV_16.pdf, 31.05.2020., 2016.
[19] "Banking sector in Serbia", Report for IV trimester (2017). National Bank of Serbia, Downloaded from the site https://www.nbs.rs/internet/latinica/55/55_4/kvartalni_izvestaj_IV_17.pdf, 27.05.2020., 2017.
[20] "Banking sector in Serbia", Report for IV trimester (2018). National Bank of Serbia, Downloaded from the site https://www.nbs.rs/internet/english/55/55_4/quarter_report_IV_18.pdf, 25.05.2020., 2018.
[21] "Banking sector in Serbia", Report for IV trimester (2020). National Bank of Serbia, Downloaded from the site https://www.nbs.rs/internet/english/55/55_4/quarter_report_I_20.pdf, 12.06.2020., 2020.
[22] "Financial sector outlook: Financial systems in the Western Balkans – Present and Future", World Bank Group Finance & Markets, 2016.
[23] S. Jovetic, "Article commentary - Correlation analysis of regional competitiveness indicators – example of the Republic of Serbia by author Darko B. Vukovic", Economic horizons Vol. 16, Br. 2, 161-163, 2014.
[24] D. Garabinovic, S. Andjelic, "The connection between the number of events and the promotional activities of local tourist organizations and hotels on the social network Facebook", Business trends, Sves. 2, No. 14: 23-35, 2019.

# CONTEMPORARY AND INTEGRATIVE APPROACH TO ONLINE EDUCATION

Olja Arsenijević, Institute for Serbian Culture Priština – Leposavić, arsenijevicolja@gmail.com
Jasmina Arsenijević, Higher school of vocational studies for teacher education in Kikinda, arsenijevicjasmina@gmmail.com

**Abstract:** *During 2020 and 2021, educational systems worldwide faced a significant challenge‑finding strategies to halt the spread of the virus. School and university closures globally until May 2020 affected nearly 90% of the world's student population (United Nations, 2020). In order not to lose the academic year 2019/2020, educational institutions at all levels developed an emergency model for online education, adopting the policy "Disrupted Classes, Undisrupted Learning" (Huang et al., 2020) and thus entering a new era of e-learning (Anwar et al., 2021). The general context of this article is the transition of higher education teaching to an online model as a consequence of the global spread of the Covid-19 virus. Since the implementation of online teaching poses significant pedagogical, technological, organizational, and economic challenges, it is important to provide a reflection on its implementation, both its positive and negative aspects. The focus of the research is the online teaching research community, with the theoretical foundation being the CoI (Community of Inquiry) model of quality.*

**Keywords:** *Community of inquiry, effectiveness, satisfaction, advantages, disadvantages, online teaching, higher education.*

## 1. INTRODUCTION

Organizing online higher education courses represents a complex and interdisciplinary undertaking. While some higher education systems and institutions had more experience, having implemented distance learning before the global pandemic, for the majority, this task was more than complex. For those more advanced with prior experience, implementing distance learning was not a stressful and difficult task. Examples include higher education in the United States, the United Kingdom, partially in Asia, and some European countries [1].

Institutions and higher education systems facing this challenge for the first time had to organize an endeavor that had not been tested before, addressing all issues on an ad-hoc basis. On an individual level, teaching staff had to simultaneously undergo training to use technological tools for online teaching, develop online learning materials, and adapt and design the teaching process in an online environment. On an institutional level, faculties were quickly faced with a greater need for IT experts, adequate software and hardware, and good internet infrastructure.

Higher education in Serbia did not escape this challenge. The 2020/21 school year is marked by a partial establishment of balance at the institutional level: some higher education institutions introduced the use of platforms for online teaching (Microsoft Teams, Moodle, Google Classroom, etc.), provided training for teachers to use them, and in some cases, a combined model with live classes. Despite this, the creation and implementation of a long-term strategic approach regarding development, planning, and adaptation of teaching were not possible due to great uncertainty about the epidemiological situation.

On the other hand, "effective online teaching is far from urgent and improvised: it requires a different design from traditional teaching, which often cannot be projected into an online environment" [2]. Developing online teaching that achieves good results and desired effects involves more than just translating in-person teaching into an online environment [1]. Furthermore, experiences show that effective online teaching needs a pedagogical approach that creates a purposeful online learning experience, motivating and engaging students, actively developing knowledge rather than leaving them in a passive position of information recipients [1]. Digital technology is not only a "different medium through which old processes take place; this medium has certain characteristics but also antinomies" that impose a reorganization of work [3].

## 2. CONCEPT OF THE COMMUNITY OF INQUIRY

The practical application of various technological solutions for online teaching and learning over the past few decades shows that organizing online classes is a complex undertaking at both the pedagogical and organizational, infrastructural, economic, and even social levels. This is supported by theories about this multidisciplinary phenomenon, developed based on pedagogical,

psychological, sociological, and technological theories, as well as previous research results and successful online pedagogical practices Garrison, Anderson and Archer [4] , such as the theories of, Anderson [5], Daniela [6], and Buckreus and Ally [7]. Their important foundation consists of learning theories: behaviorism, cognitivism, and social constructivism, often combined with technological approaches for adaptive strategies and personalized learning contexts.

