Proceedings
# of the 22nd International Conference
on Information Technology for Practice

IT for Practice 2019

October 10, 2019, Ostrava, Czech Republic

Edited by
Jan Ministr

Organized by
VŠB - Technical University Ostrava, Centre for Information Technology
European University Information Systems - CZ
Czech Society for System Integration
Regional Authority - Moravian-Silesian Region

ISBN 978-80-248-4322-3 (pdf on line)
ISBN 978-80-248-4321-6 (printed)

VSB - Technical University of Ostrava

Ministr Jan

Information Technology for Practice 2019 (IT4P-2019)

22nd international conference

October 10, 2019
Ostrava, Czech Republic

Sponsors of IT for Practice 2019

European University Information Systems

VŠB Technical University of Ostrava
Centre for Information Technology

Czech Society for Systems Integration

IT Cluster z.s.

Warsaw Management University

EDITOR

Ministr Jan

PROGRAM COMMITTEE AND REVIEWERS

CHAIRMAN

Members

All published papers have been reviewed by 2 independent reviewers before publishing. The proceedings have not been amended or proofread and editors are not responsible for the language used papers.

Copyright

Conference website

http://www.cssi-morava.cz

FOREWORD

Conference on Information Technology for Practice 2019

Ladies and gentlemen, welcome to the traditional IT for Practice 2019 conference (IT4P), the international conference. This year we organize the 22nd annual conference.

It is organized under the auspices of CIT (Center of Information Technologies VŠB-TUO), EUNIS-CZ (Association of European University Information Systems of the Czech Republic), IT Cluster zs, CSSI (Czech Society for System Integration) and Regional Office - Moravian-Silesian Regional Office. This conference is also highly appreciated by the European Union. The organizers try to register this conference in recognized databases.

According to the title of the conference, the participants come from academic staff, managers and employees of ICI, IS designers in companies and institutions, ICT providers and students. The topics of this year's conference are:

- Information Society and Education;
- Information Management and IT Innovation;
- IT in Public Administration;
- Information security.

The purpose of the organizers is to create a platform for the exchange of knowledge and skills in ICT innovation and the use of new knowledge in practice, as it is not easy to attract professionals willing to share their experience.

Thanks also to all sponsors who contributed to the financial support of the conference

We wish you to create new professional contacts and consolidate existing contacts that are useful for solving specific problems in your companies and institutions.

On behalf of the organizers

Jan Ministr November

SAD FAREWELL

With deep sadness we inform you of the death of doc. Ing. Milena Tvrdíková, CSc., who passed away January 21, 2020.

She belonged to the main organizers of the conference and participated significantly in the successful course of all conference years.

Thank You Milena

C O N T E N T S

INFORMATION SOCIETY AND EDUCATION 3

INFORMATION MANAGEMENT AND IT INNOVATION 47

IT IN PUBLIC ADMINISTRATION 113

INFORMATION SECURITY 133

INFORMATION SOCIETY AND EDUCATION

The Polish SMEs in Age of Digital Transformation

Piotr Adamczewski[1]

Abstract. Solutions Digital technologies are transforming operations, products and services in organisations large and small. Solutions of the Information and Communication Technology (ICT) are the foundation of modern economic organizations in a time of digital transformation. This article is aimed at describing the role of modern ICT trends in intelligent organizations, which are described as SMAC, *(Social, Mobility, Analytics, Cloud)* and *Internet of Things* and are becoming an essential ICT element supporting management processes. The arguments are illustrated with the results of own research conducted by the author in 2014-2018 in selected SMEs from the Polish Mazowieckie and Wielkopolskie Provinces and their reference to the general development trends in this area.

Keywords: Digital transformation, Intelligent organization, ICT, Knowledge management, SMAC.

JEL Classification: A23

1 Introduction

Digital transformation - the use of technology to radically improve performance or reach of enterprises - is a hot topic for organizations across the globe. The dynamics of market changes and the high level of turbulence in business environment make modern economic organizations face the challenge of continuous improvement in their operational methods and development. In practice, it implies the necessity to use modern ICT solutions in knowledge management, which enable to support business processes within the acquisition and reinforcement of business's competitive advantages. Within the evolution of the information society towards the knowledge society, it boils down to the treatment of modern organizations as intelligent organizations. A intelligent organization is one whose business philosophy is based on knowledge management (Grösser, 2012). This term became popular in the 1990s owing to the growing ICT development, the ynamically changing economic environment, and the increasing market competitiveness. An intelligent organization is one that

[1] WSB University in Poznań PL, Institute of Management, Poland, Adamczewski@wsb.poznan.pl.

learns and has the capacity to create, acquire, organise, and share knowledge and use it in order to raise the efficiency of its operation and increase competitiveness on the global market. The idea of such an organization is based on the systemic approach to organization, i.e. its treatment as a complex organism founded on existing structures and executed processes, focusing on the role of knowledge. In that approach, which is called ‘the fifth discipline’ by P. Senge, owing to knowledge and suitable tools all elements of an organization and its personnel can collaborate in order to achieve set objectives (Schwaninger, 2010). Thanks to that, the whole organization operates as an intelligent and successful organism in the competitive environment. This explains the mutual relationships between methods of fulfilling targets, their understanding, methods of solving problems as well as internal and external communication.

- elements of SMAC solutions are used on an increasing scale in SMEs,
- SME management pay growing attention to the implementation of SMAC systems.

The analyses are illustrated with survey results and direct observations of the author from 2014-2018 in selected 120 SMEs from Mazowieckie and Wielkopolskie provinces, Poland, with reference to the general development trends in the studied area. The survey sample was made up of micro (9%), small (56%) and medium sized enterprises (35%). Surveyed companies represent a wide range of industries: retail and wholesale trade, discrete and process manufacturing, transport, HoReCa, utilities, finance, construction, telecommunication and ICT.

2 Intelligent organizations in the digital transformation

The most important characteristics of a intelligent organization include, among other (Grösser, 2012; Schwaninger, 2010):

- fast and flexible operation,
- the ability to monitor the environment,
- the capacity to diagnose early market signals and to react to changes in the environment, and
- the ability to implement new knowledge-based solutions and achieve economic benefits therefrom.

The growing volume of information used in a intelligent organization is accompanied by its increasing importance. Peter Drucker indicated already that traditional factors of production, such as growth, labour, and capital, are losing their importance in favour of a key resource, namely knowledge applied in the creative operation of an organization. It constitutes intangible resources that are related to human actions, whose use may be the basis for gaining a competitive advantage (Schwaninger, 2010). Knowledge has to be treated as information embedded in the context of an organization and a skill to use it effectively in the organizational activity. It means that knowledge resources are data about its customers, products, processes, environment, etc. In a formalised form (documents, databases) and in non-codified forms (knowledge of staff).

In the practical dimension, the effective collaboration of such elements means the necessity to use advanced ICT solutions. Technical, technological, and organizational innovations, which have appeared in recent years, are all utilised (Adamczewski, 2017). They encompass almost all areas of a modern organization operation, starting from means of transport and equipment, through organization and material and raw material flow management, to the development of system structures that implement business processes, i.e. within logistics systems that are the essence of modern management based on ICT solutions.

The present effect of the ICT evolution in the form of the so-called third ICT platform, has been treated since 2013 as the foundation of the 4th industrial revolution, being the natural development stage of the 3rd revolution of 1969 (its symbol being electronics with its transistor and automated production). The main distinguishing element of new changes has become the redefinition of the present course of business processes that contributes to new operating models of economic organizations facing new challenges to maintain their position and expand on the market further. The industrial revolution of the 4th stage is breaking out due to (Adamczewski, 2018a; Betz, 2015; Gartner, 2018):

- the introduction of the all-present digitalization,
- decision processes based on virtual simulations and data processing in real time, and
- machine-machine and machine-man communication.

The digital transformation means a change of the present approach to a customer and a comprehensive process where an organization moves to new methods of operation using the state-of-the-art SMAC digital technology, including social media, mobility, big-data – analytics, and cloud computing. However, it has to be kept in mind that the role of digital technologies in that process is to enable the necessary changes and open an organization to new opportunities. Therefore, they should be a tool rather than the aim of transformation. The centre of the process has to be the customer and his needs, as the main driver for manufacturers and service providers. The digital transformation is no longer the method of gaining a competitive advantage – it s becoming a factor that enables to stay on the market (McConnell, 2017).

3 Trends in the digital transformation

Digital transformation is being spearheaded through a combination of software and hardware advancements. While the list of advancements is endless, the most promising technologies fall under one of the four umbrella terms described below briefly (Adamczewski, 2018b; Lechmann, 2018; Olszak, 2018).

I. The Data Science Trio refers to three advancements related to data science that are arguably causing the greatest disruptions across various industries at present. These three technologies are:

- Data Analytics and Big Data Analytics refers to a set of qualitative and quantitative methodologies used to study and extract knowledge from raw data and use it to guide business decisions. Big Data refers to gargantuan data sets that contain important information and patterns hidden among large heaps of supplemental data. Both finite data analytics and big data analytics are applicable in virtually any scenario involving a database and sufficiently large amounts of data. Scores of companies are currently hiring armies of Data Analysts to crunch through their datasets and help them improve/organize their practices and services.
- Machine Learning refers to the concept of giving computers the ability to learn on their own without human intervention. The primary usage of machine learning is to teach computers to recognize patterns

on their own in cases where human analysis is too slow, expensive, or even impossible. Machine learning has thus seen itself being employed in recommendation engines, market analyses, spam filters, network security solutions, and more. Any organization that has data-based assignments which are large & repetitive (or) involve some form of identification tasks (or) a combination of both the above, should consider exploring machine learning solutions.

- Artificial Intelligence (AI) refers to a computer possessing the ability to perform a task or tasks in a manner that is just as effective or even more effective than a human being doing the same. While machine learning deals with a computer studying data and merely outputting what it has learned, Artificial Intelligence deals with a computer studying data and taking decisions/executing tasks based on certain pre-programmed instructions. A.I is best implemented in any scenario requiring high speed and high precision decision making and task execution.

II. Internet of Things (IoT) refers to a network of interconnected physical devices and sensors that collect data and exchange it with one another using the internet as a communication platform. IoT networks allow for low cost embedded systems to be deployed into physical environments where they can continuously collect information, relay it, interpret it, and act on it accordingly. IoT helps in achieving a scenario where all variables of a physical environment can be mapped and each constituent device’s functioning can be made to depend on said variables or outputs from other device(s). For this reason, IoT has found immense value in health-care, smart cities, and smart homes.

III. Remote Work Environments. High skilled employees are very often not available at the desired location of a firm or may sometimes prefer to work from home. In the digital age, it makes no sense to compromise on talent by restricting hiring & work to a single physical location. Whether it is employees situated halfway across the world in a satellite office, or an employee situated half way across town in their own house, technological advancements such as video calls and internet-connected project management software allow us to send work to employees themselves when the reverse is not possible.

IV. Block Chain Technology. The finance industry is currently undergoing one of its largest transformations in history – thanks to blockchain. Blockchain refers to a distributed global database spanning across millions of computers all over the globe. It is not controlled by any central authority and uses state of the art cryptography to prevent unauthorized access to sensitive information such as transaction history. Blockchains have already been implemented to create cryptocurrencies (e.g. Bitcoin) which are unregulated digital currencies that offer alternatives to traditional currencies. Cryptocurrencies are used widely due to the unmatched security and freedom they offer in trading any amount of money, big or small, without having to face any bureaucratic trouble.

V. Other Promising Trends. Beyond the technologies discussed above, there are several other technologies promising digital disruption of legacy industries. Some of the most promising trends are:

- Virtual Reality and Augmented Reality VR works by simulating entirely new environments digitally while AR works by imposing simulated elements onto real environments. Both VR and AR find already finding application in the fields of gaming, health-care, and warfare.
- Internet-Based Media & Advertising. Although internet-based media & advertising is already mainstream, most companies still prefer to spend more on print and TV platforms. As the world continues its tectonic shift to Internet-based consumption, firms such as Netflix and InMobi are already capitalizing lucratively on internet revenues for media and advertising content respectively.

4 Case Study of the Polish SMEs

Research carried out by the author shows that the popularity of ICT support in management processes in SMEs can be presented as follows (percentage of analysed enterprises):

- finance and accounting – 93%,
- human resources – 81%,
- warehouse management – 72%
- production management – 28%,
- customer relationship management – 62%,

- office work support – 98% (including e-mail 98%), and
- procurement and sale process service – 68%.

The analysed enterprises use laptops and PCs in their day-to-day operations (99% of indications). On average, they hold about 18 computers. The vast majority use both land lines and smartphones. Tablets are used in every third enterprise (38%), with 6 tablets per firm on average. The above-mentioned statistics are supplemented with the 58% ratio of using online messenger systems and taking advantage of the support provided by ICT freelancers at 63%. SMEs usually do not use multi-layer data processing protections. Instead, they choose only basic anti-virus software (93%). Every second enterprise (54%) protects its data with a standardised policy of passwords that are set and managed by the management. On the other hand, less than half SMEs (49%) encode their e-mails. Only one out of three firms uses data backup (36%), including as many as 89% having that process automated. Interestingly, backup is used to secure company data more often by entities that do not consider their ICT security to be of essential importance for their business.

The readiness of the studied entities to face the challenges of digital transformation is as follows:

- 22% of respondents answered positively, confirming the implementation of such tasks,
- 12% of respondents answered that such actions would be taken soon,
- 20% of responses indicated that such actions would be taken in the near future, and
- according to 46% of respondents such actions were not being conducted and there were no such plans.

As regards the use of SMAC solutions, the statistics of the analysed entities reflect the general global trend in this respect, i.e. (Anderson, 2015; Corcoran, 2016; Riche, 2018; Schwab, 2016; Ziemba, 2017):

- a cloud is used in 18% organizations (38% of analysed population plans to start using it),
- mobility is utilised in 29% of organizations (with 15% of analysed population planning to launch it),
- analytics is applied by 9% of organizations (while 16% of studied population have plans to start it), and

- social media are declared by as many as 45% of organizations already, and their use in the near future is declared by 55% of respondents.

The development trends of Polish intelligent organizations in the digital transformation is supplemented with the following declared initiatives (Riche, 2018; Ziemba, 2017):

- office digitalization – 75%,
- modernization of ICT infrastructure – 74%,
- consolidation in ICT and advanced analytics – 55%,
- new mobile applications for personnel – 52%,
- networking – 53%, and
- mobile self-service applications for customers – 38%.

The fact of placing a customer in the centre was confirmed by responses about catching up with the dynamically evolving needs of contemporary consumers. Moreover, half of the respondents indicated the necessity to follow the changing expectations of their customers, declaring it to be their top business priority. The continuous improvement of customer satisfaction level is possible mostly owing to investments in new ICT solutions. Only owing to them shopping can be comfortable, fast, and possible at any time and place, while customer service can be effective. It also means the new opportunities in acquiring knowledge about needs, behaviour, and opinions of customers. In general, the above-mentioned study results show that Polish modern business organizations are becoming more confident in using advanced solutions of SMAC systems, to meet the challenges of digital transformation (Adamczewski, 2017; McConnell, 2017).

5 Conclusions

The dynamic economic changes and the evolution of business relationships devaluate traditional sources of competitive advantages in the SME sector, such as capital, infrastructure, access to outlets, and the quality of offered products and services. Modern enterprises that want to compete on the market effectively have to give priority to flexibility of their organization and its ability to implement innovative business models and reorganise logistics processes. Examples of numerous Polish SMEs show that the vision of a business managed in a modern way has come into the dynamic phase of realization, while the effective knowledge management with advanced ICT solutions is growing to the role of paradigm. There is no doubt that reserves still present in the SME sector can be utilised, through supporting its operation with advanced ICT systems with the dominant role of SMAC solutions.

Nevertheless, it has to be remembered that the creation and development of such smart technologies has one basic aim for businesses, namely to accelerate the development pace and improve the quality of offered products and services, while reducing operating costs. Although it seems apparently simple, paradoxically innovation of Polish business organizations from the SME sector is burdened with the concern about the unknown. SMEs are afraid of investing in solutions that are not popular yet. Nevertheless, the strategic vision of the management in such organizations will determine the directions and pace of popularising modern and effective solutions in knowledge management, which may contribute to the improvement of their competitiveness on the global market.

SMAC solutions opens up a new frontier for digital business. This is because virtually every application, service and IoT object incorporates an intelligent aspect to automate or augment application processes or human activities. Digital representations of things and organizational processes are increasingly used to monitor, analyze and control real-world environments. These digital twins combined with SMAC and immersive experiences set the stage for open, connected and coordinated smart spaces. Formal mechanisms to identify technology trends and prioritize those with the biggest potential impact on the business create competitive advantage.

Acknowledgements

This work has been supported by Project BS-PPPB16IM/2018: The Process of Digital Maturing on Polish Intelligent Organizations – WSB University in Poznań (Poland).

References

Adamczewski, P. (2018a). ‘Intelligent Organizations in Digital Age - Case Study of SMEs in Poland’, *MEST Journal*, Vol. 6, No. 2, pp. 1-11, Toronto.

Adamczewski, P. (2018b). ‘The Digital Transformation Pyramid on Intelligent Organizations’, *IT for Practice 2018*, Ed. J.Ministr, M.Tvrdikova, Technical University Ostrava, pp. 65-78, Ostrava.

Adamczewski, P. (2017). ‘E-logistics as the ICT Support in Modern Polish Organizations’. *Chinese Business Review*, Vol. 16, No. 8, pp. 391-410, New York.

Anderson, C. (2015). *Creating a Data-Driven Organization*, O’Reilly Media, Sebastopol.

Betz, C.T. (2018). *Managing Digital. Concepts and Practices*. The Open Group Press, San Francisco.

Corcoran, P., Datta, S. K. (2016). ‘Mobile-edge Computing and the Internet of Things for Consumers: Extending Cloud Computing and Services to the Edge of the Network’. *IEEE Consumer Electronic Magazine*, Vol. 5, No. 4, pp. 73–74.

Gartner (2018). *Top 10 Strategic Technology Trends for 2019*. New York.

Grösser, S.N., Zeier, R. (2012). *Systematic Management for Intelligent Organizations*. Springer-Verlag, Berlin Heidelberg.

Lechman, E. (2018). *The Diffusion of ICT*. Routledge – Taylor & Francis Group, London – New York.

McConnell, J. (2017). *The Organization in the Digital Age*. New York.

Olszak, C.M., Pełech-Pilichowski, T., Mach-Król M. (Eds.) (2017). ‘Advances in Business ICT: New Ideas from Ongoing Research’. *Studies in Computational Intelligence*, Volume 658, Springer, Berlin-Heidelberg.

Riche, N.H., Hurter, Ch. (2018). *Data-Driven Storytelling*. Taylor & Francis Group, Raton.

Schwaninger, M. (2010). *Intelligent Organizations*. Powerful Models for Systematic Management. Springer-Verlag, Berlin Heidelberg.

Schwab, K. (2016), *The Fourth Industrial Revolution*. World Economic Forum. Cologny.

Ziemba, E. (2017), ‘The Contribution of ICT Adoption to the Sustainable Information Society’, *Journal of Computer Information Systems*, Vol. 59, No 2, p. 116-126.

Results and Benefits of Erasmus+ Project IESED

Roman Danel[1 2], Michal Řepka[3]

Abstract. The paper describes international Erasmus+ project IESED (Innovative ICT Education for Social-Economic Development) solved during 2016-2019 by a consortium of several European HEI's. The aim of the project was to help with solving a lack of compatibility between European and Belarusian HEI. Project IESED arise from the Road Map for Higher Education Reform established by Belarusian Ministry of Education in 2015 for aligning Belarusian Higher Education with the Bologna Process. The paper describes actions taken with selected Belarusian HEI.

Keywords: IESED project, teaching via videoconference system, remote access to laboratory, ICT competencies, Education Road Map, Bologna Process.

JEL Classification: D8

1 Introduction

We have been working with WSG Bydgoszcz (Poland) since 2012, where we ensure several courses at the Department of Informatics and Mechatronics. One of the results of this cooperation is our involvement in the international IESED project (Innovative ICT Education for Social - Economic Development), funded by the Erasmus + programme. Within this project five Belarusian HE institutions in partnership with several EU HE institutions formed a consortium with the aim to increase the competitiveness of mentioned Belarusian HEIs and help them to fulfill requirements of the Bologna Process. The IESED project was solved between October 2016 and October 2019.

Belarusian participants:

- Belarusian State Pedagogical University named after Maxim Tank;
- School of Business of Belarusian State University;

[1] University of Economy Bydgoszcz/Department of informatics and mechatronics, Garbary 2, 85-229 Bydgoszcz, Poland, roman.danel@byd.pl.

[2] VŠB – Technical University of Ostrava/Faculty of Economics, Department of Computer Science, Sokolská třída 2416/33, 702 00 Moravská Ostrava, Czechia, roman.danel@vsb.cz.

[3] University of Economy Bydgoszcz/Department of informatics and mechatronics, Garbary 2, 85-229 Bydgoszcz, Poland, michal.repka@byd.pl.

- Vitebsk State Technological University;
- Private Institute of Management and Business;
- Belarusian State University of Informatics and Radio-electronics
- International participants of the project:
- Alytaus Kolegija (University of Applied Science, Lithuania), coordinating institution;
- University of Lille (France);
- De Montfort University (School of Computer Science and Informatics, UK, Leicester);
- University of Economy Bydgoszcz (Poland).

2 Project IESED objectives

Main aims of the IESED project is to increase the competitiveness of five Belarus universities offering education that meets changing needs of the socio-economic environment. The lack of compatibility with other similar institutions and educational frameworks, particularly in Europe, mitigates against the best interests of staff and students in Belarusian institutions in a number of ways. Most obviously, international exchanges, particularly for students are difficult to organize, since the programmes are not only organized in an insular way, but also lack a precise specification of the level at which any contributory course is delivered, being focused more on satisfying syllabus content, than building on capabilities

Specific goals of the project are:

- Development and implementation of five new flexible study programmes on the bachelor level based on new approaches satisfying ECTS in line with Bologna requirements;
- 25 courses including implementation of innovative teaching/learning methods and tools;
- Purchasing equipment for five e-Learning laboratories for partner universities from Belarus;
- English language courses for lecturers from Belarusian universities.

Project partners participate at assistance in increase of competencies of specialists in the IT field and improvement of the quality of higher education which meets changing needs of the economy of Belarus and requirements of the Bologna Process.

3 Internship „Innovative Study Methods”

In July 2017, we attended a two-week internship at WSG Bydgoszcz, where we presented our teaching experience to representatives of Belarusian universities.

During our lectures we presented experience with teaching students at a remote workplace using a videoconferencing system. Both positives and negatives were presented. The view of the cost-effectiveness of teaching using a videoconference system is a managerial view assessing the economic aspects of the issue. However, another question is the quality of education and the students´ assessment of the videoconference system. Last but not least, technical reliability and costs of maintenance also play a role. Repeated questionnaire surveys amongst the students of technical fields of automation and information science found that in general, students rate teaching via videoconference negatively and prefer live teaching

Furthermore, a system for remote access to the laboratory for automation teaching was presented. This system was developed at VŠB-Technical University of Ostrava in 2013-2015. Through an internet application, students have access to physical equipment in the laboratory of automation and distributed control. Equipment is monitored by a webcam and students can remotely perform simple experiments using robotic laboratory equipment Bioloid from the Robotis Company (South Korea). The architecture of the solution has been presented in (Řepka and Danel, 2015). A prerequisite for the functional solution is to ensure access to the controlled physical model, so that in a given time only one user can control the model. For this reason, a reservation system has been programmed within this application. The access system works in a way that any user who wants to work with this laboratory model must make a reservation for a certain period of time. In this period of time one is ensured an access to manipulate remotely with the laboratory model. Other users can only monitor what is happening there - they cannot have any influence on this model. For now, one assignment has been put into operation – control of a robotic vehicle, which can be used to present some know-how from automatic control (Řepka and Danel, 2015). The internet application for login, ordering access time and actual control of the robot were solved by students as their final thesis (Černín, 2014).

Recently, the trend is to integrate more and more digital technologies into education, use of multimedia tools, lectures in the form of videos, videos demonstrating experiments in laboratories, etc. Consequently, there is an opinion of complementing the teaching of technical subjects via videoconference with multimedia teaching materials. This is of course possible, but even the use of multimedia has its limitations and cannot absolutely replace the direct contact of teachers with students. In his book, Manfred Spitzer (2015) shows the results of a test which assessed the study results of teaching in two classes. In the first class, teaching was performed in the classical way with printed literature; while in the other class teaching was performed using tablets and multimedia teaching materials. In the case of the second class, student´s results gradually deteriorated. Spitzer gave a reason for this that studying using multimedia materials leads to compromised concentration on the actual content.

Blended learning is one of the ways how to effectively use digital technology in education and at the same time eliminate the shortcomings mentioned in the previous paragraph (Ministr and Pitner, 2014). It is a combination of face-to-face teaching with e-learning. WSG Bydgoszcz teaches some courses for distance students in the form of blended learning and the first results are positive - favorable assessment by students. (Kozel et al, 2012) points out the practical use of Facebook for universities, where the multiplication effects of this social network were activated by cooperation between teachers and students, when solving scientific and innovative projects or in the actual learning process.

In the case of subjects where experiments must be performed, examples explained and which require interaction with students, direct contact with students is more suitable. Remote access to laboratories in this field is only a complementary tool and cannot replace the presence of a teacher. Therefore, we assume that the method of providing teaching at a remote site should be a sensible compromise between cost-cutting using teaching via videoconference for selected subjects, and the direct presence of teachers in classes which require a personal approach.

4 Final project meeting and the results achieved

A number of workshops, experts' meetings and internships took place during the project (e.g. Lille - October 2017, Alytus - May 2018, Leicester - October 2018, Bydgoszcz – February 2019). At these meetings, we collaborated on modeling the profile of the IT / ICT graduate and consulted with Belarusian partners to develop curricula to match the Bologna process and credit system.

Range of challenges have hindered the progress through The Belarusian Ministry of Education Road Map (2015) in the intervening years. The process is now well behind the agreed timeline as recognized in the independent report produced through the EPCSF (Eastern Partnership Civil Society Forum) report (2015). This report was also presented at the IESED Lille meeting (2017) in summary. It provides details on the various ways in which the Road Map implementation falls short of its commitments, especially in relation to the three structural paradigms referred to from the Yerevan conference (EHEA report, 2015) aims of the conference were aligning Belarusian Higher Education with the Bologna Process in order to establish EHEA - European Higher Education Area - membership. EPCSF Report 2017 referers to the fact that the proposed three cycle system that falls short of a framework, since there is no precise specification of the nature of the learning outcomes. There is also no use of ETCS as basis for quantizing study units in the new code (complies with the 3-cycle model). The importance of integrating level expectations into any qualification's framework (QF), in particular using the well-established taxonomy founded by Bloom (Bloom et al, 1956), which is revised by few, e.g. (Anderson & Krathwohl, 2001) has also been stressed, in particular at the Lille meeting, in relation to this project. On analysis of the individual study programmes, however, there is a notion of an expectation of the amount effort required for a year of study. In otherwise, at taught level, there is, at least in some cases, an understanding of the nature of definition and use of an appropriate Higher Education QF, even new code as realized by the Belarusian MoE maybe incomplete and confusingly presented.

In some cases, at BY HEI, there are great differences between the amount of credits awarded, and the formally assigned contact hours. This is mainly to account for variations in the nature of the study units. Some naturally require less formal contact hours, and more individual study, when for example, there is a significant practical or research element.

A difficulty here, though, is that, although there is a concept credits in relation to effort, and progress is being made on aligning the amount of schedule study to a consistent amount of credit rewarded (notionally about 27 hours per BY credit), the precise number of credits required to gain a specific award at given level and status varies between programme. A 4-year specialist award (about equivalent to a first cycle Bologna award) will vary in the amount credit required between just over 200 and just under 240 credits, but generally comes in at about 220 credits. The IESED team consider that the lack of precision here undermines the concept of a QF, which clearly needs to be a consequential outcome of the overall road map.

In the context of the IESED some of these failings of the Road Map are beyond the scope and ability of the project to address, however, in relation to move toward a qualification framework, there is potential for the project to provide some useful guidance, in the form of pilot schemes of computing, within the three-cycle system, which propose and assume the nature of framework which may be eventually realized.

At the beginning of October 2019, the final meeting of the IESED project took place in Minsk. At this meeting, the whole course of the project and the state of fulfillment of the set objectives were evaluated.

As a one of key IESED project results (IESED, 2019), five new study programs were updated and innovated for the Belarusian universities (Information Resource Management, Mathematics and IT, Management with IT Specialization, Information Systems and technologies, Engineering Psychological Maintenance of Information Technologies) and 25 new courses using innovative teaching/learning methods were created. Five new laboratories were established: Resource Center of E-learning Pedagogy (Belarusian State Pedagogical University), Media Studio (School of Business), ICT Technologies Classroom (Private Institute of Management and Business, Minsk), Educational and Research Laboratory of Multimedia Technologies (Vitebsk), 3D Modelling Laboratory (Belarusian State University of Informatics and Radio-electronics). The profile of modern ICT competencies has been defined as a guide for the development of IT / ICT degree programs.

5 Conclusion

This paper gives a brief overview of the objectives and achievements of the international Erasmus+ project IESED solved in 2016-2019. The main objective of the IESED project was to improve competitiveness of Belarusian HEI by transferring ideas, expert skills and experiences from participants involved for many years in the Bologna process. We have explored in this paper the Belarus HE Roadmap for Higher Education Reform (2015) and initiatives necessary to achieve it to aligning Belarusian Higher Education with the Bologna Process principles in order to establish EHEA membership.

Acknowledgements

The project IESED was co-funded by the Erasmus+ Programme of the European Union KA2 – Cooperation for innovation and the exchange of good practices - Capacity Building in the field of Higher Education. Project number 574283-EPP-1-2016-1-LT-EPPKA2-CBHE-JP.

References

Anderson, L., & Krathwohl, D. (2001) *A taxonomy for learning, teaching and assessing: A revision of Bloom's taxonomy of educational objectives*. New York: Longman.

Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H. and Krathwohl, D. R. (1956) *Taxonomy of educational objectives: The classification of educational goals*. Handbook I: Cognitive domain. New York: David McKay Company.

Černín, J. (2014) *Usage of web application for remote control of four-wheel car model,* [In Czech: Využití webové aplikace pro vzdálené řízení laboratorního modelu čtyřkolového vozidla], bachelor thesis, supervisor: M. Řepka, VŠB-Technical University of Ostrava.

Eastern Partnership Civil Society Forum (2017) *Implementation of the Belarus Roadmap for Higher Education Reform,* [Online], Available: http://eap-csf.eu/wp-content/uploads/5th-Bologna-Report_EaP-CSF.pdf [10 Sep 2019].

EHEA Report, (2015) *Belarus Roadmap for Higher Education Reform, Yerevan Ministerial Conference,* [Online], Available: http://bologna-yerevan2015.ehea.info/files/Roadmap%20Belarus_21.05.2015.pdf [10 Sep 2019].

IESED. (2019) *Curriculum for training IT specialists,* [Online], Available: http://iesed.esy.es/pimb/ [10 Sep 2019].

Kozel, R., Poštulková, H., Friedrich, V. and Vilamová, Š. (2012) 'The cooperation of teachers and students on Facebook', *Proceedings of 20th Interdisciplinary Information Management Talks IDIMT 2012 – ICT Support for Complex Systems*, Poděbrady, Czech Republic, Linz: Trauner Verlag Universitat, pp. 277-285.

Ministr, J. and Pitner, T. (2014) ‘Towards an ecosystem for academic-industrial cooperation‘, *Proceedings of 22nd Interdisciplinary Information and Management Talks IDIMT 2014* (*Networking Societies – Cooperation and Conflict)*, Poděbrady, Czech Republic, Linz: Trauner Verlag Universitat, pp. 71-78.

Spitzer, M. (2015) *Cyberkrank!: Wie das digitalisierte Leben unsere Gesundheit ruiniert*, München: Droemer.

Řepka, M. and Danel, R. (2015) ‘Remote control of laboratory models‘, *Proceedings of CIAAF'2015 - 1st Ibero-American Conference of Future Learning Environments*, Porto, Portugal, pp. 59-63.

CRM and Artificial Intelligence

Milena Janakova[1], Petr Sauman[2]

Abstract. The article focuses on Customer Relationship Management (CRM) systems and the implementation of artificial intelligence as one of the most important innovative power in business. The top CRM vendors, such as Microsoft, Oracle, Salesforce and SAP show interest in artificial intelligence. Artificial intelligence also has a place for small business. There is more effective marketing, better customer experience, increased sales efficiency and optimal decision making. Benefit brings solutions like Acquisio, Intercom's Answer Bot, MailChimp and X.ai. Many of them are available for testing, such as open-source.

Keywords: Artificial Intelligence, CRM, Information Technology, Small Business.

JEL Classification: C88, M31

1. Introducton

CRM (Customer Relationship Management) system is a suitable information system for business and also for small business as well. This is because CRMs (CRM system) supports the collection of customer data and this data is useful for improving customer satisfaction and purchasing based on a proven strategy (Fatouretchi, 2019). In the strong competitive society, traditional markets need to build a long-term relationship with customers and ensure optimal knowledge for profit (Barbosa, 2018). Another important point of CRMs is ability to set up customer segmentation (Qian et al, 2018). The customer base is divided according to different perspectives to perform further segment analysis to have as many loyalty customers as possible.

In many cases, small businesses have difficulties with low levels of resources to support business activities. It is also a lack of human resources (specialists of information technology) to know about optimal IT (Information Technology) implementation. One solution brings artificial intelligence that works in the background and helps in the real situation. A Gartner 2019 survey shows that 37% of organizations have have

[1] University in Opava, School of Business Administration in Karvina, Univerzitni nam. 1934/3, 733 40 Karvina, Czech Republic, e-mail: mija@opf.slu.cz.

