Security Issues in Predictive Maintenance Systems, IoT Systems and Microservice-based Software Architectures

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]Universidad de Salamanca, Escuela Politécnica Superior de Zamora – Av. de Requejo, 34, 49029 Zamora, Spain
[3]University of Eastern Finland, Yliopistokatu-2, Joensuu, 80100, Finland
[4]SRM IST, ECE Department, Kattankulathur, Chennai, 603203, India

The 15th International Conference on Business Information Security (BISEC 2024) was held on November 28–29, 2024, in Niš, Serbia, organized by Belgrade Metropolitan University. The conference continues its mission of bringing together researchers, practitioners, and professionals from academia, industry, and public administration to exchange ideas, present research results, and discuss the future directions of cybersecurity and information security.

This year's main conference theme, "Security in Predictive Maintenance Systems," addressed the rising need for robust, secure, and intelligent systems that support modern infrastructures. In this context, cybersecurity plays a central role in protecting data integrity, ensuring system reliability, and preserving trust across digital environments. The conference program reflects the growing interplay between technological innovation, human factors, and governance in secure systems design.

The conference had three keynote talks. The first keynote was delivered by Georgios Ntanis from the Centre for Research and Technology Hellas (CERTH), Hellenic Institute of Transport, in Greese, who delivered the conference keynote on the topic "Critical Infrastructure Security: An Extreme Learning Machine-Based Predictive Maintenance Approach". His talk discussed an innovative predictive maintenance framework using Extreme Learning Machines (ELM) tailored for critical infrastructure protection. The talk demonstrated how ELMs can reduce downtime and improve fault prediction accuracy in industrial environments.

The second keynote entitled "LSTM-RNN Method for Anomaly-Based Intrusion Detection in Network Security" was delivered by Professor Alexander Alexandrov from the Institute of Robotics at the Bulgarian Academy of Sciences in Sofia. His paper proposed an LSTM-RNN-based intrusion detection model capable of recognizing sophisticated network threats. The model showed promising results in detecting previously unseen anomalies, offering enhanced real-time security monitoring.

The third and final keynote was given by Professor Zlatogor Minchev from the Institute of ICT at the Bulgarian Academy of Sciences in Sofia. The keynote entitled "Future Media Security Transformation in the Age of Deepfakes and Generative AI" addressed media integrity challenges, with an analysis of the risks posed by deepfakes and generative AI. The speech outlined detection techniques and ethical frameworks to mitigate misinformation and synthetic media threats.

After the keynote speeches, a round table was held on the topic of future media and security issues in the age of AI, with four speakers: Prof. Dr. Nemanja Zdravković, Dean of the Faculty of Information Technology at Belgrade Metropolitan University, Serbia, Professor Zlatogor Minchev from the Bulgarian Academy of Sciences, Plamen Kolev executive director of HiLife Media in Bulgaria, and Dr. Emilija Radibratović from the Ministry of Information and Telecommunications in Serbia.

BISEC'2024: 15th International Conference on Business Information Security, November 28-29, 2024, Niš, Serbia
*Corresponding author.
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)

A total of 32 peer-reviewed papers were accepted for presentation, covering a broad spectrum of topics including, but not limited to:

- Anomaly detection in IoT networks using machine learning techniques,
- Blockchain and secure communication in satellite and distributed infrastructures,
- Microservices vulnerabilities and mitigation techniques for distributed architectures,
- Cybersecurity awareness in digital education and ESG-driven environments,
- Privacy and trust in social networking and cloud-based platforms,
- AI-driven diagnostics in healthcare and posture monitoring,
- Cyber-physical systems and risk prediction models for maintenance and resilience.

In addition, several papers explored digital transformation in higher education, focusing on the ethical, pedagogical, and operational implications of AI in e-learning, cybersecurity culture, and student digital well-being.

Conclusion

We extend our sincere gratitude to all authors for their contributions, to the Program Committee for their dedicated review work, and to the members of the Organizing Committee for successfully preparing this year's conference. We would also like to thank all the participants, attendees, and volunteers who made BISEC-2024 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-2024 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-2024 successful conference. During the preparation of the conference, a total of 32 paper submissions were received, while 22 articles and short papers were selected for this publication.