One theoretical model that has gained significant attention in science is the so-called Community of Inquiry (CoI) model in online teaching. It was developed by Garrison, Anderson, and Archer [4] , drawing its roots from the early, progressive concepts of education and knowledge formation by renowned philosophers and founders and theorists of pragmatism.

The concept of the Community of Inquiry was primarily introduced by Peirce and Dewey, explaining the nature of the process of scientific inquiry and knowledge creation. The community of inquiry can broadly be defined as a group of learners engaged in conceptual or empirical inquiry in their search for knowledge. The community of inquiry is defined by a common desire among its members to resolve problems using a scientific attitude to assess evidence and guide action in joint effort and active collaboration. Contrary to the previous understanding of knowledge. development, Dewey and Peirce emphasized that knowledge is implanted in a social context, and its development requires interaction and active investigation. Dewey further projected this onto education, establishing that research and community constitute the essence of educational philosophy and practice, and the experience that leads to learning must include both individual and community interests [8]. Dewey also believed that collaboration that respects the individual enables students to actively construct and confirm meaning [9]. Pierce and Dewey’s ideas were subsequently expanded and applied to the online learning environment, leading to the CoI framework.

A community of inquiry is a theoretical framework for optimally designing online learning environments to support critical thinking, critical inquiry, and discourse between students and teachers [4]. Educational models help educators apply the results of educational research to the practical tasks of designing curriculum and developing and aligning educational experiences to optimize learning Online teaching in which the Community of Inquiry is developed achieves a high level of educational experience that leads to learning through the formation of a community of teachers and students who jointly explore an idea, topic, or area of common interest through research-based dialogue. The basic idea of this concept is that the community produces knowledge.

A community of inquiry developed in online teaching is viewed integrally, through the alignment of three dimensions: teaching leadership, social interaction, and cognitive engagement, all with the application of modern information and communication technology [4]. Teaching leadership involves designing, assisting, and guiding cognitive and online social processes to achieve learning outcomes; social interaction determines how socially and emotionally connected students feel to others and the online environment, and cognitive engagement describes to what extent a student is able to build meaning through reflection and communication.

This constructivist model assumes that quality online teaching requires the development of a community of participants that supports their meaningful and deep learning, primarily based on research. The focus is thus on the community of learners and their collaborative and investigative creation of meaning and knowledge; on the development of an online research community. In conditions where learning is not a process of actively constructing knowledge by the learner, teaching cannot achieve its basic purpose, which is the construction of new knowledge. It is known that the teaching process cannot be identified with the learning process, as teaching is most often a process of presentation, communication, and delivery of knowledge. The teaching process represents an irreplaceable and unique form of communication in which knowledge is created and increased for all participants in the interaction. Online teaching is observed in this model holistically and combines key elements of a learning community characterized by a collaborative and constructivist approach, creating and maintaining meaningful learning and knowledge exchange.

The CoI model includes three elements: teaching leadership, social interaction, and cognitive engagement, and their intertwining and interaction provide the structure necessary for a dynamic and deep, meaningful online learning environment and experience. In the following text, each of the three elements will be briefly explained.

Teaching leadership encompasses a broad spectrum of activities, roles, pedagogical forms, and interventions that a teacher undertakes to facilitate interaction with students in an online environment. It involves designing the teaching process with the assistance and guidance of

cognitive and online social processes, all aimed at achieving learning outcomes.

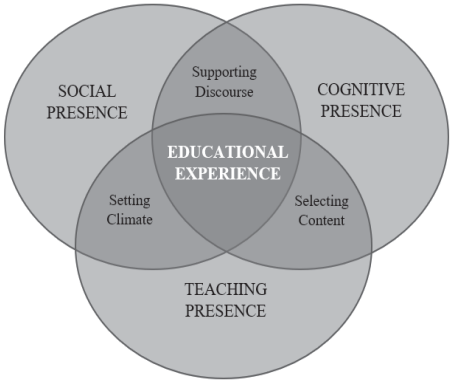



Figure 1. Community of Inquiry Framework, Source: [4].

It is necessary to formulate and communicate clear learning objectives, structure learning content, dose student activities and tasks, and closely align the assessment of learning with desired teaching outcomes. Quality teaching leadership implies that teachers design a learning environment, taking on the role of an online director" who simultaneously conceives, builds, and organizes the learning space and actively participates in it. Therefore, teachers have multidimensional roles, as they must act as facilitators, monitors, intellectual stimulators, and social supporters for online students [10]. Teaching presence positively influences psychosocial factors in student learning, such as motivation and self-efficacy. Support in teaching plays a crucial role in online education, with teacher engagement and connection with students having a positive effect on student retention in the course.