[2] University in Opava, School of Business Administration in Karvina, Univerzitni nam. 1934/3, 733 40 Karvina, Czech Republic, e-mail: O170733@opf.slu.cz.

implemented artificial intelligence in some form (Stamford, 2019). There is an interest in artificial intelligence in all industries and a number of applications. Artificial intelligence helps with e-commerce, quick learning, or market prediction (Martin, 2019):

- To maintain a competitive advantage in the market. This is useful when searching for different products using natural language processing. This artificial intelligence is part of business strategy (eBay).
- To learn anything about technology, functions with self-help. This helps to find the right book (GoodReads).
- To publish of quotes on global stock exchanges, currency pairs, and major commodities by sending economic data (NetDania Forex).

In many areas, artificial intelligence has unlimited potential to support chatbot, e-commerce, predictive analysis, process automation or virtual personal assistant (Artificial Intelligence Software, 2019). Big vendors such as Salesforce, Oracle, SAP, and Microsoft have a particular interest in artificial intelligence. The question is the usefulness of artificial intelligence for small businesses for this paper. For this purpose, a literature review was conducted that specified the possibilities of artificial intelligence (chapter 2), and selected artificial intelligence solutions monitored to learn more about them with reference to the transformation of small business (chapter 3).

2. Artificial Intelligence

From a public perspective, artificial intelligence is the ability of a machine to emulate intelligent human behavior (Merriam-Webster, 2019). Artificial intelligence has the power to create innovations for greater usefulness and efficiency (Walters, 2019), and it is necessary to use a chatbot, smarter email marketing, or to understand the customer's journey on website based on an artificial intelligence strategy (Marr, 2019).

Many IT users highly value the key features of artificial intelligence, for example (Find out more about Artificial Intelligence Software, 2019):

- Activity. Artificial intelligence monitors inputs, uses rules and procedures to calculate alternatives and make optimal decisions.

- Adaptability. Artificial intelligence uses machine learning to learn from results and improve performance.
- Concurrency. Artificial intelligence cares with multiple systems at the same time.
- Future prospectuses. Artificial intelligence searches in different scenarios to find the optimal way.
- Receiving data. Artificial intelligence works with big data at high speed.

To get a better idea of the skills of artificial intelligence, well-known artificial intelligence solutions are free of charge to try or open-source. There are solutions such as Azure Machine Learning Studio, Playment, Salesforce Einstein, and TensorFlow.

- Azure Machine Learning Studio is software designed to create, test, and implement predictive data analytics solutions in a very short time. There are best-in-class algorithms and a visual development environment that is deployed without coding knowledge (Azure Machine Learning Studio, 2019).
- Playment provides training data for machine learning, computer vision, and human-in-the-loop. It helps to collect and tag data using artificial intelligence. This solution works with micro-tasks problems for further processing by human-in-the-loop workers (Playment, 2019).
- Salesforce Einstein collects data to know recommendations and predictions based on business processes that support to connect with customers. Such CRMs is more productive and customers more satisfied (Salesforce Einstein, 2019).
- TensorFlow is an open artificial intelligence library that supports numerical computation using data flow charts. The solution is available for the server, desktop, or mobile devices (TensorFlow, 2019).

The application of artificial intelligence changes over time. There are interesting solutions that understand, search and read to learn about the development of technology, tools, and information. They are also for small business.

3. Transformation of Small Business with Artificial Intelligence

In many cases, small businesses focus on very special tasks with high added value to be competitive. In this respect, customer segmentation has an important place here for a competitive advantage (Siggelkow & Terwiesch, 2019). There is an important transformation based on four perspectives (Rouse, 2006) for small business development:

- Value of opportunity. It brings the possibility of market success and new innovations based on modern technology.
- Value of threat. It works with a scenario of failure of the company's position in the market.
- Value of competition. It enables the transformation to go a useful way to improve market position.
- Value of crises. This is a market situation that starts triggers such as cash flow problems or unemployment.

From a statistical perspective, there is an interest in the correlation between CRM, product innovation and customer satisfaction (Elfarmawi, 2019). There is no doubt about the usefulness of CRM for small business as these systems take care of customers. Particular interest is how to start marketing with artificial intelligence (Johnston, 2019), and to help develop customized products to increase business profits. Small business also has artificial intelligence solutions that help with CRM. Good help is visible for tasks as (McFarland, 2019):

- To simplify marketing.
- To improve the customer experience.
- To increase sales efficiency.
- To improve decision making.

The customer is highly educated and informed in the global information society. An existing consumer requires a personal approach and a solution with some extra bonus and artificial intelligence supports some extra with personalized marketing and e-mail, communication with customers via chatbot, or sophisticated personal assistant. Please, see Table 1.

Increase sales efficiency uses online marketing and e-mail communication, a chat solution to start communicating with customers through a website. This has to target visitors with specified criteria in natural language processing. Chatbot initiates communication with a prospective customer, and further activities are associated with interacting with a live agent or recording information for a sales representative. And a personal assistant also has an important place here.

Table 1 A list of Artificial Intelligence Solutions for Small Business, Source: own.

Artificial intelligence solution	**Function for small business**
Acquisio, AdRoll, and WordStream	To improve online marketing. To know which goods and services will have success according to the customer searches and there are also personalized recommendations.
Drift, Intercom's Answer Bot, and WhosOn	To improve customer experience and communicate with customers by chatbot for solving customer questions through the website with instant answers.
MailChimp	To integrate with e-mail communication and marketing solution. It is available to set physical and online customer list and create segmented e-mail lists by location or purchase volume.
X.ai	To improve decision making with less time on booking meetings and scheduling based on a personal assistant.

4. Conclusion

Artificial intelligence is an interesting part of IT implementation. IT users perceive their unlimited potential to help with chatbot, e-commerce, predictive analysis, process automation, or a virtual personal assistant. There are well-known solutions such as Azure Machine Learning Studio, eBay business strategy, or Salesforce Einstein. Artificial intelligence also has advantages for CRM and small business. Small businesses evaluate Acquisio, AdRoll, Drift, Intercom's Answer Bot, MailChimp, WhosOn, WordStream, and X.ai. They focus on online marketing, e-mail communication, customer experience, chatbot, and a personal assistant.

Acknowledgements

This paper was supported by the project no. SGS/19/2019, “Application of Customer Relationship Management Systems in Small and Medium-sized Enterprises” accepted in 2019.

References

Artificial Intelligence Software. (2019), [Online], Available: https://www.capterra.com/artificial-intelligence-software/ [2019].

Azure Machine Learning Studio. (2019), [Online], Available: https://studio.azureml.net/ [2019].

Barbosa, D. G. (2018) *Knowledge is Profit: The Role of Espionage and Intelligence in Business*. Manchester: Independently published. ISBN 9781980511182.

Elfarmawi, W. (2019) Correlation Between Customer Relationship Management System Usage, Product Innovation, And Customer Satisfaction. *Foundations of Management*, Vol. 11, pp. 23-32. eISSN 2300-566. DOI 10.2478/fman-2019-0002.

Fatouretchi, M. (2019) *The Art of CRM: Proven strategies for modern customer relationship management*. Birmingham: Packt Publishing. ISBN 978-1-78953-892-2.

Find out more about Artificial Intelligence Software. (2019), [Online], Available: https://artificial-intelligence.financesonline.com/ [November 05, 2019].

Johnston, B. (2019) *10 Easy Ways to Get Started with Marketing AI (Artificial Intelligence)*, [Online], Available: https://www.singlegrain.com/artificial-intelligence/10-easy-ways-to-get-started-with-marketing-ai/ [Sep 27, 2019].

Martin, S. (2019) *12 Best AI & ML Based App Ideas For Startups & SME's That’ll Make Money in 2019–20*, [Online], Available: https://towardsdatascience.com/12-best-ai-ml-based-app-ideas-thatll-make-money-in-2020-96d104b6367e [September 12, 2019].

Marr, B. (2019) *How To Develop An Artificial Intelligence Strategy: 9 Things Every Business Must Include. Forbes*, [Online], Available: https://www.forbes.com/sites/bernardmarr/2019/03/19/how-to-develop-an-artificial-intelligence-strategy-9-things-every-business-must-include/#12518cb48360 [Mar 19, 2019].

McFarland, R. (2019) *5 Ways Small Business is Using AI and Machine Learning Right Now*, [Online], Available: https://www.coxblue.com/5-ways-small-business-is-using-ai-and-machine-learning-right-now/ [Jul 9, 2019].

Merriam-Webster. (2019) *Definition of artificial intelligence*, [Online], Available: https://www.merriam-webster.com/dictionary/artificial%20intelligence [2019].

Playment. (2019), [Online], Available: https://playment.io/ [2019].

Qian, Ch., Yang, M., Li, P. and Li, S. (2018) Application of Customer Segmentation for Electronic Toll Collection: A Case Study. *Journal of Advanced Transportation*, Vol. 2018. Article ID 3635107, 9 pages. DOI https://doi.org/10.1155/2018/3635107.

Rouse, W. B. (2006) *Enterprise transformation: Understanding and enabling fundamental change*. New York: Wiley-Interscience. ISBN-10 0-471-73681-3.

Salesforce Einstein, (2019), [Online], Available: https://www.salesforce.com/products/einstein/overview/ [2019].

Siggelkow, N. and Terwiesch, Ch. (2019) *Connected Strategy: Building Continuous Customer Relationships for Competitive Advantage*. Boston: Harvard Business Review Press. ISBN 978-1-63369-7003.

Stamford, C. (2019) *Gartner Survey Shows 37 Percent of Organizations Have Implemented AI in Some Form*, [Online], Available: https://www.gartner.com/en/newsroom/press-releases/2019-01-21-gartner-survey-shows-37-percent-of-organizations-have [January 21, 2019].

TensorFlow. (2019). [Online], Available: https://www.tensorflow.org/ [2019].

Walters, N. (2019). *How Artificial Intelligence Can Help Small Businesses*, [Online], Available: https://articles.bplans.com/how-artificial-intelligence-can-help-small-businesses/ [2019].

The Study of Online Payment Systems in Poland

Anna Sołtysik-Piorunkiewicz[1], Krzysztof Pyszny [2],
Przemysław Majerczak[3]

Abstract. The article concerns the analysis of the authorization methods used in electronic payment services in terms of their security and acceptance. The purpose of the article is to identify the factors of high acceptance of online payment services by users based on research results on trust and popularity among users. The study took into account various forms of electronic payments, i.e. bank online transfer, card payments, payments via the online payment service operator, blik or sms, and the level of users' knowledge of authorization methods and their practical application to secure access to data using known data was determined technician in banking and online payment transactions.

Keywords: security, authorization, online payments, password, e-banking.

JEL Classification: L86

1 Introduction

The development of the electronic economy brings many challenges faced by the information society. On the one hand, there is a significant increase in the market share of e-customers using various electronic services in business, administration and social networks. On the other hand, there is an increase in the activity of cybercriminals, using more and more complex, exploiting technical gaps and the weakness or ignorance of IT system users in the use of security methods and data access techniques that are the basis for providing services on the Internet. According to the TNS Polska report prepared for the Association of Polish Banks and the National Clearing House in 2015, approximately 55% of bank customers made online purchases (online: *Polacy chętniej kupują…*). Currently, the European Union's cybersecurity policy focuses on the challenges related to its effective implementation in the context of providing the current political and legal framework, increasing expenditure on cybersecurity, streamlining activities for the benefit of the information society to make it more resistant to cyber-

[1] University of Economics in Katowice, Department of Informatics, University of Economics in Katowice, 1 Maja 50, anna.soltysik-piorunkiewicz@uekat.pl.
[2] Student of University Economics in Katowice, krzysztof.pyszny@edu.uekat.pl.
[3] Student of University Economics in Katowice, przemyslaw.majerczak@edu.uekat.pl

attacks (online: *Unijna Polityka Bezpieczeństwa...*). This involves raising knowledge about cybersecurity and skills in methods and techniques that can be used. This is even more an important problem, as interest in electronic banking (Michalski, 2002, p. 130-144) and various forms of payment in the information society is constantly increasing in line with the forecast of using e-services in banking (Chmielarz, 2005, p. 37) and payments in electronic commerce (Dąbrowska, Janoś-Kresło and Wódkowski, 2009, p. 69). At the same time, trust in the use of electronic forms of banking in the information society is growing, as indicated by research on social diagnosis (Czapiński and Panek, 2007, p. 170). Currently, according to the TNS Polska report published in 2018, 91% of Poles declare that using online and mobile banking is secure and 42% recognize banks in Poland as cybersecurity leaders (online: *RAPORT ZBP...*).

The purpose of the article is to examine the factors that affect the high declared level of use of electronic services and a sense of security among users of electronic payment systems. The study included questions about the trust and popularity of various forms of electronic payment, the use of data access security methods and the use of modern techniques in the implementation of online payments.

2 Overview of electronic payment systems

Electronic payment is any system used to settle financial transactions through the transfer of monetary value, and includes the institutions, instruments, people, rules, procedures, standards, and technologies that make such an exchange possible. With the advent of computers and electronic communications a large number of alternative electronic payment systems have emerged. These include debit cards, credit cards, electronic funds transfers, direct credits, direct debits, Internet banking and e-commerce payment systems. Now electronic payments is a very common way of making transactions. In Poland there are the most popular systems of electronic payment: Paypal, PayU or Przelewy24.

The development of payment systems is associated with the growing need of electronic business in the field of access to means of payment without being limited by time or place of access. Currently, the most popular forms of payment via the Internet (online: *Płatności przez internet...*) are:

- internet transfers,
- payments with payment cards,
- SMS payments,
- payments using online wallets,
- cash payments on the Internet,
- paysafe-card prepaid cards,
- blik.

The latest form of payment is blik, which has developed with the development of mobile devices and the availability of mobile phones. Blik (online: *Jak zacząć korzystać z blika...)* is a payment method available in the mobile application offered by most banks in Poland. It can be used by all owners of bank applications that provide such a payment option. It allows you to make payments in stationary and online stores, cash withdrawals and deposits at ATMs/cash deposit machines, instant transfers to a phone number between customers of different banks (so-called phone transfer), generating blik checks (a 9-digit code) used to make payments and cash withdrawals from ATMs.

3 Security methods and techniques for accessing data in electronic payments

Online services like buying online and logging into the bank's website, need to implement security systems for user authorization. During authorization, the bank never requires (*Zasady bezpiecznego korzystania*…) to provide:

- one-time code when logging into the website,
- one-time codes at the same time,
- payment card data when using the bank's website, such as: card number, expiry date and CVV2 / CVC2 code,
- personal and / or contact details (including mobile phone number) after logging into the bank's website,
- one-time code for authentication, identification, confirmation of the IP address of the computer from which the transaction is carried out.

Two-step verification (online: *Allegro – dwustopniowa weryfikacja*…), introduced in 2019 in Poland, also allows users to increase security in online payment transactions. Two-step verification is an additional level of security when logging into websites. If the website uses such a mechanism, when logging in it will require from us not only a login and password, but also a one-time code. Depending on the solution, such a code can be received by SMS or, for example, rewritten from the appropriate application. This solution means that even if the identity thief takes over our login and password, he will not be able to log into our account. The Allegro.pl auction site was the first website in Poland to introduce a two-step verification level for its users

The basic principles of online payment security (online: *Płatności przez Internet*…) are currently based on the following guidelines:

- trusted payment institutions in the PFSA,
- verified account number,
- a ban on the use of public hot spots,
- chargeback,
- a ban on using full-screen mode in the browser,
- a ban on the use of unpopular browsers.

4 Research on electronic payment systems in Poland: authorization, trust and popularity

The aim of the study was to check whether users care about their security during online payments, as well as the popularity of forms of this payment among Internet users and the use of intermediary companies in the implementation of payment services on the Internet. In order to verify the level of security and awareness of users of online banking portals, a survey was conducted using the Google Forms tool. About 60 respondents took part in the study. The survey aimed to determine the answers to the following research questions:

1) What forms of payment and intermediaries do the respondents use?
2) What kind of password the respondent use to determinate the access to the data payment:
   a) How long passwords do the respondents use?
   b) What character combinations do they use?
   c) How many passwords do they use?
3) Do they use the blik service?

4) What are the most important advantages of electronic payments for respondents?

4.1 Research methodology

The subject of the study was to determine contemporary trends in the information society in Poland among the inhabitants of the Silesian Voivodeship regarding the use of electronic payment forms, security methods and the level of user confidence. During the development of research assumptions, the survey took into an account the conclusions of reports from industry units such as banks, online payment brokers, and e-commerce institutions. The respondents were asked questions about preferred forms of payment, frequency of using various forms of payment, including also Blik, trust in online payment intermediaries they used. The users' knowledge of online banking security was also checked, and the level of security used by them in the field of data access authorization (password length, character combinations used, password change frequency) was verified.

The research group consisted of 62 people between the ages of 18 and 60, mainly students of the University of Economics in Katowice in the field of Computer Science or Computer Science and Econometrics, living in the Silesian Voivodeship. The respondents answered questions about sex, education and population size in the place of residence.

Most of the respondents were men (61%), mainly belonging to the 18-30 age range. The education of the respondents is divided into two main groups, in which secondary education constitutes 53% and higher education 45%. The origin of the respondents was very diverse, however, urban dwellers dominated from 150,000 residents up to 500,000 residents.

The CAWI method using Google Forms was used in the survey. Only survey results that were completed in full were taken into an account. Respondents could only reply once from the associated Google account. The survey was conducted in December 2019, it covered the answers to 16 questions related to the popularity and trust of various forms of electronic payment and security methods used in the authorization of data by users. The questionnaire used three forms of closed questions: single choice, multiple choice and with a five-point Likert scale assessment.

In order to verify the security of users using electronic banking, research on data access techniques used in user authorization was conducted. Therefore, the following questions were asked:

- the number of different passwords,
- password length,
- password complexity,
- using one password for multiple accounts,
- the frequency of changing the password.

In addition, respondents were asked to provide an assessment of their online security and to specify the level of trust in payments in online banking

Then, the popularity of electronic payment methods was examined. Questions were asked that allowed determining the percentage share of users using:

- online banking,
- individual payment methods,
- online payment intermediaries,
- depicted close.

4.2 Research results

Forms of payment – trust and popularity

Based on the survey, it can be concluded that the majority of respondents use online banking. It is connected primarily with the possibilities offered by banking portals in terms of the speed of payment transactions, comfort and mobility of the solution. In the fourth place among the factors affecting the use of online banking services, the respondents mentioned security.

Among the forms of electronic payment, payment by debit / credit card turned out to be the most popular, in the second place the respondents mentioned the payment by online transfer, and the third place was blik. According to earlier data provided by companies and research centers, PayU is the most popular among online payment intermediaries, Przelewy24 is in second place, and DotPay is in third place.

In the 18-30 age range, it is the main form of payment for both people with secondary and higher education. Blik and online transfer with 24% came second. The least popular is cash payment, which only three respondents chose. None of the respondents chose the traditional transfer, which was replaced by other forms of payment.

Electronic payment security

Thera are various forms of passwords in use during authorizing access to payment data or online banking usage. However, they most users often use over 12 characters in the password. Interestingly, there are also those who declared the use of only 5-character passwords, which is a clear failure to comply with the security rules on the side of payment portals. Most users use multiple passwords. Unfortunately, the survey showed that users do not change passwords, only 11% change the password once a month. The respondents nevertheless rated their safety quite high. Internet banking also enjoys great or very high trust in most respondents.

Over half of the respondents use passwords consisting of over 12 characters (52%). The study group was dominated by a password consisting mainly of uppercase and lowercase letters and numbers. Users usually use three to five passwords. Respondents are divided about using one password for multiple accounts. Half of the respondents never change their password. On a scale of one to five, respondents most often rated their security on the network at four (46%). At the same time, online payments enjoy above-average user confidence (82%).

5 Conclusions

Previous studies carried out by TNS Polska have shown that the level of trust of adult Poles in online banking has increased to 52% in recent years (online: *Polacy chętniej wybierają płatności online…*). This confirms the results of surveys carried out, in which over 80% of respondents gave a testimony to the high level of trust in online payments. The vast majority of respondents use online banking (95%). The most popular form of online payment is a debit / credit card, which was chosen by 45% of people.

Respondents most often used the services of three major online payment intermediaries: PayU, Przelewy24, DotPay. Over half of the respondents (55%) regularly use the blik service. For the studied group, the biggest advantage of this type of payment is speed (57%) as well as comfort (31%).

Studies have shown that the majority of respondents use online payments. Internet banking users use long and rather complicated passwords. Unfortunately, the fact that most of them do not change their passwords is often worrying, thus exposing themselves to the loss of their data. In addition, half of the respondents use the same password for many services as in the event of a potential leak or attack, it increases the scale of damage that can be caused. Despite the above-mentioned imperfections in user security, they accept the online payment systems because of their basic functionalities. The future research shell be conducted further and more complex reasons of high index of electronic payment in Poland.

Acknowledgements

Authors would like to thank the students of the University of Economics in Katowice in the field of Computer Science and Econometrics, for help in process of research conducting.

References

Czapiński J., Panek J. (2007), *Diagnoza społeczna 2007. Warunki i jakość życia Polaków*. Rada Monitoringu Społecznego, Warszawa.

Chmielarz W. (2005), *Systemy elektronicznej bankowości*, Difin. Warszawa.

Dąbrowska A., Janoś-Kresło M., Wódkowski, A.(2009), *E-usługi a społeczeństwo informacyjne*, Difin, Warszawa.

Michalski A. (ed.) (2002), *Wykorzystanie technologii i systemów informatycznych w procesach decyzyjnych*, Wydawnictwo Politechniki Śląskiej.

Szpringer W.(2008), *Wpływ wirtualizacji przedsiębiorstw na modele e-biznesu*, Szkoła Główna Handlowa w Warszawie, Warszawa.

Polacy chętniej kupują w Internecie, https://www.payu.pl/polacy-ch%25C4%2599tniej-wybieraj%25C4%2585-p%25C5%2582atno%25C5%259Bci-online (dostęp: 17.12.2019)

Unijna Polityka Bezpieczeństwa – wyzwania związane ze skuteczną realizacją, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_PL.pdf [22 Dec 2019].

RAPORT ZBP Cyberbezpieczny portfel, https://www.zbp.pl/getmedia/5f90b612-ac57-43fc-bc98-49870e34d555/Raport_ZBP_-_Cyberbezpieczny_Portfel [22 Dec 2019].

Płatności przez internet:wady i zalety transakcji internetowych, https://www.heuristic.pl/blog/e-commerce/Platnosci-przez-internet-wady-i-zalety-transakcji-internetowych;121.html [22 Dec 2019].

Jak zacząć korzystać z blika?, https://blikmobile.pl/faq/jak-zaczac-korzystac-z-blika/ [22 Dec 2019].

Zasady bezpiecznego korzystania z konta bankowego, https://www.najlepszekonto.pl/zasady-bezpiecznego-korzystania-z-konta-bankowego [22 Dec 2019].

Allegro – dwustopniowa weryfikacja, https://www.spidersweb.pl/2017/06/allegro-dwustopniowa-weryfikacja.html [22 Dec 2019].

Płatności przez Internet: 7 nowych zasad bezpieczeństwa, https://www.bankier.pl/wiadomosc/Platnosci-przez-internet-7-nowych-zasad-bezpieczenstwa-3270798.html?fbclid=IwAR0Xkg0qEpdGpHxQy5Jq3NxsAYZVf3ZQi7mm8XNXzupIQL0y1M3n8h0gsMw [22 Dec 2019].

Polacy chętniej wybierają płatności online, https://www.payu.pl/polacy-ch%25C4%2599tniej-wybieraj%25C4%2585p%25C5%2582atno%25C5%259Bci-online [22 Dec 2019].

The Impact of Case Studies on the Quality of Students' Knowledge of Information Systems

Šilerová, Edita[1], Hřebejková, Jana[2]

Abstract. The subject of information systems is included in the study plans very logically in the third year of the bachelor's degree. Students have already graduated from the field of economy, management, marketing, psychology, computer science. Thus, they have already obtained enough opportunities during the study to create the prerequisites for creating a quality information system. The course combines students of several fields - Operation and Economics, Business and Administrative and Informatics, Public Administration and Regional Development. The composition of the team is very beneficial for the creation of the initial phases of the information system. The output of teamwork is the creation of information strategy, software development, testing and other phases up to the implementation of the information system module.

Keywords: information strategy, information systems, team cooperation, project, implementation

JEL Classification: Q59

1 Introduction

Today, information systems are increasingly being given power and strength throughout society. Information systems are becoming spells throughout society. Companies, government, and all organizations very often use words - the information system is responsible. Information systems and information and communication technologies, in most cases so far, can do nothing more than we (the company, state administration,…) set in our requirements. From this it can be deduced that it is very important that there are experts in the team involved in the various phases of the information system life cycle. The subject Information Systems included in the curricula of several study programs creates the prerequisites for the composition of a qualified team. The students of the study program Operation and Economics will gain theoretical and practical knowledge of the operation of the company. Students in the field of Business and Administration after two years of study have knowledge especially in the field of accounting, corporate records,

[1],[2] Czech University of Live Sciences Prague, department of Information Technologies, Prague 6, Kamýcká 129, silerova@pef.czu.cz.

banking, taxes. The field of Public Administration and Regional Development will prepare students with knowledge of state administration, relation to the European Union. An important role in such a team is played by students of the Computer Science program, who during their studies mainly focus on algorithmization, programming, computer networks, and security. Then the composition of study groups through the entire cross-section of disciplines will allow the creation of a team that has the prerequisites to participate in the creation of a quality information system. Dirks, J.L. (2019) they came to concluded ´Strategies such as multidisciplinary participation, clarifying team resources and goals, and creating practice scenarios can increase the effectiveness´.

A study group composed of students of all fields corresponds to the situation in the company. Agarwal, F. and Ahmed, F. (2017) say ´It encourages collaborative and participatory learning among students and promotes self-learning, critical thinking, and non-linear learning skills. Collective learning extension emphasizes teamwork, coordination, and strengthening interpersonal skills, preparing the students as the next-generation workforce.´

Rob, M.A., Etnyre, V. (2015) the say ´Such a course must provide not only an understanding of the development, applications, and management of information systems, but also some experience on these concepts taught in the classroom. The latter requires innovative ideas and changing modes of instruction, which may include activities for students such as hands-on practice with common IT tools and technologies, case studies, group projects, and group presentations. Engagement of students through various course activities is the key factor in creating a suitable learning environment for students.´.

2 Result and Discusion

We have all met information systems - a student, for example, while studying. Through the module of study they are enrolled in the schedule, enrolled for examinations, they can follow the schedule of teachers and others. So far, there has been no one to complain about the information system. After many discussions it can be said that they do not even know who they are complaining about. Many questions can be asked here:

a. On the computer - probably yes,

b. On the program - about 50% of the answers, many respondents did not know what it was, only 10% of the respondents answered probably no,

c. identify how people are involved in the information system life cycle.

Students of the subject Information Systems also do not know much about information systems before its completion. The advantage is that they know about the existence of software, but they don't know much about how a person is involved in the process. The main aim of the course Information Systems is to gain practical experience and knowledge based on theoretical knowledge (lectures, individual stage)

Students acquire basic theoretical knowledge in lectures. The seminars are attended regularly every two weeks. At the first seminar the student creates a team. There are about 15 students in the team, the ideal situation is when there are students of all disciplines - Operations and Economics, Business and Administration, Informatics, Public Administration and Regional Development. Students have already experienced teamwork in many subjects. In no subject, however, the result did not require cooperation of a student of various disciplines. At the first seminar, students get a team formed and tasked to create roles in the system just as they work in a company. One of the students must lead the team. The group will be the one who is responsible for creating the system in the company. Furthermore, the student chooses the roles of analysts, designers, programmers, testers and roles that are responsible for routine administrative work. Based on many years of experience it can be stated:

- students have a big problem setting roles - only in one case one student wanted to manage the whole team
- students have difficulty following the schedule
- students have a big responsibility problem - regular submission of work
- lower ability to determine the responsibilities of individual team members, control them and publish the outputs of each team member
- it is convenient for students to see concrete results of their work
- consult external companies
- look for example situations proactively.

During the first weeks of the semester, seminars are held regularly. Students must get used to the work system. There are two to three teams in each seminar. Teams must work independently because at the end of the semester they will defend their work against other teams. It is therefore necessary during the semester to ensure that each team can work independently. He had a room for the students to meet (seminar). Students who attend one exercise together know each other well. Occasionally, students from different teams tried to get information from the other team. Based on the experience of the team's work, it should be noted that this did not affect the project results.

Each team met regularly and drew minutes of each meeting. He passed the minutes to the practitioner and consulted the solution procedure and other suggestions for completion of the work once every two weeks.

The result of the project was a functioning small module of the information system, most often the module accounting, warehouse and more. The project also included an economic calculation of the expected price of such a created project.

At the end of the semester, the student presented their project. They had to explain the solution procedure, the chosen methodology, the chosen technologies and create the marketing of the module.

Based on several years of using this model of the project in practice can be stated:

- the students rated the project very positively - there could be no one in the team who would be involved in the project processing (it is very often the case that some students do not work when processing projects in other subjects)
- students saw a concrete result of their work, which they could directly implement in practice - in two cases they expanded the project and used it for their company
- several students were so satisfied with their role in the team that they are currently working on this position
- in many cases, students had to exchange roles

The evaluation of the students of this effective project management depends on the composition of the team. In a team where it was difficult to look for the team leader, the group enjoys the hard work and the results they have answered. In the case of the team composition was excellent and to give responsible results, presentation and appetite for the project of other staff.

3 Conclusion

The processing of projects in the team is very positive for students. Especially for real projects simulating the situation in practice. For the elaboration of such a project it is necessary that the students' study not only theory, they also try to gain knowledge from practice. It is very important to have a team of different experts in this project - just as the situation in the company works. So far, students have only processed projects in teams of students from one study program. The greatest benefit is the cooperation of students from different study programs with different knowledge. In such a team, students are connected with knowledge of economics, informatics, state administration, management, marketing. There will be a model situation that actually exists in every company.

It is therefore possible to recommend the same solution procedure in different subjects of study, where possible, team composition when processing a project from several study programs.

Acknowledgements

This article was created with the support of the Internal Grant Agency (IGA) of FEM CULS in Prague, no. 2019A0010 – „User behavior modeling and disseminating of disinformation on Twitter network in the Czech Republic“.

References

Dirks, J.L. (2019) 'Effective Strategies for Teaching Teamwork'. *Critical Care Nurse*. vol. 39, no. 4, pp. 40-47.

Agarwal, N., Ahmed, F. (2017) ´Developing collective learning extension for rapidly evolving information system courses´. *Education and Information Technologies*. vol. 22, no. 1, pp. 7 – 37.

Rob, M.A., Etnyre, V. (2015) ´Student Perceptions in Teaching Principles of Management Information Systems´. Journal of Education of Business. vol. 90, no. 7, pp. 379-384

INFORMATION MANAGEMENT AND IT INNOVATION

'.

Current Trends in Hardware Development of Artificial Neural Networks

Vyacheslav Chaplyha[1], Mykhailo Mysyk[2], Nataliya Abashina[3]

Abstract. Article analyzes current trends in artificial intelligence systems, in particular, artificial neural networks of different architecture and complexity of training algorithms. The dynamics of publications relative to the main types of hardware for their implementation is estimated. A significant increase in the number of studies regarding optical neural networks is predicted.

Keywords: artificial intelligence systems, artificial neural networks, hardware, current trends.

JEL Classification: C82, C88, C55

1 Introduction

Artificial intelligence systems (AIS) are already widely used in everyday life and have a growing impact on society. We deal with AIS when we book a cab, search the web, or use a Google translator. Not only do AIS confidently take on the functions that only humans have been able to cope with until recently (natural language recognition and synthesis, scene recognition, or driving, even in the difficult conditions of modern metropolitan areas), but often exceed human capabilities, such as in the medical fields. diagnostics and complex poker games. Catherine D. Schuman et al. (2017), Pooja Jawandhiya (2018) note that artificial neural networks (ANN) of different architecture and complexity of training algorithms are most often a means of implementing such systems.

Even if ANN is implemented solely by software, the feasibility of its implementation and the effectiveness of its practical application for solving certain tasks is completely determined by the characteristics

[1] Lviv National Agrarian University, Department of automation and computer-integrated technologies, 1 V. Velykogo str., Dublyany, Zhovkva district, Lviv region, 80381, Ukraine, 4vyach@gmail.com.

[2] Ukrainian National Forestry University, Department of automation and computer-integrated technologies, 11 Zalizniaka str., Lviv, 79044, Ukraine, mmmstd@i.ua.

[3] L'viv National Medical University, Department of Ophthalmology, 69 Pekarska str, Lviv, 79010, Ukraine, 4vyach@ukr.net.

of the hardware on which these programs will be executed. The development of AI technologies depends on the capabilities of the equipment that maintains them, their performance, power consumption, connection speed and others. The high computing power of modern equipment, in itself, is the reason for a sharp increase in the number of developments related to artificial intelligence. However, the amount of data continues to grow exponentially, and the corresponding advances in computing performance are gradually exhausting themselves. Therefore, the problem is the choice of hardware implementation or only to accelerate the work of the ANN at the stage of choosing its architecture and teaching method.

2 Trends in hardware development of artificial neural networks

Today there are a great number of publications on this issue - the search for keywords yields 57450 results (Fig. 1).

