Cyber Resilience in the Business Environment: Insights from AI-based Solutions and Data Protection Standards

Nemanja Zdravković[1], Miguel Ángel Conde[2], Sonsoles López-Pernas[3] and Ponnusamy Vijayakumar[4]

[1]Faculty of Information Technology, Belgrade Metropolitan University, Tadeuša Košćuška 63, Belgrade, 11000, Serbia
[2]University of León, Engineering School, Campus de Vegazana S/N, León, 24071, Spain
[3]University of Eastern Finland, Yliopistokatu-2, Joensuu, 80100, Finland
[4]SRM IST, ECE Department, Kattankulathur, Chennai, 603203, India

The main focus of the BISEC-2022 was cyber resilience. Participants had the opportunity to hear the latest information in the field of network infrastructure protection, protection standards in the business environment, blockchain technologies in the financial sector, but also in the machine learning sectors, especially in distributed machine learning – federated learning. The participants got to know each other and exchanged experiences about the latest advanced techniques for protecting critical infrastructure, as well as about the use of artificial intelligence in protecting critical infrastructure. There was also talk about Data Protection Standards in the RS and EU Laws related to data protection. The dean of the Faculty of Information Technology at Belgrade Metropolitan University, Prof. Dr. Miroslava Raspopović Milić, opened the conference and pointed out that new technologies and standards in data protection drive today's and future business environment. Lecturers from public and private institutions and Serbian politics and economy presented their current solutions and works that are current or will find their application in the future. The conference proceedings present a compilation of selected nine accepted articles and short papers at the conference out of 15 paper submissions received.

It was highlighted that the number of different exploitations over the Internet is growing year by year. Cybersecurity can therefore no longer be viewed in isolation from real-world security. Leading experts in the field of information security from the country and the region exchanged experiences related to the latest technologies and standards that are applied in practice when it comes to the protection and security of information and communication systems, especially in the field of blockchain technologies and federated machine learning. It was pointed out that it is of great importance to have a solid cooperation between the economy, the public sector and the academic community in the field of information security and communication systems.

The conference had two keynote talks. The first keynote was delivered by Professor Ponnusamy Vijayakumar from SRM IST University in India, who delivered the conference keynote on the topic "Federated Machine Learning and Blockchain." His insightful talk shed light on the challenges and opportunities of implementing federated machine learning with added security with blockchain. The keynote paper is part of these proceedings and it brings up important point on the merging of two novel distributed technologies.

The second keynote was delivered by Professor Slavko Gajin from the School of Electrical Engineering, University of Belgrade. In his paper, prof. Gajin presented a comprehensive method for entropy-based network traffic anomaly detection and classification that relies on flow data, both from a research and implementation aspects. Starting from the well-known entropy-based approach, the paper revealed the results of our methodic work in solving the main challenges in designing an efficient anomaly detection solution empowered with the original classification method.

Julijana Mirčevski presented the paped entitled "Security of financial software to support cryptocurrency trading", which focused on the use of different software tools necessary for financial institutions handling cryptocurrency trading.

Andreja Samčović presented the paper entitled "Methods of Monitoring and Collection of User Data on the Example of Facebook" giving a global overview on the tools and processes that are used every day to collect data on all platforms where the social networks are present. The paper focused on drawing the attention of users in all the ways in which the owners of the social networks monitor and record activities of the users.

Sara Nikolić's paper "A comparison on Hyperledger

BISEC'22: 13th International Conference on Business Information Security, December 03, 2022, Belgrade, Serbia
nemanja.zdravkovic@metropolitan.ac.rs (N. Zdravković); mcong@unileon.es (M. Á. Conde); sonsoles.lopez@uef.fi (S. López-Pernas); vijayakp@srmist.edu.in (P. Vijayakumar)
0000-0002-2631-6308 (N. Zdravković); 0000-0001-5881-7775 (M. Á. Conde); 0000-0002-9621-1392 (S. López-Pernas); 0000-0002-3929-8495 (P. Vijayakumar)

consensus mechanism security and their applications" analyzed the security properties of the most popular Hyperledger DLTs' consensus mechanisms, with an emphasis on security and computational complexity. The focus of the papers was on the similarities and differences between the DLTs, comparing them to Bitcoin's proof-of-work and Ethereum's proof-of-stake, with the goal to find the most and least secure.

Zlatogor Minchev presented the paper "Proactive Identification of Future Cyber Threats", which outlined a methodology for joint exploration of cyber threats, using both expert and machine intellect. A combined assessment was performed on the accomplished results with a simulated futuristic environment, adding human-in-the-loop biometric response.

Dušan Simjanović's paper "Cyber Security Criteria: Fuzzy AHP approach" presented two groups of criteria with a total of eight sub-criteria affecting cyber security, and their ranking using Fuzzy Analytical Hierarchy Process, in which data/password leaks, phishing detection and DoS attack detection were recognized as the most important sub-criteria.

Nemanja Veselinović presented the paper "Countering Cybersecurity Threats with AI", with an emphasis on the role of artificial intelligence in cyber attacks. The paper discussed the role of machine learning, as well as deep learning methods, highlighting the most useful methods in cybersecurity application.

Finally, Miloš Milašinović's paper "Data Protection Standards in the Business Environment" presented multiple security frameworks with an emphasis on legal and technical aspects, necessary for a company's compliance process with the GDPR. With regards to the necessary implementation of technological solutions, the paper presented several suggestions for the development of application support that could be applicable and in compliance with the GDPR.

Conclusion

We extend our gratitude to all of the authors who contributed with their research for these proceedings. We would also like to thank all the participants, attendees, and volunteers who made BISEC-2022 a successful and productive event. We hope that discussions, open dialogues, and identified issues and potential research topics will contribute to the advancement of the field of business data security, novel attack prevention and protection schemes, and cybersecurity overall.

Acknowledgment

The BISEC-2022 conference was cosponsored by the Ministry of Science, Technological Development, and Innovations of the Republic of Serbia. The conference organizers would like to acknowledge this support and partnership, which helped out in making the BISEC-2022 successful conference. During the preparation of the conference, a total of 15 paper submissions were received, while 9 articles and short papers were selected for this publication.