The second element of the CoI model is social interaction, measuring the extent to which students feel socially and emotionally connected with others and the online environment in which they learn. Social interaction is crucial for student engagement, as a sense of belonging significantly influences student involvement in learning experiences. In the online context, intentionally orchestrated, multiple opportunities for engagement with others are necessary for students to compensate for the lack of direct physical presence and contact. Social constructivism is the fundamental concept on which the role of social interaction in online learning is based. According to social constructivism, learning is shaped by context, and an individual's mind is formed through social processes [11], as meaning is constructed through communication, collaboration, and interaction.

The third element is cognitive engagement, representing the process of a student's interaction with learning content, i.e., the extent to which a student can build meaning through reflection and communication. Cognitive engagement involves phases of developing students' interest in the subject by posing problems, the research phase, reflection on problems and possible solutions, and the phase of problem-solving and its application. While the teacher initiates and organizes these phases, they are largely the result of social interaction among students in an atmosphere of proactivity, dialogue, and reflection. Cognitive engagement regulates how students progress in learning – how they approach new problems, develop understanding, and convey it in communication and interaction with the teacher and other students.

The CoI model theoretically assumes that social interaction is a mediator between teaching and cognitive engagement, but teaching presence directly creates and maintains social interaction and cognitive engagement. While teaching leadership and social interaction are crucial factors in learning, cognitive engagement is their result – it describes the learning process itself. Teaching leadership and social interaction create a shared space for teaching and students worlds, making up a common process and activities that occur within the community of teachers and students. Cognitive engagement, on the other hand, represents the private world of students, the process that happens within the students themselves. Creating this connection between shared and private worlds of students is a key concept for creating and supporting learning in the educational process.

## 3. HOW COMMUNITIES OF INQUIRY DRIVE TEACHING AND LEARNING IN THE DIGITAL AGE

The development of communities of inquiry, highly engaged in the co- creation, discovery and development of knowledge, capabilities and skills, is enabled by learning management systems, collaborative platforms and social-constructivist teaching activities [4]. It is explored here the current state of communities of inquiry (COI) in teaching and learning in the digital age, including the technology to support learner presence [12] and personal learning environments. It also argues for the communities of inquiry model to evolve into a learning model, that recognizes the importance of motivation, self-efficacy and personal skills in effective communities of inquiry. In this part we deal with five key questions examined through the lens of the Community of Inquiry Model: What skills and abilities need to be developed for teachers and learners to fully

leverage the power of communities of inquiry? What are the prerequisites for effective learning? What are we learning from the growth of peer-to-peer learning and peer assessment which supports the power of communities of inquiry? What can be emerging technology approaches to adaptive learning and adaptive assessment bring to the practice of communities of inquiry? What are the known best practices and emergent next practices for communities of inquiry? What are examples of communities of inquiry in action from a variety of settings around the world?

## 4. THE EVALUATION OF THE COMMUNITY OF INQUIRY MODEL

The Community of Inquiry (COI) has emerged in the past two decades as the most widely cited model for both course development and teaching research in online education [13]. The numerous scientific papers in which Garrison, Anderson, and Archer presented the model, the three presences (social, teaching, and cognitive) and their research methods have been cited countless times. In addition, the COI model has been used to develop many online courses and programs and has been used as the conceptual model for hundreds of thesis and research studies [14].

**Integrating the New Technologies:** The COI model has shown itself to be popular as a model to support research and course development not only within the online conferencing context in which it evolved, but also with new technologies as they have emerged. Figure 3 illustrates the increasing number of references to the COI overall and also shows that the model is robust enough to be useful when applied to a variety of intercultural contexts and technologies used to support distributed learning. These include blogs, immersive reality systems, synchronous technologies, wikis and MOOCs. More importantly, these references also show results of model implementation in practice and usually detail associated challenges, including technological issues, lack of familiarity, less than enthusiastic adoption and how the absence of one of the presences (notably effective teaching presence) can decrease the efficacy of the learning. As COI is essentially a social-constructivist model, it is also somewhat surprising to see its applicability to even the so called xMOOCs, which are based largely on cognitive-behaviorist pedagogies [15]. Holstein and Cohen [16] analyzed large numbers of student perceptions of successful Coursera MOOCs and found that constructing a successful MOOC can be accomplished by including all of the presence elements" – including social presence.

**Threaded Discussions:** Here has been very little innovation used in the threaded conference systems since our very early work in the 1990s. Experimental systems that support like "buttons" [17] or that force students to classify or add descriptive metadata or tags to their response have been shown to induce increases in at least social presence and commonly all three presences. There has also been work using machine algorithms to classify or highlight student messages requiring instructor feedback but none of these have resulted in widespread implementation in existing LMS systems. It seems that the now venerable threaded discussion continues to dominate online education, as it is as familiar to both students and teachers today as the systems we originally used to develop and validate the model. Perhaps the simple threaded discussion, like email, meets the needs of most teachers and thus there is little demand for systemic improvements. It is interesting to speculate whether mobile apps, with their more immediate response messaging that dominate both social and commercial communications, will dethrone the asynchronous threaded discussion in the near or distant future.

**Improving Student Postings:** Despite the lack of technical innovation, teachers using COI pedagogical models have incorporated a variety of protocols and best practices to enhance the value of student postings.