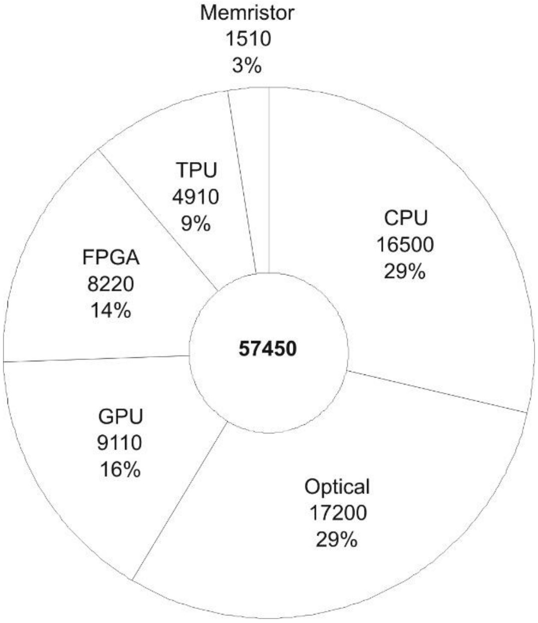


Figure 1 Share of different types of ANN hardware in publications 2014-2018 Google Scholar results, Source: own.

And these are considered only the most common hardware. The most thorough analysis of the hardware selection problem for ANN has been done by Catherine D. Schuman et al. (2017), Pooja Jawandhiya (2018). Of particular note is the work by Catherine D. Schuman et al. (2017), which analyzed more than 500 publications and examined virtually all the physical principles on which ANN hardware can be built. The vast majority of other publications, such as Zhang, Q. et al. (2019), Khan, A. et al. (2019), Tavanaei, A. et al. (2018), Kim, L. W. (2018), Forssell, M. (2017), Sartin, M. A. & da Silva, A. C. (2014), An, H. et al. (2018), Colburn, S. et al. (2018), Matt Kennedy (2018), are mostly reports of individual research results published at least one year after their receipt. Thus, in the existing publications there are practically no attempts to evaluate the dynamics of research of the main hardware of the ANN, usually only the distribution of their number by groups of these or other means, which makes it impossible to reasonably predict the prospective means of the implementation of the ANN at the stage of their design. Therefore, it is urgent to evaluate the dynamics of the number of publications on at least the main types of hardware.

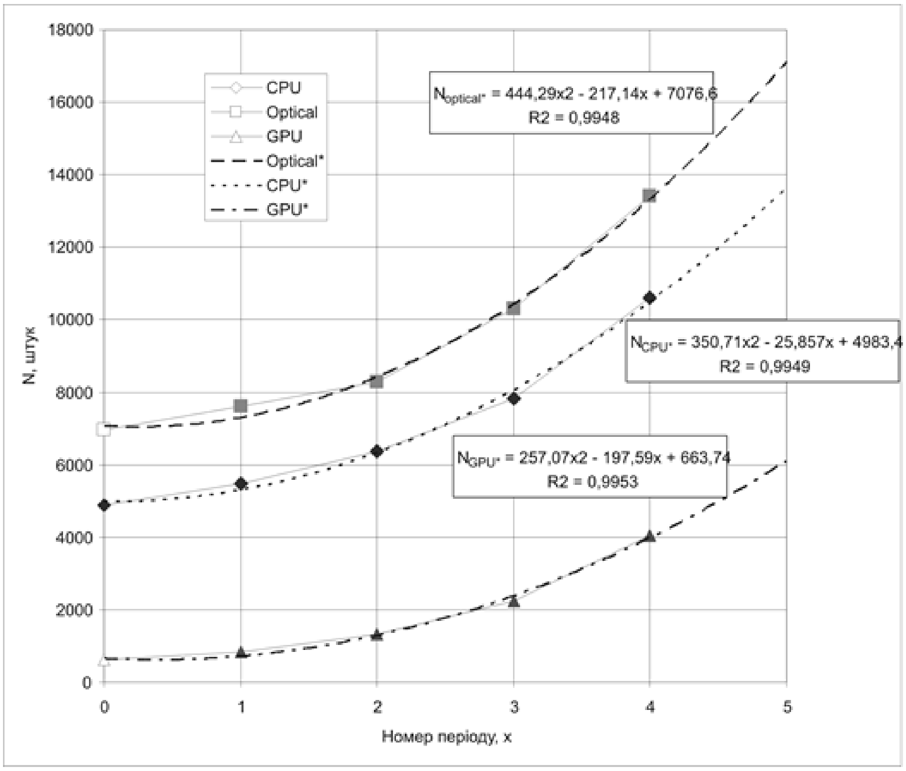


Figure 2 Dynamics of the number of publications for 2014-2018, dedicated to the implementation of SNM models by means of general-purpose processors (CPU), graphics processors (GPU) and optical devices, Source: own.

As can be seen from the graphical interpretation of the distribution of the number of studies by major groups of hardware (Fig. 1), the largest and almost equal shares are the research of means based on general-purpose processors (CPU) and optical systems (Optical in Fig. 1). Such a distribution is natural, since traditional CPU-based systems are the most common computing tools, and the results of the study of optical systems for the implementation of ANN can lead to the development of the most high-speed devices and, therefore, are obviously of great commercial importance and appropriate funding. The smallest share of memristor-based remedies can be explained by the need for access to sophisticated equipment for their physical implementation, which is not available to all researchers. A similar pattern is observed in the case of analysis of the dynamics of publications (Fig. 2 - Fig. 4) for the selected period.

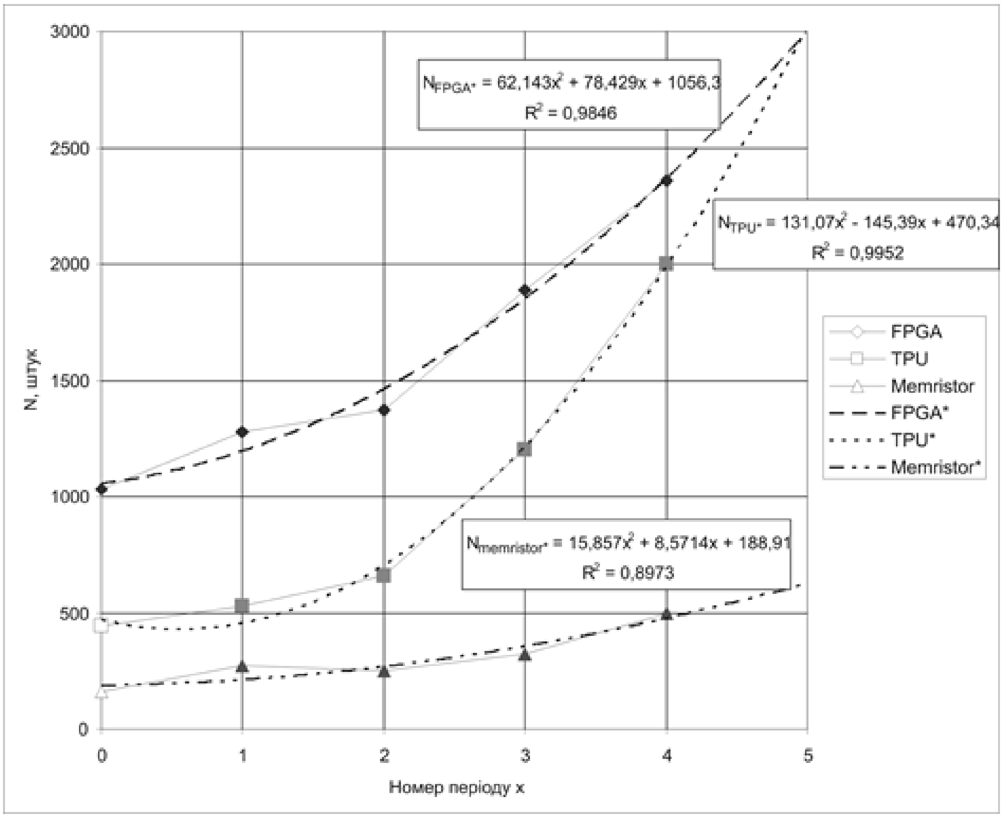


Figure 3 Dynamics of the number of publications for the years 2014-2018, dedicated to the implementation of ANN models by means of programmable logic arrays (FPGA), tensor processors (TPU) and topological isolators, Source: own.

In Fig. 2 - Fig. 4 the zero period corresponds to 2014, the fifth period corresponds to 2019. As can be seen from Figs. 2, the increase in the number of publications for at least the next year, with respect to the most common funds, can be reliably predicted from the data of the five previous years. With regard to less common means (Fig. 3, Fig. 4), even a short-term forecast of trends in their development should be made only on the basis of data for three years, rejecting the data for the two previous periods (Fig. 4).

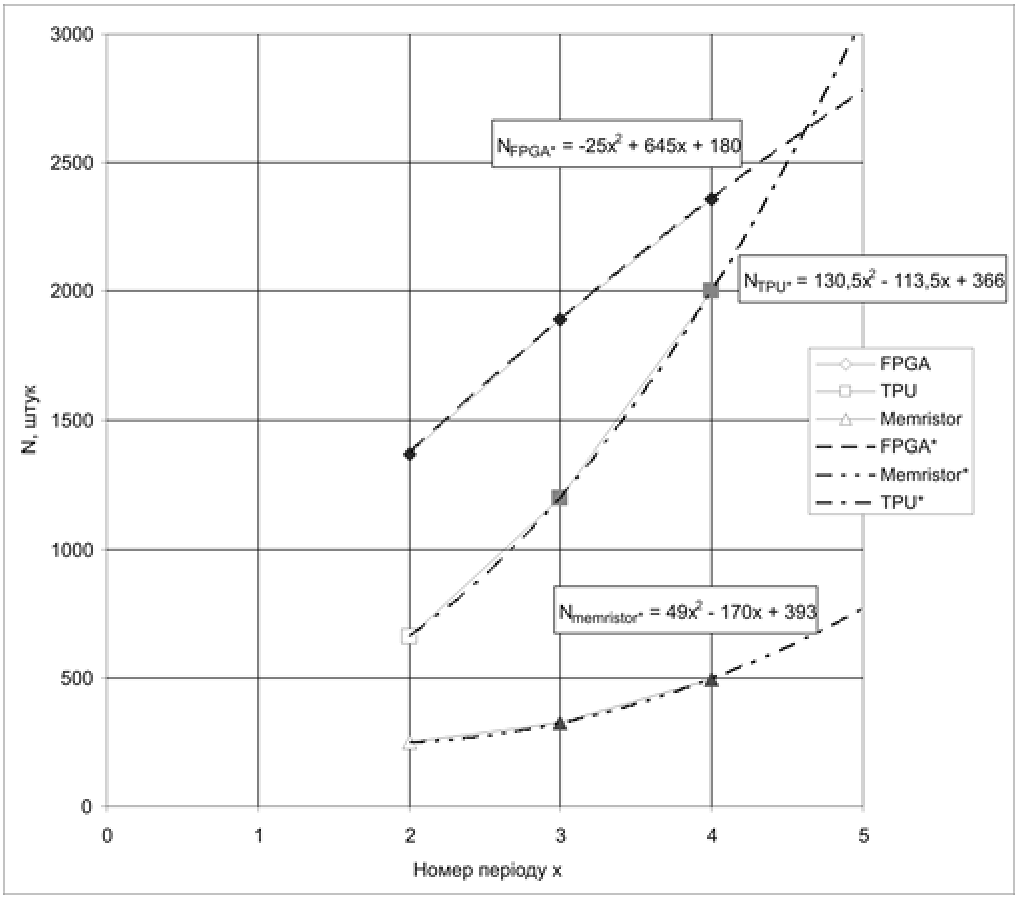


Figure 4 Forecast of the number of publications based on data for 2016-2018, Source: own.

3 Conclusion

The amount of ANN research conducted with the use of General Purpose Processors (CPUs), Graphics Processors (GPUs) and optical devices will soon demonstrate a significant and stable growth rate with a significant predominance of optical neural networks, including those implemented using 3D printing technology.

With regard to the use of other means, by the end of 2019 we can expect a slowdown in the use of programmable logic arrays. Instead, there will be a significant increase in the number of TNA studies based on tensor processors.

References

Schuman, C. D. et al. (2017*) A survey of neuromorphic computing and neural networks in hardware* [Online], Available: https://arxiv.org/abs/1705.06963 [22 Aug. 2019].

Jawandhiya, P. (2018) 'Hardware design for machine learning'. *International Journal of Artificial Intelligence and Applications (IJAIA),* Vol 9 Issue 1, pp.63-84.

Zhang, Q. et al. (2019) *Recent advances in convolutional neural network acceleration* [Online], Available: https://arxiv.org/abs/1807.08596 [17 Aug. 2019].

Khan, A. et al. (2019) *A Survey of the Recent Architectures of Deep Convolutional Neural Networks* [Online], Available: https://arxiv.org/ftp/arxiv/papers/1901/1901.06032.pdf [17 Aug. 2019].

Tavanaei, A. et al. (2018) *Deep learning in spiking neural networks. Neural Networks* [Online], Available: https://www.sciencedirect.com/science/article/pii/S0893608018303332 [22 Aug. 2019].

Kim, L. W. (2018) 'DeepX: Deep learning accelerator for restricted boltzmann machine artificial neural networks'. *IEEE transactions on neural networks and learning systems,* Vol 29 Issue 5, pp.1441-1453.

Forssell, M. (2017) *Hardware Implementation of Artificial Neural Networks* [Online], Available: https://pdfs.semanticscholar.org/5040/0b7455647e2c02127df63515738fc6c26310.pdf [15 Aug. 2019].

Sartin, M. A. & da Silva, A. C. (2014) 'ANN in hardware with floating point and activation function using hybrid methods'. *Journal of Computers,* Vol 9 Issue 10, pp. 2258-2266.

An, H. et al. (2018) *Learning Accuracy Analysis of Memristor-based Nonlinear Computing Module on Long Short-term Memory* [Online], Available: https://dl.acm.org/citation.cfm?id=3229889 [17 Aug. 2019].

Colburn, S. et al. (2018) *An Optical Frontend for a Convolutional Neural Network* [Online], Available: https://arxiv.org/ftp/arxiv/papers/1901/1901.03661.pdf [22 Aug. 2019].

Matt Kennedy (2018) *3D-printed Deep Learning neural network uses light instead of electrons* [Online], Available: https://newatlas.com/diffractive-deep-neural-network-uses-light-to-learn/55718/ [22 Aug. 2019].

Micro-genetic Training of Neural Networks Used for Stochastic Time Series Prediction

Martin Maděra[1]

Abstract. This paper discusses a usage of genetic and micro-genetic algorithms for a training of neural networks used as an approximation for ARIMA model for a stochastic time series prediction. It shows that micro-genetic algorithms can train the neural networks equally well with less amount of computational resources as traditional genetic algorithms. The stochastic time series in the discussed case is real-world data, a currency exchange rate with 1-minute resolution.

Keywords: ARIMA models, Neural networks, Learning algorithms, Genetic Algorithm, Micro-genetic algorithm.

JEL Classification: C63, C61, C53

1. Intriduction - Used data and methods

The stock values or currency exchange rates can be precisely predicted using ARIMA models (autoregressive integrated moving average models) which work well in situations when the users are not strictly time constrained. Creating an ARIMA model can be very demanding on computational resources and time especially when a large data set is used for making the model. The process of creating an ARIMA model is also hard to parallelize which means it cannot fully use the computational potential of nowadays computers. Artificial neural networks are mathematical models which can approximate every math function (Hornik, Stinchcombe, and White 1989) including an ARIMA model and can be developed (trained) using machine learning algorithms. This paper discusses a micro-genetic algorithm for training a neural network and compares it to a genetic algorithm.

The chosen data set for prediction is high frequency trading data representing a currency exchange rate between Czech Koruna (CZK) and Euro (EUR) for the 1st week of December 2018. The data were analysed, pre-processed and an AR prediction model was created. Multiple neural networks

[1] 1Department of Economics, VŠB – Technical University of Ostrava, Sokolská tř. 33, Ostrava 70200, Czech Republic, e-mail: martin.madera@vsb.cz

were trained using genetic and micro-genetic algorithms with different parameters. Results were then compared using Mean Squared Error (MSE).

The data used for research discussed in this paper were published by GAIN Capital company and are freely available at http://ratedata.gaincapital.com/.

The data comes in CSV (Comma Separated Values) format and data for exchange rate of CZK (Czech Koruna) to EUR (Euro) for the 1st week of December 2018 was used. The data set starts at the 2nd December 2018 17:02:14 and ends at the 17th December 2018 16:59:55. It contains 60586 values. It should have 1-minute time resolution however some values are duplicate, some are missing.

For creating a prediction model for a time series, the series must be free of duplicate values and the values must be evenly spaced in time. The STATA software was used for this. After removal of duplicates and interpolating the missing values, the time series showed a declining trend, see Figure 1.

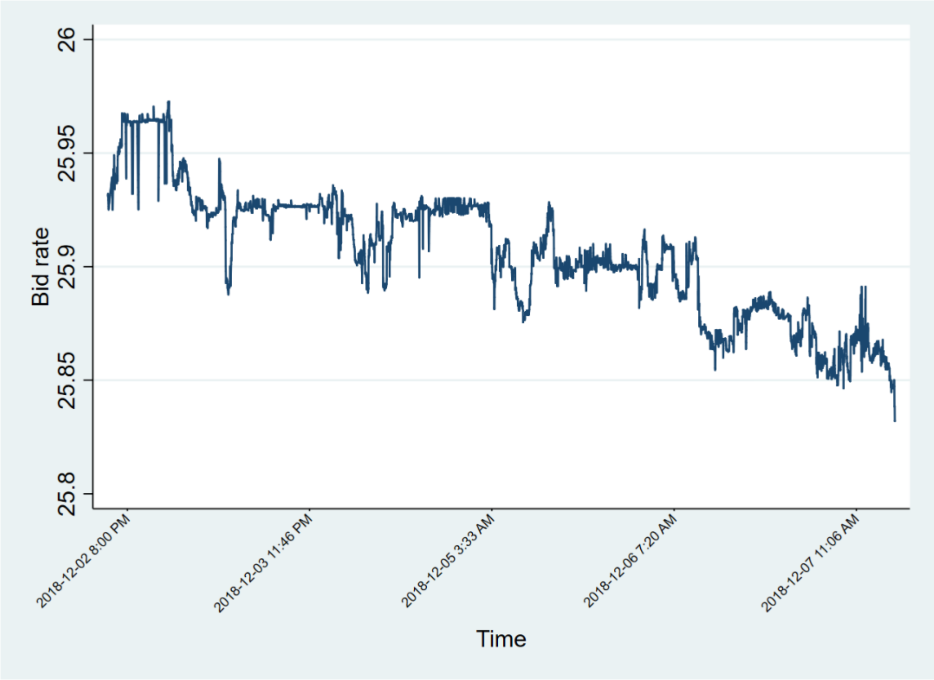


Figure 1 Original time series, CZK/EUR exchange rate, Source: own.

For successful usage of the Box-Jenkins method for creating an ARIMA (autoregressive integrated moving average) model, the data should be stationary. If the time series is log transformed and differentiated, the trend disappears, see Figure 2. (Marček 2013)

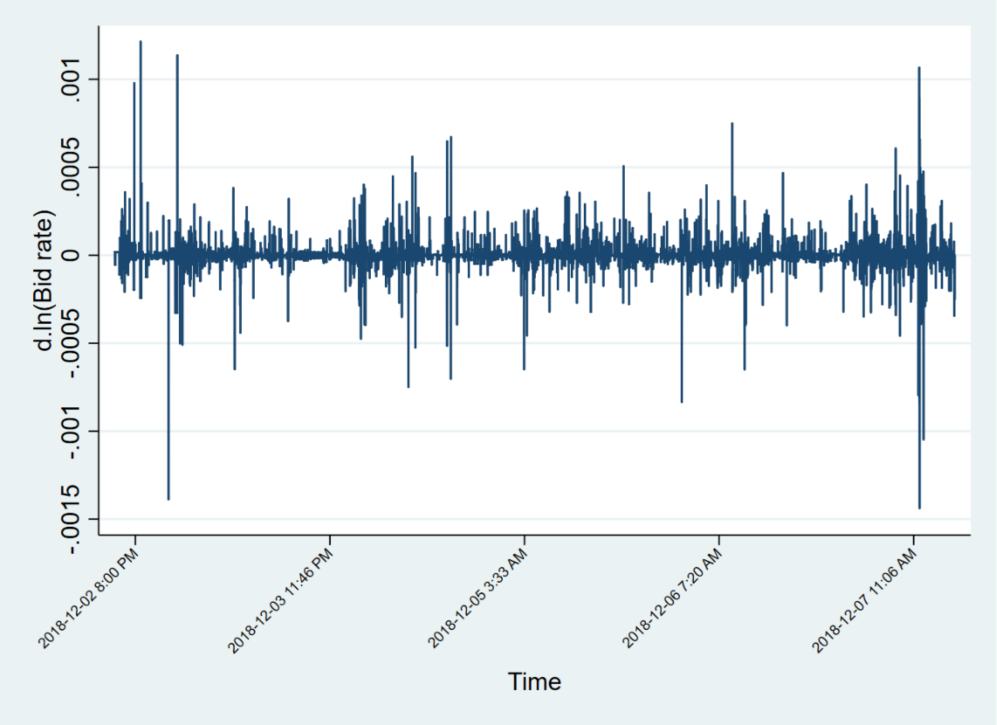


Figure 2 Exchange rate, log transformed and differentiated. Source: own.

2. Neural network

The ARIMA model computed by STATA software for predicting this time series is based on 10 auto-regressive and 10 moving average values. Therefore, the network should have 20 neurons in the input layer. It is crucial that the values of (input + bias) in the neural network are rather small because sigmoid function is used as an activation function of the one hidden layer. The last, output layer has the identity function the activation function and has only 1 output neuron. Based on empirical experience the good size of the hidden layer is 25 neurons. Larger size did not provide better results while smaller provided worse.

The resulting shape of the network was three layers, having 20 – 25 – 1 neurons each.

The time series data was split into training and evaluation data so the training data consist of 90% of the original series. After training of the neural network was finished, Mean Squared Error (MSE) was computed for evaluation data. When the MSE for evaluation data started to raise, the training was stopped because this is a usual sign of overfitting and overtraining.

Predictions for the evaluation data was then calculated using the trained network and stored into a CSV file for further analysis.

3. Genetic and micro-genetic algorithm

Genetic algorithms traditionally work with genes either 0 or 1. For this application, this is inadequate, because this algorithm need to find weights and biases of a neural network, which can be an arbitrary floating point decimal numbers. On the other hand, for genetic algorithms to be efficient, the state space needs to be limited. Therefore, each parameter is transformed into interval [0, 1]. An individual for the genetic algorithm then consists of floating point numbers from [0, 1] interval and count of parameters in intervals equals to count of all weights and biases of the network.

Selecting individuals for crossbreeding uses a rank-selection technique (Saini 2017). From a technical point of view, a linked-list is constructed and the worst individual is added once, second worst twice etc. Therefore the best individual in population consisting of 300 individuals is 300x more likely to be chosen than the worst. In contrast to technique based solely on a loss function value, if one individual is much better than others, it does not prevent others from being chosen for cross breeding. The rank selection helps preventing a loss of diversity in population.

Loss function of this algorithm reconstructs a neural network from each individual and uses the training data to compute predictions. Predictions are compared to expected (correct) values and Mean Squared Error is computed for each individual. This is the result of a loss function. The lower, the better (some genetic algorithms use vitality function – the higher, the better).

The micro-genetic algorithm is a modification of a genetic algorithm which works with smaller populations. Since smaller populations are prone to a loss of diversity, the algorithm has to eventually be restarted with elites being retained.

Table 1 Parameters of genetic algorithm (Source: Own processing)

Parameter name	Value
Number of crossbreds	Size of population - (elites + randoms)
Number of randomly generated individuals	1 - 4 depending on population
Number of elites	1
Probability of mutation	1%

As mentioned earlier, neural networks were trained using a genetic and a micro genetic algorithm with different population sizes. The target was to train a network with MSE function of a validation data set being under 1.0 x 10^{-7} value. It is also a condition of training stopping (second one is MSE starting to raise on validation data which is a sign of overtraining). Table 1 gives the training parameters used in GA and MGA algorithms. Each algorithm with particular population size was run 12 times and the lowest and highest time was then removed, removing outliers.

As shown in the Table 2 and Figure 3 when going from genetic to micro-genetic algorithms (from 300 population to 30 in this case), the needed number of generations went up. Since the population is much smaller, calculating the fitness of the generation is faster as well. In this case, the genetic algorithm with population 600 had population too large for this problem, slowing the convergence of the algorithm down. The last one, micro genetic algorithm with population size of 6, the population size is too small and the convergence is slow as well. An optimal compromise in this case was the population of size 20.

Table 2 A summary of the predicted accuracy and needed time of calculations related (Source: Own processing)

Population	Mean number of generations	Mean time [ms]	MSE [x 10^{-8}]
	Statistical B-J approach		
		overnight	1.44
	Neural network GA learning		
600	12.0909	98 047.73	3.52
300	19.9090	27 290.18	9.40
	Neural network MGA learning		
30	114.2727	25 168.64	7.65
20	135.3636	20 871.55	5.98
10	300.6364	24 677.18	7.04
6	797.7273	51 542.55	7.73

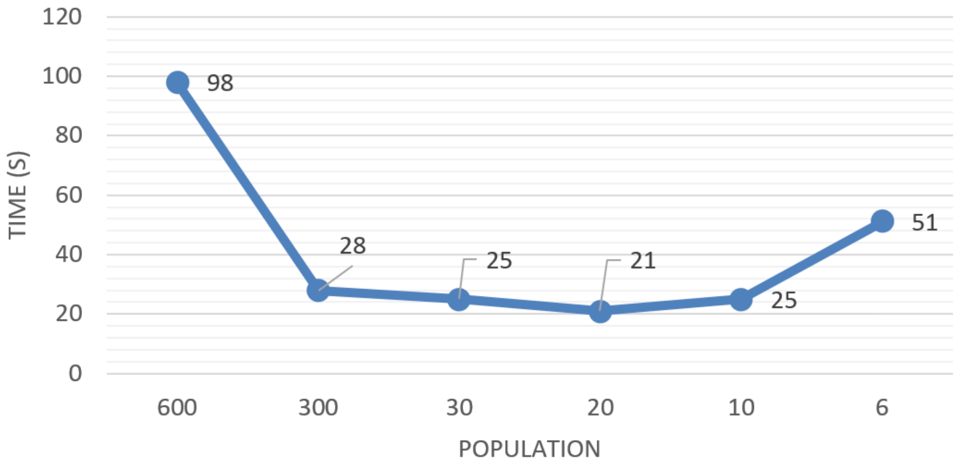


Figure 3 Time needed to train GA and MGA algorithm related to the size of populations (GA population size 300 and 600; MGA 6, 10, 20, 30), Source: own.

4. Conclusion

It was shown that the GA and MGA can be used to train a feed-forward neural network to approximate an ARIMA model for predicting high frequency time series data. Although the implementation of the algorithm has room for improvement, for example various selection techniques can be used for this purpose, or apply hybrid learning algorithm for three-layered neural networks, which can accelerate numerical calculations.

In the future our main research objective is to apply the developed metaheuristic on various datasets. Selected metaheuristics will be tested with different parameter combinations and the combination of parameters which can yield approximate feasible solution in an acceptable computation time.

Acknowledgement

This article was created with the financial support of the Student grant competition EkF, VŠB-TU Ostrava as part of project SP2019/81.

References

Hornik, K., M. Stinchcombe, and H. White (1989). "Multilayer feedforward networks are Universal approximators". In: Neural Networks Volume 2 (Issue 5), pp. 359–366. ISSN: 0893-6080. URL: https://doi.org/10.1016/0893-6080(89)90020-8.

Marček, D. (2013). Pravdepodobnostné modelovanie a soft computing v ekonomike. VŠB-TU Ostrava, 2013. ISBN: 978-80-248-2955-5.

Saini, N. (2017). "Review of Selection Methods in Genetic Algorithms". In: International Journal Of Engineering And Computer Science 6 (12), pp. 261–263. ISSN: 2319-7242. DOI:10.18535/ijecs/v6i12.04.

An Indoor Space Mapping with a Drone

Marek Malina[1], Jaroslav Zacek[2]

Abstract. This study aims to design an algorithm capable of providing the online indoor mapping. Current approaches often do not take drone architecture into account. The algorithm is designed for a drone architecture with Raspberry Pi and two LiDAR devices, one to guarantee better and more accurate classification and detection and the other to create a visualization of the visited area. For online indoor mapping, it is crucial that the drone must cover all accessible areas through our designed algorithm.

Keywords: explore the frontier, indoor mapping, drone, exploration, robot navigation

JEL Classification: L86

1. Introduction

Industry 4.0 is slowly taking its place in today's lives, and people gradually realize that everything can be automized potentially. Commonly, it's the human who explores and maps the environment, but this can be changed. We can see how robot vacuum cleaners are becoming more and more popular, and these robots have to create maps of their surroundings if they want to be efficient and faster.

The autonomous exploration of the indoor area is still an unsolved domain of artificial intelligence. Because there is no single scope solution for this problem, many new articles are published these days. The indoor mapping process consists of many partial tasks, but we can split it mainly into three main tasks: exploration, mapping, and classification. This study aims to demonstrate how we could, by a simple change, improve the basic exploration algorithm.

A basic map from the indoor mapping process can look as it is shown in Figure 1.

[1] University of Ostrava, Faculty of Science, Department of Informatics and Computer Management, 30. dubna 22, 702 00 Ostrava, marek.malina@osu.cz

[2] University of Ostrava, Faculty of Science, Department of Informatics and Computer Management, 30. dubna 22, 702 00 Ostrava, jaroslav.zacek@osu.cz

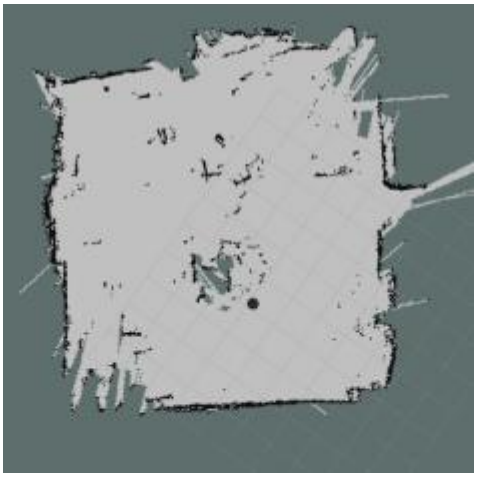


Figure 1: Explored map through an algorithm, Source: Topiwala, Inani, and Kathpal (2018).

Similar algorithms from which the robot creates this map of the surroundings could be used even for a drone. The drone can also improve the map because it moves vertically. Thanks to some sensors, it can create a 3D scan of the objects inside the environment and build-up a full 3D map of the indoor areas.

What sensors and devices could be used for indoor space mapping through a drone is described in the next chapter.

2. Drone architecture

Our architecture is designed to solve three main tasks: navigation, mapping the indoor space, and object classification. The devices which are used for our solution were selected for their low weigh so the drone could easily lift off.

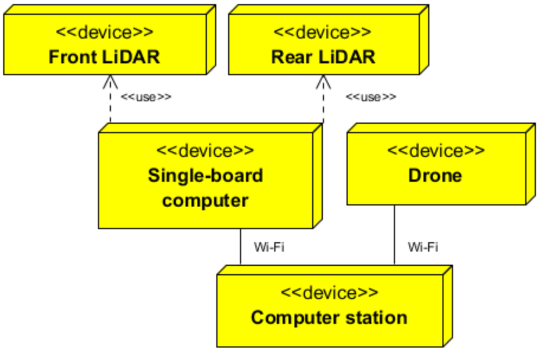


Figure 2: The drone architecture, Source own.

One of the best solutions for getting information about the environment is to use the Lidar device. It is used commonly in archeology, geography, or autonomous cars. Compared to e. g. Radar, it has a very good depth measurement accuracy. Our selected Lidar devices have the accuracy of units of centimeters; it differs with a distance of an obstacle. There are even much more precise devices on the market, but also heavier and more expensive. Lidar works by emitting a laser beam in one direction. The beam is then reflected from an obstacle back, and the distance between the obstacle and Lidar can be then calculated. [Wu et al., 2018]

We can easily create the visualization of the surrounding environment from the Lidar data. We need a localization system and merge it with the corresponding measurement. Also, the Lidar could correct the localization process if it has some measurement deviation. An exact position can be discerned by using multiple Lidar devices or a single device rotating around its axis [Kumar et al., 2017]. Lidar can help with classification and image processing. Our drone has only a monocular camera built-in, so the spatial perception is lost. The front Lidar can bring back this information, and the system gets a better overview of the environment. For example, stair detection is almost impossible using the only monocular camera.

2.1. Technological components

Devices used as a part of the architecture:

- **Front Lidar** - serves to get information about the distance between Lidar (drone) and obstacle. Its main objective is to help with immediate object classification.
- **Rear Lidar** - scanning and mapping the environment that drone passed through.
- **Single-board computer** - connects both of Lidar devices, camera, gathers measured data, and sends them to the computer station.
- **Computer station** - collects all data, analyzes, and evaluates them. It also serves to execute drone’s commands and creates a visual map of the environment.
- **Drone** - an autonomous robotic unit for acquiring data about the indoor environment.

These are the specific devices that were selected: LeddarTech Vu 8 Channel Module, 100°/3°, RPLIDAR A3, Raspberry Pi 3 B+, Intel NUC Hades Canyon 8i7HNKQC and the drone Matrice 100.

3. Navigation

The navigation problem could be divided into two main parts - global navigation and local navigation. The aim of the first part is to provide a general orientation in a large space to capture marking points and state our boundaries. Common approach is to determine a starting point (could be more than one) and iteratively explore the nearest neighbor points. The most suitable approach for our exploring is to use a graph space representation.

