Computer Modeling in Engineering & Sciences

Tech Science Press

Doi:10.32604/cmes.2025.074581

EDITORIAL

Introduction to the Special Issue on Emerging Technologies in Information Security

Jawad Ahmad[1], **Mujeeb Ur Rehman**[2,*] **and Wadii Boulila**[3]

[1]Cyber Security Center, Prince Mohammad Bin Fahd University, Alkhobar, 31952, Saudi Arabia
[2]School of Computer Science and Informatics, De Montfort University, Leicester, LE1 9BH, UK
[3]Robotics and Internet-of-Things Laboratory, Prince Sultan University, Riyadh, 12435, Saudi Arabia

*Corresponding Author: Mujeeb Ur Rehman. Email: mujeeb.rehman@dmu.ac.uk

Received: 14 October 2025; Accepted: 16 October 2025; Published: 26 November 2025

The recent years have witnessed unprecedented growth in digital infrastructure, driven by rapid advances in cloud computing, the Internet of Things (IoT), smart cities, healthcare informatics, and industrial automation. While these technologies have improved efficiency and connectivity, they have also created complex vulnerabilities that more sophisticated cyber adversaries can exploit. Cybersecurity is no longer a static domain but a constantly evolving field where threats such as ransomware, advanced persistent threats, and zero-day exploits demand adaptive, intelligent, and proactive responses. Emergent technologies such as artificial intelligence (AI), deep learning, distributed architectures, chaos theory, and post-quantum cryptography are transforming the way we conceptualise and implement information security. These approaches offer not only enhanced accuracy and robustness but also scalability, adaptability, and resilience across diverse, resource-limited environments. Consequently, the goal of this Special Issue on Emerging Technologies in Information Security is to compile innovative contributions that advance the boundaries of theory and practice in this swiftly evolving field.

We received submissions from around the world, and after a thorough peer-review process, 15 high-quality papers were accepted for publication. These studies provide new insights into AI-powered intrusion detection, resilient cryptographic solutions, network and cyber-physical system security, and challenges related to post-quantum security. In the following sections, we will highlight the accepted papers and discuss common research trends and lessons learned from this collection.

1 Artificial Intelligence and Machine Learning for Security

AI and ML are transforming cybersecurity by enabling automated threat detection, classification, and response at scales that traditional systems cannot match. A large proportion of accepted papers use AI techniques, showing its importance in modern security research.

- Alsoufi et al. [1] propose an anomaly-based intrusion detection model that combines sparse autoencoders with convolutional neural networks. Tested on the Bot-IoT dataset, their framework achieves nearly perfect detection accuracy while maintaining very low false positives, demonstrating how AI can overcome the limitations of traditional rule-based systems across diverse IoT environments.
- Latif et al. [2] introduce a hybrid model enhanced with oversampling that combines Vision Transformers (ViT) and one-dimensional CNNs for ransomware detection. By using SMOTE to address class imbalance, their model achieves 98% accuracy on the UNSW-NB15 dataset,

demonstrating that transformer-based architectures can complement CNNs for effective feature extraction.

- Martins et al. [3] improve semantic malware classification by dividing Portable Executable (PE) files, focusing on distinctive header features. Their deep learning method achieves 99.54% accuracy, demonstrating the potential of semantic segmentation to combat polymorphic malware variants.
- Al-Ghanem et al. [4] present MAD-ANET, an attention-based deep neural network designed for both binary and multi-class malware detection. Their model delivers excellent performance (99.5% binary accuracy and 97.9% multi-class accuracy) on the CIC-MalMem-2022 dataset while remaining lightweight enough for practical applications.
- Alshehri et al. [5] develop a hybrid Wasserstein GAN–GAN-autoencoder (WGAN-AE) intrusion detection framework tailored for IoT. The system attains high accuracy on large-scale datasets such as 5G-NIDD and IDSIoT2024, while operating with microsecond-level latency and minimal memory overhead, making it suitable for resource-constrained IoT deployments.
- Alassafi and Hasan [6] propose a dual-channel attention BiLSTM framework that not only achieves high detection accuracy (98.96%) but also includes a risk assessment module for prioritizing mitigation strategies. This combination of detection and proactive risk evaluation marks a step toward adaptive and self-healing security systems.

Collectively, these contributions reveal a clear trend: AI-driven security is shifting from basic detection to adaptive, context-aware, and lightweight solutions, making them more practical for real-world settings ranging from IoT devices to large-scale networks.

2 Cryptography, Encryption, and Data Protection

Alongside AI-driven analytics, cryptography remains the backbone of secure communications. This Special Issue features contributions that explore both traditional cryptography and emerging post-quantum methods.

