Computer Modeling in Engineering & Sciences

Tech Science Press

https://doi.org/10.32604/cmes.2026.083347

EDITORIAL

Introduction to the Special Issue on Machine learning and Blockchain for AIoT: Robustness, Privacy, Trust and Security

Ji Su Park[1,*], **Pan Yi**[2] **and Jong Hyuk (James) Park**[3]

[1]Department of Computer Science and Engineering, Jeonju University, Jeonju, Republic of Korea
[2]Department of Computer Science, Georgia State University, Atlanta, GA, USA
[3]Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul, Republic of Korea

*Corresponding Author: Ji Su Park. Email: jisupark@jj.ac.kr

Received: 02 April 2026; Accepted: 09 April 2026; Published: 27 May 2026

Artificial Intelligence of Things (AIoT) is considered a collaborative application of artificial intelligence (AI) and the Internet of Things (IoT). The AIoT system realizes real-time information acquisition through IoT sensors and performs intelligent data analysis tasks anywhere along the terminal-edge-cloud continuum, forming a smart and supportive ecosystem. However, AIoT systems face threats related to IoT data trust, system robustness, security, and privacy, making them susceptible to massive cyberattacks. This special issue on Machine Learning and Blockchain for AIoT was designed to showcase applications of machine learning and blockchain within the security domain of AIoT environments, as well as novel methodologies for addressing real-world challenges. The following summary synthesizes the key insights derived from these studies, highlighting their contributions to expanding both the theoretical horizons and practical applications of security within the AIoT landscape.

The paper by Alharbi et al. [1] proposes a routing framework for AIoT that combines AI-based Software-Defined Networking (SDN) with blockchain technology. This study focuses on establishing trust-based communication by integrating device behavior analysis with distributed ledger technology to address the security vulnerabilities and scalability issues inherent in existing IoT systems. The SDN controller gathers global network information to optimize decision-making, while the blockchain's Proof-of-Authority (PoA) consensus algorithm ensures data immutability and device authentication. Trust scores are calculated dynamically by comprehensively considering a node's forwarding reliability, blockchain-based records, and AI-derived anomaly scores. This multi-parameter approach contributes to blocking malicious nodes and selecting the optimal transmission paths for data delivery. Experimental results demonstrate that the proposed framework achieves significant improvements over existing technologies, reducing energy consumption by 48% and packet loss by 49%. Furthermore, it demonstrated its efficiency by recording improvements of 46% in response time and 45% in data transmission rate, respectively. Consequently, this system supports stable and lightweight computing in resource-constrained IoT environments while enhancing the quality of real-time services. Future research plans include integrating deep learning models to further bolster the security of large-scale systems.

The paper by Baek et al. [2] proposes HyMNeT—a hybrid intrusion detection system based on multivariate network traffic features—to address security vulnerabilities arising in 6G-based AIoT environments. HyMNeT employs Mutual Information Maximization (MIM) to select key features exhibiting high

correlation with labels, and applies the Maximal Information Coefficient (MIC) to eliminate redundancy among these features. Furthermore, it utilizes the Reference Vector Guided Evolutionary Algorithm (RVEA) to automatically derive the optimal combination of thresholds that maximizes MIM scores while minimizing MIC scores. The researchers constructed a set comprising just 11 core multivariate features by combining packet header information and statistical flow characteristics extracted from the BoT-IoT and ToN-IoT datasets. When this feature set was used to train four machine learning models (DT, GBM, XGBoost, and RF), the system achieved high average accuracy and precision scores exceeding 0.9844 on the BoT-IoT dataset. Notably, HyMNeT demonstrated consistent and robust detection performance across various attack types, despite utilizing a significantly smaller number of features compared to existing studies. In conclusion, this system enables efficient real-time intrusion detection in resource-constrained AIoT environments and suggests potential avenues for future expansion into lightweight, deep learning-based feature abstraction technologies.

The paper by Ullah et al. [3] proposes an innovative four-tier architecture—MBID (Multi-Tier Blockchain Intrusion Detection)—to address the security and scalability challenges inherent in large-scale IoT networks. This system comprises device, edge, fog, and cloud layers; specifically, the edge layer leverages Physics-Informed Neural Networks (PINNs) to detect anomalies in real time. Notably, by integrating domain knowledge into the detection process, the system achieves a high accuracy rate of 99.84% and an ultra-low latency of 0.40 ms. To mitigate bottlenecks within the blockchain network, the architecture incorporates Dynamic Sharding technology, enabling parallel processing capabilities. Furthermore, the system ensures both security and efficiency through a dual consensus mechanism, utilizing Honesty-based Distributed Proof-of-Authority (HDPoA) in the fog layer and DPoS in the cloud layer. Experimental results demonstrate a throughput of 214.57 TPS with a three-shard configuration, thereby validating a scalable pathway capable of accommodating millions of devices. In terms of storage efficiency, the system optimizes IPFS-based distributed storage, reducing blockchain storage requirements by over 80%. In conclusion, MBID implements Zero Trust principles within a decentralized framework, presenting a security solution optimally tailored for modern IoT networks.