3.1. Global

The intuitive idea how to perform a space search is to mark one node as a start node. This node is usually where the drone is starting with exploration task. There is also a set of goal nodes which are not fully known by the time of start because we do not have a full picture of inner space yet. We can determine goal nodes by visual confirmation or lidar input in t_0 at the beginning. There is a dynamic list of unexplored nodes and we use it to add new nodes with potential to be explored in each and every iteration. The visual representation is shown in Fig. 2.

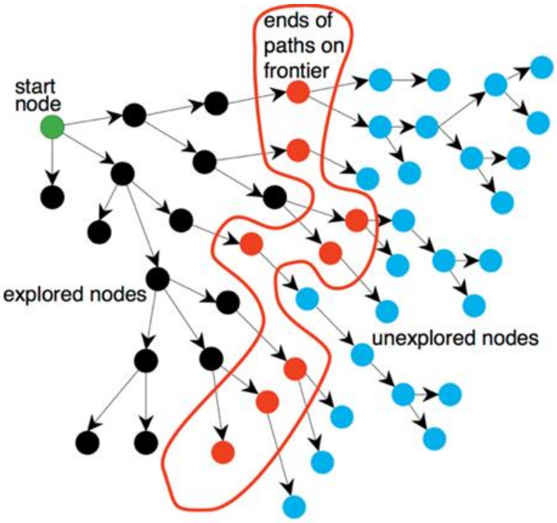


Figure 3: Graph searching, Source: Poole & Mackworth.

```
procedure Search(G, S, goal)
    Inputs
        G: graph with nodes N and arcs A
        S: start node
        goal: Boolean function of nodes
    Output
        path from S to a node for which goal is true
        or $\perp$ if there are no solution paths
    Local
        Frontier: set of paths
    Frontier:=$\{\langle n\rangle: n \in S\}$
    while Frontier$\neq\{\}$ do
        select and remove $\langle n_0,\ldots,n_k\rangle$ from Frontier
        if goal($n_k$) then
            return $\langle n_0,\ldots,n_k\rangle\langle n_0, \ldots, n_k\rangle$
        Frontier:=Frontier $\cup \{\langle n_0, \ldots, n_k, n\rangle:\langle n_k, n\rangle \in A\}$
    return $\perp$
```

Figure 4: The algorithm itself is show in pseudo-code, Source: own.

The method requires three inputs – graph with all known nodes and associated arcs, start node, and the set of markers where is our desired destination. The algorithm iterates over the set of possible paths from the beginning to the end and creates a union of the current path and new node. If the node is marked as a destination node, the algorithm ends and returns the path. The main concern of this algorithm applied to our case is the fact that it is not deterministic, and theoretically, we can get a stack overflow problem by expanding nk node while drone moves and finds another possible path. Therefore, we have to state some conditions to prevent these states. Another problem is with computing complexity. The algorithm itself is not power-consumption friendly. We had to apply some mechanisms to minimize the count of starting nodes. That can be realized in many ways. For example, we are using the fact that drone exists in a three-dimensional environment. We can change the altitude and get another visual confirmation in special cases such as false corner identification because of common objects in the scene (chair, boxes, etc.).

3.2. Local

„Local navigation aims to solve the problem of how to best advance a robot along a given 'global' trajectory, given obstacles in the immediate vicinity,

physical limitations, and current inertial state of the robot.“ [Dowling et al., 2018]

In other words, it is a path planning problem. We have not completely decided on which specific algorithm we should use for local navigation because our work is currently focused on solving the global strategy. What we know is that some standard solutions like the Dijkstra algorithm or the BFS will not work efficiently in 3D space. For example, people could enter the currently scanning room, and some previously available paths would not be possible.

```
procedure Path_planning(O,C,s, g)
    Inputs
        O: a list with open nodes
        s: start node
        g: goal node
        goal: fill C with nodes from s to g with the smallest eval func
    Output
        a path from s to the selected frontier
        or ⊥ if there are no solution paths
    put node_start in the O with f(node_start) = h(node_start) (initialization)
    while the O is not empty {
        take from the O the node node_current with the lowest
        if(node_current) = g(node_current) + h(node_current)
        if node_current is g break
        generate each state node_successor that come after node_current
        for each node_successor of node_current {
            set successor_current_cost = g(node_current) + w(node_current, node_successor)
            if node_successor is in the O {
                if g(node_successor) ≤ successor_current_cost continue
            } else if node_successor is in the C {
                if g(node_successor) ≤ successor_current_cost continue
                move node_successor from C to O
            } else {
                add node_successor to the O
                set h(node_successor) to be the heuristic distance to g
            }
            set g(node_successor) = successor_current_cost
            set the parent of node_successor to node_current
        }
        add node_current to the C
    }
if(node_current != g) exit with error (O is empty)
```

Figure 5: The procedure algorithm itself is in pseudo-code, Source: own.

So far, we have chosen the A* path planning algorithm [Hart et al., 1968] because of its common usage in this area. This algorithm is basically the Dijkstra algorithm, except it uses heuristic in addition. It keeps a set of open nodes from which selects the node with the smallest evaluation function value. This node is then added to a set with closed nodes.

The starting node could be a drone starting position or previously visited frontier. The goal is in our case the selected frontier which we want to explore. In the end, we have the optimal path for the next exploration. We could even enhance the evaluation function with the battery cost of drone maneuverability.

Conclusion

In this paper, we have described how the indoor space mapping could work. First, we had explained three main tasks in which the mapping process consists and then we focused our work on the one containing exploration of the environment. We had presented our drone architecture and took as a groundwork the Explore frontier algorithm for global exploration and the A* algorithm for local exploration otherwise also known as pathfinding. We even enhanced the basics of the Explore frontier algorithm with some vertical movement adjustments for eliminating non-frontiers (little higher obstacles). As the next step we want to implement this proposed solution to our drone architecture and test it in real indoor environments.

Acknowledgements

The paper was supported by the grant provided by Ministry of Education, Youth and Sport Czech Republic, reference no. SGS05/Přf/2019.

References

Dowling, L., Poblete, T., Hook, I., Tang, H., Tan, Y., Glenn, W., Unnithan, R. (2018) *Accurate indoor mapping using an autonomous unmanned aerial vehicle (UAV)* [online], Available: https://arxiv.org/abs/1808.01940 [20. Oct 2019].

Hart, P. E., Nilsson, N. J., Raphael, B. (1968). A Formal Basis for the Heuristic Determination of Minimum Cost Paths. *IEEE Transactions on Systems Science and Cybernetics SSC4*. 4 (2): 100–107. 10.1109/TSSC.1968.300136.

Kumar, A., Patil, K., Patil R., Park, S., and Chai, Y. (2017). *A LiDAR and IMU Integrated Indoor Navigation System for UAVs and Its Application in Real-Time Pipeline Classification*. Sensors (Basel, Switzerland). 17. 10.3390/s17061268.

Poole, D., Mackworth, A. (2017) Artificial Intelligence 2E, Available: https://artint.info/2e/html/ArtInt2e.Ch3.S4.html [1. Sep 2019].

Topiwala A., Inani, P., and Kathpal, A. (2018). *Frontier Based Exploration for Autonomous Robot* [online]. 10.13140/RG.2.2.34130.40641. Available: https://arxiv.org/ftp/arxiv/papers/1806/1806.03581.pdf [20. Oct 2019].

Wu, Q., Sun, K., Zhang, W., Huang, C., and Wu, X. (2016). *Visual and LiDAR-based for the mobile 3D mapping*. In: 2016 IEEE International Conference on Robotics and Biomimetics (ROBIO). IEEE, s. 1522-1527. 10.1109/ROBIO.2016.7866543.

Determination of Fuzzy Relations for Economic Fuzzy Time Series

Dušan Marček[1]

Abstract. Most models for the financial time series have centered on autoregressive (AR) processes. Traditionally, fundamental Box-Jenkins analysis have been the mainstream methodology used to develop time series models. We describe developing a fuzzy regression model, i.e. determining and developing of fuzzy time series models, calculating of fuzzy relations, calculating and interpreting the outputs. The fuzzy rules are generated using the neural network with SCL-based product-space clustering. Forecasts of a fuzzy time series model is compared with statistical AR(1) model.

Keywords: Time series models, fuzzy time series models, neural networks, product-space clustering

JEL Classification: C13, G32

1 Introduction

The fuzzy time series models have been in use in analyses for many years. Lots of issues of journal Fuzzy Sets and Systems as well as many others have been articling whose analyses are based on the fuzzy regression and fuzzy time series models. From reviewing of these papers, it became clear that in economic applications the use of method is not on the same level as analyses using classical linear regression. Computers play an important role in fuzzy regression analyses and dynamic processes. Economic time series analysis is concerned with estimation of complicated relationships among groups of variables. Very frequently, in such cases more sophisticated approaches are considered, which are based on the human experience knowledge and consist of series linguistic express in the form of an if … then” fuzzy rule. Most of these approaches are based on the use fuzzy/non-fuzzy neural networks (Horikawa, et.al, 1992, Zadeh, L.A., 1992).

The primary objective of this paper is a focused introduction to the fuzzy time series model and its application to the analyses and forecasting from classical regression model of view. In Section 2, we introduce the conventional and fuzzy time series modelling methods.

[1] VŠB-Technical University of Ostrava, Ostrava, Czech Republic, dusan.marcek@vsb.cz

Section 3 shows how to combine neural and fuzzy systems to produce fuzzy rules. Concluding remarks are given in Section 4.

2 Quantitative Fuzzy Time series Modeling Methods

Quantitative modelling approaches of both conventional and fuzzy time series can be grouped into two types: time series method and causal methods. In practice, there are many time series in which successive observations are dependent, i.e. there exists an observational relation

$$R = \{(y_t, = f(y_t, y_{t-1}), (y_{t-1}, y_{t-2}), \ \dots \ \} \subseteq Y_t \times Y_{t-1} \qquad (1)$$

where Y_t, Y_{t-1} denote the variables and y_t, y_{t-1} denote the observed values of Y_t, Y_{t-1} respectively.

The most often used model is, however, an explicit function

$$f: \ Y_{t-1} \to Y_t, \qquad (2)$$

This means that we look for some relation instead of function, or for function f such that the condition $f(y_{t-1}) = y_t$ for t = 1, 2, …, N are violated. Very often the linear function (Markov process)

$$y_t = f(y_{t-1}, \phi_1, \varepsilon_t) = \phi_1 y_{t-1} + \varepsilon_t \qquad (3)$$

is used, where ε_t is white noise with mean zero and variance σ^2 and is normally distributed. Equation (3) is called an autoregressive process of the order p = 1 abbreviated AR(1).

The AR(1) is special case of a stochastic process which is known as ARMA(*p, q*) (Auto-Regressive Moving Average) model defined as

$$y_t = \phi_1 y_{t-1} + \phi_2 y_{t-2} + \dots + \phi_p y_{t-p} \ + \varepsilon_t + \theta_1 \varepsilon_{t-1} + \theta_2 \varepsilon_{t-2} + \dots + \theta_q \varepsilon_{t-q} \qquad (4)$$

where $\{\phi_i\}$ and $\{\theta_i\}$ are the parameters of the autoregressive and moving average parts respectively, and ε_t is white noise with mean zero and variance σ^2 and is normally distributed. ARMA(*p, q*) process can be considered as an approximate AR(p) model of the form

$$y_t = \phi_1 y_{t-1} +, \phi_2 y_{t-2} + \ \dots \ \phi_p y_{t-p} + \varepsilon_t \qquad (5)$$

In the case of fuzzy time series the fuzzy relational equations can be employed as the models. Analogously to conventional time series models, it is assumed that the observation at the time *t* accumulates the information of the observation at the previous time, i.e. there exists a fuzzy relation such that

$$y_t^j = y_{t-1}^i \circ R_{ij}(t, t - 1), \qquad (6)$$

where $y_t^j \in Y_t$, $y_{t-1}^j \in Y_{t-1}$, $i \in I$, $j \in J$ and J are indices for set Y_t and Y_{t-1} respectively “∘” is the sign for the *max-min* composition, $R_{ij}(t,\ t - 1)$ is the fuzzy relation among the observations at *t* and *t – 1* times. Then we can written

$$Y_t^j = Y_{t-1}^i \circ R_{ij}(t, t - 1) \tag{7}$$

Equation (6) is equivalent to the linguistic condition

$$\text{”if } y_{t-1}^i \text{ then } y_t^j \text{”} \tag{8}$$

we have $R_{ij}(t,\ t - 1) = y_{t-1}^i \times\ \ y_t^j$, where “×“ is the Cartesian product and therefore

$$R(t,t-1) = \max_{i,j}\{\min(y_{t-1}^i, y_t^j)\} \tag{9}$$

Equation (9) is called a first-order model of the fuzzy time series Y_t with lag *p = 1.*

The first-order fuzzy time series model can be extended to *p*-order model in the form

$$Y_t = (Y_{t-1} \times Y_{t-2} \times \ldots \times Y_{t-p}) \circ R_{\mathrm{a}}(t,t-p), \tag{10}$$

or

$$y_t^j = (y_{t-1}^{i1} \times y_{t-2}^{i2} \times \ldots \times y_{t-p}^{ip}) \circ R_p(t,t-p) \tag{11}$$

where $R_{\mathrm{a}}(t,t-p)$ is fuzzy relation among Y_{t-1}, Y_{t-2}, ..., Y_{t-p}.

Equation (9) is called a first-order model of the fuzzy time series with lag p = 1.

The first-order fuzzy time series model can be extended to p-order model in the form

$$Y_t = (Y_{t-1} \times Y_{t-2} \times \ldots \times Y_{t-p}) \circ R_{\mathrm{a}}(t,t-p), \tag{10}$$

or

$$y_t^j = (y_{t-1}^{i1} \times y_{t-2}^{i2} \times \ldots \times y_{t-p}^{ip}) \circ R_p(t,t-p) \tag{11}$$

where $R_{\mathrm{a}}(t,t-p)$ is fuzzy relation among Y_{t-1}, Y_{t-2}, ..., Y_{t-p}.

Equation (10) is equivalent to statement

$$\text{if “} y_{t-1}^{i_{i1}} \text{ and } y_{t-2}^{i_{i2}} \text{ and … and } y_{t-p}^{i_{ip}} \text{ then } y_t^j \text{”} \tag{12}$$

All of the univariate fuzzy time series models can be extended to the econometric fuzzy time series model. See Marcek, 2015 for details.

3 Extracting of Fuzzy Relation Using Competitive Neural Networks

To find exact of fuzzy relations, we will use methods based on a model of a process and illustrate how sophisticated obtain the fuzzy rules of the type of (8) or (11). Neural networks can adaptively generate the fuzzy rules purely from data using the fuzzy sets theory and neural networks. a simple example.

Let as consider the 514 monthly inflation observations for the forty-three years 1956-1998[1] (see Figure 1). This time series a no apparent trend or periodic structure. To build a forecast model the sample period for analysis y1,…,y344 was defined, i.e. as the period over which the forecasting model can be developed and estimated, and the ex post period y345,…,y514 as validation data set.

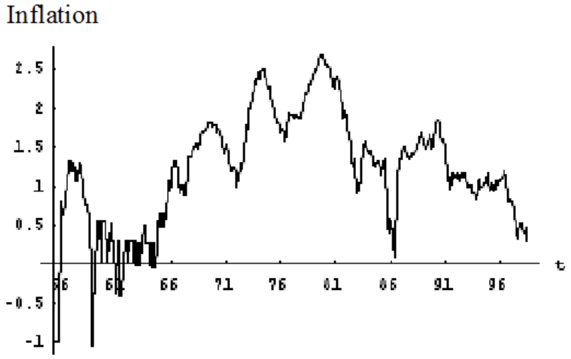


Figure 1 Natural logarithm of monthly inflation from February to November 1998, Source: own

Using time series data and traditional statistical tools as the autocorrelation function (ACF), the partial autocorrelation function (PACF) and the Akaike Information Criterion the model is estimated as (Therien, 1992, Marcek, 2003)

$$\hat{y}_t = -0{,}1248\, y_{t-1}\,,\ t = 1, 2, ..., 344$$

where y_t are the calculated values of inflation. We will further suppose that the potential inputs, which were chosen based on statistical analysis, are crisp data. Sometime it may be advantageous to convert them into fizzy sets (linguistic values). Then the fuzzy time series modelling procedure consist

[1] http://neatideas.com/data/inflatdata.htm

on an implementation several steps. In the literature this modelling approach is known as the fuzzy rule-based system (see *Figure 2*).

The fuzzy rule-based system in *Figure 2* has three blocks: block for fuzzification of input variables, knowledge base block, and defuzzification block.

Firstly, in the fuzzification block, we specified input and output variables. The input variables x_{t-1} is the lagged first difference of inflation values and is calculated as $x_{t-1} = y_{t-1} - y_{t-2.}$, $t = 3, 4, \ldots$. The output variable x_t is the first difference of inflation values and it is calculated as $x_t = y_t - y_{t-1.}$, $t = 2, 3, \ldots$. The variable ranges are as follows:

$$-0.75 \le x_t, x_{t-1} \le -0.75$$

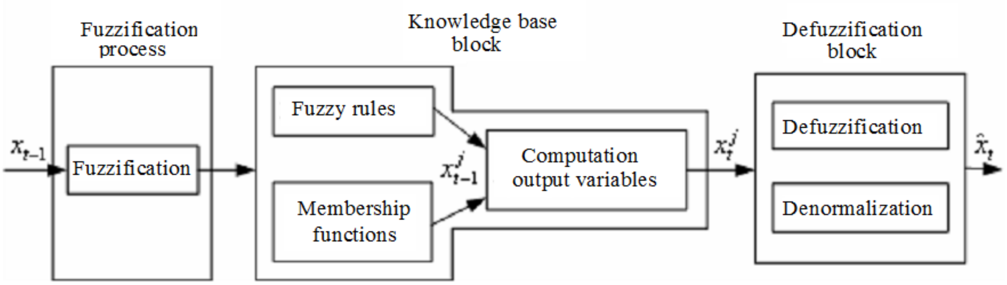


Figure 2 Structure of fuzzy system for inflation forecasts, Source: own.

These ranges define the universe of discourse within which the data of x_{t-1} and x_t are, end on which these fuzzy sets to be, specified. The universe of discourse we divided into the seven intervals.

Next, we specified the fuzzy-set values of the input and output fuzzy variables. The fuzzy sets numerically represent linguistic terms. Each fuzzy variable assumed seven fuzzy-set values as follows: NL: Negative Large, NM: Negative Medium, NS: Negative Small, Z: Zero, PS: Positive Small, PM: Positive Medium, PL: Positive Large.

Fuzzy sets contain elements with degrees of membership. Fuzzy membership functions can have different shapes. The triangular membership functions were chosen. Figure 3 shows membership function graph of the above fuzzy sets.

The input and output spaces we divided into the seven disjoint fuzzy sets. From membership function graphs μ_{t-1}, μ_t Figure 3 shows that the seven intervals [-0,75; -0,375], [-0,375; -0,225], [-0,225; -0,075], [-0,075;

0,075], [0,075; 0,225], [0,225; 0,375], [0,375; 0,75] correspond to NL, NM, NS, Z, PS, PM, PL, respectively.

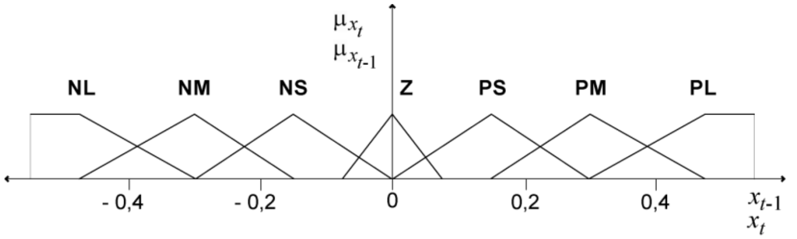


Figure 3 Fuzzy membership functions of fuzzy variables x_{t-1} and x_t, Source: own.

Next, we specified the fuzzy rule base or the fuzzy relation bank. The above specified interval $-0.75 \le x_t, x_{t-1} \le -0.75$ portioned into seven non-uniform subintervals that represented the seven fuzzy sets values NL, NM, NS, Z, PS, PM, PL assumed by fuzzy variables x_{t-1} and x_t. The Cartesian product of these subsets defines 7× 7 = 49 fuzzy cells in the input-output product space R^2. As mentioned in (Kosko, 1992) these fuzzy cells equal fuzzy rules. Thus, there are total 49 possible rules and thus 49 possible fuzzy relations.

We can represent all possible fuzzy rules as 7-by-7 linguistic matrix (see Figure 4). The idea is to categorize a given set of distribution of input vector $\mathbf{x}_t = (x_{t-1}, x_t)$, t = 1, 2, …, 344 into 7× 7 = 49 classes, and then represent any vector just by the class into which it falls.

The neural network shown in Figure 5 was used to generate structure knowledge of the form “if A, then B” from a set of numerical input-output data.

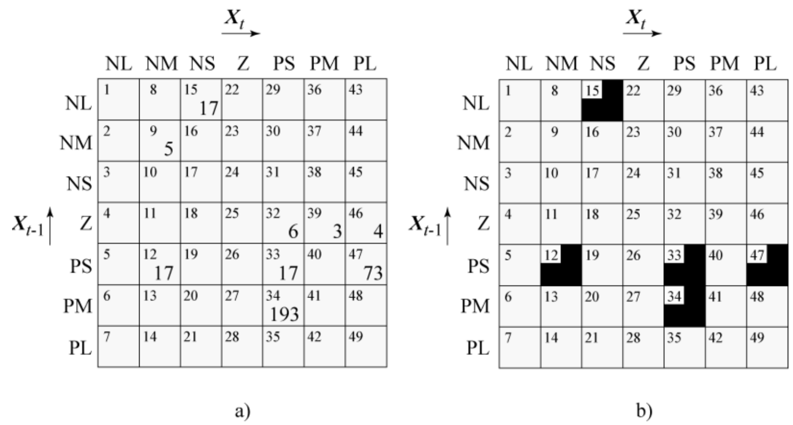
We used SCL (Supervised Competitive Learning) (Marcek, 2002) to train the neural network in Figure 5. We used 49 synoptic quantization vectors. For each random input sample $\mathbf{x}_t = (x_{t-1}, x_t)$, the winning vector $w_i = (w_{1i'}, w_{2i'})$ was updated by the SCL algorithm according to

$$\left.\begin{aligned}\tilde{w}_{1i'} &\leftarrow \tilde{w}_{1i} + \eta\ (\tilde{x}_{1t} - \tilde{w}_{1i})\\ \tilde{w}_{2i'} &\leftarrow \tilde{w}_{2i} + \eta\ (\tilde{x}_{2t} - \tilde{w}_{2i})\end{aligned}\right\} \quad \text{if } i = i' \qquad \left.\begin{aligned}\tilde{w}_{1i'} &\leftarrow \tilde{w}_{1i} - \eta\ (\tilde{x}_{1t} - \tilde{w}_{1i})\\ \tilde{w}_{2i'} &\leftarrow \tilde{w}_{2i} - \eta\ (\tilde{x}_{2t} - \tilde{w}_{2i})\end{aligned}\right\} \quad \text{if } i \ne i' \ ,$$

where i' is the winning unit defined as

$$\left\| \tilde{\mathbf{w}}_{i'} - \tilde{\mathbf{x}}_t \right\| \le \left\| \tilde{\mathbf{w}}_i - \tilde{\mathbf{x}}_t \right\|$$

for all i, and where $\tilde{w}_i$ and $\tilde{x}_i$ are normalized versions of w_i and x_i, respectively, and η is the learning coefficient.



a)

X_{t-1} \ X_t	NL	NM	NS	Z	PS	PM	PL
NL	1	8	15 17	22	29	36	43
NM	2	9 5	16	23	30	37	44
NS	3	10	17	24	31	38	45
Z	4	11	18	25	32 6	39 3	46 4
PS	5	12 17	19	26	33 17	40	47 73
PM	6	13	20	27	34 193	41	48
PL	7	14	21	28	35	42	49

b)

X_{t-1} \ X_t	NL	NM	NS	Z	PS	PM	PL
NL	1	8	15 ■	22	29	36	43
NM	2	9	16	23	30	37	44
NS	3	10	17	24	31	38	45
Z	4	11	18	25	32	39	46
PS	5	12 ■	19	26	33 ■	40	47 ■
PM	6	13	20	27	34 ■	41	48
PL	7	14	21	28	35	42	49

Figure 4: Distribution of input-output data (x_{t-1}, x_t) in the input-output product space $X_{t-1} \times X_t$ (a). Bank of fuzzy rules of the time series modelling system (b), Source: own.

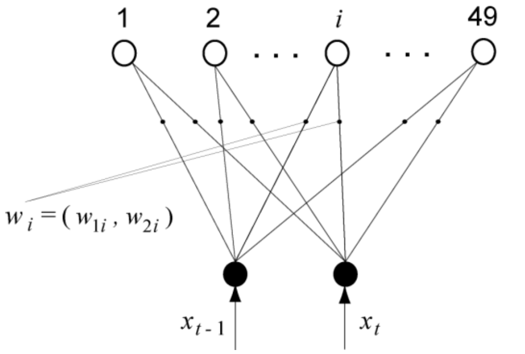


Figure 5: The topology of the network for fuzzy rules generating by SCL-based product-space clustering, Source: own

Supervised Competitive Learning (SCL)-based product-space clustering classified each of the 344 input-output data vectors into 9 of the 49 cells as shown in Figure 4 (a). Figure 4 (b) shows the fuzzy rule bank. For example, the fuzzy rule of 34th block corresponds to the following fuzzy relation

$$\text{IF } x_{t-1}^{i} = \text{PM} \text{ THEN } x_t^{j} = \text{PS}. \tag{13}$$

We added a rule to the rule bank if the count of input-output vectors in particular cells was larger than the value 0.05 N, where N = 344 is number of data pairs (x_{t-1}, x_t), in the input and output series. For example, the most frequent rule represents the cells 34. From most to last important (frequent) the fuzzy rules are (PM; PS), (PS; PL), (NL; NS), (PS; PL) a (PS; PS).

Finally, we can determine the output action given the input conditions. The Mamdani´s implication (Mamdani, 1977) was used. Each rule produces the output fuzzy set clipped at the degree of membership determined by the input condition and the fuzzy rule. When the input value, say $x_{t-1}^{i} = x_{344}^{i}$,is applied to the model (6), the output fuzzy value $x_t^j = x_{345}^j$ can be calculated. It is possible to compute the output fuzzy value x_t^j by the following simple procedure consisting of three steps:

- Compute the membership function values $\mu_{NL}(x_{t-1}),....\mu_{PL}(x_{t-1})$ for the input x_{t-1} using the membership functions in Figure 3.
- Substitute the computed membership function values in fuzzy relations (8), (12).
- Apply the max-min composition to obtain the resulting value of fuzzy relations. x_t^j

Following the above principles, we have obtained the predicted fuzzy value for the inflation $x_t = x_{345}^j = 0.74933$.

The inflation values in the output x_t^j, *t* = 345, 346, … are not very appropriate for a decision support because they are fuzzy sets. To obtain a simple numerical value in the output universe of discourse, a conversion of the fuzzy output is needed. This step is called defuzzification. The simplest defuzzification scheme seeks for the value $\hat{x}_t$ that is of middle Membership in the output fuzzy set. Hence, this defuzzification method is called the Middle of Maxima, abbreviated MOM. Following this method, we have obtained the predicted value for the $\hat{x}_{345}$= - 0.15. The remaining forecast for ex-post forecast period *t* =346, 347, … may be generated in a similar way.

As a final point, let us examine what has been gained by use of fuzzy time series model over an ordinary AR(1) model for the output $\hat{x}_{345}$. For this purpose, we have computed prediction limits on the one-step-ahead forecast from the AR(1) model, and fuzzy time series model. The 95 percent interval around the actual inflation value based on the statistical theory is

$\hat{x}_{345} = \pm u_{1-\alpha/2}\hat{\sigma}_{\varepsilon}(1+\phi_1^2)^{1/2} = 0.00312 \pm 1.96\ 0.15476(1+(-0.1248)^2)^{1/2} =$ $(-0.0442; 0.05043)$, where $\hat{x}_{345}$ represents the forecast for period t = 345 made at origin t = 344, $u_{1-\alpha/2}$ is a 100(1-$\alpha/2$) percentage of the standard normal distribution, and $\hat{\sigma}_{\varepsilon}$ an estimate of the standard deviation of the noise. An intuitive method for constructing confidence intervals for fuzzy time series model is simply the defuzzification method First of Maxima and First of Minima to obtain the prediction limits on the one-step-ahead forecast. In our example, the “confidence” interval for fuzzy time series value $\hat{x}_{345}$ = 0.00312 is (-0.30256 to 0.3088). The actual value for the AR(1) model does not fall within the forecast interval, and moreover, its sign is opposite to the forecast value sign.

4 Conclusion

In this paper, we have presented an application of the fuzzy tine series model to forecast an autoregressive process. This formal framework is based on the statistical approach, the AR(1) model and the neural network with the SCL clustering technique.

1. The comparison of proposed techniques with statistical approaches, the AR(1) model generates worse one-step-ahead forecasts. Furthermore, pure statistical models will involve more greater computational effort, and will more difficult to modify.
2. The method may be of real usefulness in practical applications, where the expert usually cannot explain linguistically what control actions the process takes or there is no knowledge of the process. In principle a neural network can derive this knowledge from data.

Acknowledgement

This article was created with the financial support of the Student grant competition Faculty of Economics, VŠB-TU Ostrava as a part of project SP2019/81, and also partially supported within Operational Program Education for Competitiveness – Project No. CZ.1.07./2.3.00./20.0296. An earlier version of this paper was presented in the C&I, Vol. 22, 2003.

References

Song, Q., Chisson, B.S. (1993) Fuzzy Time Series and its Models. Fuzzy Sets and Systems. Vol-54, pp. 269-277.

Zadeh, L.A. (1975) The concept Linguistic Variable and its Applications to Approximate Reasoning. Parts 1_3, Inform Si., Vol. 8, pp. 199-249; Vol. 8 pp. 301-357; Vl. 9., pp. 43-80.

Kosko, B. (1992) *Neural Networks ad Fuzzy Systems - a Dynamical System Approach to Machine Intelligence*. Prentice-Hall International, Inc.

Therien, C.W. (1992). Discrete Random Signal Processing. Prentice-Hall, USA.

Marček, D. (2003). Determination of Fuzzy Relations for Economic Time Series Models by NN. Computing and Informatics. Vol. 22, pp. 457-471.

Mamdani, E.H. (1977). Application of a fuzzy Logic to Approximate Reasoning Using Linguistic Synthesis. IEEE Trans. Compt., Vol.26, pp. 1182-1191.

Marček, D. (2002). *Neural Networks and Fuzzy time Series with Applications in Economics*. Silesian University (In Czech).

Internet of Things and Industrial Standards

Pavel Sládek[1], Miloš Maryška [2], Lea Nedomová [3], Petr Doucek [4]

Abstract. The concept known as the "Internet of Things" (IoT) is a connection between the physical and virtual worlds. The term Internet of Things is defined in different ways and we are explaining some of them and we are identifying key factors, which are leading to implementation of the IoT solution into companies. The indivisible part of IoT concept is communication between internet things equipment and servers or data warehouses. This paper is analyzing existing standards of IoT and reference model of IoT. The goal of this paper is specifying the most important standards, which are influencing IoT world and world of communication around the appearing IoT networks. Basis of the model is TCP/IP communication model. Accent of the article is focused on further four layers – application, transport, network and network interface. For each layer are presented main international standards with their analysis and briefly evaluation of its applicability in IoT area.

Keywords: Internet of Things, IoT standards, Industrial Internet of Things.

JEL Classification: L86, C88

1. Introduction

The concept called the “Internet of Things” represents a real interconnection of the physical and virtual world. This concept is nothing new in the business environment where it has been gradually developing for several decades. The concept continues to improve as the entire world of information technologies keeps dynamically developing. When looking closely, we can see high dynamics of used methods, implemented technologies and their interconnection. A more detailed view of the latest development and

[1] University of Economics, Prague/Faculty of Informatics and Statistics, department of Information Technology, pavel.sladek@vse.cz.
[2] University of Economics, Prague/Faculty of Informatics and Statistics, department of Information Technology, milos.maryska@vse.cz.
[3] University of Economics, Prague/Faculty of Informatics and Statistics, department of System Analysis, lea.nedomova@vse.cz.
[4] University of Economics, Prague/Faculty of Informatics and Statistics, department of System Analysis, doucek@vse.cz.

expected trends in the Internet of Things is provided e.g. in (Velosa et al, 2018).

The term “Internet of Things” (IoT) was mentioned for the first time in 1999 in the elaboration (Ashton, 2009). It evolved between 1999 and 2017, and other related terms appeared, such as Industry 4.0 (in 2011) or the Industrial Internet of Things (in 2012) (Elrod, 2016).

The term Internet of Things can be defined in different ways. A key definition is that of the International Organization for Standardization (ISO) that defines Internet of Things as ***an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and virtual world and react*** (ISO/IEC 20924:2018). The International Telecommunication Union (ITU) defines Internet of Things slightly differently, i.e. ***as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies*** (International Telecommunication Union, 2012). The company Gartner came up with the simplest and most widely used definition of the IoT concept. According to Gartner, IoT is ***the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment***.

The Institute of Electrical and Electronics Engineers (IEEE) defines the following features that a system must have to be considered an Internet of Things (Minerva et al, 2015):

- Interconnection of Things;
- Connection of Things to the Internet;
- Uniquely Identifiable Things;
- Ubiquity;
- Sensing/Actuation Capability;
- Embedded Intelligence;
- Interoperable Communication Capability;
- Self-configurability;
- Programmability.

The launch and implementation of Internet of Things is driven by two main forces. The first force is a technological process, the penetration of information technologies into an ever-increasing number of products and lower prices of information technologies and their components and network connection. The other force is the human need to be more and more connected to immediate events in an increasingly wider environment. It is about expanding computation power from one device into an environment that becomes an interface.

