Assurance of Information Systems' Quality and Security

Ivan Izonin[1], Tetiana Hovorushchenko[2] and Peter Popov[3]

[1]*Department of Artificial Intelligence, Lviv Polytechnic National University, Lviv, Ukraine*
[2]*Department of Computer Engineering & Information Systems, Khmelnytskyi National University, Khmelnytskyi, Ukraine*
[3]*School of Science & Technology, Department of Computer Science, City University of London, London, United Kingdom*
E-mail: ivanizonin@gmail.com; tat_yana@ukr.net; p.t.popov@city.ac.uk
**Corresponding Author*

1 Introduction

Currently, all areas of human activity are related to information systems, so the current problems in the use of information systems are currently reliable protection of information from cyber threats and malware and quality assurance of information systems. The amount of information is constantly growing, so the issue of information security is becoming more acute. The need for quality and safety is based on the fact that errors and failures in the information systems, the impact of malware threaten disasters that lead to human casualties, environmental cataclysms, significant time losses and financial damage, or at least reputational damage to the company. Known methods and tools in the field of cybersecurity and quality assurance are unable to provide reliable protection of information from malware, detection and disposal of malware, as well as unable to ensure the required level of quality of information systems. Therefore, special attention in the direction of development and implementation of effective information systems is currently needed in the field of quality and security of information systems.

Achieving high quality information systems, as well as their cybersecurity is a key factor in their effective use and one of the main needs of customers.

This Special Issue aims to disseminate and discuss the quality and security of information systems. There are 8 original science-intensive studies in our Special Issue on the following topics:

- Information Systems' Quality
- Information Systems' Security
- Information Systems' Reliability
- Cybersecurity in Information Systems' Domain

Some of it was accepted after a careful review and published in the proposed special issue.

2 Review of the Accepted Works

Paper [1] provides tools to help intelligently build cybersecurity systems using field programmable gate arrays (FPGAs). For the qualitative analysis of FPGA-based matching schemes, the classification of efficiency criteria and related indicators is considered. A method of rapid calculating numerical characteristics of the FPGA-based signature system components is proposed as a quantitative assessment tool. This method based on the use of so-called estimation functions allows avoiding the time-consuming execution of the digital circuit synthesis procedure. The rapid quantification method allows developers of hardware-accelerated cybersecurity systems to even apply it at each iteration within the optimization procedure cycle.

In [2], the authors propose the method of increasing Smart Parking software system security based on integrating the middleware in Smart Parking System software architecture. The proposed method takes into account all the criteria for Smart Parking System software security, i.e. parameters of safe access to the database, client program security, server security and API security and provides a complex solution for increasing the safety of Smart Parking software system. The proposed method allows taking into account all the criteria for increasing the Smart Parking System software security in complex using security middleware.

Paper [3] investigates the fragment of the enterprise management system, and an analysis of possible directions of attacks on the printing enterprise by malicious software was perform. The scenario of cognitive modeling of the influence of an internal criminal who exploits the vulnerabilities of the software and hardware components of the control system is considered. The average assessment of local risks, which is formed using an ensemble of cognitive maps, is better from the point of view of dispersion of assessments of the state of target concepts. The performed scenario modeling showed that the use of the specified means of protection and organizational measures allows reducing the assessment of local risks by 12–18%. This technique allows obtaining a qualitative and quantitative assessment of risk indicators, taking into account the entire set of objective and subjective factors of uncertainty.

Paper [4] is dedicated to the development of a strategic and goal-oriented management system behaviour line, which requires informational and intelligent data processing at the highest level using cognitive creative methods. In the event of active threats complex on man-made systems in a certain region (resource, cognitive, system, information) and natural disasters or military operations, the threats lead to active destruction or failure of the production process. In order to functionally withstand related production structures, when loyal to the industrial relations concept, they need to integrate at the strategic management level on common goal basis to reduce risks. For each level of the infrastructure hierarchy, oriented towards strategic goals in the global infrastructure dynamic environment, methods of assessing the situation to detect failures and the actions of attacks have been developed, based on which countermeasures are formed depending on the type of threats.

Paper [5] investigates the development of a language-independent repetition detector and expand its capabilities. In the development and operation of the language-independent incremental repeater detector, it was decided to conduct experiments for five open source systems for evaluation using the industrial detector SIG (Software Improvement Group), including the use of a tool syntactic analysis. But there was the question of extending the algorithm for additional detection of duplication and redundancy in the code, which was proposed by Hammel, and how improvements can be made to achieve independence from the programming language. The idea of this approach is that according to the original study, the operation of calculating the entire block index with repeats and redundancy from scratch is very time consuming. Therefore, it is proposed to use LSH (locally sensitive hashing) to obtain an effective assessment of the similarity of software project files.