Most often these include providing assessment rubrics, providing model student answers or defining response protocols and sharing exemplar contributions from past courses. Many teachers also advocate making student posting compulsory to receive passing course credits, offe "bonus marks" for participation or, as I do, require students to provide a final summary post, describing and reflecting upon their contributions to the COI.

**Technology: New and Old:** As noted earlier, the COI model can be applied to courses based on a variety of technologies. Given the speed of change of pedagogical and communications technologies that we have witnessed since the COI model was developed twenty years ago, it is tempting to say that things will likely slow down now and allow us and our institutions to catch up! Unfortunately, this is likely a delusional belief in that technologically induced change continues and the need for educators and administrators to be both open to learning themselves and experimenting with their students in new learning communities is critically important. It has been shown before, that educational technologies largely do not disappear [18]. For example, blackboards, television, printed books and many other technologies are still used -

despite the adoption of newer technologies. Thus, the palette of delivery and communications options grows larger and the successful teacher learns not only to effectively use what they are most familiar and proficient with, but also to experiment and adopt new tools that may increase the efficacy of students' educational experience.

**Learning Activities:** The selection or design and facilitation of learning activities are key components of teaching presences and critical to the emergence of all three of the presences. As is often remarked 'it is nott what you 've got, but what you do with it that counts.' Key to the development of cognitive presence is the development (both planned and spontaneous as opportunities arise) of effective questions. Richardson, Sadaf, & Ertmer [19] found making certain that questions were perceived as authentic and grounded in at least the possible personal experiences of learners induced the development of cognitive presence.

They concluded that "with appropriate tasks, careful wording of instructor prompts, clear guidelines, and examples for participants, an imposed time limit and, possibly, the assignment of grades, the medium can provide students with opportunities for developing higher-order thinking."

**Integration of Social Media:** With the predominance of social media available and used today, participants (both teachers and students) have a great many tools that can be used to enhance their social presence beyond the institutional learning management system. Even without conscious effort, many of us are creating a net presence that is found by search engines constantly combing social and educational web sites. Anderson [5] believes that it is necessary to actively build and manage presence on social networks and to develop personal learning environments so as to maximize the effect and authenticity of our net presence. Moving outside the protective walls of the institutional LMS, however, gives rise to potential for privacy invasion and commercial and political exploitation by the owners of these networks.

The march of progress over the past two decades has also seen the call for additional "presences" with a goal of more completely describing the educational experience. These include vicarious presence, emotional presence and autonomy presence (Lam, 2015). There have been efforts to expand the social presence category in the COI model (especially for application in blended contexts) to include affective association, emotional presence, community cohesion, instructor involvement, interaction intensity, and knowledge and experience. I would argue that each of these already exists in the original model, but further definition helps focus on particular salient components of social presence.

None of these proposed additions has received wide adoption and there is certainly something to be said for the parsimonious advantage of only three presences. However, my biggest concern with the existing COI model is that while it helps construct and define an effective teaching model, we all know that the effectiveness of teaching is equally dependent on the learners. Anderson's thoughts went in the direction of the effectiveness of teaching, which largely depends on the students Therefore, he advocated adding the presence of a "learner presence" described and measured by Shea and Bidjerano [12]. They illustrate learner presence as in Figure 4 and note its components of effort, self- efficacy, and othe forms of student self-regulation. This addition also brings the model more in line with notions of self-directed learning that predominate in connectivity and heutagogical based learning designs. Finally, the notion of measurement and support of learner presence allows the COI to evolve beyond a teaching model to a 'teaching and learning' model and thus moves it beyond formal schooling and educational contexts. It is no longer enough for teachers to ask what types of presence(s) do I need to develop in my teaching, but rather how do I match my teaching model and behavior with the learning capacities of the learners.

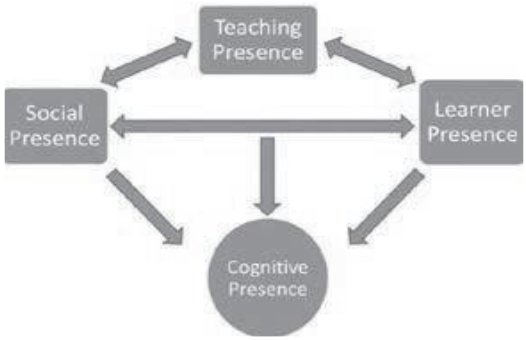



Figure 3. Suggestions for a revised COI Model from Shea and Bidjerano [12]

## THE FUTURE OF COMMUNITIES OF INQUIRY AND EMERGING TECHNOLOGIES

One of the challenges of all social-constructivist learning models - including the COI - is scaling up to meet demand and so increase access by large numbers of learners. Traditionally, distance education institutions have done this by breaking large courses into smaller tutorial groups and supporting these groups with tutors in face-to-face or

online groups. It is very rarely seen this model increased beyond 40 or 50 students and 20-30 students is the norm. This limitation prevents large scaling of COI modeled learning as costs tend to increase directly with the number of students [20]. Industrial and post-industrial models attempt to address this limitation by increasing student-student interaction or by, for example, increasing teaching presence through use of recorded video, automated and pre-set responses and pre-programmed teaching tools such as computer assisted learning, simulations and games. Most recently, MOOC models are evolving that focus not on the learning group like the COI model, but on a network of learners working on a course of studies [15]. Networks are less formally structured than groups, more flexible in the entrance and exit of members and tend to expand beyond a single structured course similar to the so-called groups (actually networks) that are created or emerge on Facebook, LinkedIn and other social networking systems. The informal nature of communication has evolved outside of formal education.