The implementation of IoT provides major business benefits, which is proven e.g. by a detailed analysis of opportunities associated with the implementation of IoT in energy supply (Sládek and Maryska, 2017). High benefits of IoT are expected especially in production enterprises and other organizations with standardized processes (e.g. hospitals).

Currently, the main problem is that there is not a clear definition of the standards, based on which all manufacturers and providers would deal with the world of IoT.

The goal of this article is to define and summarize the basic standards that can and should be used for the Internet of Things in a real business environment.

2. Internet of Things Standards

The “Internet model” that contains four layers described in IETF RFC 1122 and 1123 (Braden 1989a; 1989b) can be considered the basic reference model for the organization of IoT standards. The defined layers help to categorize communication protocols, and a group of protocols in the Internet model is sometimes referred to as a group of Internet protocols. The Internet model has the following layers:

- Network access layer;
- Network layer;
- Transport layer;
- Application layer.

An alternative to the Internet model is the IOS/OSI model that contains seven layers and is described in (Zimmermann, 1980). Since the protocols designed based on the OSI model are less used than the protocols from the ICP/IP family, we feel that it is better to use the Internet model to define the layers.

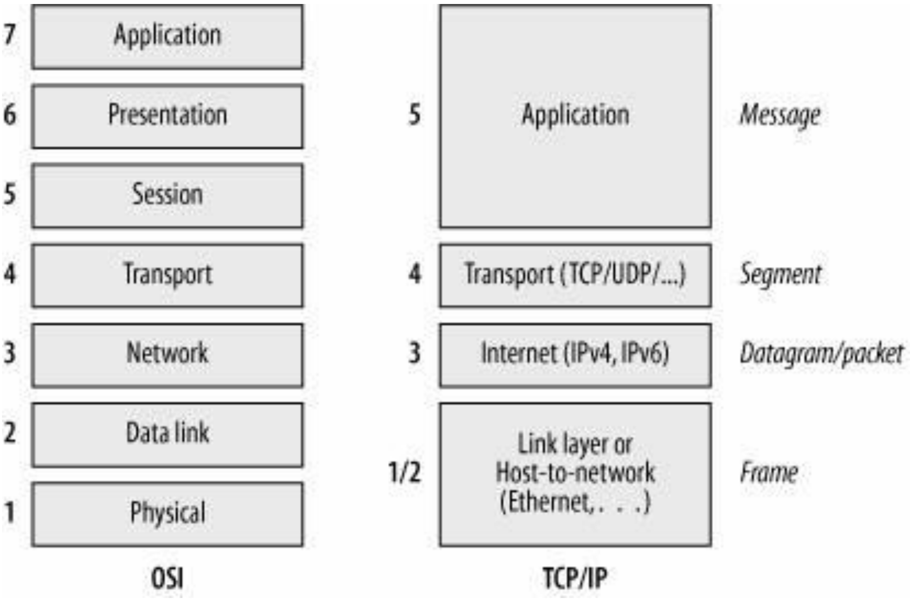


Figure 4 The four layers of the ICP/IP Internet model vs. the seven layers of the reference ISO/OSI model, Source Embeddedlinux 2019.

Specialized technologies meeting the needs of the IoT concept are being developed and standardized (Li et al, 2015). Standardization somewhat lags behind the needs for interoperability on different layers of IoT architecture (Sheng et al, 2013). IoT solutions use a combination of well-tested technologies and must search for the latest technologies that are able to meet special needs. Standardization plays a key role in ensuring interoperability and in scaling solutions (Perera et al, 2014).

2.1. Network access layer

The network access layer handles everything that has to do with controlling a specific transmission route and direct sending and receiving of data packets. It depends on the used transmission technology. The network access layer provides access to the transmission medium and there are many protocols that provide these services.

NFC

NFC (Near Field Communication) is a protocol for communication between two devices that are several centimeters from each other. NFC is standardized as ISO 18092 (ISO/IEC 18092 2013). It is used mainly in mobile phones for payment communication, but its potential use is much wider, including the transmission of standard data. NFC devices can work in different modes, e.g. they can simulate a contactless card as an NGC tag scanner or exchange data with an equivalent device.

RFID

RFID (Radio Frequency Identification) uses electromagnetic fields to exchange information between a tag and a scanner. A tag includes an identifier obtained through the reader and sent for further processing. Tags and readers are active or passive, depending on their power source. The distance at which a tag can be read depends on the used power source and can be as long as dozens of meters. The typical reading distance is dozens of centimeters (Weis, 2007).

UWB

UWB (Ultra Wideband) is a wireless technology designed for a very short range. It sends very short low-energy pulses in a wide band. Since it uses a wide band and a low-energy transmitter, it can reuse the used frequencies and mask the signal in the noise of transmission channels (Gungor and Hancke, 2009; Lee et al, 2007).

Contiki, TinyOS, RIOT, LiteOS

Special operating systems are being developed for an environment that is considerably limited in terms of computation power, memory and power. These systems include Contiki, TinyOS, RIOT and LiteOS, but there are others as well, and are typically used in devices with battery-operated sensors. Specialized operating systems are more effective in utilizing limited sources available in such an environment (Postscapes 2019a; Postscapes 2019b).

2.2. Network layer

The network layer is primarily based on IP (Internet Protocol) but contains other protocols as well. IP is designed to prefer speedy data transmission over reliable data transmission. This is why it was decided to choose connectionless transmission since it does not correct errors during transmission. These properties can be resolved in the transport or application layer. Connectionless transmission is more robust than connection-oriented transmission because it is more resistant to any potential failure of transmission routes.

IPv4

Internet Protocol version 4 (IPv4) is the fourth version of the Internet protocol that became the core networking protocol when the Internet took off. It is a connectionless protocol designed for packet-switched networks. A device is unequivocally identified by a 4-byte address and theoretically provides 2^{32} potential addresses, i.e. about four billion addresses (Postel, 1981a).

IPv6

Internet Protocol version 6 (IPv6) is the sixth version of the Internet protocol that overcomes several key limitations of IPv4. The main advantages of IPv6, as compared to IPv4, include a larger address space, integrated security mechanisms, Quality of Services mechanisms (QoS) and automatic configuration and mobility support.

6LoWPAN

6LoWPAN is an acronym of IPv6 over Low-Power Wireless Personal Area Networks. It is IPv6 adjusted to connection through technologies compatible with the IEEE 802.15.4 wireless standard (Postscapes, 2019a). The goal of 6LoWPAN is to bring the advantages of standard IP networks to low-power sensor and wireless networks that often used proprietary technologies in the past (Gartner IT Glossary, 2019a).

IPSec

Internet Protocol Security (IPSec) is a group of protocols securing communication through the Internet protocol (IP) that authenticates and encrypts every packet of data flow. IPSec also includes protocols for establishing mutual authentication between agents and negotiating cryptographic keys to be used during the session. IPSec works in the network layer (Dhall et al, 2012).

2.3. Transport layer

The transport layer provides end-to-end communication services for applications. The main task of the transport layer is to provide transmission between end participants of communication, which - in the case of the Internet model architecture - are application programs. The transport layer can control the flow of data in both directions, ensure transmission reliability and change connectionless transmission in the network layer to connection-oriented transmission. The following two main protocols are used – TCP (Transmission Control Protocol) for connection-oriented communication and UDP (User Datagram Protocol) for connectionless communication.

TCP

TCP (Transmission Control Protocol) is a connection-oriented protocol that guarantees delivery of data and keeps the same order. A message lost in transmission is resent. Messages are delivered in the same order in which they were sent. This may result in blocking a time-critical message behind non-critical messages with low priority (Joshi et al, 2018; Postel 1981b).

UDP

UDP (Universal Datagram Protocol) is a stateless transmission protocol providing non-guaranteed delivery of messages. A message lost in transmission is not resent. It does not guarantee that messages are delivered in the same order in which they were sent (Joshi et al, 2018; Postel 1980).

2.4. Application layer

Application layer protocols can be divided into user and support protocols. There are a lot of user protocols and their number keeps increasing over time. Support protocols include e.g. DNS (Domain Name System) for translation of domain names to IP addresses, DHCP (Dynamic Host Configuration Protocol) for dynamic configuration of network hosts and SNMP (Simple Network Management Protocol) for network management. We will focus on the following user protocols:

- **DDS** (Data Distribution Service) is an open connectivity standard for Industrial Internet of Things (IIoT) applications. The main purpose of DDS is to interconnect components (devices, gateways or applications) with other components in order to implement real-time systems and the systems of systems (Joshi et al, 2018).

- **CoAP** (Constrained Application Protocol) is an HTTP-inspired protocol that has been designed to be lightweight and more powerful. The CoAP specification is maintained by IETF. In general, it is used in operation systems.
- **MQTT** (Message Queuing Telemetry Transport) is an open standard maintained by OASIS and requiring the use of TCP. Its design and original purpose were to collect data from telemetry or remote monitoring and to deliver them to the follow-up IT infrastructure. MQTT is designed to be open, simple and easy-to-implement and to allow one server to service thousands of lightweight clients (Joshi et al, 2018; Lampkin, 2012).
- **OPC UA (**Object Linking and Embedding for Process Control Unified Architecture) is mainly used in the manufacturing industry to communicate with industrial devices. OPC UA was preceded by OPC. It unifies different original OPC specifications and switches from API to the network protocol. OPC UA architecture distinguishes between servers and clients (Joshi et al, 2018).
- **AMQP** (Advanced Message Queuing Protocol) is a standard for message-oriented middleware (MOM, Message Oriented Middleware). It supports non-synchronized program communication between two or more application components, applications or systems (Gartner IT Glossary, 2019b). AMQP is standardized as the intentional standard ISO/IEC 19464:2014 and maintained by OASIS.
- **Fieldbus** refers to a group of technologies designed for distributed management and control of real-time industrial devices. Fieldbus, i.e. a group of technologies and not just one technology, is standardized as IEC 61158 (IEC 61158:2019). In general, Fieldbus technologies have low interoperability that is however increasing thanks to a gradual adoption of Ethernet and IP technology (Joshi et al, 2018).

Other protocols are as follows:

- HTTP/REST
- WS/SOAP
- XMPP
- Websocket

Unfortunately, we cannot analyze them due to the limited scope of this article and therefore we refer to the primary source Sládek, 2019.

3. Usage of IoT Standards

One of examples how can be used above-mentioned standards, is reading of pumped water in drainage wells. The pump is fitted with a water meter, which measures the amount of pumped water.

Reading of water meters and checking of pump operation is carried out at regular monthly intervals. Status check and record keeping is a manual activity. Information on the amount of pumped water is entered into the information system only to the system processing waste reporting and water management.

In our case, we have, used following protocols mapped to TCP/IP model.

- Network access layer our case is based on Sigfox.
- On the level of Network Layer it was IPv4.
- Transport Layer is based on TCP
- Application layer is based on HTTP/REST.

4. Conclusions

Specialized technologies satisfying the needs of the IoT concept are being developed and standardized. Standardization somewhat lags behind interoperability needs at different layers of IoT architecture. IoT solutions use a combination of well-tested technologies and must search for new technologies to satisfy special needs. Standardization plays a key role in ensuring interoperability and in scaling solutions.

This article analyzes technological standards applicable to the Internet of Things and the Industrial Internet of Things. It categorizes and briefly describes relevant standards. The identified relevant standards are then a key input for identifying Industrial IoT components.

Identification of IoT components is crucial for setting up the architectural framework for designing architectural solutions. The main problem of current frameworks is that they work on an abstract level with abstract components.

Acknowledgements

Paper was processed with contribution of long term support of scientific work on Faculty of Informatics and Statistics, University of Economics, Prague (IP 400040).

References

Ashton, K. (2009) *That „Internet of Things" Thing, RFID Journal,* [Online], Available: http://www.rfidjournal.com/articles/view?4986 [18 Aug 2019].

Braden, R. (1989a) *Requirements for Internet Hosts - Application and Support IETF RFC 1123,* [Online], Available: https://tools.ietf.org/html/rfc1123 [28 May 2019].

Braden, R. (1989b) *Requirements for Internet Hosts - Communication Layers IETF RFC 1122,* [Online], Available: https://tools.ietf.org/html/rfc1122 [18 Jun 2019].

Dhall, H., Dhall, D., Batra S. and Rani, P. (2012) Implementation of IPSec Protocol. In: *2012 Second International Conference on Advanced Computing Communication Technologies* [Online], pp. 176–181. DOI:10.1109/ACCT.2012.64

Elrod, K. (2016) *IoT, IIoT, Industry 4.0: What's the difference and does it matter? - Sealevel* [Online], Available: http://www.sealevel.com/community/blog/iot-iiot-industry-4-0-whats-the-difference-and-does-it-matter/ [18 Jun 2019].

Embeddedlinux (2019) Available: http://www.embeddedlinux.org.cn/linux_net/0596002556/understandlni-CHP-13-SECT-1.html [18 Aug 2019].

Gartner IT Glossary (2019a) *6LoWPAN* [Online], Available: https://www.gartner.com/it-glossary/6lowpan/ [28 April 2019].

Gartner IT Glossary (2019b) *Advanced Message Queuing Protocol (AMQP)* [Online], Available: https://www.gartner.com/it-glossary/advanced-message-queuing-protocol-amqp/ [18 May 2019].

Gungor, V. C. and Hancke, G. P. (2009) Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches. *IEEE Transactions on Industrial Electronics* [Online], **56**(10), pp. 4258–4265. DOI:10.1109/TIE.2009.2015754.

IEC 61158-1:2019 *Industrial communication networks - Fieldbus specifications - Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series* [Online], International Electrotechnical Commission Available: https://webstore.iec.ch/publication/59890 [18 May 2019].

ISO/IEC 20924:2018 *Information technology- Internet of Things (IoT)- Vocabulary* [Online], International Organization for Standardization. Available: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/94/69470.html [18 April 2019].

ISO/IEC 18092:2013 Information technology-Telecommunications and information exchange between systems-Near Field Communication-Interface and Protocol (NFCIP-1) [Online], International Organization for Standardization. Available: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/66/56692.html [18 Jun 2019].

International Telecommunication Union (2012) *Overview of the Internet of things, Recommendation ITU-T Y.2060* [Online], Available: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 [15 May 2019].

Joshi, R., Mellor S. and Didier, P. eds. (2018) *The Industrial Internet of Things Volume G5: Connectivity Framework* [Online], Industrial Internet Consortium. Available: https://www.iiconsortium.org/pdf/IIC_PUB_G5_V1.01_PB_20180228.pdf [18 April 2019].

Lampkin, V. (2012) *What is MQTT and how does it work with WebSphere MQ? (Application Integration Middleware Support Blog)* [Online], Available: https://www.ibm.com/developerworks/community/blogs/aimsupport/entry/what_is_mqtt_and_how_does_it_work_with_websphere_mq?lang=en [18 April 2019].

Lee, J., Su, Y. and Shen, C. (2007) A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. In: *IECON 2007 - 33rd Annual Conference of the IEEE Industrial Electronics Society*: *IECON 2007 - 33rd Annual Conference of the IEEE Industrial Electronics Society* [Online], pp. 46–51. DOI:10.1109/IECON.2007.4460126

Li, S., Xu, L. D. and Zhao, S. (2015) The internet of things: a survey. *Information Systems Frontiers* [Online], **17**(2), pp. 243–259. DOI:10.1007/s10796-014-9492-7

Minerva, R., Biru, A. and Rotondi, D. (2015) *Towards a definition of the Internet of Things (IoT)* [Online], IEEE Internet Initiative. Available: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf [18 Aug 2019].

Perera, C., Liu, C. H., Jayawardena, S. and Chen, M. (2014) A Survey on Internet of Things from Industrial Market Perspective. *IEEE Access* [Online], **2**, pp. 1660–1679. DOI:10.1109/ACCESS.2015.2389854

Postel, J. (1980) *User Datagram Protocol IETF RFC 768* [Online], Available: https://www.ietf.org/rfc/rfc768.txt [18 Jun 2019].

Postel, J. (1981a) *Internet Protocol IETF RFC 791* [Online], Available: https://tools.ietf.org/html/rfc791 [18 Jun 2019].

Postel, J. (1981b) *Transmission Control Protocol IETF RFC 793* [Online], Available: https://tools.ietf.org/html/rfc793 [18 Jun 2019].

Postscapes (2019a) *IoT Software | 2018 Guidebook on Tools, OS and Frameworks* [Online], Available: https://www.postscapes.com/internet-of-things-software-guide/ [18 Aug 2019].

Postscapes (2019b) *IoT Standards & Protocols Guide 2019 - Comparisons on Network, Wireless Comms, Security, Industrial* [Online], Available: https://www.postscapes.com/internet-of-things-protocols/ [18 April 2019].

Sheng, Z., Yang, S., Yu, Y., Vasilakos, A. V., McCann, J. A. and Leung, K. K. (2013) A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities. *IEEE Wireless Communications* [Online], **20**(6), pp. 91–98. DOI:10.1109/MWC.2013.6704479

Sládek, P. and Maryska, M. (2017) Internet of things in energy industry. In: *IDIMT 2017: Digitalization in Management, Society and Economy - 25th Interdisciplinary Information Management Talks*. s. 411–418.

Velosa, A., Schulte, W. R., Lheureux, B. and Nuttall, N. (2018) *Hype Cycle for the Internet of Things,* [Online], Gartner, Inc. Available: https://www.gartner.com/document/3883066?ref=solrAll&refval=217565777&qid=ea4f1da5a14b4eca86b030 [18 April 2019].

Weis, S. A. (2007) *RFID (Radio Frequency Identification): Principles and Applications* [Online], Available: http://www.nfc-off.ch/uploads/4/5/1/2/45128343/rfid-article_mit_usa.pdf [18 Aug 2019].

Zimmermann, H. (1980) OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection. *IEEE Transactions on Communications* [Online], **28**(4), 425–432. DOI:10.1109/TCOM.1980.1094702

Using Information Technologies in Recycling Electrical and Electronic Equipment

Jan Turay[1], Lenka Tkačíková[2], Josef Bělica[3], Jan Vašek[4]

Abstract. Industry 4.0 together with environmental legislative has created new challenges for enterprises. One of these challenges is recycling electrical waste. The aim of the article's authors is to verify the advantage of using information system in recycling electrical waste. The verification is done by the focus group method. At first, the article introduces the newest valid legislative; moreover authors focus on the ASEKOL collective system and information technologies used for entering information into this system and the ways of calculating recycle fee and lastly on the environmental invoicing.

Following the outputs of the focus group, attended by four environmental specialists, it can be stated that the collective recycling system significantly reduces transaction costs for waste electrical and electronic equipment (furthermore WEEE) management. Secondly, that the ASEKOL information systems are user friendly and understandable, even though, the environmental invoicing lacks the necessary transparency.

Keywords: Industry 4.0, information technology, recycling, electrical and electronic equipment, environmental invoicing, focus group.

JEL Classification: Q56, M15

1. Introduction

The concept of Industry 4.0 has created new challenges for industrial enterprises such as digitalization, advanced automation of industrial production and all related processes, or the definition of medium and long-term corporate digital strategies (Mařík et al., 2018; Yan et al. 2017). All that

[1] Ing. Jan Turay, VŠB - Technical University of Ostrava, Faculty of Mining and Geology, Department of Economics and Control Systems, 17. listopadu 2172/15, 708 00 Ostrava, Czech Republic, jan.turay.st@vsb.cz .

[2] Ing. Lenka Tkačíková, VŠB - Technical University of Ostrava, Faculty of Mining and Geology, Department of Economics and Control Systems, 17. listopadu 2172/15, 708 00 Ostrava, Czech Republic, lenka.tkacikova.st@vsb.cz .

[3] Ing. Josef Bělica, VŠB - Technical University of Ostrava, Faculty of Mining and Geology, Department of Economics and Control Systems, 17. listopadu 2172/15, 708 00 Ostrava, Czech Republic, jan.turay.st@vsb.cz .

[4] PhDr. Jan Vašek, MSc., CVUT - MIAS School of Business, Management, jan.vasek@cvut.cz .

requires close association of independent working units to create fully integrated, fully automated and optimized production and information flow through a global network. In practice, this means that not only the product itself, but also sensors, devices and IT systems form complex chains with reach and scope going beyond the extend of the organization itself (Mařík et al., 2016).

One of these new, autonomous ecosystems is an integrated material and individual component recycling system for electrical and electronic waste (Wang and Wang, 2019), enabling businesses to achieve sustainable production and resource efficiency across the entire supply chain and product life cycle.

The authors of this article have decided to verify whether and how selected information systems may help the pursuit to meet legislative standards set to all producers of electrical products. They have decided to use the technique of focus group. The aim of this paper is to present the ASEKOL collective system that offers its members many interesting features for example available collection points, physical collection and recycling of electrical waste, recording and reporting results to regulatory authorities. Besides meeting the legislative requirements the system significantly helps to fulfil recycling goals set by the European Union to its Member States and therefore also to the Czech Republic. Above all, the authors want to show how information technologies developed by ASEKOL facilitate the course of recording, processing, evaluating and reporting the electronic and electrical equipment waste recycling.

The article has the following structure: The second section shortly introduces the valid legal framework for the e-waste recycling and the third section reflects the advantages and disadvantages of collective systems. The forth part introduces the ASEKOL collective system from the information technologies used for entering information point of view, but also in perspective of how the recycle fee is calculated and environmental invoicing is prepared.

2. Legal framework

The obligation to recycle electronics in the Czech Republic has been in place since 2005 and is fully in line with the 3R strategy: refuse, reuse or recycle

(Tseng et al., 2018). Non-negligible quantities of glass, metal, non-metal, plastic and rare materials can be obtained from electrical waste (currently it specifies the obligations of producers and importers when placing products on market in terms of waste management and recycling (EU, 2019):

- Directive 2012/19/EU of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE). In practice, this means actively preventing the generation of WEEE, promoting the re-use and recycling of WEEE and, above all, the efficient use of resources and secondary raw materials.
- Directive 2008/98/EC of the European Parliament and of the Council on waste. According to this Directive, businesses must protect the environment and health while placing emphasis on good waste management, ensuring technologies for recovery and recycling of waste and aiming at reducing resource consumption and best use.
- Directive 2009/125/EC of the European Parliament and of the Council defining eco-design requirements for products and energy performance. Businesses must create an ecological profile for all products and assess the environmental impact at each stage of their life cycle.
- Directive 2011/65/EU of the European Parliament and of the Council on the restriction of the use of certain hazardous substances in electrical and electronic equipment. This Directive also contains a list of exemptions (i.e. specific criteria), which are not covered by the restriction for a limited period. As the technology has been quickly developing, the list of exemptions is continually updated. And thus manufacturing companies shall design and create products in accordance with this Directive and importers must always check that the equipment has been approved and complies with the Directive. And least but not last, also distributors must ensure compliance with the standards for all offered products.

With the rapid progress of science, knowledge and technological development, it can be expected, that the environmental legislation will continue to be updated. As example can be used the directives included in Circular Economy Package, which came into force on 4th July 2018. One of these directives amends directive 2012/19/EU on waste electrical and electronic equipment (WEEE) (Podlasová et al., 2018). It is clear, that the above legislation places high demands on market participants. In terms of implementation, companies must (1) choose between an individual or collective recycling system, (2) create an efficient process to select and transport to the recycling place, recycle and return the recyclate to the market, (3) create a mechanism to successfully fund recycling (4) and also take advantage of incentives for eco-design (Atasu and Wasenhove, 2012). Other option is Environmental Management System (EMS) (Ministr, 2013), or cooperation with universities (Ministr and Pitner, 2015). Other legal aspects of environmental issues described, for example, Kozel et al. (2015).

The scope of the article does not allow for detailed discussion of all four aspects. The following section therefore focuses only on the choice between the individual and collective recycling system in the Czech Republic.

3. Collective recycling systems

The legislation implies that manufacturers and importers are obliged to keep records of: all products placed on the market, number of products withdrawn from the market, the way of their removal, and lastly their recycling rate. In practice, companies either fulfil this obligation individually or they use the form of collective system. Understandably, companies choose such way of recycling, which minimises their overall ownership cost.

For individual execution each industrial producer must apply to be put on the list of producers of electrical and electronic equipment maintained by the authorities of the Ministry of Environment (hereinafter referred to as MoE) and keep records on the market of these electrical and electronic equipment as well as recovered WEEE, starting with collection, treatment, recovery or disposal. Consequently, by 31 March of each year, the company must prepare an annual report for the previous calendar year on compliance with the obligation to take back electrical equipment and separate collection through the Integrated Environmental Reporting System (hereinafter ISPOP). The main reason why large companies, in particular, opt for an administrative and process-intensive individual system is the control of recycling and the ability to efficiently use the ecological design of their products (Esenduran and Kemahlıoğlu-Ziya, 2015). In 2017 only 49 producers individually complied with their obligations and none of them supplied electrical equipment for domestic use (MŽP, 2019a).

The vast majority of companies engage in a collective system that provides for the collection, processing, commercialization and professional disposal of equipment, administration and communication with the MoE. The state authorities then aggregate the information, process it statistically and transmit it to the EU bodies. A key benefit of the collective system is the economies of scale stemming from lower unit costs for the collection and recycling of e-waste, including collection, transport, disassembly, environmental disposal of hazardous substances and the processing of recyclable materials. (Esenduran and Kemahlıoğlu-Ziya, 2015). The authors of the article used qualitative research to verify their research theses. Specifically, they used the focus group method, which was attended by four environmental specialists for smaller businesses and regular ASEKOL users. The focus group results show significant transaction and administrative cost savings (see **Table 1** with illustrative quotations).

Table 1 Illustrative quotations of the focus group participants. Source: own findings

"If we were to [recycle] ourselves, we could not sell to households at all."
“I see further savings in communication with state authorities. … We would have to hire a full time employee or outsource this activity. ”
“The price list is transparent and so it is easy to estimate the amount we have to spend on e-waste recycling."
"Legislation is complex and extensive…with ASEKOL we know that it is being obeyed.”
"The system is standardized and the only thing you need to do is to enter data into the system every quarter and everything gets automatically calculated."
“We have not calculated how much we save by using the collective system, but quite frankly, it must be millions.”
"We would certainly like to avoid recycling fees, but at least we only pay a symbolic fee to participate in the collective system."

The following section will introduce the ASEKOL collective system and IT technologies that the company uses for information collection and fees and environmental invoicing calculation.

4. ASEKOL collective system

At present, there are altogether 15 collective systems operating at the market, namely: Asekol, a.s., Asekol solar s.r.o., Bren s.r.o., ČEZ Recylace s.r.o., ECOPARTNER s.r.o., EKOLAMP s.r.o., ELEKTROWIN a.s., FitCraft Recyklace s.r.o., MINTES Solutions s.r.o., PV Recovery, s.r.o., Recycling Systems, s.r.o., Rema PV Systém, a.s., Rema Systém, a.s., REsolar s.r.o., RETELA, s.r.o. (MŽP, 2019b). Organizations differ in market share, number of members, and range of scope and volume of processed WEEE.

One of the largest collective take-back and recycling systems is operated by ASEKOL, company founded in 2005 by significant producers and importers of consumer, computing and telecommunications technology such as Samsung or LG (Asekol, 2018). The company serves its customers as a contractual provider of nationwide system for take-back of electrical and electronic equipment, i.e. setup, operation and gradual expansion of the collection network, collection and transport of WEEE and its subsequent recycling, as well as data processing and annual reporting to ISPOP according to the requirements of Directive 2012/19/EU of the European Parliament and of the Council on waste electrical and electronic equipment and the relevant Czech legislation.

One option, how to collect WEEE is special red container, which are located in the cities across the Czech Republic. The owner of these containers is ASEKOL company. In this area can be used RFID chips (Danel, 2016). By the use of GRPS data these RFID chips send data on how full the containers are to their owners (Podlasová et al., 2017; Kozel et al., 2018).

In order for the whole system to function properly, it is necessary to create a relatively sophisticated information management system that can be divided into steps, which are described in the following subsections.

4.1. Entering information

Entering information in the ASEKOL Information System is to be done on a quarterly basis via Internet interface. Producers or importers simply enter which types of electrical equipment and how many pieces they put on a market and the approximate weight of these products. The same is done for products withdrawn from the market due to reclamation or refurbishment.

As of January 2019, six groups of electrical and electronic equipment (EU, 2019) are inserted into the ASEKOL Information System in accordance with WEEE Directive 2012/19/EU: (1) Temperature exchange equipment, (2) Screens, monitors, and equipment containing screens having a surface greater than 100 cm2, (3) Lamps, (4) Large equipment (any outside dimension greater than 50 cm). This does not include devices from group 1-3, (5) Small equipment (no external dimension greater than 50 cm). (6) Small IT and telecommunication equipment (no external dimension more than 50 cm).

Respondents agree that the information entry system is user-friendly, as illustrated in Table 2, which evaluates the software against the ISO 25000 criteria (ISO, 2019). The only major weakness is the absence of data input error prevention mechanisms, such as the choice of the wrong group of WEEE, which is essential to calculate the fee.

"It has happened several times that we had made a mistake while choosing the group of the equipment. I have noticed immediately as the fee was unusually high. But the statement cannot be corrected; you always have to create a correction report and start communicating with Asekol. It's not difficult, but it takes time. (Focus group participant).

Table 2 Qualitative evaluation of IS Asekol user friendliness according to ISO 25000 (2019) criteria, Source: own findings

Criteria	Comment
Appropriateness/ Recognisability	Suitable for reporting, further processing and subsequent environmental billing.
Learnability	Intuitive, very easy to understand at first login.
Operability	Easy to use, easy to navigate between screens.
User error protection	There are no reliable mechanisms to prevent serious errors, such as choosing the wrong group of WEEE.
User interface aesthetics	User-friendly interface
Accessibility	Possibility to connect from any device using a password or from a designated device via a certificate. Any trained layman is easily able to understand the system.

4.2. Recycling fee calculation

Based on entered information, the system generates summary of reported EEE groups and the exact amount of recycling fees. At the same time, the member is charged a symbolic fixed system fee for participation in the collective system. The collected fees, as well as the revenues from the sale of the recyclate, will then be used by Asekol to finance the collection and recycling of waste.

Recycling fee amount depends on the type of electrical equipment. The algorithm is completely transparent and is based on a tariff that is accessible to all Asekol members.

4.3. Environmental invoicing

Asekol submits the data to the MoE for control, aggregation and subsequent statistical processing and also publishes its own statistics (see the following subsections), which the focus group participants use for certification according to ISO 14001, measuring triple responsibility (i.e. economic, social and environmental impact) and decisions on eco-design and marketing communication.

4.3.1. Collection network and collected electrical waste

Table 3 is based on Asekol's annual reports and shows that since 2005 the company has managed to build a wide and dense network of collection points and red containers for collection of WEEE and, on the top of that, to collect 219 361 tonnes of used electrical equipment (Asekol, 2018). One of the focus group participants’ reports complete this statistics with not only the size of the collection network, but above all, the quantity and percentage of recovered electric waste.

Table 3 Selected indicators of Asekol, Source: own processing based on Asekol data (2018)

Year	Collected amount of electrical waste [t]	Number of collection points	Number of placed red containers for electrical waste [pc]	Electrical equipment take-back per capita [kg]	Electrical equipment take-back from the amount put on the market [%]
2006	5 792	2 171	-	0.56	15
2007	9 182	4 053	-	0.9	25
2008	12 928	6 019	-	1.24	35
2009	17 186	10 641	-	1.65	40
2010	16 558	11 152	-	1.57	64
2011	17 657	13 122	-	1.67	47,6
2012	17 139	15 087	-	2.39	54.96
2013	15 692	15 935	1 987	1.49	-
2014	16 981	16 800	2 109	1.62	-
2015	17 743	17 053	2 252	-	50
2016	19 554	16 098	2 821	-	69
2017	19 185	16 687	3 377	-	62
2018	18 640	17 157	3 594	-	59

4.3.2. Environmental impact

In its annual reports and publications, Asekol seeks to systematically raise awareness of the importance of WEEE recycling. In particular, respondents appreciate both aggregate and individual environmental invoicing based on selected WEEE for a given year. The report shows real savings in electricity, CO2, oil and drinking water (see Table 4). Asekol uses third-parties algorithms for the calculation and, according to the focus group participants if the company had published the methodology, it would have significantly increased the credibility of invoicing for internal and external stakeholders.

"When I work with these figures internally, I'm constantly facing the problem of scepticism as we do not know the exact method Asekol uses to calculate these figures. Our managers, therefore, refuse to state them in our annual reports or on our social media pages. Which is a pity, as it would be a great opportunity for Asekol to get free advertisement." (Focus group participant).

Table 4 Aggregate environmental accounting of the company, Source: own processing based on Asekol (2018)

Year	Electricity savings [MWh]	CO2 savings[t]	Oil savings [l]	Drinking water savings [l]
2014	219 255	-	11 232 559	948 614
2015	209 672	45 641	9 782 532	909 355 320
2016	263 344	56 580	13 619 607	1 204 156 000
2017	262 447	54 575	14 703 550	1 156 447 000
2018	251 436	53 312	13 514 996	1 064 661 280

5. Conclusion

In this article, we have introduced Asekol and showed that the Asekol collective system significantly reduces transaction costs for companies. The reason for these savings is that the companies do not have to set up collection points, arrange collection, treatment and disposal of WEEE or to keep records of take-back and separate collection of electrical equipment and then enter records into ISPOP. At the same time, the information system for entering information, calculating the fee and generating reports from a user point of view is very simple and clear. The only weakness is the non-transparent calculation of electricity, CO2, oil and drinking water savings.

From a societal perspective, the Asekol Collective System succeeds in contributing the recycling target defined by the European Union: for example, in 2015 it was 70% for material recovery and 70% for recovery. Asekol was able to reach 80% for material recovery and 95% for recovery (Asekol, 2018).

