electronics

MDPI

Editorial

Security and Privacy in Networks and Multimedia

Tomasz Rak * and Dariusz Rzonca

Department of Computer and Control Engineering, Rzeszow University of Technology, Powstancow Warszawy 12, 35-959 Rzeszow, Poland; drzonca@kia.prz.edu.pl
* Correspondence: trak@kia.prz.edu.pl

1. Introduction

The digital era has significantly transformed the dissemination of information and business operations, creating an intricate web of interconnected systems. As technology continues to advance, so do the complexities of maintaining robust security and privacy across these networks. This Special Issue, "Security and Privacy in Networks and Multimedia", seeks to explore the forefront of research in protecting data networks and multimedia systems against evolving security threats. The articles included in this issue highlight innovative solutions and ongoing research aimed at enhancing security and privacy in various technological environments.

2. Resilient Forecasting and Supply Chain Security

In the realm of smart cities, accurate electricity load forecasting is crucial for grid stability. Mohd Hafizuddin Bin Kamilin and Shingo Yamaguchi present a resilient forecasting network that uses a collective intelligence predictor to mitigate the impact of missing values induced by cyberattacks. This approach decentralizes forecasting processes, achieving remarkable accuracy even under significant data loss scenarios.

Helen C. Leligou and colleagues delve into cybersecurity within supply chain systems, specifically focusing on the farm-to-fork use case. Their FISHY platform integrates machine learning and blockchain technologies to detect security threats and provide evidence for mitigation policies. This innovative approach ensures comprehensive protection for complex supply chain networks.

3. Advanced Detection Methods and Network Privacy

Addressing the threat of jamming in next-generation communication systems, Cem Örnek and Mesut Kartal propose a jamming detection method leveraging the Error Vector Magnitude metric. This method enhances sensitivity and provides critical jammer frequency information, ensuring robust protection for 5G and LTE networks.

Marko Mićović, Uroš Radenković, and Pavle Vuletić explore Format-Preserving Encryption for network layer privacy protection. Their LISPP system, implemented on smart network interface cards, achieves high throughput with minimal delay, proving effective for production networks.

4. Intrusion Detection and AI-Enhanced Security

Hyeon gy Shon and colleagues introduce a semi-supervised alert filtering method for network security. By incorporating semi-supervised clustering, their approach significantly reduces false alerts, conserving resources and improving detection accuracy.

The integration of artificial intelligence in network security is exemplified by Latifah Almuqren and her team's Improved Sine Cosine Algorithm with Deep Learning-Enabled Security Solution (ISCA-DLESS). This method combines feature selection and hyperparameter tuning to enhance anomaly detection, achieving impressive accuracy on benchmark datasets.

check for updates

Citation: Rak, T.; Rzonca, D. Security and Privacy in Networks and Multimedia. *Electronics* **2024**, *13*, 2887. https://doi.org/10.3390/electronics13152887

Received: 17 July 2024
Accepted: 18 July 2024
Published: 23 July 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

5. Generative Approaches and Adversary Impact Mitigation

Hao Yang and co-authors tackle the class imbalance problem in Network Intrusion Detection Systems with their SPE-ACGAN method. This resampling approach improves detection performance across various classifiers, addressing the prevalent issue of imbalanced training samples.

Mohd Anjum and his team propose a Permutated Security Framework for IoT security, utilizing end-verifiable keys to manage transactions securely. Their approach adapts to system changes, mitigating adversary impact and service failures while enhancing transaction security.

6. Explainable Security Solutions and Advanced Cryptographic Techniques

Suleiman Y. Yerima and Abul Bashar focus on detecting evasive malicious PDF documents through explainable ensemble learning methods. Their system effectively detects hidden malicious content in PDFs, offering robust security against sophisticated attacks.

Maaz Ali Awan and colleagues discuss the potential of Radio Frequency Fingerprinting in enhancing the cybersecurity of smart grids. Their deployment framework leverages deep learning for effective classification and rogue device detection, bolstering smart grid security.

7. Network Layer Privacy and Anomaly Detection

Raad A. Muhajjar and his team present a hierarchical key management method for wireless sensor networks in medical environments. Their approach ensures data confidentiality and integrity, providing a secure framework for sensitive health data transmission.