- Li et al. [7] propose an image-hiding technique in the wavelet domain using dynamic region attention. The approach demonstrates resilience against noise, cropping, and compression attacks, ensuring that hidden images can be reliably retrieved even after substantial distortions. This has implications for secure multimedia communication and copyright protection.
- Alqahtani [8] introduces an AI-powered encryption scheme for medical images, utilizing convolutional autoencoders to compress high-resolution images into compact representations before executing a four-stage encryption process. This work illustrates how AI can improve both efficiency and robustness in protecting sensitive healthcare data.
- Usama et al. [9] introduce IDCE, a hybrid technique combining Huffman coding for compression with chaotic Tent and Arnold cat maps for encryption. Their findings demonstrate that IDCE provides strong confidentiality and high compression ratios, making it especially suitable for environments with limited bandwidth or storage.
- Medani et al. [10] enhance satellite image security by proposing a chaos-based encryption scheme that embeds encrypted watermarks before applying multiple chaotic encryption layers. By incorporating SHA-512 hashing and DNA encoding, their system ensures confidentiality, authenticity, and resistance against brute-force and statistical attacks.
- Asiri and Malwi [11] address the emerging challenge of post-quantum cryptography with a novel two-dimensional Trigonometric-Rational-Saturation (TRS) chaotic system. Combined with the NEQR model for quantum image representation, their scheme offers strong resistance to statistical and differential attacks while preserving high entropy and unpredictability.

Together, these contributions emphasize two trends: the combination of AI with cryptography for improved efficiency and security, and the rise of chaos-based and post-quantum methods that prepare us for future threats from quantum computing.

3 Networks, IoT, and Cyber-Physical Systems

As critical infrastructure becomes increasingly interconnected, safeguarding networks and cyber-physical systems becomes crucial. Several articles in this Special Issue explore innovative frameworks for adaptive, scalable, and resilient network security.

- Mehmood et al. [12] compare centralized, single-controller, and distributed multi-controller SDN architectures. Their results show that distributed SDN with the ISSLM algorithm significantly enhances throughput, bandwidth utilization, and latency, providing practical insights into secure and efficient data center management.
- Baccouri and Abdellatif [13] introduce BIG-ABAC, a big-data-driven attribute-based access control framework that provides response times in milliseconds while meeting HIPAA and GDPR standards. This demonstrates the viability of scalable, regulation-compliant access control systems in fields such as healthcare and smart cities.
- Khan et al. [14] develop a secure energy management system for smart communities that integrates LSTM forecasting, heuristic optimization, and secure peer-to-peer trading protocols. Their system reduces costs, improves efficiency, and maintains confidentiality, paving the way for sustainable, resilient smart grids.
- Zhukabayeva et al. [15] focus on wireless sensor networks (WSNs), proposing a graph-based and simulation-driven approach to detect anomalies and attacks such as wormhole intrusions. With precision and recall above 0.95, their method provides an effective solution for safeguarding smart city infrastructures and other sensor-rich environments.

These contributions focus on emerging security frameworks that are context-aware, regulation-compliant, and adaptive in real-time for IoT, SDN, and smart community infrastructures.

4 Concluding Remarks

The 15 contributions featured in this Special Issue showcase the various aspects of modern cybersecurity research. From lightweight AI models for IoT intrusion detection to chaos-based methods for post-quantum image encryption, these papers highlight the potential of emerging technologies to simultaneously improve security, scalability, and efficiency.

From this collection, three main insights can be drawn:

1. **AI-driven security dominates current research.**
   Most contributions in this Special Issue use AI and deep learning to improve malware detection, anomaly detection, and intrusion prevention. This shows the community's recognition of AI as a key part of modern cybersecurity. However, these approaches face challenges such as explainability, resistance to adversarial attacks, and energy efficiency that remain unresolved. Solving these issues will be essential for turning AI-driven models into trustworthy, real-world solutions.
2. **Cryptographic innovation is diversifying.**
   Classical encryption methods are being enhanced by chaos-based, AI-driven, and post-quantum techniques. This indicates a shift toward layered, hybrid security strategies that balance computational efficiency with resilience against emerging threats, such as quantum computing. Contributions in this issue highlight the potential of chaos theory to generate unpredictable, high-entropy keys and the role

of AI in improving the integration of compression and encryption. This diversity suggests that no single cryptographic approach will be enough; instead, multi-paradigm solutions will shape the future of security.

3. **System-level resilience is increasingly prioritised.**
   Several works emphasize the importance of scalability, compliance, and resilience at the network and system levels. Contributions on distributed SDN architectures, adaptive access control (BIG-ABAC), and secure smart grid management show that researchers are moving beyond algorithm-level improvements to develop comprehensive frameworks that operate reliably in complex infrastructures. This trend highlights a recognition that real-world cybersecurity solutions must address not only technical robustness but also regulatory compliance, interoperability, and user trust.