Some of the COI constructs cross easily to network models, but others suffer from the need for time synchronization, and the often overwhelming presence of teacher assessment that can inhibit opportunity for networks to fully develop. Jon Dron and Anderson researched and developed tools for learning in ‘sets’ - the aggregation of all those with interest in a topic but who have no interest in developing a closer and more time dependent network or a group. The classic example is the set of individuals who work creating Wikipedia articles and the larger set of those who garner information on a particular topic from them. Learning in sets allows, but does not demand, contributions, recommendations or assessments and thus reduces demands for structured time and personal interaction [15].

Humans evolved in groups (mostly families and larger kin and tribal groups) and these have evolved to create the social glue that facilitates learning and enhances motivation in the COI model. The continuing popularity of the model, through different technologies, shows that group based learning is still highly valued and the most common way in which at least young people engage in both formal and informal learning. The value of new models will be most important in providing lifelong learning opportunities for personal, community and career development.

**REFERENCES**

[1] Rapanta, C. Botturi, L. Goodyear, P. „Online University Teaching During and After the Covid-19 Crisis: Refocusing Teacher Presence and Learning Activity“, Postdigital Science and Education 2, 923-945. doi:10.1007/s42438-020-00155-y. 2020.

[2] Arsenijević, J. Belousova, A. Tushnova, Y. Grosseck, G. Mesaroš Živkov, A. . „The Quality of Online Higher Education Teaching During the Covid-19 Pandemic“, International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE), 10 (1), 47-55. doi:10.23947/2334-8496-2022-10-1-47-55 . 2022.

[3] Andevski, M. Arsenijević, J. „Medijska participativna kultura kao pravac upravljanja razvojem obrazovanja, U Milisavljević, Vladimir, Nauka i globalizacija, Filozofski fakultet Univerziteta u Istočnom Sarajevu: Pale, str. 693-709. Pale, Sarajevo, 2014.

[4] Garrison, D.R. Anderson, T. Archer, W. „Critical inquiry in a text-based environment: Computer conferencing in higher education“ The Internet and Higher Education, 2, 87 -105. 2000.

[5] Anderson, T. „Three Pillars of Educational Technology: Learning Management Systems, Social Media, and Personal Learning Environments“ - Parts 1-3. http://teachonline.ca/tools-trends/how-use-technologyeffectively/three-pillars educationaltechnology. 2016.

[6] Daniela, L. Pedagogies of Digital Learning in Higher Education. London, Routledge. 2020.

[7] Buckreus, K. Ally, M. „Smart Practices: Machine Intelligence for Transforming Pedagogy and Learning. Emerging Technologies and Pedagogies in the Curriculum. Bridging Human and Machine: Future Education with Intelligence. Ed. Shengquan Yu, Mohamed Ally, Avgustos Tsinakos. doi: 10.1007/978-981-15-0618-5_4. 2019. Springer. Singapore. 2019.

[8] Dewey, J. „My pedagogic creed. In J. Dewey, Dewey on education (pp. 19-32). Teachers College, Columbia University, New York, 1959.

[9] Swan, K. Garrison, D. R. Richardson, J. C. „A constructivist approach to online learning: The community of inquiry framework“, In C. R. Payne (Ed.), Information technology and constructivism in higher education: Progressive learning frameworks (pp. 43-57). IGI Global, Hershey, 2009.

[10] Sayad, G. Hasliza, N. Ramayah, S. „How Higher Education Students in Egypt Perceived Online Learning Engagement and Satisfaction during the COVID-19 Pandemic“, Journal of Computer Education, 8(4), 527–550, 2021.

[11] Bandura, A. „Social cognitive theory: an agentic perspective“ Annu Rev Psychol. 52 (1), 1-26, 2001.

[12] Shea, P. Bidjerano, T. „Learning presence: Towards a theory of selfefficacy, self regulation, and the development of a communities of inquiry in online and blended learning environments“, Computers & Education, 55(4), 1721-1731, 2010.

[13] Bozkurt, A. Akgun-Ozbek, E. Yilmazel, S. Erdogdu, E. Ucar, H. Guler, E. Goksel Canbek, N. „Trends in distance education research: A content analysis of journals 2009-2013“, The International Review of Research in Open and Distributed Learning, 16(1), 2015.

[14] Kineshanko, M. A thematic synthesis of community of inquiry research 2000 to 2014. (EdD), Athabasca University, Athabasca, 2016.

[15] Anderson, T. Dron, J. „Learning technology through three generations of technology enhanced distance education pedagogy“, European Journal of Open, Distance and E-Learning, 2012/2, 2012.

