Computer Modeling in
Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2024.058939

EDITORIAL

Introduction to the Special Issue on Advanced Security for Future Mobile Internet: A Key Challenge for the Digital Transformation

Ilsun You[1,*], Xiaofeng Chen[2], Vishal Sharma[3] and Gaurav Choudhary[4]

[1]Department of Financial Information Security, Kookmin University, Seoul-si, 02707, Republic of Korea

[2]School of Network and Information Security, Xidian University, Xi'an, 710071, China

[3]School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast (QUB), Belfast, BT7 1NN, UK

[4]Centre for Industrial Software (CIS), The Maersk Mc-Kinney Moller Institute, University of Southern Denmark, Sønderborg, 6400, Denmark

*Corresponding Author: Ilsun You. Email: isyou@kookmin.ac.kr

Received: 24 September 2024 Accepted: 26 September 2024 Published: 31 October 2024

Mobile internet technologies have transformed our daily lives, allowing us to connect, communicate, and access various services and applications anytime and anywhere. These technologies are set to play a significant role in the next generation of digital transformation, further increasing their impact by integrating with emerging technologies like 6G, quantum computing, and generative AI.

However, the increasing reliance on mobile internet technologies also brings significant security challenges. As mobile devices become central to both personal and professional activities, they become attractive targets for cyber threats. The convergence of advanced technologies introduces new vulnerabilities that can be exploited by malicious actors. For instance, with 6G's anticipated ultra-low latency and massive connectivity, the attack surface for potential cyber threats expands dramatically. Similarly, quantum computing can break existing encryption methods. Therefore, this brings a need for the development of quantum-resistant algorithms. Generative AI, while offering enhanced capabilities, may also be used to create sophisticated phishing attacks, malicious codes, or deepfake content that could affect users and bypass traditional security measures.

In this Special Section of the CMES Journal, 18 high-quality papers with rigorous reviews have been published. This section attracted top-quality papers from various researchers in future mobile internet security. With CMES Journal broad reach, we are optimistic that these articles will grab significant attention and popularity among researchers working in similar domains.

Malware detection in the context of future mobile internet security is becoming increasingly critical as mobile devices continue to be the primary gateway for digital interactions. The future of mobile internet, with advancements such as 6G, quantum computing, and the proliferation of IoT devices, will introduce both new opportunities and challenges for malware detection. Ban et al. [1] presented a study on the effectiveness of adversarial examples in Malware Detection. An et al. [2] proposed a new approach to counter cyberattacks using the increasingly diverse malware in cyber security. In this scheme, authors proposed a dual Siamese network-based detection framework that utilizes byte images converted from malware binary data to grayscale and opcode frequency-based images generated after extracting opcodes and converting them into 2-gram frequencies. Han et al. [3] introduced a machine-learning framework for analyzing network traffic in IoT security incidents.

Kim et al. [4] proposed a response strategy using a Reinforcement-Learning-based cyber-attack-defense simulation tool to address continuously evolving cyber threats.

For effective intrusion detection and anomaly detection, Kim and Kim [5] proposed a reconstruction error-based anomaly detection method using an autoencoder (AE) that utilizes packet metadata excluding specific node information. Furthermore, Kil et al. [6] focused on a memory-efficient intrusion detection approach incorporating multi-binary classifiers using optimal feature selection. Jeon et al. [7] examined methods for effectively utilizing machine learning-based malicious traffic detection approaches for lightweight devices. Furthermore, Jeon et al. [8] proposed an Internet of Wearable Things threat analysis framework (IWTW) framework that can derive security threats through systematic analysis of IoWT attack cases and possible security threats and perform cyber threat analysis based on them. Ji et al. [9] proposed an encrypted cyberattack detection system for IoT (ECDS-IoT), which derives valid features through statistical analysis of encrypted traffic and performs cyberattack detection in encrypted network traffic occurring in the IoT environment.

Network security is critical to securing communication and data integrity within any connected system, and its importance is magnified in the context of future mobile internet technologies. Hermosilla et al. [10] addressed the complex security challenges of 5G Networks by developing a dual-system model that integrates a proactive Network Application Validator with a Reactive, AI/ML-Driven Security System. Park et al. [11] presented a study on the investigation of Open-RAN specifications. Sánchez et al. [12] presented a probabilistic trust model and control algorithm designed to detect and mitigate malicious information injection attacks within edge computing environments. Cho et al. [13] proposed a novel system for encrypting personal information within the footage.

Furthermore, Chen et al. [14] proposed a low-energy data encryption (LEDE) method in which a modified version of AES and device system time are employed to enhance the security of the transmitted data and reduce the energy consumption of mobile devices. Park et al. [15] proposed a cross-domain bilateral access control protocol for blockchain-cloud-based data trading systems. Quantum-resistant encryption and cryptography for future mobile internet security grab significant attention. Jeon et al. [16] presented a new framework to construct quantum circuits of substitution boxes (S-boxes) using system modelling. Sarang et al. [17] focused on privacy and security concerns in Avtar and metaverse technologies. The authors determined the most significant threat for each component's cyberattacks that will affect user data and Avatars. ML and AI are poised to play a transformative role in advancing security for the future mobile internet, addressing the growing complexity and scale of threats in the digital landscape. Xu et al. [18] proposed the FedAdaSS algorithm, an adaptive parameter server selection mechanism designed to optimize the training efficiency in each round of FL training by selecting the most appropriate server as the parameter server.