Looking ahead, future research must not only improve detection accuracy and encryption strength but also address the gap between experimental prototypes and real-world systems. Promising areas include lightweight AI for edge devices, post-quantum secure protocols, and explainable threat intelligence for critical infrastructure. We believe that this Special Issue will motivate further collaboration between academia and industry and will serve as a useful reference for researchers, practitioners, and policymakers working to develop secure and trustworthy digital ecosystems.

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

References

1. Alsoufi MA, Siraj MM, Ghaleb FA, Al-Razgan M, Al-Asaly MS, Alfakih T, et al. Anomaly-based intrusion detection model using deep learning for IoT networks. Comput Model Eng Sci. 2024;141(1):823–45. doi:10.32604/cmes.2024.052112.
2. Latif MA, Mushtaq Z, Rahman S, Arif S, Mursal SNF, Irfan M, et al. Oversampling-enhanced feature fusion-based hybrid ViT-1DCNN model for ransomware cyber attack detection. Comput Model Eng Sci. 2025;142(2):1667–95. doi:10.32604/cmes.2024.056850.
3. Martins E, Higuera JB, Sant'Ana R, Higuera JRB, Montalvo JAS, Castillo DP. Semantic malware classification using artificial intelligence techniques. Comput Model Eng Sci. 2025;142(3):3031–67. doi:10.32604/cmes.2025.061080.
4. Al-Ghanem WK, Qazi EUH, Zia T, Faheem MH, Imran M, Ahmad I. MAD-ANET: malware detection using attention-based deep neural networks. Comput Model Eng Sci. 2025;143(1):1009–27. doi:10.32604/cmes.2025.058352.
5. Alshehri MS, Saidani O, Malwi WA, Asiri F, Latif S, Khattak AA, et al. A hybrid wasserstein GAN and autoencoder model for robust intrusion detection in IoT. Comput Model Eng Sci. 2025;143(3):3899–920. doi:10.32604/cmes.2025.064874.
6. Alassafi MO, Hasan SH. Dual-channel attention deep bidirectional long short term memory for enhanced malware detection and risk mitigation. Comput Model Eng Sci. 2025;144(2):2627–45. doi:10.32604/cmes.2025.064926.
7. Li Z, Wu Y, Mazroa AA, Jiang D, Wu J, Zhu X. Image hiding with high robustness based on dynamic region attention in the wavelet domain. Comput Model Eng Sci. 2024;141(1):847–69. doi:10.32604/cmes.2024.051762.
8. Alqahtani F. AI-powered image security: utilizing autoencoders for advanced medical image encryption. Comput Model Eng Sci. 2024;141(2):1709–24. doi:10.32604/cmes.2024.054976.
9. Usama M, Aziz A, Alsuhibany SA, Hassan I, Yuldashev F. IDCE: integrated data compression and encryption for enhanced security and efficiency. Comput Model Eng Sci. 2025;143(1):1029–48. doi:10.32604/cmes.2025.061787.
10. Medani M, Said Y, Adnan Othman N, Yuldashev F, Kchaou M, Aldawood FK, et al. Chaos-based novel watermarked satellite image encryption scheme. Comput Model Eng Sci. 2025;143(1):1049–70. doi:10.32604/cmes.2025.063405.
11. Asiri F, Malwi WA. Enhancing post-quantum information security: a novel two-dimensional chaotic system for quantum image encryption. Comput Model Eng Sci. 2025;143(2):2053–77. doi:10.32604/cmes.2025.064348.

12. Mehmood KT, Atiq S, Sajjad IA, Hussain MM, Basit MMA. Examining the quality metrics of a communication network with distributed software-defined networking architecture. Comput Model Eng Sci. 2024;141(2):1673–708. doi:10.32604/cmes.2024.053903.
13. Baccouri S, Abdellatif T. BIG-ABAC: leveraging big data for adaptive, scalable, and context-aware access control. Comput Model Eng Sci. 2025;143(1):1071–93. doi:10.32604/cmes.2025.062902.
14. Khan M, Faisal M, Albogamy FR, Diyan M. Deep learning and heuristic optimization for secure and efficient energy management in smart communities. Comput Model Eng Sci. 2025;143(2):2027–52. doi:10.32604/cmes.2025.063764.
15. Zhukabayeva T, Desnitsky V, Abdildayeva A. Wireless sensor network modeling and analysis for attack detection. Comput Model Eng Sci. 2025;144(2):2591–625. doi:10.32604/cmes.2025.067142.