Paper [6] considers the use of blockchain technology to ensure the security of medical decision support systems (MDSS). This research is devoted to development of blockchain-based MDSS (regarding possibility or impossibility of organ and tissue donation/transplantation, regarding possibility or impossibility of using reproductive technologies in the treatment of infertility). The developed blockchain-based medical decision support system provides reliable protection and security of medical information through the use of blockchain technology, provides support of decision regarding possibility or impossibility of organ and tissue donation/transplantation, provides support of decision regarding possibility or impossibility of use of reproductive technologies in the infertility treatment. The proposed blockchain-based medical decision support system: automates medical decision-making processes, minimizes the human factor and its influence on the medical decision process, and takes into account the norms of current legislation when making medical decisions, thereby allowing not to pay for the services of a hired lawyer, and also works with verified and protected medical data entered in the blockchain, which allows you to get rid of leaks of medical information and to ensure reliable protection of medical data.

Paper [7] investigates the applicability of the Kolmogorov–Wiener filter to the prediction of heavy-tail processes, for example, to the prediction of telecommunication traffic in systems with data packet transfer. Authors generate stationary heavy-tail modelled data similar to fractional Gaussian noise and investigate the applicability of the Kolmogorov–Wiener filter to data prediction. Both non-smoothed and smoothed processes are investigated. It is shown that both the discrete and the continuous Kolmogorov–Wiener filter may be used in a rather accurate short-term prediction of a heavy-tail smoothed stationary random process. The paper results may be used for stationary telecommunication traffic prediction in systems with packet data transfer.

Paper [8] is devoted to the development of an energy-saving clustering hierarchical algorithm for Wireless Sensor Networks (WSNs); it is an improvement of Low-Energy adaptive Clustering Hierarchy (LEACH) algorithm. The aim of this algorithm is to minimize power consumption by the appropriate election of new cluster heads in every data transfer round and avoid network collisions. This goal achieved by using an efficient function to select the best cluster heads nodes in each round, which takes into account the current energy in the sensors. The proposed algorithm improves the cluster formation process by relying on the shorter distance to the base station. The Time Division Multiple Access (TDMA) mechanism also utilized to schedule the transmission of data packets to cluster heads nodes and to avoid data packet collisions at the base station. The proposed energy-saving clustering hierarchy algorithm has improved the performance of the LEACH algorithm in term of enhancing network lifetime and increasing network throughput.

Acknowledgments

We would like to thank the Editor-in-Chief of the Journal of Cyber Security and Mobility for the possibility to organize our Special Issue. In addition, we thanks the whole Journal team, internal and external reviewers for their excellent and tireless work. We sincerely thank all authors for the interesting papers! We hope that our Special Issue results make a significant contribution to the development of methods for information systems' quality and security.

References

[1] Hilgurt, S., Davydenko, A., Matovka, T., Prygara, M.: Tools for Analyzing Signature-based Hardware Solutions for Cyber Security Systems. Journal of Cyber Security and Mobility. 1–21 (2023).

[2] Hovorushchenko, T., Pavlova, O., Kostiuk, M.: Method of Increasing the Security of Smart Parking System. Journal of Cyber Security and Mobility. 1–15 (2023).

[3] Shepita, P., Tupychak, L., Shepita, J.: Analysis of Cyber Security Threats of the Printing Enterprise. Journal of Cyber Security and Mobility. 1–16 (2023).

[4] Sikora, L., Lysa, N., Tsikalo, Ye., Fedevych, O.: System-information and cognitive technologies of man-made infrastructure cyber security. Journal of Cyber Security and Mobility. 1–21 (2023).

[5] Pravorska, N.: Additional Detection of Clones Using Locally Sensitive Hashing. Journal of Cyber Security and Mobility. 1–21 (2023).

[6] Hovorushchenko, T., Hnatchuk, Ye., Osyadlyi, V., Kapustian, M., Boyarchuk, A.: Blockchain-Based Medical Decision Support System. Journal of Cyber Security and Mobility. 1–18 (2023).

[7] Gorev, V., Gusev, A., Korniienko, V., Shedlovska, Ya.: On the Use of the Kolmogorov–Wiener Filter for Heavy-Tail Process Prediction. Journal of Cyber Security and Mobility. 1–19 (2023).

[8] Salman, F.M., Taha, M. A.: Optimization of LEACH Protocol for WSNs in Terms of Energy Efficient and Network Lifetime. Journal of Cyber Security and Mobility. 1–15 (2023).

Biographies

Ivan Izonin is an Associate Professor at the Department of Artificial Intelligence of Lviv Polytechnic National University, Ukraine. He received his MSc degree in Computer science in 2011 and his MSc degree in Economic cybernetics in 2012. He received a Ph.D. in Artificial Intelligence in 2016. His main research interests are focused on computational intelligence, high-speed neural-like systems, non-iterative machine learning algorithms, and ensemble learning.

Tetiana Hovorushchenko is the Head of Computer Engineering and Information Systems Department of Khmelnytskyi National University, Ukraine. She received her MSc degree in Computer engineering in 2002. She received a Ph.D. in Information Technologies in 2007 and a Dr.Sc. in Information Technologies in 2018. Her main research interests are focused on medical decision support systems, software quality evaluation and assurance.

Peter Popov is an Associate Dean (International) at the School of Science & Technology, Department of Computer Science of City University of London, United Kingdom. He received his MSc degree in Computer engineering in 1982. He received a Ph.D. in Information Technologies in 1989. His main research interests are focused on software dependability.