[16] Holstein, S. Cohen, A. „The Characteristics of Successful MOOCs in the Fields of Software, Science, and Management, According to Students' Perception“, Interdisciplinary Journal of E-Learning & Learning Objects, 12, 2016.

[17] Makos, A. Oztok, M. Zingaro, D. and Hewitt, J. "Use of a "Like" Button in a Collaborative Online Learning Environment", American Educational Research Association (AERA), 2013.

[18] Dron, J. Anderson, T. „The future of e-learning“, In C. Haythornthwaite, R. Andrews, J. Fransman, E. Meyers (Eds.), The Sage handbook of e-learning researchpp. 537- 556). London, Sage, 2016.

[19] Richardson, J. C., Sadaf, A., & Ertmer, P. A. (2012). Relationship between types of question prompts and critical thinking in online discussions. Educational Communities of Inquiry: Theoretical Framework, Research and Practice: Theoretical Framework, Research and Practice, ed. Z. Akyol and DR Garrison, 197-222.

[20] Bates, A. W. Technology, E-learning and Distance Education. Routledge, New York, 2005.

# INFOTECH

# 2020

# 2021

# 2022

# 2023

# 2024

# PROGRAMS

# Infotech 2020 – Program

*Aranđelovac, 24 – 25 June*

**Invited Keynote Lectures:**

- Fifteen Years of eGovernment in Serbia, *Dejan Vidojević*
- A Cloud Based IoT System for Real-time and Adaptive Weather Forecasting in Mauritius, *Pawan Fowdur*

**Session 1: Cybersecurity & GDPR**

- Forecasting Software Vulnerability Totals Using Long Short Term Memory (LSTM) Neural Networks, *Michael T. Shrove, Emil Jovanov*
- Fake News Detector Algorithms, *Vladimir Mladenović, Asutosh Kar, Danijela Milošević, Ivona Radojević Aleksić*
- Hybrid Detection of Fake Accounts on Social Networks, *Danijela Milošević, Amita Nandal, Arvind Dhaka, Vladimir Mladenović, Ivona Radojević Aleksić*
- Technical Standards in Biometrics: Security Mechanisms of ISO 24745 Standard, *Milorad Milinković*
- Data Privacy and Certification According to the New ISO 27701 Standard, *Vladan Pantović*
- Security Analysis of Mobile Payment Applications on the Android Operating System, *Miloš Antonijević, Goran Lazarov*
- Integrity and Hash Functions, *Dušan Rajčević, Ana Veljić, Aleksandar Šijan*

**Session 2: Crisis and Technology**

- How to Lead your Organization in Crisis to the Place where Knowledge Meets Change? *Milan Šmigić, Miroslav Ćurčić*
- Web 2.0 Technologies in the Time of COVID Crisis from the Knowledge Management Perspective, *Mladen Opačić, Mladen Veinović*
- The Challenges of Delivering Seminars Remotely, *Deasún Ó Conchúir*
- Control of Workplace Environmental Factors Using Modern Technologies, *Nebojša Ćurčić, Novak Milošević*
- Transforming International Corporate Learning during COVID-19, *Michael Bittle*

**Session 3: ICT Development and Application**

- First Experiences in the Application of the Central Audio Library of the University of Novi Sad and Directions for Further Development, *Vlado Delić, Dragiša Mišković*
- Application of Parametric Rectified Linear Unit (PReLU) into Speech Recognition Model, *Robin Singh Bhadoria, Atharva Nimbalkar, Ram Korde, Munish Khanna*
- Exposing a KNIME-Based Data Science Workflow via a Restful Web Service, *Petar Prvulović,* Nemanja Radosavljević, Dušan Vujošević

- Application of New Technologies in Transfer of Knowledge and Information in Agriculture, *Marija Nikolić, Tamara Paunović*
- Contemporary Informatics in Biomedicine, *Olja Arsenijević, Marija Lugonjić, Polona Šprajc*
- Global Distance Learning Platform Supported by the Digital Community Experience (FutureLearn), *Miloš Milašinović, Miloš Jovanović, Dijana Bursać, Jelisaveta Aleksić*
- Analysis of the use of information and communication technologies in companies in the Republic of Serbia, *Slađana Vujičić, Olivera Pavlović, Aleksandar Gajić*
- Application of an Advanced Information System in order to Support the Improvement of the e-Learning System, *Goran Jocić, Đorđe Pucar, Luka Ilić*

**Session 4: ICT Recent Trends and Challenges**

- Recent Trends and Open Research Challenges in Energy-Efficiency of 5G ICT Infrastructure, *Zoran Bojković, Dragorad Milovanović, Vladimir Terzija, Vladan Pantović*
- Opportunities and Challenges of 5G Technology in Healthcare 4.0, *Rajko Terzić, Vladan Pantović, Dragorad Milovanović*
- Identification of Gifted Students Using Machine Learning Techniques, *Milan Cicvarić, Jelena Pejčić, Pavle Milošević, Aleksandar Rakićević*
- Intangible Investments in Marketing Digital Communications in the Serbian Banking Sector, *Maja Cogoljević, Tamara Vesić, Vladan Cogoljević*
- Use of Blockchain Technologies in Education - Literature Review and Advices for Application in Serbia, *Dušan Nešić*
- Development of New Internet Economy and the Impact of ICT Infrastructure, *Vladimir Obradović*
- Natural Human Computer Interaction Based on Eye Movement, *Željko Gavrić, Miroslav Minović*
- Exploring Industry 4.0 Paradigm as Applied to Project Management. A Proof of Concept, *Paolo Eugenio Demagistris, Waseem Khan*