References

Asekol (2018) ‘Výroční zprávy 2007-2018’, [Online], Available: https://www.asekol.cz/asekol/o-nas/vyrocni-zprava/ [12 Sep 2019].

Atasu, A. and Van Wassenhove, L. N. (2012) ‘An operations perspective on product take-back legislation for e-waste: Theory, practice, and research needs.’ *Production and Operations Management,* vol. 21, no. 3, pp. 407-422.

Danel, R. (2016) ‘Trends in information system for production control in the raw industry’ *Liberec Information Forum – LIF 2016,* Liberec, pp. 19-26.

Esenduran, G. and Kemahlıoğlu-Ziya, E. (2015) ‘A comparison of product take-back compliance schemes.’ *Production and Operations Management,* vol. 24, no. 1, pp. 71-88.

EU (2019) ‘SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY.’, [Online], Available: https://eur-lex.europa.eu/legal-content [10 Sep 2019].

Iso25000.com (2019) *ISO* [Online], Available: https://iso25000.com/index.php/en/iso-25000-standards/iso-25010/61-usability [20 Sep 2019].

Kočí, D. I. V. (2015). '*LCA sběru a recyklace drobného elektroodpadu.*’ TVIP, [Online] Available: http://www.odpadoveforum.cz/TVIP2015/prispevky/018.pdf, [10 Aug 2019].

Kozel, R. et al. (2018) ‘Innovations in waste management’ *26th Conference on Interdisciplinary Information Management Talks (IDIMT): Strategic Modeling in Management, Economy and Society – 26th Interdisciplinary Information Management Talks 2018,* Linz, pp. 119-126.

Kozel, R. et al. (2015) ‘Legal aspects of environmental issues in the Czech Republic’ *15th International Multidisciplinary Scientific Geoconference and EXPO, SGEM 2015,* Sofia, pp. 703-709.

Mařík, V. et al. (2018) ‘*Industry 4.0 – the initiative for the Czech Republic’*, [Online], Available: http://ricaip.eu/wp-content/uploads/2018/11/Industry-4-0_The-Initiative-for-the-Czech-Republic.pdf [7 Aug 2019].

Mařík, V. et al. (2016) *Průmysl 4.0: výzva pro Českou republiku*. Praha: Management Press.

Ministr, J. (2013) ‘Modelling and Simulation Support of EMS Processes.’ *10th IFIP WG 5.11 International Symposium on Environmental Software Systems (ISESS),* Berlin, pp. 571-578.

Ministr, J. and Pitner, T. (2015) ‘Use of non-investment subsidies in academic and business co-operation’ *IDIMT 2015: Information Technology and Society - Interaction and Interdependence - 23rd Interdisciplinary Information Management Talks 2015,* Linz, pp. 141-146.

MŽP (2019a) ‘*Vybraná data týkající se nakládání s odpadními elektrickými a elektronickými zařízeními (OEEZ) v České republice.*’, [Online], Available: https://www.mzp.cz/C1257458002F0DC7/cz/odpadni_elektronicka_zarizeni_nakladani_cr/$FILE/OODP-vybrane_ukazatele_elektrozarizeni-19_08_2019.pdf [20 Sep 2019].

MŽP (2019b) ‘*Kolektivní systémy.*’, [Online], Available: https://isoh.mzp.cz/WebElektro/ [20 Sep 2019].

Podlasová, A. et al. (2018) ‘Information technologies in context of new European Union legislation’ P*roceedings of the 21st International Conference on Information Technology for Practice 2018,* Ostrava, pp. 231–237.

Podlasová, A., Šikýř, P and Bařinka, K. (2017) ‘Information technology in waste management’ *20th International Conference on Information Technology for Practice 2017,* Ostrava, pp. 305-312.

Tseng, M. L. et al. (2018) ‘Circular economy meets industry 4.0: can big data drive industrial symbiosis?’ *Resources, Conservation and Recycling*, vol. 131, pp. 146-147.

Yan, J. et al. (2017) ‘Industrial big data in an industry 4.0 environment: Challenges, schemes, and applications for predictive maintenance.’ *IEEE Access,* vol. 5, pp. 23484-23491.

Wang, X. V., and Wang, L. (2019) ‘Digital twin-based WEEE recycling, recovery and remanufacturing in the background of Industry 4.0.’ *International Journal of Production Research*, vol. 57, no. 12, pp. 3892-3902.

Information Management and IT Innovation in the Measuring Subsystems of Industry 4.0

Svyatoslav Yatsyshyn, Bohdan Stadnyk [1], Yaroslav Yanyshyn [2]

Abstract. The improving of quality and efficiency of technological processes has been provided the exceptional importance to the flow and amount measurements of different substances. The high claims for accuracy in online mode with ability to control flows of indefinite phase and structural state make the Coriolis flowmeters an indispensable multi-parametric measuring means. It is not possible without the involvement of the Information management that is a cycle of processes that support identifying information needs of the developers and consumers, acquiring information, organizing and storing information, developing information services, disseminating and using information on the metrological properties.

Keywords: information management, measuring subsystem, production branch, Coriolis flow meter, uncertainty

JEL Classification: C8, C93, D24

1 Importance of the measuring subsystems for Industry 4.0

In complex decisions, not only in information exchange, for example, managing information systems for the promotion of goods, but also in production with its complex and often indiscriminate equipment (we mean unique equipment – nano measuring machines - or especially responsible information-measuring equipment - Coriolis flow meters (Bronkhorst Products Prospect, 2019) many consumers' efforts are required to improve the quality of the production cycle by organizing information system management.

Therefore, Metrology 4.0 considers such equipment, not only to make sure that the flow meter is working and that its use is efficient enough, and that the information system implemented on its basis is, firstly, fast and efficient, secondly, highly precise, not only at a single multi-parameter

[1] Lviv Polytechnic National University, Department of Information-Measuring Technologies, Lviv, Ukraine, e-mail: slav.yat@gmail.com.

[2] Lviv National Agrarian University, Faculty of Economics, Dublyany, Lviv region, Ukraine, rectorat@lnau.edu.ua.

point, but also at a sufficient number of points, and thirdly, the replication of this stage (data measuring and processing) of the production is quick and easy. This means that scaling in the form of the proliferation of these state-of-the-art multi-parameter measuring instruments can be implemented much easier than before. The implementation of this type of management allows the Coriolis flow meters used in the oil and gas industry to correctly enter the input accounting by the amount (mass, volume) of the extraction resources, dividing them into the fractions, and at the same time, by types - solid (rock, clay, sand), liquid (water, oil, etc.) and gas.

In the metrological sense, the Coriolis flowmeter consists of appropriate sensors and peripherals, as well as microprocessor unit for processing the received signals. Sensors determine flow (flow rate), density, and temperature, and output information to the computing unit that acts as the brain of the measuring mean and whole the system, providing access to the display, the main menu and information output devices to interact with other subsystems. Peripherals provide monitoring, alarms and additional features such as batch control and more accurate fluid density at the gas stations.

Nowadays we are assisting in the 4 industrial revolution. According to the analysis the emerging job sectors of this revolution are Energy, Financial Services, Health, ICT, Media & Entertainment, and Logistic. All these changes are possible due to the recent developments in metrology. As a matter of fact, monitoring remote physical phenomena and trying to control them is possible thanks to the developments of new sensors, acquisition techniques, improvements of data acquisition systems, and so on Program IEEE Workshop for Industry 4.0 (2020).

1.1 Coriolis flowmeters in Industry

The number of technological processes that require the control of the quantity of a substance leads to improving the accuracy of flow meters (hereinafter referred to as FM). The temperature, density, and purity of the controlled substance make a significant contribution to cost of measurement processes. Particularly challenging is determining mixtures composition, for example, the air-liquid suspensions in the oil and gas, chemical industry, and filling bottles with beer as liquid-air mixture.

In order to optimize the choice of methods for measuring flows, one should thoroughly evaluate the advantages of different classes of FMs by linking them to issues. It should be noted that due to the development of modern technologies, there have been recently developed FMs that operate in real-time and are able to provide measured data on an instant basis, which significantly simplifies the operation of technological installations.

A variety of measurement environments characterized by different physical and chemical properties, as well as the various requirements offered by the industry to metrological characteristics and reliability of FMs, have led to the creation of means based on different methods. The benefits of Coriolis BM are obvious, so they are used in a number of industries. Here the Coriolis force acts on the movement of fluid from the inlet to the outlet of the VM, and accordingly, on the walls of the tube on which it flows. As the fluid flows in the two branches of the Coriolis tube are opposite in direction, so also the forces arising there are also directed similarly. Consequently, under the action of the resultant force, the same parts of 2 branches shift relative to one another, approaching or moving away. The offsets are fixed by the inductive or capacitive encoders positioned on the bends (at the entrance to the branch and at the exit).

At the absence of flow in the tube, its vibration at the inlet and outlet coincide, i.e. there is no phase shift between them. When the fluid flow in the tube appears, the tube branches bend in proportion to the mass flow rate. Therefore, between the vibrations of the input and output branches a phase shift arises. The microcontroller processes this information and uses it to determine the mass flow rate. The temperature of the measuring tubes is recorded in several places. It is necessary to eliminate the methodic error of the flow measurement due to the viscosity and the temperature dependences.

The ability to measure several process parameters simultaneously opens up completely new applications. Mass flow rate, density, and temperature can be used to obtain other values, such as volume flow, solids content, concentration, and complex density function. Outgoings of the most complex liquid environments (pure substances and solutions, various fuels, natural oils, animal fats, alcohol, latex, juices, gases, and many others, including suspensions of indefinite structure and pressure) can also be measured.

2 Metrology 4.0 and Information Management

Improvements in the FM accuracy are becoming increasingly important in the light of improved software for measuring instruments. In the case of the design of the Coriolis FMs equipped with a computing unit to process information from sensor signals, these problems become especially relevant in accordance with our opinion (Yatsyshyn et al. 2015). Their transformation function is the dependence of the mass or volume of a liquid on its flow rate through a given cross-section; it depends on the hydrodynamic regime of the flow of fuel and lubricants through the FM, their viscosity, etc.

It is determined by comparing the time (phase shift) characteristics of 2 identical sensors at the input and output of the FM; the faster fluid flow corresponds to the larger time-phase discrepancy between these characteristics. The measurement error is determined mainly by the error of the phase shift of the characteristics and is, for example, ± 0.5 % in general for the FM application of EMERSON series. This is a viscous component of instrumental error.

2.1 Achievements of metrology and their analysis

An important factor in the inaccuracy and uncertainty of FM transformation function seems to be the temperature regime of the flow of fluid, which is significantly dependent on the temperature of the liquid or reservoir where it is stored, the temperature of the measuring instrument, the hydrodynamic regime of fluid flow through the FM. For example, gasoline is considered to be one of the fractions of oil with a certain variation in chemical composition, and hence the viscosity. The lighter fractions are collected nearby its surface, where they are captured when pumped. In addition, the process of transfusion of fluid from one tank to another is a transient process in hydrodynamic and thermal engineering senses.

In our opinion, the main problems of improving the accuracy of FM on the Coriolis effect are following:

- Hydrodynamic, thermal, electrical and other processes in the FM that cause poor reproducibility of transformation function have not been fully studied. They form the viscosity and temperature components of the instrumental error of the FM;

- Four most exact resistance thermometers produced made from the platinum wire and built-in FM to minimize its instrumental error, are inherent in a significant constant of thermal inertia of ~ 60 seconds. For comparison, a film platinum resistance thermometer has much lower inertia (~ 0.5 sec.), but a much worse reproducibility of transformation function. In addition, resistance thermometers require independent power supply while measuring. As a consequence, questions arise about the feasibility of using such FMs, for example, when refueling cars.
- In the case of a single measurement, and such can be considered the process of filling the tank of a car with the fuel, the classical approach of errors is not adequate and the concept of measurement result assessment can and should be based on an uncertainty approach (Warsza, 2014).

2.2 Industry Problems of the accuracy of temperature measurement in FM

Due to the manufacturing features, the transformation function of FM of one batch is characterized by a certain spread. In turn, the FM manufacturer takes into account that when installing 2 frequency sensors in the path of determining the amount of fuel and 4 temperature sensors in the path of introducing the temperature correction, it is not possible to achieve maximum identity of the mentioned function. This leads to the necessity of individual calibration of each FM, trying to minimize instrumental error to ± 0.1% (for the most accurate types of FM).

The calibration is most likely performed at one point of the calibration characteristic at the moment of fixing the impact factors, the number of which is quite significant (different temperatures of storage and transportation, different viscosity, etc.). This procedure meets the single-parameter measuring means. Nevertheless, input accounting for raw materials in oil and gas production is realized with the help of multi-parameter FM. Therefore, the latter with an instrumental error that, when calibrated, has a manufacturer-guaranteed spread (coverage interval) (Fig. 1) significantly expands its own coverage interval during operation. In addition, in practice dynamic error arises, due to the significant inertia of the resistance thermometers as well as methodical error increases due to the self-heating of the sensor by electricity while measuring.

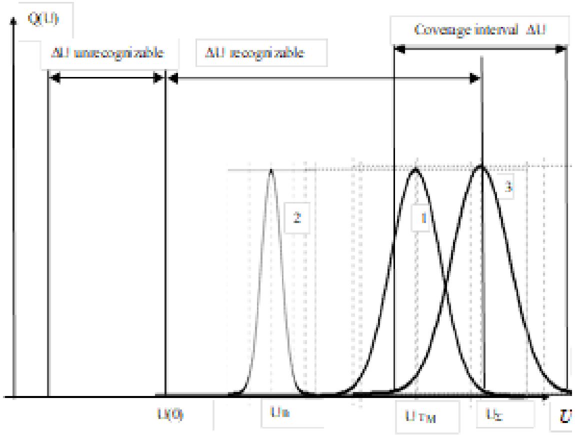


Figure 5 Instrumental error U_{Σ} of flow meter (3), as the sum of its 2 components: viscosity (1) and temperature (2) - with an uncertainty of each of them, expressed by the coverage interval

For positively correlated components, the limit value of error is defined as (A + B) at its coverage interval, obtained by summing the relevant intervals of A-component and B-component. For the negative correlation of these error components (K_{cor}= -1) we can obtain (A – B). And for at their mutual independence or lack of correlation, the RMS value of A and B is derived. When such studies relate not to the 2 components of the error but to a significant amount, the additional studies are required to find the correlation factors of the impact values.

5.1 Problems of metrological data acquisition and management

For the Coriolis FMs as multi-parametric measuring means it is needed the extensive research aimed at determining the field of permissible errors/uncertainty while measuring the specified range of measured values. This is not possible for such a complex device as the Coriolis flowmeter without the involvement of the information management. The latter is a cycle of processes that support identifying information needs of the developers and consumers, acquiring information, organizing and storing information, developing information services, disseminating and using information. Aslett

(2018) makes a strong case for data catalog adoption and underlines the growing importance of data catalogs for enabling modern analytics. “Data catalogs have become key components of data governance, master data management, self-service analytics, and self-service data preparation offerings,” he notes. “They also help support the identification and discovery of data to fuel machine learning and other data science projects.”

Conclusion

Due to the great cost of the complex research, it seems timely creating the data catalog – Knight (2017) – especially for the multi-parameters measuring means to give the breakthrough in their data management (Metrology 4.0). Moreover, the data catalogs emerge as key enablers for nowadays data management and prerequisite for function the Big Data in Industry 4.0.

Acknowledgments

The authors express their gratitude to the staff of the Department of Information and Measurement Technologies of the Lviv Polytechnic National University, Ukraine, for the assistance provided and full assistance in the preparation of this article.

References

Bronkhorst Products. (2001) *Mini Cori-Flow^{TM} Coriolis Mass Flow Meters & Controllers,* [Online], Available: https://www.bronkhorst.com/int/products/liquid-flow/mini-cori-flow/?gclid= [19 Aug. 2019].

IEEE (2020) *Program of the IEEE Int. Workshop for Industry 4.0 and IoT* [Online], Available: http://www.metroind40iot.org/home [23 Aug. 2019].

Yatsyshyn, S. Stadnyk, B. Lutsyk and Bunyak L. (2015) ‘Handbook of Thermometry and Nanothermometry’, Barcelona: IFSA Publishing.

Warsza Z., Korczynski Je. (2014) ‘Improving the Type A uncertainty evaluation by refining the measurement data from a priori unknown systematic influences’, *Advances in intelligent systems and computing, no.267. Recent Advances in Automation, Robotics and Measuring Techniques,* Switzerland, Springer International Publishing, pp.721-733.

Aslett M. (2018) *The Analyst Report. Learn about the biggest breakthrough in data management in the last decade: data catalogs*, [Online], Available: https://www.alation.com/data-management-with-data- catalogs/ [19 Aug. 2019].

Knight M. (2017) *What is a Data Catalog*, [Online], Available: https://www.dataversity.net/what-is-a-data-catalog [11 Aug. 2019].

IT IN PUBLIC ADMINISTRATION

Innovations in Public Administration: The Determinants of Development, Ways of Generating and Approach to Public Management Models

Katarzyna Baran[1]

Abstract. In scientific discourse, innovation in the public sector is becoming an increasingly attractive, necessary and desirable topic. Although innovation should not be seen as a way to solve all socio-economic problems the public sector is facing, it certainly helps to improve the performance of public organisations and to use resources more efficiently. The aim of this article is to identify the determinants of the growing popularity of innovation in public administration and the typical for this sector ways of generating innovation. The starting point is the mere introduction of the concept of public sector innovation and the types of innovation used. This part also presents popular research results focused on the issues of public administration innovation. The factors of innovation development in the public sector and the ways of generating innovation, i.e. diffusion, organisational learning and isomorphism, are described in turn. The approach to innovation in public management models is also described.

Keywords: public sector, public administration, innovation, innovation in public organization

JEL Classification: H83

1 Introduction

The dynamization of transformation processes, influenced mainly by constant changes in the political and economic environment, makes the public sector function in specific conditions. Such a complex situation also causes the public administration to face a double challenge. On the one hand, it must ensure stability of the institutional environment, on the other hand, it must respond to development challenges, including determining the trajectories of social and economic development

Public institutions are also a key category in the process of creating innovations. The aim of this paper is to identify the determinants

[1] Cracow University of Economics, College of Public Administration and Economy, kat.baran94@gmail.com.

of the growing popularity of innovation in public administration and the typical for this sector ways of generating innovation. First of all, it was decided to discuss definition of innovation in public sector and the types of innovation, including popular research results focused on the issues of public administration innovation. The following part of the article contains the factors of innovation development in the public sector and the ways of generating innovation. In particular, diffusion, organisational learning and isomorphism, are described in turn. The approach to innovation in public management models is briefly described.

2 Development of innovation in public sector

2.1 Definition and types of innovation in public administration

The starting point for further considerations on the essence (significance) of innovativeness in public administration are the definition criteria of this concept. In the area of the public sector, innovations should be considered as the implementation of a new or significantly improved change, the effect of which is the increase in the effectiveness and efficiency of a public institution. When analysing the constituent elements of this definition, the introduced change must represent a new approach in relation to the previous context. Secondly, the innovation itself must be put into practice, i.e. it must not remain an idea. The latter refers to the results of the change, which should lead to better performance of public sector entities, including their increased efficiency and effectiveness, and increasing satisfaction of end-users of public services OECD (2015).

The next issue concerns the types of innovation used. In relation to the nature of the public sector, we distinguish the following innovations:

- process (improvement of quality and effectiveness of external and internal processes taking place in the organisation);
  - administrative (creation of new organisational forms, introduction of new management methods and techniques as well as new working methods);
  - technological (creation or use of technology in the process of providing public services);
- product or service (creation of new products or public services),

- organizational/ governance (creating new forms and processes for solving social problems);
- conceptual (introduction of new concepts, reference frameworks, paradigms for changing the nature of the problem and its possible solutions) Vries, Bekkers and Tummers (2014).

2.2 Determinants of development innovation in public organization

Focusing on the main stimulators of innovation development in public administration, one can distinguish:

- increasing competitive pressure;
  - internal (competition of public institutions to become a champion of innovation and to attract a wider group of service users);
  - external (loss of a monopoly position of the public sector in the process of providing services to the private and civil sectors);
- growing social expectations (the provision of public services should be cheaper, more efficient, of better quality, more personalised and environmentally friendly);
- constant increase in the effectiveness of public services (the issue of maintaining fiscal consolidation while increasing the amount of public services provided);
- the growing multitude and complexity of social and economic issues (going beyond the autarky vision of public administration, building multilateral alliances);
- the increasing globalisation (strengthening the capacity of the public sector to control, adapt and anticipate the opportunities and constraints of globalisation processes);
- digitalization (technology development favours the optimization of public institutions and has a quantitative and qualitative impact on the process of providing public services);
- the need to strengthen the social legitimacy of public institutions (innovation as a panacea for stagnation of public value resulting from, inter alia, weakness of the ruling party's accountability mechanism, overgrown bureaucracy and low effectiveness of public services).

The first condition results from the very nature of public administration. The organisational culture of public institutions, within which internal and external factors driving innovation can be identified, is of particular importance here. The former are related to the ambitions of the employees, their willingness to learn new skills and to see their own added value. On the other hand, external drivers of innovation are very typical and concern the distribution of resources such as rewards, salary structure, career advancement, power, etc. As far as the importance of these aspects is concerned, more and more emphasis has been placed recently on informal incentives relating to hierarchical relations, teamwork, initiating experiments or tolerance of failures. Here, a special role is played by political leaders and managers, whose task is to set the pace and direction of the innovation process, stimulate employee involvement and reduce their aversion to risk OECD (2015).

On the other hand, privatisation processes and market liberalization mean that an increase in the competitiveness of the public sector results, among other things, in the personalization of public services and their quantitative growth. In the era of growing needs and expectations of diverse social groups, public organisations are somehow forced to break the deadlock and compete with other sectors of public life. Consequently, the recipients of public policies are beginning to be treated as consumers who consciously choose an offer that meets their increasingly sophisticated expectations Windrum and Koch (2008).

Another group of determinants includes macro-economic factors that can both favour the process of innovation and have a dissimulative effect on it. This phenomenon is particularly relevant for globalisation and digitisation Sörensen and Torfing (2012). Climate change (displacement of dirty technologies), social stratification, poverty, crisis of work automation, urbanisation (urban sprawl) and looped problems should also be mentioned here Osborne and Brown (2005).

The last variable, apart from measurable benefits of using innovations in the public sector (greater transparency and economization of public institutions), also points to dual function of public administration. On the one hand, public institutions in the era of social and economic changes must maintain their stability and identity - values that are the basis for the functioning of public administration. On the other hand, due to the multiplicity and nature of these changes, they must be able to respond to emerging challenges Boin and Christensen (2008).

2.3 Popular results focused on public administration innovation

Public sector innovation has been explored by the European Commission (EC) for many years. One of the Commission's documents assessing the level of public sector innovation in the European Union (EU) is the European Public Sector Innovation Scoreboard (EPSIS). The results of the report unequivocally indicate a different level of public sector innovativeness in particular EU countries. Among the avant-garde countries with the highest level of innovation in public institutions are Denmark, Luxembourg, Malta, the Netherlands, Portugal, Sweden and Switzerland. On the other hand, countries with a low potential for public administration innovation are Bulgaria, the Czech Republic, Germany, Greece, Hungary, Italy, Lithuania, Poland and Slovakia EPSIS (2013). The research also shows that the implementation of innovation in European countries mainly concerned advanced information and communication technologies (ICT), which, according to the respondents, significantly influenced the effectiveness of public policies, inter alia, by increasing the quantity and quality of public services EPSIS (2013).

Another important conclusion, however, is that in the European Union there has been a division into countries which, while accepting some risk of failure and error, decide to introduce disruptive innovations (involving a complete change of mechanism or system) and countries which are beneficiaries of good practices Bekkers, Tummers and Vooberg (2013).

3 The ways of generating innovation in public sector

In the analysis of the relations between innovation and public administration, the way in which they are generated is also an important issue. Among the basic mechanisms of generating innovations in the public sector, one can distinguish:

- diffusion;
- organizational learning;
- isomorphism.

The diffusion process is about creating innovation systems, understood as specific structures of interaction between citizens, business sector, academy and research and development environment. Such networks to achieve a high efficiency, require a high degree of openness on the part of traditional organisational structures of public administration, efficient communication, strict definition of the scope of duties and responsibilities, as well as mutual trust between stakeholders. In the case of diffusion, the activity of civil society, necessary to meet the full condition of co-designing public services, is also important. Another necessary element of this process is the already mentioned trial and error process, which is the basis for the creation of new ideas and solutions. Bouckaert and Pollitt (2011).

Within the public sector, innovation creation is often also identified with organisational learning, which is somewhat more complex. It requires the ability and willingness of stakeholders to cooperate, join and share ideas. It is also important to exchange resources, such as knowledge, information and experience, which can hinder innovation or provide a basis for generating new ideas and concepts. It is worth noting that public institutions which do not demonstrate organizational learning abilities will significantly limit their adaptation potential, which means that they will not be able to properly perform the public tasks assigned to them. In some cases, it may even lead to the fact that the activity of public sector institutions will be simply dysfunctional Olejniczak (2012). The mature learning organisation also opposes the phenomenon of vertical silos of the public sector, which, due to weak information flow, may significantly weaken the innovative potential of public administration units.

A third of the ways in which innovation is generated in the public sector stems from environmental pressures leading to the convergence of public organisations, i.e. the adoption of compatibility features by imitating mutually applied solutions Vries, Bekkers and Tummers (2014). The convergence of public institutions can take place within a specific public service sector (e.g. education, health care) or can be the result of general changes such as new systems and working methods or new ideas and technologies. However, in some cases it can take the form of a myth or a ceremony. The literature on the subject distinguishes three sources of isomorphic change: political pressure, e.g. introduction of new legal regulations (forced isomorphism), standard reaction to uncertainty and risk reduction by copying good practices (mimetic isomorphism) and the desire to increase the professionalism of the office within the framework of existing norms and values (normative isomorphism) DiMaggio, Powell (2009); Bekkers et al (2013). The logic of copying is often linked to the strategy of an organization's leader. It is his task to observe the successes of other organizations in the process of adapting to the surrounding reality and to identify current trends.

3.1 An approach to innovation in models of public management

The approach of public administration to innovation can also be considered from the perspective of the applied models of public management Podgórniak-Krzykacz (2014). The basic division distinguishes between bureaucratic, market and participatory models.

The bureaucratic model is directly related to the legal culture of public administration. Its dominance confirms the view that public institutions have little or limited capacity to implement innovation. In this sense, legal culture should rather be treated as a barrier to the absorption of innovation. A strong orientation towards bureaucratic fashion causes the superiors to passively observe the transformational changes taking place. The main activities of public sector institutions focus on standardization and formalization of practices Olejniczak (2012). Initiatives to implement innovation are usually stifled. Resistance is particularly encountered by transformational innovations, which are accused of weakening the autonomy of the state apparatus. Only incremental innovations, involving a slight improvement of organisational aspects of the functioning of public sector institutions Bekkers, Tummers, and Vooberg (2013) are applied.

The pressure to change the way public services are provided by increasing their efficiency and effectiveness results directly from the concept of public management (New Public Management). In this model, the quality of public services is ensured by advanced management techniques, the primacy of market mechanisms and contracting Olejniczak (2012). A special type of innovation, called managerial innovation, was distinguished in the market concept Chowdhury and Shil (2016). It manifests itself in decentralisation of tasks and responsibilities, establishment of task forces, reduction of hierarchies, development of e-government and evaluation of public policies. The innovations listed above are aimed primarily at increasing the effectiveness of public institutions, as well as at better matching the offer of public services to the growing social expectations Podgórniak-Krzykacz (2014).

Slightly convergent application objectives, but different instruments and mechanisms characterise the model of public co-determination. The key elements of this model are increased social participation, negotiation and networking. Innovative solutions here primarily involve creating a platform for exchanging and sharing resources, such as time, people, money, information, knowledge, competences, political support, which are considered to be the main drivers of innovation. This cooperation within the network not only facilitates the release of innovations, but also enables the free dissemination of applied practices and the creation of space for their further diffusion. This toolkit can be used both to improve cooperation conditions and better coordination of collective actions, as well as provide a basis for increased transparency of public administration activities Bekkers, Tummers and Vooberg (2013).

Both the market approach and the stakeholder cooperation model create the atmosphere for the development of innovation. This applies not only to institutional solutions, but also to the way of thinking about organisation and the possibility of their impact on the environment, including the creation of specific public values.

4 Conclusion

To sum up, the development of innovation in public administration is not so much a needed process as a necessary one. The problem is that public institutions often limit their activities to the creation and implementation of innovations due to a lack of confidence in the effectiveness of existing instruments and methods. This is why the main activities of national and international actors should focus on changing the mindset of policy makers and citizens. The public sector should resign from the passive attitude of the observer and permanently join the process of creating innovations, which in the face of constantly changing civilisation challenges and universal dynamisation of economic processes is an inseparable element of development and transformation for the public sector.

References

Bekkers. V., Tummers. L., Stuijfzand, B.G. and Voorberg, W. (2013), *Social Innovation in the Public Sector: An Integrative Framework*, *LIPSE Working Paper Series* No. 1, Rotterdam, pp. 6-8, 30.

Bekkers, V., Tummers, L. and Vooberg, W., *From Public Innovation to Social Innovation in the Public Sector*: *A Lecture Review of Relevant Drivers and Barrier, EGPA Conference 2013,* Public Administration, Technology and Innovation (PATI), Rotterdam, 2013. pp. 6-16.

Boin, A. and Christensen T. (2008) *The Development of Public Institutions. Reconsidering the Role of Leadership*, *Administration & Society Journal*, pp. 271-272.

Chowdhury, A., Shil, N. Ch. (2016), *Innovation in Public Sector Management Control Systems in the Context of New Public Management: A Case of an Australian Public Sector Organization*, *Journal of Entrepreneurship, Management Innovation* 12(4), pp. 100.

DiMaggio, P.J. and Powell, W. W. (2009) *The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields*, *American Sociological Review*, vol. 48, No. 2, pp. 150

European Commission (2013) *European Public Sector Innovation*, pp. 33, 53.

OECD (2015) The *Innovation Imperative in the Public Sector, Setting an Agenda for Action,* OECD Publishing, Paris, pp. 7-16

Olejniczak, K. (2012) *Organizacje uczące się. Model dla administracji publicznej*, *Wydawnictwo Naukowe Scholar*, Warszawa, pp. 29.

Osborne, S. and Brown, L. (2005) *Managing Change and Innovating in Public Services Organization*, *Routledge,* pp. 11-21.

Podgórniak-Krzykacz, A. (2014) *Innowacje w samorządzie terytorialnym*, *Uniwersytet Łódzki*, Łódź, pp. 5, 13-15.

Pollitt, Ch. and Bouckaert G. (2011) *Public Management Reform: A Comparative Analysis-New Public Management Governance, and the Neo-Weberian State*, *Oxford University Press*, New York, pp. 9-11).

Vries, H., Bekkers V. and Tummers L. (2014) Innovation in the Public Sector: *A Systematic Review and Future Research Agenda, EGPA Conference 2014*. Public Administration. Vol. 94, No. 1, Rotterdam, pp. 6,15.

Windrum, P., Koch, P. (2008) *Innovation in Public Sector Services. Entrepreneurship, Creativity, Management*, Edward Elgar, Bodmin.

Using Geoinformation in Public Administration on Regional Level

Ivana Čermáková[1]

Abstract. Using of spatial information in public administration in actual topic. The possibilities of using geoinformation are in each aspect of human life, e.g. urban planning, monitoring of greenness (passport) or crisis management. Public administration provided the data at the national level because of accessibility to everyone. But the data are not enough for using on the regional level of public administration. So, regions and big cities created their own source of spatial data. The thesis is focuses on source and using of spatial data on regional level. The possibilities of future development are listed also.

Keywords: geoinformation, public administration, spatial data, source of spatial information

JEL Classification: R19, Z19

1 Introduction

Geoinformation are its using is a very popular topic in a modern society. It means, that the society is focused on and wants to be informed about a landscape, their changes and the possibilities of the changes. Using the Geographic Information Systems (GIS) and geoinformation saving time and money. These are part of the reasons why the public administration started using the geoinformation. Public administration provides the data at the national level mainly. But the accessary and the focus of the data wasn´t enough for the needs of the regions. So, most of the regions or big cities created their own source of spatial data.

The thesis is focused on source and using of spatial data on the regional level. Problematic of geoinformation and their using in national level and regional level is included also. The thesis compared the possibilities the geoinformation through whole world. Because the trend of using geoinformation is global. Possibilities of using geoinformation in future are included also.

[1] VSB – Technical University of Ostrava, Department of Applied Informatics, Sokolská třída 33, Ostrava 1, 702 01, Czech Republic, ivana.cermakova@vsb.cz

2 Geoinformation

The term geoinformation can be conceptualize in a number of ways. One of the most used definition explain geoinformation like information used for geographic services, geoinformatics, spatial position and spatial monitoring (Shaytura, 2018). Geoinformation can be explain like information that support the discipline of photogrammetry and remote sensing also (Lazaridou and Patmios, 2012). So, geoinformation can be explain like information which have some spatial context and can be used for information systems work with the spatial data.

2.1 Geoinformation at national level

Geoinformation at a national level provides many states, but for the thesis are chosen two states, whose are leaders in e-government and using the geoinformation. The leaders are Estonia and Austria. In the thesis is contained the Czech Republic because of using the geoinformation by the author.