Finally, we are pleased with the technical depth of this special section and believe that it will significantly contribute to the advancement of future mobile internet security. We also hope the research presented here will inspire further exploration and innovation in these focused areas. In conclusion, we sincerely thank all the authors for their high-quality contributions and the reviewers for their efforts in ensuring the quality of this special section. We also extend our thanks to the Editor-in-Chief and the dedicated staff members for their invaluable support and guidance.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare they have no conflicts of interest to report regarding the present study.

References

1. Ban Y, Kim M, Cho H. An empirical study on the effectiveness of adversarial examples in malware detection. Comput Model Engi Sci. 2024;139(3):3535–63. doi:10.32604/cmes.2023.046658.
2. An B, Yang J, Kim S, Kim T. Malware detection using dual siamese network model. Comput Model Eng Sci. 2024;141(1):563–84. doi:10.32604/cmes.2024.052403.
3. Han SJ, Yoon SS, Euom IC. The machine learning ensemble for analyzing internet of things networks: botnet detection and device identification. Comput Model Eng Sci. 2024:141(2):1495–1518. doi:10.32604/cmes.2024.053457.
4. Kim B-S, Suk H-W, Choi Y-H, Moon D-S, Kim M-S. Optimal cyber attack strategy using reinforcement learning based on common vulnerability scoring system. Comput Model Eng Sci. 2024;141(2):1551–1574. doi:10.32604/cmes.2024.052375.
5. Kim MG, Kim H. Anomaly detection in imbalanced encrypted traffic with few packet metadata-based feature extraction. Comput Model Eng Sci. 2024;141(1):1–607. doi:10.32604/cmes.2024.051221.
6. Kil Y, Jeon YR, Lee SJ, Lee IG. Multi-binary classifiers using optimal feature selection for memory-saving intrusion detection systems. Comput Model Eng Sci. 2024;141(2):1473–93. doi:10.32604/cmes.2024.052637.
7. Jeon S, Oh Y, Lee Y, Lee I. Suboptimal feature selection techniques for effective malicious traffic detection on lightweight devices. Comput Model Eng Sci. 2024;140(2):1669–87. doi:10.32604/cmes.2024.047239.
8. Jeon GH, Jin H, Lee JH, Jeon S, Seo JT. IWTW: a framework for IoWT cyber threat analysis. Comput Model Eng Sci. 2024;141(2):1575–622. doi:10.32604/cmes.2024.053465.
9. Ji IH, Lee JH, Jeon S, Seo JT. Encrypted cyberattack detection system over encrypted IoT traffic based on statistical intelligence. Comput Model Eng Sci. 2024;141(2):1519–49. doi:10.32604/cmes.2024.053437.
10. Hermosilla A, Gallego-Madrid J, Martinez-Julia P, Ortiz J, Kafle VP, Skarmeta A. Advancing 5G network applications lifecycle security: an ML-driven approach. Comput Model Eng Sci. 2024;141(2):1447–71. doi:10.32604/cmes.2024.053379.
11. Park H, Nguyen T-H, Park L. An investigation on open-RAN specifications: use cases, security threats, requirements, discussions. Comput Model Eng Sci. 2024;141(1):1–41. doi:10.32604/cmes.2024.052394.
12. Sánchez BB, Ramón A, Tomás R. A probabilistic trust model and control algorithm to protect 6G networks against malicious data injection attacks in edge computing environments. Comput Model Eng Sci. 2024;141(1):1–654. doi:10.32604/cmes.2024.050349.
13. Cho CH, Song HM, Youn T-Y. Practical privacy-preserving roi encryption system for surveillance videos supporting selective decryption. Comput Model Engi Sci. 2024;1–21. doi:10.32604/cmes.2024.053430.
14. Chen L, Tsai K, Leu F, Jiang W, Tseng S. Time parameter based low-energy data encryption method for mobile applications. Comput Model Eng Sci. 2024;140(3):2779–94. doi:10.32604/cmes.2024.052124.
15. Park Y, Shin SJ, Shin SU. Cross-domain bilateral access control on blockchain-cloud based data trading system. Comput Model Eng Sci. 2024;141(1):671–88. doi:10.32604/cmes.2024.052378.
16. Jeon Y, Baek S, Kim J. A novel framework to construct S-box quantum circuits using system modeling: application to 4-bit S-boxes. Comput Model Eng Sci. 2024;141(1):545–61. doi:10.32604/cmes.2024.052374.
17. Sarang AD, Alawami MA, Park K-W. MV-Honeypot: security threat analysis by deploying avatar as a honeypot in COTS metaverse platforms. Comput Model Eng Sci. 2024;141(1):655–69. doi:10.32604/cmes.2024.053434.
18. Xu Y, Zhao B, Zhou H, Su J. FedAdaSS: federated learning with adaptive parameter server selection based on elastic cloud resources. Comput Model Eng Sci. 2024;141(1):609–29. doi:10.32604/cmes.2024.053462.