Mohammad Jamoos and co-authors introduce a data-balancing approach based on Generative Adversarial Networks for network intrusion detection systems. Their model addresses imbalanced datasets, enhancing the detection rate of minority class attacks.

Saini and Islam focus on the security of the CAN bus, which is widely used in automotive applications. They propose a hardware prototype (FPGA) of an intrusion detection system for the CAN bus, enabling attack detection and response in case of bus-off attacks.

8. Conclusions

The articles in this Special Issue collectively advance the state of the art in network and multimedia security, offering innovative solutions to pressing challenges. From resilient forecasting networks and comprehensive supply chain security to advanced jamming detection and AI-enhanced anomaly detection, these studies contribute significantly to the ongoing efforts in securing our increasingly digital world.

Conflicts of Interest: The authors declare no conflicts of interest.

List of Contributions

1. Kamilin, M.H.B.; Yamaguchi, S. Resilient Electricity Load Forecasting Network with Collective Intelligence Predictor for Smart Cities. *Electronics* **2024**, *13*, 718. https://doi.org/10.3390/electronics13040718.
2. Leligou, H.C.; Lakka, A.; Karkazis, P.A.; Costa, J.P.; Tordera, E.M.; Santos, H.M.D.; Romero, A.A. Cybersecurity in Supply Chain Systems: The Farm-to-Fork Use Case. *Electronics* **2024**, *13*, 215. https://doi.org/10.3390/electronics13010215.
3. Örnek, C.; Kartal, M. Securing the Future: A Resourceful Jamming Detection Method Utilizing the EVM Metric for Next-Generation Communication Systems. *Electronics* **2023**, *12*, 4948. https://doi.org/10.3390/electronics12244948.
4. Mićović, M.; Radenković, U.; Vuletić, P. Network Layer Privacy Protection Using Format-Preserving Encryption. *Electronics* **2023**, *12*, 4800. https://doi.org/10.3390/electronics12234800.
5. Shon, H.G.; Lee, Y.; Yoon, M. Semi-Supervised Alert Filtering for Network Security. *Electronics* **2023**, *12*, 4755. https://doi.org/10.3390/electronics12234755.
6. Almuqren, L.; Maray, M.; Aljameel, S.S.; Allafi, R.; Alneil, A.A. Modeling of Improved Sine Cosine Algorithm with Optimal Deep Learning-Enabled Security Solution. *Electronics* **2023**, *12*, 4130. https://doi.org/10.3390/electronics12194130.

7. Yang, H.; Xu, J.; Xiao, Y.; Hu, L. SPE-ACGAN: A Resampling Approach for Class Imbalance Problem in Network Intrusion Detection Systems. *Electronics* **2023**, *12*, 3323. https://doi.org/10.3390/electronics12153323.
8. Anjum, M.; Shahab, S.; Yu, Y.; Guye, H.F. Identifying Adversary Impact Using End User Verifiable Key with Permutation Framework. *Electronics* **2023**, *12*, 1136. https://doi.org/10.3390/electronics12051136.
9. Yerima, S.Y.; Bashar, A. Explainable Ensemble Learning Based Detection of Evasive Malicious PDF Documents. *Electronics* **2023**, *12*, 3148. https://doi.org/10.3390/electronics12143148.
10. Awan, M.A.; Dalveren, Y.; Catak, F.O.; Kara, A. Deployment and Implementation Aspects of Radio Frequency Fingerprinting in Cybersecurity of Smart Grids. *Electronics* **2023**, *12*, 4914. https://doi.org/10.3390/electronics12244914.
11. Muhajjar, R.A.; Flayh, N.A.; Al-Zubaidie, M. A Perfect Security Key Management Method for Hierarchical Wireless Sensor Networks in Medical Environments. *Electronics* **2023**, *12*, 1011. https://doi.org/10.3390/electronics12041011.
12. Jamoos, M.; Mora, A.M.; AlKhanafseh, M.; Surakhi, O. A New Data-Balancing Approach Based on Generative Adversarial Network for Network Intrusion Detection System. *Electronics* **2023**, *12*, 2851. https://doi.org/10.3390/electronics12132851.
13. Saini, R.; Islam, R. Reconfigurable CAN Intrusion Detection and Response System. *Electronics* **2024**, *13*, 2672. https://doi.org/10.3390/electronics13132672.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.