# Infotech 2021 – Program

*Aranđelovac, 23 – 24 June*

**Invited Keynote Lectures:**

- Ten Strategic Technology Trends for Post-Covid 19 Economy, *Petar Kočović, Muthu Ramachandran*
- Use of Wearables and IoT Technology in the Fight Against the COVID-19 and Future Pandemics, *Emil Jovanov*

**Accepted Plenary Presentations:**

- Man in the Fourth Industrial Revolution with Reference to Serbia, *Života Radosavljević, Maja Anđelković, Dragana Radosavljević*
- Digital Enablers of Construction Project Governance, Demagistris Paolo Eugenio, *Petruzzi Sandro, Pampaloni Rodolfo, Milan Šmigić, De Marco Alberto, Khan Waseem, Ottaviani Filippo Maria*
- Experiences of Leveraging IT for Business Opportunities in the EU, *Deasún Ó Conchúir*
- Rethinking Smart Bus Service in the COVID-19 Era, *Anshu Prakash Murdan*
- Fingerprint Reader in Signing Digital Transactions, *Marija Bogićević Sretenović, Bojan Jovanović*
- Design Guidelines for Creating Adequate Mobile Learning Application, *Vanja Mišković, Željko Gavrić, Miroslav Minović*
- Convergence and Interoperability for the Internet of Media Things and Big Media, *Dragorad Milovanović, Vladan Pantović*
- Traffic Analysis of A3 Topology Construction Protocol in Wireless Sensor Networks, *Petar Prvulović, Nemanja Radosavljević, Dušan Vujošević, Aleksandar Gavrić*
- A Scalable, High-Throughput, Fault-Tolerant System for Spatial and Temporal Dimension Reduction in Wireless Sensor Networks, *Aleksandar Gavrić, Dušan Vujošević, Nemanja Radosavljević, Petar Prvulović*
- Benefits of Cyber Web Traps based Machine Learning Attacks Detection, *Vladan Todorović, Branislav Todorović, Nikola Stevanović*
- Internet Services in COVID-19 Pandemic: Consumption Trends and Performance Metrics, *Rajko Terzić, Dragorad Milovanović*
- Information Security and Data Protection - Review of Security of Personal Data in Geodetic Databases of the Republic of Serbia, *Zagorka Gospavić, Vladan Pantović, Milutin Pejović, Slavko Vasiljević*
- 5G-ICT Infrastructure for Innovative Financial Services, *Drago Indjić, Dragorad Milovanović, Vladimir Radojević*
- The Role of Information Technology in Logistics, *Slađana Vujičić, Mirjana Radović Marković, Kabir Shajahan, Rossitsa Chobanova*
- ICT in the Digital Transformation of Organization, Ivan Gjorgjievski
- The Role of Individual Coaching in Times of Social and IT Changes in Organizations, *Biljana Galovska*
- Virtual Personal Branding, *Daniela Karadakov*

- The Role of Information Technology in the Development of Entrepreneurship, *Slađana Vujičić, Zorana Nikitović, Dušan Marković, Dunja Komnenović*
- GraphQL API Gateway in Microservice Architecture, Jelica Stanojević, *Uroš Šošević*
- Possibilities of Biometric Face Recognition of Persons With a Mask During the Covid-19 Pandemic, *Bojan Marčeta, Ivan Milenković*
- Digital Transformation of the Business Process - DMSC in the Ministry of Interior of the Republic of Serbia, *Damir Amedovski, Slobodanka Zdravković, Dejan Đorđević, Slaviša Đukanović*
- Discrete Logarithm Problem and Cryptography, *Miomir Radovanović*

# Infotech 2022 – Program

*Aranđelovac, 8 – 9 June*

**Invited Keynote Lectures:**

- Towards AI-Native Architecture in 6G, *Tasos Dagiuklas*
- IoT-based Adaptive Control of Building Passive Measures: The Next Step in Promoting Energy Efficiency in Buildings, *Mahendra Gooroochurn*

**Accepted Plenary Presentations:**

- Further Development of Standardization in Information Security - The Example of ISO 27001 and ISO 27002, *Vladimir Simić, Vladan Pantović*
- Impact of Mobile Network Technology on Public Health and Environment: 5G Deployment and 6G Development, *Rajko Terzić, Dragorad Milovanović*
- Smart City and Digital Cultural Immersion: Two Experiments, *Drago Indjic*
- Cyber Security Support for Financial Forensics, *Goran Lazarov*
- NIST CyberSecurity Framework: Preparation Steps for Successful Assessment, *Kristijan Lazić, Vladan Pantović*