Estonia used for providing geoinformation geoportal. The geoportal is provided like map server or flash map server. Both are in Estonia and English language. The map server contains information about cadastral dividing of the state. The basic task, fertility zones, maps with various ratio scale, flood zones and similar information are provided also. The flash server provides the dynamic information about geographical longitude and latitude. Map server provide next possibilities for the citizens: map server, maps, data, spatial data infrastructure and buying datasets. (Tallin, 2016)

Austria provide free portal of geoinformation, which is divide to 12 sections. The sections are next : 9 sections are for the each part of the state, base map, topographic map and INSPIRE data. The project INSPIRE is project of European Union (EU) focused on geoinformation. The portal is in Deutsch and English Language. (Austria, 2016)

The Czech Republic provide the INSPIRE data also. The other maps are provided online or by Web Map Services (WMS). It means : ortophoto maps, cadastrale maps, army maps, topographic and aerial maps. Using of metadata is possible also. The website is in Czech and English language. (Cenia, 2015)

2.2 Geoinformation at regional level

It is visible that the data which are provided on the national level are not enough detailed and focused on concrete topics. So, the regions and big cities created their own source of geoinformation. The portals or geoportals are typical for the national level. But regions and cities provided the data in a number of ways. The source of geoinformation aren´t paid by state. So, the institution (region or the city) decides how many money comes to this project. But they decides about the scope of this project. So the city or region give the money only on the information which can provides, e.g. passports or brownfields.

The first sample is Boston city in USA. The city provide the geoportal divided to two parts. First part is focused on data providing and contains maps through open data, actual traffic map, car sharing map and bike sharing map. All the maps are immediately actualized. The second part of the geoportal is focused on citizens and their abilities of map creating. So, the citizens can create their own maps and routes. The map creating course is contained also. (Boston, 2016)

Hamburg, city in Germany, provide geoportal also. But the geoportal is available only in Deutsch language. The possibility of buying the data is covered. The geoportal contains maps through time horizon, which users can chose. Cadastral maps, aerial maps and planning map can be chosen. (Hamburg, 2016)

Thessaloniki, citi in Greece, provide the geoportal in Greek and English language divided to two parts. First part is GIS. The users can use the GIS for searching or simple analysis creating, e.g. available bike for sharing or nearest possible way. The second part is focused on spatial infrastructure. Have a visible tram station or parking zones is available. This part of geoportal is created like the base information for citizens for each day. (Thessaloniki, 2016)

Prague, the capital city of the Czech republic, provides geodata through more webpages. The first is geoportal. The geoportal has a concept of most using services on the first page. So, the users can download the documents or maps, import geodetic documentation, provide geodata, e-import, e-export and open data. The maps on the first page are available only in Java. Then, the geoportal is divided to seven parts : maps, data, services, documentation, research, about geoportal and links. The section maps, data a services is interesting from geoinformation view. The section maps contain base online map. But the users can check next layers to visible view: archive map, traffic map topografphic map and maps focused on important areas. Section data is divided to data, metadata and searching in open data. Section services provide browsing, quering and searching services. The quering and serching services aren´t available now. (Prague Institute of Planning and Development, 2013)

Map of passports (green vegetation) is another Prague´s web page providing geoinformation. All city districts are contained. The web page allows see the passports in the area and users can chose another spatial information visible in map, e.g. bicycle kickstand, areas where people can buy bioproducts, no-smoking areas or baby-friendly areas. 1 792 places in Prague are listed now (Automat, 2010). Another big cities in Czech republic have map of passports also, e.g. Hradec Králové. The map allows see the base map or orthophoto map through 2011 and 2019. The users can create their own notes to the map, distance measuring or export the map. Information about each greeness is visible after zoom in the object. The map is very detailed and for example each tree has identification number and basic notes (T-Mapy, 2017).

Prague is focused on crisis management also. The geoinformation are distributed by portals of each city district, e.g. District no. 8 provide the floods map and intagrated saving system map (map show where are the nearest offices of the saving system) (MČ Praha 8, 2012). Hradec Králové has portal of crisis management (T-Mapy, 2017). The map includes information about position of sirens, offices of integrated saving system and other necessary known object in the case of dangers. Středočeský district, district close to Prague city, has crisis portal which inform about actual situation and potentional hazards through the map (Středočeský kraj, 2015). Some cities are focused on floods information distributed through geoportals. One of them is Hradec Králové, city in the Czech Republic. The flood zones are visible in the map. The map can be used like base for decisions about assurance of buildings (T-MapServer, 2017).

The public administration is focused on monitoring and changing the landscape also. Using of brownfields is increasing now. So, the regions and big cities create their own geoportal contains mainly maps regarding brownfields. Moravskoslezký region has geoportal where citizens can see the map of brownfields. The regenerated objects are visible also. The citizens can join to effort reconstruct the brownfields or make a proposals how the objects can be reconstructed and which function the objects should have after (Moravskoslezký kraj, 2019). Jihomoravský region has concept of brownfield like map of brownfields, where citizens can download the documentation about each project (RRAJM, 2019). The Brno city, capital city of the Jihomoravský region, the problematic of brownfields presents through portal contains base map. The base map can be change to the aerial map. The information from cadastre and other information are visible after click on the brownfield (Statutární město Brno, 2019).

3 Possibilities comparison of using geoinformation in regional level

The using geoinformation can be divide to the two parts. First part focused on information about some actual topic. It´s portals or websites where the users have visible the data, but they can´t do anything else. The users are only actualized immediately. The second part is more focused on needs of citizens. So, the people see the actual situation and can set the information which they need. It means connected layers with various datasets, creating ways from point A to point B or find the nearest bike track with share bicycles.

It´s visible, the second part is more important for the citizens and public administration. The possibilities of using the geoinformation of one area of interest and connected with next data are giant. Public administration is to knowing the phenomena and try to reacting. But still are many cities and regions which this trend saving money and time through the geoinformation and share the information to the citizens ignored.

4 Future of geoinformation in public administration in regional level

Increasing using of geoinformation not only in public administration is clear. Some of the big cities react on the trend and they try to create platform where will be available spatial information of the area for each area of interest.

Prague is typical representative. The city provided the geodata regarding basic information, actual information and information from area of interest, e.g. passports or crisis management. But still they don´t have together on one platform. It´s clear, the future of the geoinformation in public administration is in connection the information and their using. The effort is visible, but the most of the cities and region are on the start and some just unbegun.

5 Discussion

Questions about financing the geoportals and other platform is the key problem. The national geoportals are funded from national budget. But the regional and city portals are funded by regions and cities. It´s one of reasons why some cities and regions don´t have still the geoportal. Because they don´t have a money for creating the platform and servicing. Mainly, this problematic is hard to solve in the case of small cities which want to provide the geoinformation, but the budget is small and they can´t funded the portals.

6 Conclusion

Using geoinformation in public administration is actual topic. The public administration provides the geodata on national level mainly. But the accessary for need regions and big cities isn´t enough. So the regions and big cities created their own platform where provide the geoinformation which needs and wants.

Article contains evaluation of the situation on the national and regional level. The possibilities on next development in the case of platform in regional level are contained also. Connection and using the geodata for needs not only the public administration but for the citizens also is the future development. The key problem is funding of the platforms, because the development and service of the platform is not cheap and most of small cities doesn´t have enough money in the budget for financing this project.

References

Austria (2016) *Geoland.at: the free geodata portal of austria*, [Online], Available: http://geoland.at/ [23 May 2016].

Automat (2010) *Zelená mapa Prahy.* [Online], Available: http://zelenamapa.cz/ [7 Jul 2019].

Boston (2016) *Boston Maps: City of Boston – Mapping and Analysis Platform,* [Online], Available: http:boston.maps.arcgis.com/home/ [23 May 2016].

Cenia (2015) *Geoporal,* [Online], *Available: http://geoportal.gov.cz/* [24 May 2016].

Hamburg (2016) *Hamburg Service- Geoportal,* [Online], Available: http://www.geoportal-hamburg.de/ [24 May 2016].

Lazaridou, M. A. and Patmios, E. N. (2012) 'Photogrammetry-remote sensing and geoinformation', *22nd Congress of the International Society for Photogrammetry and Remote Sensing, ISPRS 2012*, Australia, pp. 69-71.

MČ Praha 8 (2012) *Městská část Praha 8,* [Online], *Available: https://m.praha8.cz/Mapy-krizoveho-rizeni.html* [9 Jul 2016].

Moravskoslezský kraj (2019) *Brownfieldy v Moravskoslezském kraji,* [Online], *Available: https://brf-msk.cz/* [1 Jul 2019].

Prague Institute of Planning and Development (2013) *Geoportal Praha,* [Online], Available: http://www.geoportalpraha.cz/ [30 May 2016].

RRAJM (2019) *Brownfieldy,* [Online], *Available: https://www.brownfieldy-jmk.cz/* [1 Jul 2019].

Shaytura, S. V. et al. (2018) 'Geoinformation services in spatial economy'. *International Journal of Civil Engineering and Technology.* Vol. 9, no. 2, pp. 829-841.

Statutární město Brno (2019) *Mapový portal Brno,* [Online], Available: http://gis.brno.cz/portal// [9 Jul 2019].

Středočeský kraj (2015) *Středočeský kraj: Portál krizového řízení,* [Online], Available: https://pkr.kr-stredocesky.cz/pkr/mapa-stranek/ [9 Jul 2019].

Tallin (2016) *Estonian Land Board: Geoportal,* [Online], Available: http://geoportaal.maaamet.ee/eng [23 May 2016].

Thessaloniki (2016) *Municipality of Thessaloniki: Urban Planning Department,* [Online], Available: http://gis.thessaloniki.gr/fp/index_en.html/ [24 May 2016].

T-MapServer (2017) *Mapa záplavových území,* [Online], Available: http://mapserver.mmhk.cz/tms/hkpovoden/ [9 Jul 2019].

T-Mapy (2017) *Mapa passportu zeleně,* [Online], Available: http://geoportal.mmhk.cz/mapa/ [9 Jul 2019].

INFORMATION SECURITY

Secure Data Transmission in Wireless Sensor Networks of the Internet of Things

Olexander Beley[1]

Abstract. Security studies of the Internet of things are increasingly attracting the attention of academia. This study addresses three key security requirements with an emphasis on the IoT system: authentication, privacy, and access control. It addresses security issues that have not yet been resolved, and discusses problems and future trends in the field of the Internet of things. Given the features of the devices, as well as their various nature, security issues of network interaction require consideration of new aspects. Most of the security threats identified were related to unencrypted data, personal data collection, vulnerable user interfaces and insecure connections. The main security problems are related to the fact that the existing methods and means of protection were originally developed for desktop computers and did not take into account the features and limitations of the Internet of things. Today, along with the adaptation of existing security technologies, standardization issues in the field of the Internet of things are important.

Keywords: Internet of things, network connectivity, security system, standardization, authentication, access control

JEL Classification: C66, C92

1 Introduction

The IoT concept includes many different technologies, services, standards and is perceived as the cornerstone in the market of information and communication technologies (ICT) for at least the next ten years. From a logical point of view, the IoT system can be represented as a set of jointly interacting smart devices. From a technical point of view, IoT can use various ways of data processing, communication, technology and methodology, based on their purpose. For example, an IoT system can use the capabilities of a wireless sensor network (WSN), which collects environmentally relevant environmental information (Belej, O.; Lohutova, T.; Banaś, M.;, 2019). A high level of heterogeneity, combined with a wide range of IoT systems, is expected to increase the number of threats to the security of device owners,

[1] Lviv Polytechnic National University, Department of Computer-Aided Design, Ukraine, Lviv, 5 Mytropolyt Andrei str., Building 4, Room 324, tiger_oles@i.ua, Oleksandr.I.Belei@lpnu.ua.

which are increasingly used for the interaction of people, cars and things in any variation. Traditional security and confidentiality measures cannot be applied to IoT technologies, in particular because of their limited computing power. In addition, the large number of target connected devices poses a scalability problem. At the same time, in order to achieve recognition by users, it is imperative to ensure security, confidentiality, and trust models that are appropriate for the IoT context (Belej, Olexander, 2019). To prevent unauthorized users from accessing the system, authentication and authorization mechanisms should be used, and security, confidentiality and integrity of personal data should be guaranteed. Relative to the personal data of users and information, protection and confidentiality should be ensured, primarily because devices have access to it and are able to manage it. Finally, trust is the main problem, because the IoT environment is characterized by various types of devices that must process data in accordance with the needs and rights of users (Belej, 2019).

Most recently, work has begun to address these issues. For example, the authentication protocol for IoT, presented in (Joux, 2000), uses a lightweight encryption method based on the XOR operation.

Access control refers to resource usage permissions for different IoT network entities. In (Kim , Chang , Suh , & Shon , 2016), two entities are defined: data owners and data collectors. Users and things, as data holders, should only allow the transfer of information that is necessary to perform a specific task. At the same time, data collectors must be able to identify or authenticate users of things as the legal owners of the data from which it is collected.

The publication (Ministr J., 2014) also focuses on data outsourcing. In particular, due to the large amount of streaming data, companies may not acquire the resources necessary to deploy data stream management systems (DSMS). It is proposed to delegate the storage and processing of the stream to a specialized third party with a strong DSMS infrastructure. The question of trust arises: a third party can act maliciously, for example, in order to increase their profits. The solution is to adopt a method for authenticating the stream so that clients can verify the integrity and relevance of the data received from the server. At the same time, the method should satisfy the requirements of IoT devices characterized by limited resources in terms of energy consumption, computing power, and memory.

Regarding the issues raised, several new solutions have recently been proposed. In (Nix , 2016), an authorization scheme for devices with limited resources is presented, which combines the technology of physically nonclonable functions (TPNF) with a built-in Subscriber Identity Module (SIM). The first provides low-cost, secure, anti-theft security keys for M2M (MACHINE-to-MACHINE) devices. The second provides mobile communications that guarantee scalability, interoperability, and compliance with security protocols.

2 The Structure of Wireless Sensor Network forthe Internet of Things

The structure of the Internet of things in the general case can be represented as a combination of the following elements: directly the “things”; network; data centers.

Thus, approaches to building a security system should consider each of the structural elements and still solve the problems that arise when combining several devices and creating a network. “Things” today are not only personal items of ordinary consumers, but also various equipment that is actively used in many areas of activity - trade, transport, medicine, construction, banking, sports, etc. It follows that the Internet of things is most often heterogeneous network, i.e. devices of various classes and types are combined and interact with each other.

Recommendations for protecting information on the Internet of things are aimed at improving the security of devices, networks and data (Saadeh , M.; Sleit, A.; Qatawneh , M.; Almobaideen W. A;, 2016).

First of all, IoT devices, as a rule, due to their portability and mobility, are physically accessible to attackers and can be stolen to gain access to sensitive data and establish communication with other network devices. To prevent this threat, it is necessary to provide physical protection, for example, by using protective covers on devices or cases that provide for restrictions on direct access to devices. In addition to direct access, devices can provide remote access to update configuration data or software. To protect against this, it is necessary to provide for the closure of software ports and the use of strong passwords at the level of downloading and updating firmware, which will prevent access to the device if it is compromised.

At the same time, on the other hand, many IoT devices are becoming vulnerable to cyberattacks because their software is not updated in a timely manner. To minimize such risks, it is recommended to implement an automatic update by default, because, even if software updates are released on time, consumers do not always install them manually immediately after the release.

Attention should also be paid to the organization of data storage on the devices themselves, because often this information is related to the user's personal data, financial transaction data and data on critical objects of various fields of activity.

Safety must be ensured both throughout the entire period of the product’s functioning and after its decommissioning. Cryptographic keys must not be stored in non-volatile memory of the device in open form. In addition, disposal of decommissioned devices may be envisaged.

To protect networks, first of all, methods of “strong authentication” should be provided, including, for example, two-factor authentication, assignment of “hard-coded” unique identification and authentication data, as well as the use of modern secure protocols (Tvrdikova, 2016). Cryptographic algorithms must be adapted to the Internet of things.

In order to minimize the risks of denial of service attacks against devices, it is recommended that the bandwidth of the network of devices of the Internet of things be limited, both at the software and hardware levels. In case of detection of suspicious traffic, devices should provide the ability to signal with the subsequent analysis of the identified threat.

Data protection is primarily ensured through the use of cryptographic methods adapted to the features of devices with disabilities. If the device is compromised, it should be possible to urgently erase key information used in cryptographic operations.

The listed features of the Internet of things impose restrictions when building a security system in such a network. The usual methods of protecting information in wireless networks may not be enough, or they may not be applicable due to the restrictions imposed by the Internet of things.

The main methods for ensuring security, as in traditional networks, remain encryption, identification/authentication, and the introduction of physical security measures.

The security system should be designed to provide protection for devices and gateways, the transmission network, as well as applications that are deployed to ensure the functioning of the devices.

Encryption is a widely used, effective and flexible enough solution to ensure the confidentiality of information and create a security system. However, any encryption, and especially strong one, requires an increase in productivity and additional computing resources, which is not always possible in the conditions of the Internet of things.

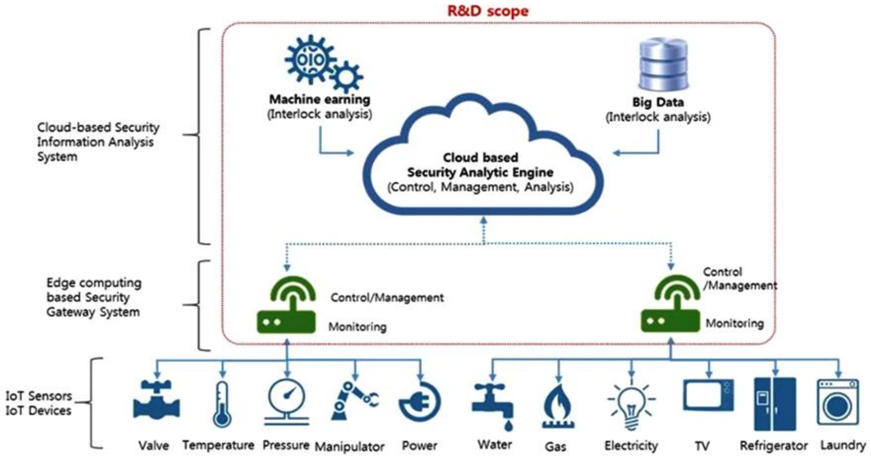


Figure 1 Scheme of step-by-step implementation of the DEU association stage, Source: owner.

As for authentication, the researchers proposed a fairly large number of approaches that could be implemented to solve security problems. One common method is two-factor authentication. For example, one-time password authentication (OTP). With this approach, after providing the credentials, the user or device must also present a one-time password generated by the key distribution center, thereby confirming its authenticity. This method does not require additional computing resources or storage from the devices, but it is not applicable for devices that, for example, simply cannot support the ability to enter the received one-time password. The same problem is relevant for the authentication method, the second factor of which is the hardware identifier.

The proposed methods also include authentication using cryptography based on elliptic curves. Despite the fact that in this case the necessary basic parameters of the elliptic curves are not calculated by the devices themselves, after the calculation, a sufficiently large amount of data must be transferred, which may be limited by the network bandwidth.

Thus, the various existing authentication methods are applicable to a single network and a separate class of devices. The application of uniform methods and means is complicated by the lack of standardization and heterogeneity of such networks.

3 Device Authentication Protocol in the IOT Wireless Network

The proposed protocol provides operation in scenarios with a potentially unstable connection from the managing center (MC) to the user system (US), as well as in the case of the possibility of making direct connections between the delegated device and the authentication of different users.

The problem is solved by combining the solutions considered in systems with public key infrastructure, which are responsible for the initial generation of keys and certificates, as well as solutions that allow direct connection in the absence of communication with the public key infrastructure.

The main options for cryptographic solutions for potential use in this protocol are proposed below. To obtain the result of the data hash function algorithms can be used classical public key cryptosystem protocols can be used. Protection against attacks of the “man-in-the-middle” type can be implemented using the classic Diffie-Hellman protocol or the Elliptic curve Diffie-Hellman (ECDH).

The authentication protocol for the delegation of rights to use electronic devices consists of certain operational steps (steps): (1) the initial association of the new device; (2) transfer of the device for a certain period of time; (3) returning the device to use by the owner; (4) device dissociation.

Also, during the operation of the protocol, the MC key is entered, which is associated with the Alice user. This key allows you to provide symmetric encryption of the data transmitted and stored on the DED, and also serves as an additional protection against leakage of confidential Alice user information stored on a separate DED. Further protocol steps are indicated by the corresponding numbers in fig. 2.

1. The Alice user generates the MC secret key for the new DED w_i and transmits it over the secure channel.
2. DED w_i transfers the result of the execution of the hash function from its own software to the MC using a secure channel *(hash (SW_i))*.
3. User Alice transfers his public key PK_A and ID_A to the US.
4. MC generates US certificate for Alice. The certificate has the form $cert_A = sign_{cloud}(w_i, ID_A, hash(SW_i))$. This step is carried out in order to ensure system data integrity.
5. The MC, using a secure channel, transfers the $cert_{cloud}$ to the Alice user.
5. The Alice user signs the certificate received from the MS with his $cert_A = sign_A(cert_{cloud})$.
7. The Alice user submits a certificate to the DED.

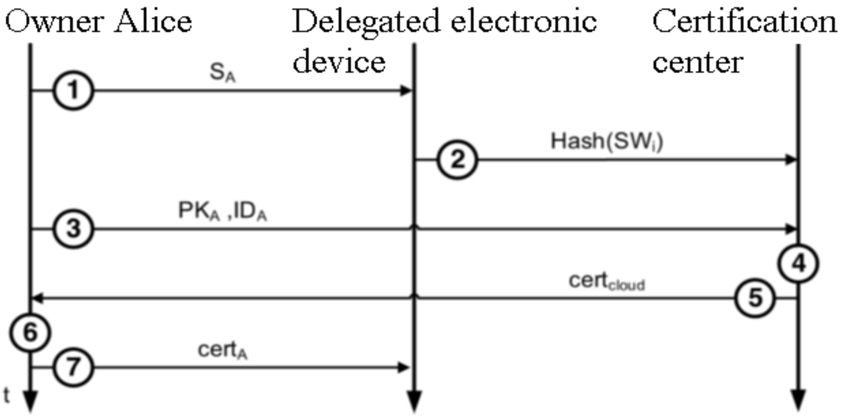


Figure 2 Scheme of step-by-step implementation of the DED association stage, Source: own.

Transferring the device for some time to use by another user. The functioning of the system can occur in two modes: in the presence of a connection to the MC and in the absence of a connection. In the first case, MC is fully responsible for authentication, respectively, fig. 1. In the absence of a stable connection with the MC, the delegation protocol requires a direct connection between the user agents and the delegated DED. The protocol steps performed at this stage are shown in Fig. 2 and 3, protocols 2A and 2B, respectively. This scenario describes the lease of an electronic device with the conditions and time of use of the DED.

Protocol 2A - the presence of a stable connection for both users (Fig. 3).

1. User Alice sets the maximum delegation time (t_d) for DED wi using a service message signed by $m[D]_A = sign_A(w_i, t_d, ID_A, ID_A, \{\text{other delegation conditions}\})$, according to step 1.
2. User Alice transfers $m[D]_A$ to the MC using a secure channel, according to step 2.
3. The MC verifies the authenticity of the message from Alice using PK_A. If the test fails, the protocol stops working according to step 3.
4. The MC signs the delegation message $m[D]_{cloud} = sign_{cloud}(m[D]_A)$ according to step 4.
5. The MC transmits $m[D]_{cloud}$ and $cert_A$ for Bob, in accordance with step 5.
6. User Alice sends the service message $(m[C(S_A)]_A)$ to the DED, deleting the private key MC from the DED, in accordance with step 6.
7. If the user Bob does not trust Alice, the protocol performs step 7. The DEU is reset to the factory settings. The reset occurs with the $m[D]_{cloud}$ and the $cert_{cloud}$ certificate stored in the secure storage. These values were obtained in step 6 of the initialization protocol in order to preserve data integrity and confirm ownership rights in the absence of connection with the MC. User Bob compares the result of the hash function from the current DED software with that stored in $cert_{cloud}$. If they do not match, the algorithm stops execution. Thus, the Bob user loses the ability to use the DED, since it is assumed that the software could be skommeted by the owner. It is important to note that the protected timer and storage remain unchanged even when reset to factory settings.

8. If user Bob trusts Alice, the software component of the DED remains unchanged, and the temporary user has the opportunity to use the software of the device owner.
9. User Bob generates an S_B secret key for direct interaction between the DED, according to protocol step 12.
10. User Bob sends the S_B to the DED via a secure channel, as described in step 9.
11. To ensure data integrity, the Bob user calculates a new value $sign_B(w_i, SW_i)$.
12. In case of expiration of the td delegation timer on the DED side, the device parameters are reset to the factory settings while maintaining the contents of the protected storage. The timer can be remotely updated if there is a simultaneous connection to the owner's MC using the service message $m[D]_A = sign_A(w_i, t_d, ID_A, ID_A, \{\text{other delegation conditions}\})$.

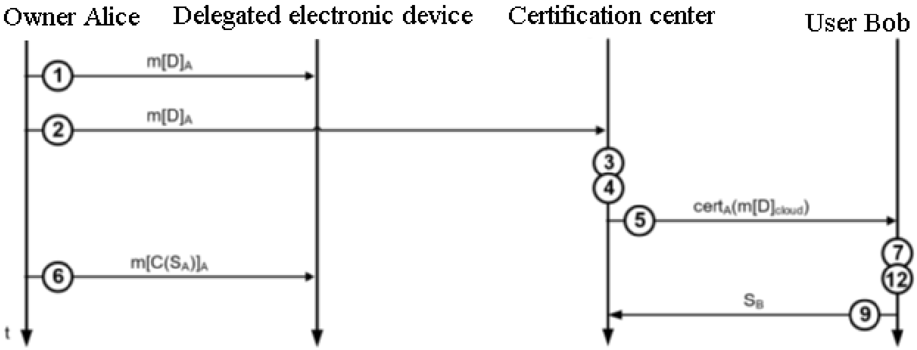


Figure 3 Scheme of step-by-step implementation of the delegation of DED in the presence of a stable connection with the SA, Source: own.

Protocol 2B - the absence of a stable connection for at least one of the users (Fig. 4).

1. User Alice sets the maximum delegation time t_d to DED w_i using a service message signed by $m[D]_A = sign_A(w_i, t_d, ID_A, ID_B, \{\text{other delegation conditions}\})$, according to step 1.
2. The Alice user passes the certA to the Bob user over the secure channel, according to step 2.
3. Bob authenticates $cert_A$ using $cert_{cloud}$. If the test fails, the protocol stops working, according to step 3.

4. User Alice sends the service message $(m[C(S_A)]_A)$ to the DED, deleting the private key S_A from the DED, according to step 4.
5. If the user Bob does not trust Alice, the protocol is run in accordance with step 5. The DED is reset to the factory settings.

The reset occurs with the $(m[D)]_{cloud})$ and the certcloud certificate saved in the secure store. These values were obtained at step 6 of the initialization protocol in order to preserve data integrity and confirm ownership in the absence of connection to the S_A. User Bob compares the result of the hash function from the current DED software with that stored in certcloud. If they do not match, the algorithm stops execution. Thus, the Bob user loses the ability to use the DED, since it is assumed that the software could be compromised by the owner. It is important to note that the protected timer and storage remain unchanged even when reset to factory settings.

6. If user Bob trusts Alice, the DED software component remains unchanged, and the temporary user has the opportunity to use the device owner's software.

User Bob generates an S_B secret key for direct interaction with the DED, according to step 10.

8. The user Bob transfers the S_B to the DED via a secure channel, according to step 11.
9. To ensure data integrity, Bob calculates the new value of $sign_B(w_i, SW_i)$.

In the case of the expiration of the t_d delegation time on the DED side, the device parameters are reset to the factory settings while maintaining the contents of the protected storage. The timer can be updated using the service message $m[D]_A = sign_A(w_i, t_d, ID_A, ID_B, \{\text{other delegation conditions}\})$ if there is a direct connection between users.

11. The user Bob sends the S_B to the DED via a secure channel, according to step 9 in Fig. 4.
12. To ensure data integrity, the Bob user calculates a new value $sign_B(w_i, SW_i)$.

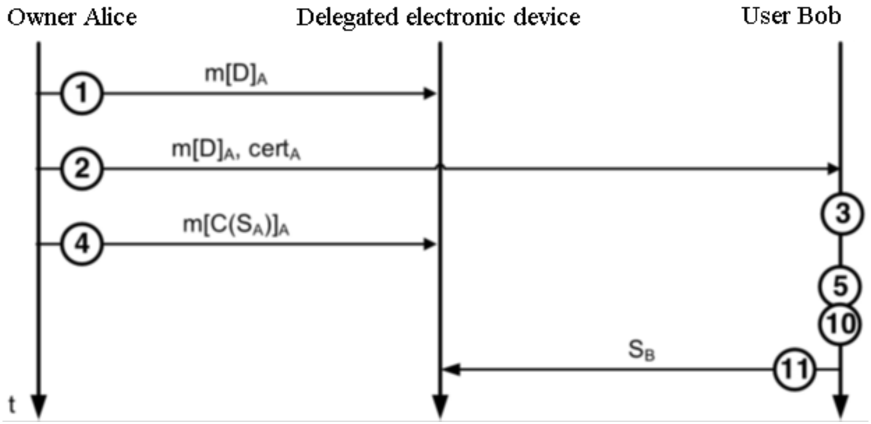


Figure 4 The scheme of step-by-step implementation of the DED in the absence of a stable connection with the CA, Source: owner.

Returning the device to the owner after temporary use of the DED by another user. The functioning of the system can occur in two modes: in the presence of a connection with the MC and without such a connection. The corresponding steps are shown in fig. 5 (protocol 3A) and 6 (protocol 3B). In the first case, similar to delegation, the MC is fully responsible for authentication. In the absence of a stable connection with the MC, the device return algorithm requires direct connections between user accounts and the delegated DED.

Protocol 3A - the presence of a stable connection for both users (Fig. 5)

1. User Bob generates a service message signed by SK_B as $m[R]_B = sign_A(w_i, R)$, according to step 1.

User Bob transmits $m[R]_B$ to the MC using the secure channel, according to step 2.

3. The MC verifies the authenticity of the message from Bob using SK_B. If the test fails, the protocol stops working, according to step 3.
4. The MC signs the return message $m[R]_{cloud} = sign_{cloud}(m[R]_B)$, according to step 4.
5. The MC transmits the $m[R]_{cloud}$ to Alice, according to step 5.
6. User Bob sends the service message $m[C(S_B)]_B$ to the DED, deleting the S_B secret key from the DED, according to step 6.
7. If the Alice user does not trust Bob, step 7. The DED is reset to the factory settings and the data is stored in a secure storage. Alice's user account

compares the result of the hash function from the current DED software with that stored in certcloud. If they do not match, the protocol stops working. Thus, the Alice user loses the ability to use the DED, since it is assumed that the software could be compromised by the owner. It is important to note that the protected timer and storage remain unchanged even when reset to factory settings.

8. If the Alice user trusts Bob, the DED software component remains unchanged, and the device owner has the opportunity to use the software installed during the delegation process.
9. The Alice user generates an S_A secret key for direct interaction with the DED, according to step 8.
10. User Alice transfers the S_A to the DED using a secure channel, according to step 9.
11. To ensure data integrity, the Alice user calculates a new value $sign_A(w_i,SW_i)$. Only the $cert_A$ and certcloud are in the secure DED storage.

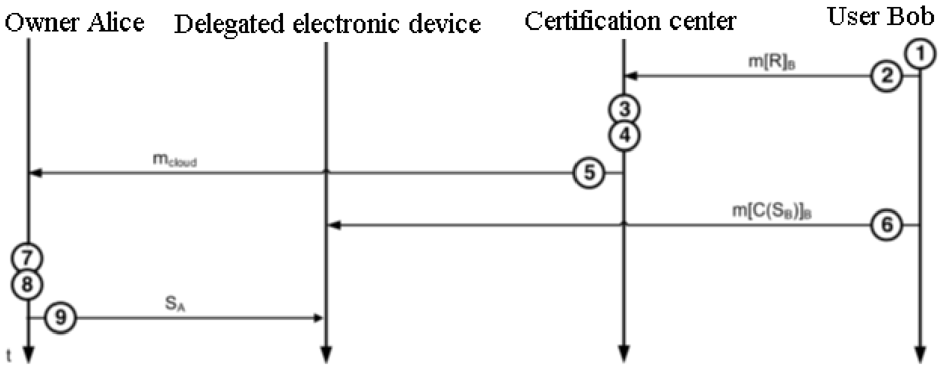


Figure 5 Scheme of step-by-step execution of the stage of returning DED in the presence of a stable connection with the SA, Source: owner.

Protocol 3B - the absence of a stable connection for at least one of the users (Fig. 6)

1. User Bob generates a service message signed by SK_B as $m[R]_B = sign_A(w_i,R)$ according to step 4.
2. User Bob transfers $m[R]_B$ to user Alice via a secure channel, as per step 2.
3. Alice authenticates $m[R]_B$ using certcloud. If the verification fails, the protocol stops its work, according to step 3.

4. User Bob sends the service message $m[C(S_B)]_B$ to the DED, deleting the S_B secret key from the DED, according to step 4.
5. If the Alice user does not trust Bob, the protocol operates according to step 5. The DED is reset to the factory settings with the data stored in the secure storage. Alice's user account compares the result of the hash function from the current software of DED with that stored in certcloud. If they do not match, the protocol stops working. Thus, the Alice user loses the ability to use the DED, since it is assumed that the software could be compromised by the owner. It is important to note that the protected timer and storage remain unchanged even when reset to factory settings.
6. If the Alice user trusts Bob, the DED software component remains unchanged, and the owner has the opportunity to use the device's temporary user software.
7. The Alice user generates the SA secret key for direct interaction with the DED, according to step 10.
8. User Alice transfers the SA to the DED through a secure channel, according to step 11.
9. To ensure data integrity, the Alice user calculates a new value $sign_A(w_i, SW_i)$. Only the $cert_A$ and $cert_{cloud}$ are in the secure DED storage.

