Security Issues in Robotic Platforms, Sensor Networks and Smart Cities

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-2023 were security issues and challenges and means to overcome them. Participants had the opportunity to hear the latest information in the field of security issues in robotics, wireless sensor networks (WSNs), Unmanned Aerial Vehicles (UAVs), as well as new lightweight blockchain-based solutions. The participants got to know each other and exchanged experiences about the latest advanced techniques for protecting robotic platforms, WNSs and web security. There was also talk about the security issues already identifies for future smart cities, and means of their mitigation. The President of Belgrade Metropolitan University, Prof. Dr. Dragan Domazet, opened the conference and pointed out that new methodologies, standards, and approaches in data protection, driven by disruptive technologies such as Web3, blockchain and smart devices are crucial to develop a better and safer future. Lecturers from both public and private institutions 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 24 paper submissions received.

The growing complexity of interconnected systems in WSNs, robotics, and web security has highlighted new vulnerabilities and potential exploits. Addressing these challenges requires a holistic approach, recognizing that cybersecurity cannot exist in isolation from broader security concerns. It was emphasized that the need for collaboration between industry, government sectors, and academia is a must in order to navigate the intricate landscape of cyber threats with the ultimate goal to mitigate them. A need exist for enhanced security measures, especially in light of emerging technologies like autonomous robotics and the evolving landscape of web-based threats. This underscores the critical role of adopting robust standards and technologies such as blockchain and advanced machine learning techniques to fortify our information and communication systems against ever-evolving cyber risks.

The conference had two keynote talks. The first keynote was delivered by Adrián Campazas-Vega from the Robotics Group from the Universitsy of León, in Spain who delivered the conference keynote on the topic "Cybersecurity Issues in Robotic Platforms" His talk discussed ongoing security challenges in commercial robots such as the popular Unitree A1. The goal of the talk was to identify vulnerabilities in such platforms in order to take into encourage other researchers or companies in the field to strengthen security protocols and standards for commercially available robots

The second keynote entitled "Future of Smart Cities Security Challenges – Proactive Modelling & Identification" was delivered by Professor Zlatogor Minchev from the Institute of ICT at the Bulgarian Academy of Sciences in Sofia. His paper was an outline to a comprehensive analytical intelligence framework (i-framework) for studying the problem of future smart city security challenges, adding a scenario-based proactive analysis, combined with system modelling and results hybrid multicriteria validation. The intelligent part comes from different AI models that are implemented in the process, giving supportive and generative added values.

Professor Miloš Kostić from The Faculty of Information Technology at Belgrade Metropolitan University presented the paper "Gamification as a Tool for Elevating Password Strength Awareness", which explred the concept of a two-dimensional game in which players face specific challenges aimed at replacing existing weak passwords with new, stronger ones, while avoiding the loss of access to various platforms.

The next paper, entitled "Secure Course Completion Credentialing Using Hyperledger Fabric" explored a so-

BISEC'23: 14th International Conference on Business Information Security, November 24, 2023, Niš, 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)

lution based on Hyperledger Fabric, for issuing and validating documents from Higher Education Institutions (HEIs), such as diplomas and diploma supplements. With a minimal needed number of functionalities, such as issuance and verification, the presented lightweight system can be deployed on a trustful environment, e. g. faculties from the same university, or a consortium of universities.

Yaina Pandith's paper explored deep blockchain architectures, involving the introduction of higher-layer blockchains, which summarize their blocks through anchor transactions integrated into the blocks of lower-layer blockchains. The advancements presented in this paper form a solid foundation for the development of scalable web applications. This research would enable further innovative solutions in various industries that can scale modern web applications successfully, ensuring unwavering data integrity, enhanced security, and optimized efficiency.

Professor Alexander Alexandrov from the Institute of Robotics, Bulgarian Academy of Sciences in Sofia presented two papers. The first paper, entitled "Energy-Efficient Routing in UAVs Supported Perimeter Security Networks" examined the integration of group of UAVs into perimeter security, evaluating their effectiveness, operational frameworks, technological advancements, and potential future developments. The paper analyzes and implemented a PSO (Particle Swarm Optimization) algorithm, related to group of UAVs trajectory optimization, review case studies, and identify key considerations for effective development. The second paper "Reducing the WSN's Communication Overhead by the SD-SPDZ Encryption Protocol" introduced a protocol which enhances the privacy-preserving attributes and efficiency of its predecessors. The presented SD-SPDZ protocol integrates advanced cryptographic techniques, offering a more robust and scalable solution for secure computations in WSNs.

The next paper, "The Interplay of Social and Robotics Theories in AGI Alignment: Navigating the Digital City Through Simulation-based Multi-Agent Systems" by Ljubiša Bojić and Vladimir Đapić delved into the task of aligning Artificial General Intelligence (AGI) and Large Language Models (LLMs) to societal and ethical norms by using theoretical frameworks derived from social science and robotics. This paper presented an innovative simulation-based approach, engaging autonomous so-called "digital citizens" within a multi-agent system simulation in a virtual city environment.

Finally, the paper "Data Protection Standards in the Business Environment" presented advanced security technologies and mechanisms which could be suitably employed within the Spring Framework for creating secure and scalable web applications. The analysis outlined advantages and challenges of each of the presented mechanisms, coupled with integration considerations, especially when complex business scenarios arise. Ultimately, this exploration was intended to enhance comprehension surrounding progressive security measures applicable to the Spring environment thereby equipping developers with improved capacity for constructing more resilient application solutions.

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-2023 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-2023 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-2023 successful conference. During the preparation of the conference, a total of 28 paper submissions were received, while 9 articles and short papers were selected for this publication.