# Infotech 2023 – Program

*Aranđelovac, 7 – 8 June*

**Invited Keynote Lectures:**

- Technical Evolution of 5G Mobile Connectivity Network: 3GPP 5G-Advanced Standardization Project, *Dragorad Milovanović*
- The Position, Role and Competences of Data Protection Officers in the EU Law, *Tihomir Katulić*

**Accepted Plenary Presentations:**

- Blockchain and Smart Contracts: The Enhanced Supply Chain, Dušan Mitrović, *Miloš Milovanović, Miroslav Minović*
- Front-end Test-Driven Development: React Example, *Stefan Milanović, Jelica Stanojević, Miroslav Minović*
- Cyber Space as the Fifth Dimension of Conflict and Cyber Warfare with Reference to Cyber Terrorism*, Olgica Vulević*
- The Use of Information and Communication Technologies in Companies in the Republic of Srpska, *Slađana Vujičić, Jasmina Šljivić, Ljiljana Tomić, Milivoje Ćosić, Aleksandra Mesarević*
- Cybersecurity and Security of Network and Information Systems in European Union Law, *Vesna Ćorić, Ana Knežević Bojović, Slavica Banić*
- Analysis of information security in the Republic of Serbia and the Republic of Srpska, *Slađana Vujičić, Biljana Dimitrić, Gorana Tomanović, Boro Krstić*
- ChatGPT: Impact of Language Models for Information Security*, Vladica Ubavić, Marina Jovanović-Milenković, Oliver Popović, Marija Boranijašević*
- Comparative Analysis of In-House AI Development vs. Artificial Intelligence-as-a-Service (AIaaS), *Milan Djorđević*
- Exploring the Integration of Technology in PMO: Current Trends and Future Perspectives, *Milan Djordjević, Vladan Pantović*
- Project Management Body of Knowledge Life Cycle*, Vladan Pantović, Milan Šmigić*
- Transformation of Traditional Methods of IT Marketing and Advertising: Machine Learning vs. Cookie Consent Systems*, Radmila Marković*

# Infotech 2024 – Program

*Aranđelovac, 5 – 6 June*

**Invited Keynote Lectures:**

- SMART HEALTH HOME: Technology Adoption and Social Impact, *Vladimir Brusić*
- Modern Web Technologies and Marketing: Possibility and Challenges, *Filip Jovanović*

**Accepted Plenary Presentations:**

- Learning Deep Denoisers for Low Field Magnetic Resonance Imaging from Unlabeled Data, *Nikola Janjušević*
- Data Engineering (Big Data, Machine Learning, Deep Learning), *R. Ismibeyli, Q. Mezahim, S. Selimxanova, A. Jamilya, F. Xalilov*
- Digital Ecosystem, R. Ismibeyli, S. Selimxanova, D.Xurshudov, Q.Mezahim, *F. Xalilov*
- Information Technologies and its Application Areas, *Karimli Leyla Eldar, Abdullayev Vugar Hajimahmud*
- Multi-Layer Low-Cost Smart Air Solution with Embedded Hardware and Cloud Application, *Stefan Stefanović, Teodora Stamenkov, Amela Zeković, Slavica Marinković*
- Possibilities of Applying Generative Artificial Intelligence in Architecture, *Dušan Mitrović, Miroslav Minović, Miloš Milovanović*
- Transforming Project Management with Artificial Intelligence, *Milan Šmigić, Vladan Pantović*
- Standardization Activities in Developing, Providing, and Using AI-based Products and Services: Requirements and Management systems, *Dragorad Milovanovic, Vladan Pantović*
- Trends of Progress in Application of Artificial Intelligence in Healthcare: Support for Diagnosis and Treatment in Personalized Medicine, *Dragorad Milovanović, Rajko Terzić*
- Raising the Level of Employees Awareness of the Security Aspects of Using computers, the Internet, Social Networks and Online Communications, *Saša Zečević, Marija Vidrić, Vladan Stevanović*
- Survey Analysis of User Cybersecurity Practices and Exposure to Cyber Threats, *Mladen Opačić, Vladan Pantović, Velimir Štavljanin, Dejan Vidojević*
- Information System Protection, Containers, Physical and IT Protection, *Vladimir Đokić, Dragana Đokić, Zoran Avramović, Željko Stanković*
- The Analysis of the Usage of Information and Communication Technologies in Enterprises of the Republic of Serbia and the Republic of Srpska, *Slađana Vujičić, Ljiljana Tomić, Boro Krstić, Jasmina Šljivić, Biljana Dimitrić*
- Predictive Data Analytics in Modern PMO, *Milan Djordjević*
- High-Tech Crime and Identity Theft: Challenges, Methods and Prevention, *Olgica Vulević*
- Leveraging Artificial Intelligence for Enhanced e-Commerce Performance, *Petar Ilić, Jelica Stanojević, Miroslav Minović*
- Contemporary and Integrative Approach to Online Education, *Olja Arsenijević, Jasmina Arsenijević*

**AUTHOR INDEX**