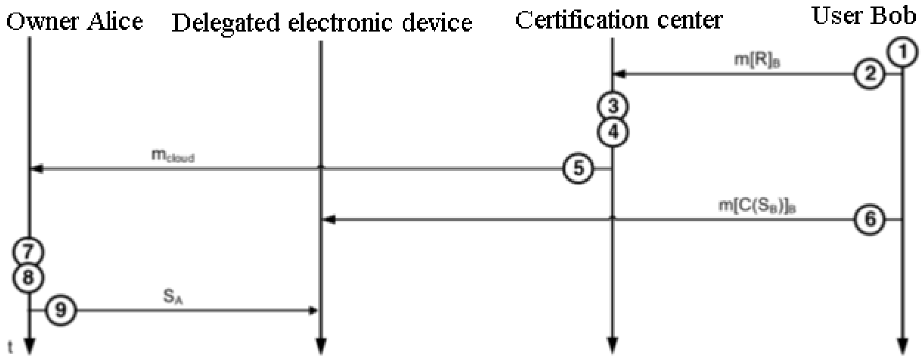


Figure 6 Scheme of step-by-step completion of the return of DED in the absence of a stable connection with the SA, Source: owner.

In device dissociation are two possible options for the functioning of the protocol: manual and automatic dissociation. In manual dissociation, the owner and DED communicate through a direct channel. The owner's Alice sends a control message that resets the DED to the factory settings. Automatic dissociation is possible by a predefined timer, which performs a similar procedure for the expiration of the delegation time of the device in case of non-return.

Protocol 4A - Manual Dissociation of DED:

1. Owner Alice generates a service message signed by SK_A as $m[F]_A = sign_A(w_i, F)$.
2. User Alice sends $m[R]_B$ to the DED through a secure channel.
3. The DED is reset to the factory settings with the cleaning of the secure storage.
4. The DED device can be restored only by using the factory key and with a connection to the S_A.

Protocol 4B is executed when the device was not returned according to the conditions of delegation, lost or stolen. All personal data of the owner and user must be destroyed in order to prevent potential malicious use.

1. During the initial association of the device, the owner of Alice optionally generates a service message signed by SK_A, $m[E]_A = sign_A(w_i, t_e)$, where te is the value of the countdown timer for automatic dissociation. DED refers to a timer during operation in order to detect potential processing.
2. In the case of processing, the DED is reset to the factory settings, clearing the protected storage.
3. The DED device can be restored only when using the factory key and if there is a connection with the CA.

After a detailed review of the proposed protocol, it is important to note potential attacks on its operation. One such attack is phishing. In this case, the attacker Eve may appear to be Bob's trusted user with IDB during the delegation process between Alice and Bob. If Alice cannot verify the authenticity of the request source, the attack is considered successful. The main scope of attack is in the field of wearable electronics, as devices of this type often do not have an additional visual channel (for example, a display) for additional confirmation of the delegation procedure. In the modern world, there is no solution that fully protects against phishing attacks, however, multifactor authentication techniques can reduce the likelihood of an attack's success.

Another important attack on the protocol is the classic middleman attack. In our case, the attacker Eve requests $m[D]_A$ for Bob (ID_B) from Alice, pretending to be Alice (ID_A), and at the same time passes $m[D]_A$ for user Bob. As a result, Eve does not get the ability to use the device, however, it can monitor the delegation process.

One of the most interesting attacks is an attack using an infected device. Consider the following example. After an intruder intercepts the correct $m[D]_A$ about delegating the w_k device, Eve creates an infected device, which appears to be w_k and always sends the correct hash (SW_k) value. Such a device allows, for example, to monitor user activity Bob.

At the same time, protocols that use digital signatures are especially vulnerable in terms of confidentiality, since they usually involve unambiguous confirmation from a trusted entity. In other words, the user cannot later deny the fact of delegation. Protocols based on zero-disclosure evidence rely on this feature to enhance security, however, they cause additional confidentiality complications.

4 Conclusion

The authentication protocol for electronic devices monitoring is presented, developed for use in conditions of unstable communication with a certification center. Algorithms that implement the stages of functioning of the proposed protocol can be implemented both in the form of software for a universal computer of any architecture, and in the form of hardware for a specialized computer of any architecture. The protocol can be used in places with lack of infrastructure, because for the implementation of delegation does not require a constant connection to the SA.

The proliferation of IoT services requires security and privacy to be guaranteed. The review of publications published in the works clearly demonstrates how many unsolved problems remain, sheds light on the areas of research in the field of IoT security. Until now, a single concept has not been formulated regarding the requirements of security and confidentiality in such a heterogeneous environment using various communication technologies and standards. Appropriate solutions need to be developed and implemented. They should be platform independent and allow guaranteeing access control and confidentiality of users and things, reliability among devices and users, adherence to certain privacy security policies. Research is required on IoT security in mobile devices, which is becoming more widespread today. Much effort has been (and will be) made by the world scientific community to solve existing unsolved problems. At the same time, in the process of work, there will be many new questions that are yet to be faced. This article will be useful in choosing further areas of research and will contribute to the massive deployment of IoT systems in the real world.

References

Artyshchuk, Iryna; Belej, Olexander; Nestor, Nataliya. (2019). 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM). *Designing a Generator of Random Electronic Message Based on Chaotic Algorithm* (pp. 1-5). Polyana, Ukraine: IEEE.

Belej, O. (2019). Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. *The Cryptography of Elliptical Curves Application for Formation of the Electronic* (pp. 68-83). Springer, Cham: Advances in Intelligent Systems and Computing.

Belej, O.; Lohutova, T.; Banaś, M. (2019). 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM). *Algorithm for Image Transfer Using Dynamic Chaos* (pp. 1-5). Polyana, Ukraine: IEEE .

Belej, Olexander. (2019). 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM). *Algorithm for Image Transfer Using Dynamic Chaos* (pp. 1-5). Polyana, Ukraine: IEEE.

Belej, Olexander; Artyshchuk, Iryna; Sitek, Wojtek. (2019). The CEUR Workshop Proceedings. *The controlling of transmission of chaotic signals in communication systems based on dynamic models* (pp. 483-497). Zaporizhya: CEUR .

Beley O., Chaplyha V. (2017). IT4P - Information Technology for Practice 2017. *A management of cloud services in social-economic system* (pp. 156-16). Ostrava: HSB-TU.

He, D.; Zeadally, S. (2015). Internet of Things Journal. Vol. 2. No. 1. *An analysis of rfid authentication schemes for Internet of Things in healthcare environment using elliptic curve cryptography* (pp. 72–83). IEEE .

Hummen , R., Ziegeldorf , J., & Shafagh, H. (2013). Proc. of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy. *Towards viable certificate-based authentication for the Internet of Things* (pp. 37–42). ACM.

Joux, A. (2000). International Algorithmic Number Theory Symp. *A one round protocol for tripartite Diffie–Hellman* (pp. 385–393). Springer.

Kim , H., Chang , H., Suh , J., & Shon , T. (2016). Proc. of Internat. Conf. on Industrial Engineering, Management Science and Application. *A study on device security in IoT convergence* (pp. 1–4). Kim H.J., Chang H.S., Suh J.J., Shon T.S.: IEEE.

Ministr J., F. J. (2014). Proceedings of the 17th International Conference on Information Technology for Practice 2014. *Testing the Quality of Software in the Form of Services*, (pp. 121-127). Ostrava.

Nix , J. (2016). M2M and IoT technologies, Llc. . *Systems and methods for "machine-to-machine" (M2M) communications between modules, servers, and an application using Public Key Infrastructure (PKI)* . M2M and IoT technologies.

Saadeh , M.; Sleit, A.; Qatawneh , M.; Almobaideen W. A. (2016). Proc. of Cybersecurity and Cyberforensics Conference. *Authentication techniques for the Internet of Things: A survey* (pp. 28–34.). IEEE.

Tvrdikova, M. (2016). Proceedings of the 19th International Conference on Information Technology for Practice. *'Cloud Computing sn Management*, (pp. 69-78). Ostrava.

Wander, A.S.; Gura , N.; Eberle , H.; Gupta , V.; Shantz, P. (2015). Proc. of 3rd IEEE Internat. Conf. on Pervasive Computing and Communications. *Energy analysis of public-key cryptography for wireless sensor networks* (pp. 324–328). IEEE.

Secure Software Modeling Methods for Forensic Readiness

Lukas Daubner[1], Tomas Pitner[2]

Abstract. Proactive preparation of software systems for forensic investigation (forensic readiness) during the software development process, has been addressed only recently and has many open challenges. Representation of the forensic concerns and specific requirements of forensic readiness is one of them. A common way of representing concepts in software development is modeling. This paper is focused on the possibility of reusing existing secure software modeling methods for the needs of forensic readiness.

Keywords: Forensic Readiness, Forensic-Ready Software, Forensic-by-design, Software Development, Software Modeling, Digital Forensics

JEL Classification: K24

1 Introduction

For critical systems, it is important to be prepared for forensic investigation in case of an incident. This incident is often cybersecurity-related but can also be result of a natural disaster or serious failure. Digital forensics is concerned with the investigation that aims to uncover what happened, who is responsible, when, where and how it happened, based on digital evidence (Casey, 2011). However, a proper investigation of such kind of incident is a delicate and time-consuming process. To prepare for the possibility of investigation, there is a concept called forensic readiness.

The notion of forensic readiness coined by (Tan, 2001), was formulated to make the digital forensic investigation more effective and in some sense, possible. It is a concept of measures, which aids investigation in case of an incident. Opposed to the forensic investigation itself, which is inherently reactive, forensic readiness is a proactive measure. Forensic readiness can be understood as an umbrella term for any systematic preparation for investigation of an incident.

[1] Masaryk University, Brno, Czechia, daubner@mail.muni.cz
[2] Masaryk University, Brno, Czechia, tomp@mail.muni.cz

Originally, forensic readiness was formulated as a series of general guidelines. Later it was expanded and approached in a more process-oriented manner (Rowlingson, 2004). The forensic readiness touches, among others, aspects of the collection, proper handling, and presentation of digital evidence. It is also dealing with staff training and policies to ensure proper handling of incident form forensics point of view. In general, the employment of forensic readiness greatly increases the likelihood of a successful forensic investigation.

The idea to tackle forensic readiness in the scope of software engineering has started to emerge only recently (Pasquale et al., 2018). The aim is to systematically support the development of forensic-ready software systems, i.e. systems that support the potential forensic investigation in a forensically sound way (McKemmish, 2008). Example of such support is proactive securing of evidence while ensuring its non-repudiation, or data provenance. In legal terms, it refers to, for example, maintaining the chain of custody (Casey, 2011). The concept is sometimes called forensic-by-design (Ab Rahman et al., 2016).

From the software engineering point of view, the forensic readiness can be seen as a high-level non-functional requirement on the system. The same idea applies to security, which is also viewed as a high-level non-functional requirement, decomposable into multiple security concerns. Similar to security, it is important to consider forensic readiness early in software development because, as a non-functional requirement, it can affect the software architecture (Chung et al., 2012). However, while there is considerable support for the representation of security concerns using software modeling methods, for forensic readiness, there is not.

This paper is focused on identifying the similarities between forensic readiness and security requirements. Using those similarities, existing modeling methods for relevant security concerns are inspected for potential usage in modeling forensic-ready software systems.

The paper is structured as follows. Section 2 identifies relevant forensic readiness concerns in terms of security. Section 3 analyses plausible security modeling methods that cover identified concerns. Finally, Section 4 concludes the paper.

2 Forensic Readiness Concerns in Security

There are many similarities between forensic readiness concerns and security concerns in terms of software systems. Many of those are referring to the same property, or they are partially overlapping. In some cases, the forensic readiness concern refers to highly specialized applications of particular security concern. The work by (Pasquale et al., 2018), which is essentially a starting point for research in the field of forensic-ready software systems, elicitated the forensic-readiness requirements (concerns). This list is used in this section as a base set for comparison with the security concerns.

The forensic-readiness concerns and its relevancy in terms of security are described in Table 1.

Table 3 Forensic readiness concerns

Forensic readiness concern	**Short description**	**Relevant security concern**
Availability	Evidence data are preserved and useable	Yes
Relevance	Only the evidence that is relevant to the investigation is proactively preserved	No
Minimality	No unnecessary evidence is proactively preserved	No
Linkability	Evidence can be linked with other evidence	No
Completeness	Evidence should be sufficient for decision making	No
Non-repudiation	Evidence should be authentic and not tampered with	Yes
Data provenance	Evidence should keep data about its origin, ownership, and operations	Yes
Legal compliance	Data preservation process must comply with law and regulations	No

Out of the forensic readiness concerns, three was identified to have, at least partially, relevant counterpart in security concern. Availability was identified as is overlap with audit and logging, which are often considered as security concerns. Both audit and logging are important sources of digital evidence (Grajeda, Breitinger, and Baggili, 2017). Non-repudiation, a security concern by itself further implies integrity which needs to be satisfied. Specifically, in the field of forensic readiness, the non-repudiation is aimed at the evidence and its metadata. Finally, data provenance is associated with auditing, which also, as an important source of evidence metadata, need strong guarantees for non-repudiation.

On the other hand, the important aspect that distinguishes the forensic readiness concerns and security concerns is the difference between legal and technical understanding of the concept, which might differ. Specifically, security is focused on the technical aspect, while forensic readiness is more concerned with the legal aspect because the evidence produced by the forensic investigation is intended to be used in the court of law. An example of a difference in understanding is non-repudiation (Mccullagh and Caelli, 2000). Despite the difference, the technical point of view still has an important role.

3 Security Modeling Methods for Forensic Readiness

Based on the identified security concerns, suitable modeling methods that address them are analyzed. Two reviews, by (Nguyen et al., 2015) and by (Van den Berghe et al., 2017), focused on the secure software modeling methods are chosen as a basis for examination. The former focuses on Model-Driven Development approach, whereas the latter considers more general approach focusing on design notations.

The reviews are examined for those methods that, at least partially, cover the identified concerns. Concretely, those are auditing, integrity, logging, and non-repudiation. Approaches that are aimed narrowly on a specific domain were excluded, as well as those focused on threat modeling. The results are summed in Table 2.

Table 4 Security modeling methods

Source	Domain	Approach	Security concerns
(Jürjens, 2002)	General	UML profile	Integrity, Non-repudiation
(Hafner and Breu, 2009)	Distributed workflow	UML profile	Integrity, Non-repudiation
(Gilmore et al., 2011)	SOA	UML profile	General non-functional requirements
(Sánchez et al., 2010)	General	AOM, UML profile	Integrity
(Almorsy, Grundy, and Ibrahim, 2012)	General	AOM, UML	Integrity
(Fernández-Medina et al., 2007)	Data Warehouses	UML profile	Integrity, Non-repudiation, Auditing
(Sánchez et al., 2009)	General	DSL	Integrity

The most mature approach is UMLsec by (Jürjens, 2002). It is a UML profile that tackles multiple security concerns. Specifically, for forensic readiness concerns, it has support for integrity and non-repudiation. Both of those are considered on the object level, which is very useful for securing of evidence inside the system, as it is not limited to the messaging level. The method is suitable for general-purpose, has tool support, and most importantly, it provides ways for formal verification. Such properties make it an ideal candidate for further research in the forensic readiness field.

The work by (Hafner and Breu, 2009) called SECTET-framework presents a UML profile that deals with securing intra-organizational distributed workflows. The relevant concerns, integrity and non-repudiation, are only tackled using Object Constraint Language (OCL) at the messaging level.

Methods focused strictly on Service-Oriented Architectures (SOA) like work by (Gilmore et al., 2011) are not considered in this paper because of their narrow focus. They typically use the models to generate WS-SecurityPolicy to address the concerns. While this is indeed useful in the SOA domain, it cannot be used in a general system.

An interesting method is based on Aspect-Oriented Modelling (AOM). The main advantage is a clear separation of concerns, so the particular property is encapsulated and can be modeled independently on the rest of the system. However, all such relevant methods found tackles only the integrity concern. The approach by (Sánchez et al., 2010) is an example of the aspect-oriented method, using the UML profile. This particular approach is interesting for forensic readiness concerns, because it is not focused only on security, but aimed as a general-purpose approach. There is also an aspect-oriented method by (Almorsy, Grundy, and Ibrahim, 2012) that weaves the aspects at runtime, which allows for dynamic adaptation. Such a method might be interesting in dynamically configuring logging aspects for evidence collection.

While domain-focused methods are not considered in this paper, the method by (Fernández-Medina et al., 2007) is mentioned for its description of the auditing concern. Such support is important for ensuring the availability of evidence, but not explicitly tackled by the previous ones.

The last relevant method is ModelSec by (Sánchez et al., 2009). It focuses on capturing and managing security requirements using models and generating code artifacts based on them. The models and transformations are defined for each phase of software development. For forensic readiness concerns, it only supports integrity, but since the method is meant to be general-purpose, the Domain Specific Language (DSL) and meta-models could be extended.

4 Conclusion

Secure software modeling methods were found to be a promising basis for defining methods for representation of forensic readiness concerns. The methods can be utilized to support forensic readiness, even though there are differences between legal and technical understanding, which is critical to address in the domain of digital forensics.

This paper identified software modeling methods for secure software, applicable for modeling of forensic-ready software systems. The methods that are addressing the security concerns were exploited due to partial overlap with forensic readiness concerns. Although no method is directly applicable for forensic-ready software systems, potential ways to extend them were identified.

Future research should further elaborate on the differences between the legal and the technical understanding of concerns. Such knowledge can then be used to formulate concrete meta-model for representing forensic readiness concerns, that would align well with legal understating while remaining useable for software engineer without forensics or legal expertise.

Acknowledgements

This research was supported by ERDF "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

References

Ab Rahman, N. H., Glisson, W. B., Yang, Y. and Choo, K. R. (2016) ‘Forensic-by-Design Framework for Cyber-Physical Cloud Systems‘. *IEEE Cloud Computing.* vol. 3, no. 1, pp. 50-59.

Almorsy, M., Grundy, J. and Ibrahim, A. S. (2012) ‘MDSE@R: Model-Driven Security Engineering at Runtime’, *Cyberspace Safety and Security*, Berlin, pp. 279-295.

Casey, E. (2011) *Digital evidence and computer crime: forensic science, computers and the Internet* 3rd ed., Waltham, MA: Academic Press.

Chung, L., Nixon, B. A., Yu, E. and Mylopoulos, J. (2012) *Non-functional requirements in software engineering*, Vol. 5. Boston, MA: Springer Science & Business Media.

Fernández-Medina, E., Trujillo, J., Villarroel, R. and Piattini, M. (2007) ‘Developing secure data warehouses with a UML extension’. *Information Systems*, vol. 32, no. 6, pp. 826-856.

Gilmore, S., Gönczy, L., Koch, N., Mayer, P., Tribastone, M. and Dániel, V. (2011) ‘Non-functional properties in the model-driven development of service-oriented systems’, *Software & Systems Modeling*, vol. 10, no. 3, pp. 287-311.

Grajeda, C., Breitinger, F., and Baggili, I. (2017) ‘Availability of datasets for digital forensics – And what is missing‘. *Digital Investigation* vol. 22, pp. S94-S105.

Hafner, M. and Breu, R. (2009) ‘Modeling Security Critical SOA Applications’, *Security Engineering for Service-Oriented Architectures*, Berlin: Springer.

Jürjens, J. (2002) ‘UMLsec: Extending UML for Secure Systems Development’, *«UML» 2002 — The Unified Modeling Language*, Berlin, pp. 412-425.

Mccullagh, A. and Caelli, W. (2000) ‘Non-Repudiation in the Digital Environment‘. *First Monday*. vol. 5.

McKemmish, R. (2008) ‘When is Digital Evidence Forensically Sound?‘, *Advances in Digital Forensics IV*, Boston, MA: Springer US, pp. 3-15.

Nguyen, P. H., Kramer, M., Klein, J., and Traon, Y. L. (2015) ‘An extensive systematic review on the Model-Driven Development of secure systems’. *Information and Software Technology.* vol. 68, pp. 62-81.

Pasquale, L., Alrajeh, D., Peersman, C., Tun, T., Nuseibeh, B. and Rashid, A. (2018) ‘Towards Forensic-ready Software Systems’, *Proceedings of the 40th International Conference on software Engineering: New Ideas and Emerging Results (ICSE-NIER ’18)*, New York, NY, USA, pp. 9-12.

Rowlingson, R. (2004). ‘A Ten Step Process for Forensic Readiness‘, *International Journal of Digital Evidence*, vol. 2, no. 3

Sánchez, Ó., Molina, F., García-Molina, J. and Toval, A. (2009) ‘ModelSec: A Generative Architecture for Model-Driven Security’, *Journal of Universal Computer Science*, vol. 15, no. 15.

Sánchez, P., Moreira, A., Fuentes, L., Araújo, J. and Magno, J. (2010) ‘Model-driven development for early aspects’, *Information and Software Technology*, vol. 52, no. 3, pp. 249-273

Tan, J. (2001) *Forensic readiness*, [Online], Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.644.9645&rep=rep1&type=pdf [23 Mar 2001].

Van den Berghe, A., Scandariato, R., Yskout, K. and Joosen, W. (2017) 'Design notations for secure software: a systematic literature review', *Software & Systems Modeling,* vol. 16, no. 3, pp. 809-831.

Interconnected Cybersecurity System

Jan Ministr[1], Josef Fiala[2]

Abstract. The cyberthreats have become harder to stop for this reason most organizations are moving from isolated security point product to an interconnected security system. The choosing a interconnected cybersecurity system is a serious management decision with a long-term impact on the operation of the information system in the organization. The article describes the key factors to consider when choosing a interconnected cyber security system and its impact on the organization.

Keywords: cyber attack, cyber security, interconnection, tracking activities, ransomware.

JEL Classification: K24

1. Introduction

IT system is fundamental to the effective, safe-running of all organizations. This connected network of devices, networks, data and workloads enables people to work productively – sharing data, accessing resources, tracking activities. The ensuring cyber security is now increasingly costly for organizations. 87% of IT managers agree that in the last year malware threats have become more complex and businesses lose on average seven working days per month identifying and repairing infected computers (Sophos, 2018).

Point security product are no longer enough because the cyberthreats work as a system. First, we need to understand the cause of the problems, that is, the security threats that we want to eliminate. Cybercriminals don't use single techniques and technologies in their attacks (Chaplyha & Nyemkova, 2017). Instead, they use multiple techniques in connected, coordinated assaults. A cyber attack usually includes the following steps:

- *initial attack* such as phishing email that includes a malicious URL, clicking on which connects you to a command and control center;

[1] VSB - Technical University of Ostrava, Faculty of Economics, University of Economics, department of Applied Informatics, jan.ministr@vsb.cz.
[2] Warsaw Management University, Faculty of J. A. Comenius Karvina, josef.fiala@pedagogikakarvina.cz.

- *second attack* that using a combination of credential theft, privilege escalation, and malicious executables;
- *ultimate goal,* which could be stealing your data, or holding your data for ransom.

The disadvantage of unconnected point security solutions is that they struggle to fight back against these complex, coordinated attacks. That's why organizations are introducing an interconnected cybersecurity system with integrated products working together to outsmart today’s hackers. Only 16% of Chief information security officers are able to collect, analyze, and respond to 75% or more of their security event telemetry today (Forbes, 2019).

2. Structure of Interconnected Cybersecurity System

An effective integrated information system contains four basic elements:

- *central management* that allows to see and control everything in one place;
- *integrated components* they represent any different elements working harmoniously together;
- *automated actions* they provide sequential behavior based on pre-agreed criteria;
- *extendability* when the interconnection Cybersecurity system can grow as requirements grow.

These four elements are what transform point products into a system. The stronger each of these components, the stronger the system.

The same principles apply to cybersecurity. The cybersecurity technology platform sits at the heart of the system, enabling IT teams to manage all their security services (endpoint protection, firewall, mobile, email, wireless, encryption, user education) via a single interface as shows fig.1. These services actively work together, sharing information and automatically responding to issues and events. The greater the integration, the more effective the system (Franke, 2019).

The interconnected cybersecurity system should add value to the whole business and an effective solution that will enable:

- *reducing cyber risk* so that reduce attack exposure and significantly increase response time in case of infection;
- *increasing visibility* with gaining deeper and wider insight into safety of property, it allowing to make informed and accurate decisions (Chaplyha & Melnik, 2019);
- *Increasing productivity* so that it reduce the impact of computer security on the IT team and users throughout the organization;
- *saving* money by switching from point products to a computer security system what allows to reduce on-board costs, integration and training, as well as day-to-day system management overhead. Reseller consolidation also benefits from non-IT functions such as purchasing and legal;
- *displaying security value* what reduce time spent solving everyday problems, a computer security system can free up IT teams to work on business-oriented projects. Increased protection and resulting reduction of user downtime also allows a wider organization to appreciate the value of security (Nguyen, 2015).

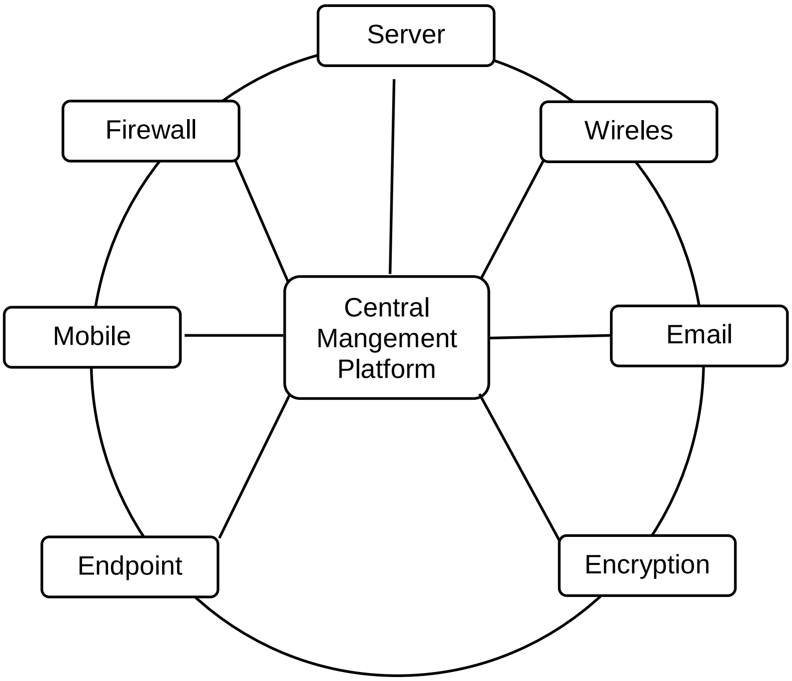


Figure 6 Structure Interconnected Cyber Security System, Source own.

3. Key Characteristics of Interconnected Cybersecurity System

To get the most out of your cyber security system, consider the following four key features:

3.1. Breadth of protection

It means to ensure there are options to extend the Interconnected cybersecurity system in the future to it can grow with business. It is therefore necessary to pay attention to the following characteristics (Vilamova et all, 2015):

- *Range of security services.*
- *Communication between components.*
- *Ease of expansion.*
- *Additional costs.*

3.2. Product integration

The point of a security system is synergy of its individual parts. Individual products working together to deliver benefits that are not possible on their own. The core benefits of a security system fall into two categories (Caravelli & Jones, 2019):

- *Zero-touch,* automated response that represents how do the products work together to automate previously manual tasks.
- *Cross-estate* visibility that represents how does the product integration elevate visibility across the organization. It delivers real-time incident analysis and cross-estate reporting, giving instant insights that can act on.

When considering product integrations is useful think about what will be most useful to organization (Diogenes & Ozkala, 2019).

3.3. Operational efficiency

The simpler the system, the better the opportunities it offers can be exploited. Highly complex and difficult-to-use solutions have limited benefits and can be difficult for IT teams that need to manage them. Specific areas to focus on are (Beley & Chaplyha, 2017):

- *Applicability*, it means how quickly and easily you can deploy, monitor and manage your system. The more control consoles are located in one place, the better.
- *Overhead*, it depends on whether the system is cloud-based or if you need to fund and maintain local servers.
- *Consistency* which ensures that screens and visual representations are consistent across all screens.

3.4. Product Leadership

Transition to a synchronized security system should not compromise protection. It's good to start with products that are great in their own right, and even better together, paying attention to the following:

- *Industry verification* that means looking for products that work well in both performance tests (such as SE Labs, AV-Test) and market analyst ratings (such as the Gartner Magic Quadrant).
- *Customer feedback* that represents opinions of cyber security customers.
- *Recognized leaders* when is to consider products that industry analysts recognize as leaders.

4. Conclusions

An interconnected cyber security system is a very effective way of defending cyber attacks. However, it requires a balanced approach to all the features of such a security to be considered in order to achieve a synergistic effect.

Currently, there are several variants of the solution on the market, so it is necessary to carefully consider which option will be the most suitable for the given organization, because it is a strategic decision.

Acknowledgements

This paper was supported within Operational Programme Education for Competitiveness – Project No. CZ.1.07/2.3.00/20.0296.

References

Beley, O. and Chaplyha, V. (2017) ‘The Application of Neural Networks for the Intelligent Analysis of Multidimensional Data‘, *Proceedings of 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*. Kharkiv, Ukraine, pp. 400-404.

Caravelli, J. and Jones, N. (2019) *Cyber Security Threads and responses for Government and Business*, Santa Barbara: Praeger.

Diogenes, Y. and Ozkala, E. (2019) *Cyber security – attack and Defense Strategies*, 2nd ediion, Birmingham: Pakt Publishing.

Forbes.com, *Chief Information Security Officer Priorities For 2019*, [Online], Available https://www.forbes.com/sites/oracle/2019/01/17/chief-information-security-officer-priorities-for-2019/#62641d8a6937 [15 May 2019].

Franke, D. (2016) *Cyber Security Basics: protect your organization by applying the fundamentals*, South Carolina: CreateSpace Independent Publishing Platform.

Chaplyha, V. and Melnik, N. (2019) ‘The Models and Information Technologies of the Risk-oriented Assessment of the Banks' Performance‘, *Proceedings of 21th Conference Information Technology for Practice 2019*, Ostrava, pp. 131-140.

Chaplyha, V. and Nyemkova, E. (2017) ‘Using Non-Uniform Sampling in Real-Time Correlation Processing of Authentication Signals‘, Proceedings of 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)‘, Kharkiv, Ukraine, pp. 474-476.

Nguyen, P. H., Kramer, M., Klein, J., and Traon, Y. L. (2015) ‘An extensive systematic review on the Model-Driven Development of secure systems’. *Information and Software Technology*. vol. 68, pp. 62-81.

Sophos, *The Dirty Secrets of Network Firewalls, Sophos*, [Online], Available https://www.insight.com/en_US/content-and-resources/brands/sophos/the-dirty-secrets-of-network-firewalls-infographic.html [30 April 2018]

Vilamova, S., Kiraly, A., Kozel, R., Jankovska, K., Papousek, D. (2015) ‘The use of selected statistical methods as an objective tool of company's management‘, *Proceedings of International Conference on Engineering Science and Production Management (ESPM)*, Kosice, Slovakia, pp. 317-320.

Statement of the Publication Ethics and Publication Malpractice

IT for Practice’s Publication Ethics and Publication Malpractice Statement is based, in large part, on the guidelines and standards developed by the Committee on Publication Ethics (COPE).

We expect all parties commit to these publication ethics. We do not tolerate plagiarism or other unethical behaviour and will remove any manuscript that does not meet these standards.

The relevant duties and expectations of authors, reviewers, and editors are set out below:

Author Responsibilities

- Authors must certify that their manuscripts are their original work.
- Authors must certify that the manuscript has not previously been published elsewhere.
- Authors must certify that the manuscript is not currently being considered for publication elsewhere.
- Authors must notify us of any conflicts of interest.
- Authors must identify all sources used in the creation of their manuscript.
- Authors must report any errors they discover in their manuscript.

Reviewer Responsibilities

- Reviewers must notify us of any conflicts of interest.
- Reviewers must keep information pertaining to the manuscript confidential.
- Reviewers must bring to the attention of the Editor-in-Chief any information that may be reason to reject publication of a manuscript.
- Reviewers must at any time evaluate manuscripts only for their intellectual content without regard to race, gender, sexual orientation, religious belief, ethnic origin, citizenship, or political philosophy of the authors.
- Reviewer who feels unqualified to review the research reported in a manuscript or knows that its prompt review will be impossible should notify us and excuse himself from the review process.

Editorial Board Responsibilities

- The Editorial Board must keep information pertaining to submitted manuscripts confidential.
- The Editorial Board must disclose any conflicts of interest.
- The Editorial Board must evaluate manuscripts only for their intellectual content.
- The Editorial Board is responsible for making publication decisions for submitted manuscripts.

List of Authors

Author:	Team of Authors	
Editors	Jan Ministr	
Department, Institute	Centre of Information Technology	9870
Name:	Proceedings of the International Conference on Information Technology for Practice 2019	
Place, year of publishing:	VŠB – Technical University of ostrava,2019, 1st Edition	
Number of pages:	171	
Published:	VŠB - Technical University of Ostrava, 17. listopadu 15/2172 708 33 Ostrava - Poruba	
Printing:	Edtorial Center VŠB – Technical University of Ostrava	
Number of Copies*:*	80	
ISBN	978-80-248-4322-3 (pdf on line) 978-80-248-4321-6 (printed)	

Unsaleable

Suggested form of citation

AUTOR, A. Title paper. In: MINISTR, J. (eds.). *Proceedings of the 22nd International Conference on Information Technology for Practice 2019*. Ostrava: VSB - Technical University of Ostrava, 2019, pp. xxx-xxx. ISBN 978-80-248-4321.

ISBN 978-80-248-4322-3 (pdf on line)
ISBN 978-80-248-4321-6 (printed)