The paper by Yu and Won [4] proposes a novel Port-based Pre-Authentication (PAPC) scheme that grants network access only after successful authentication, thereby facilitating the implementation of a Zero Trust security model. While existing methods—such as Port Knocking (PK) and Single Packet Authentication (SPA)—suffered from limitations such as the reliance on plaintext communication or the requirement for dedicated client software, the proposed approach overcomes these drawbacks by embedding encrypted data directly within the port number sequence itself, thereby supporting both protocol independence and a clientless environment. To enhance security, the system employs AES-128 encryption and HMAC-SHA256 for integrity verification, while utilizing nonces and timestamps to effectively mitigate replay attacks. Notably, the system incorporates a Temporary Key Management System (KMS); this mechanism generates and utilizes cryptographic keys exclusively during the authentication process, deleting them immediately thereafter to eliminate the long-term risks associated with key compromise. Furthermore, the system employs a signature-based avoidance algorithm that automatically steers clear of well-known or potentially hazardous port ranges, thereby preventing network conflicts. Experimental results, validated through a web-based prototype, demonstrated an unauthorized access detection performance (F1-score) exceeding 95% and confirmed the system's lightweight nature, proving its feasibility for deployment on resource-constrained AIoT devices. Consequently, this research holds significant value for presenting a highly interoperable security architecture that is readily applicable to future network ecosystems—including browser-based systems and AIoT environments.

The paper by Tan et al. [5] proposes a novel defense mechanism designed to counter backdoor attacks in a Federated Learning environment, wherein malicious participants embed hidden triggers into the model. While existing defense methods based on Differential Privacy (DP) effectively thwart such attacks, they suffer from a drawback: they significantly degrade the model's original performance (specifically, its accuracy on the main task). To address this issue, the researchers devised a two-stage defense framework that pre-filters models prior to aggregation, capitalizing on the observation that backdoor samples exhibit Out-of-Distribution (OOD) characteristics. In the first stage, an indicator task is utilized to identify and preemptively exclude model updates suspected of being infected with backdoors. By filtering out these contaminated models upfront, the framework is able to drastically reduce the amount of noise that must be injected during the second stage—the application of Differential Privacy. Experimental results using the CIFAR10 and FEMNIST datasets demonstrated that the proposed method exhibits superior defensive performance, suppressing backdoor accuracy to below 15%. Furthermore, unlike conventional defense techniques, it successfully maintained high accuracy on the main task by minimizing performance degradation caused by noise injection. In conclusion, this study effectively strikes a balance between security and practical performance in Federated Learning by integrating OOD detection with Differential Privacy.

The paper by Alahmari and Alkharashi [6] proposes a novel privacy-preserving Federated Learning framework—dubbed PEFLID-CSAAI—to address security and data privacy challenges within Internet of Things (IoT) environments. This technique prevents the exposure of sensitive information by training models locally on individual devices rather than transmitting data to a central server. The researchers enhanced system efficiency by optimizing data formats through the introduction of Z-score normalization during the data preprocessing stage, and by selecting only the most critical features using the Osprey Optimization Algorithm (OOA). A Self-Attention-based Variational Autoencoder (SA-VAE) was employed for intrusion detection and classification tasks, and the model's hyperparameters were fine-tuned using the Chameleon Swarm Algorithm (CSA) to achieve optimal performance. Experimental results utilizing the BoT-IoT dataset demonstrated that the proposed model achieved high accuracy rates of 97.38% in binary classification and 98.42% in multi-class classification. These figures attest to the model's superior performance across all metrics—including accuracy, precision, and F1-score—when compared against existing state-of-the-art models such as CNN-LSTM and RNN. In conclusion, this paper presents a robust security solution that is scalable even within resource-constrained IoT networks and capable of responding sensitively to dynamic threats. This framework is expected to hold significant practical value in real-world cybersecurity applications, particularly in sectors where security is paramount—such as medical devices and smart factories.

In the paper by Park and Lee [7], the Lightweight Multi-Key Secure Aggregation (LMSA) framework is proposed as an innovative federated learning system designed to reconcile real-time diagnostics with privacy preservation within resource-constrained medical AIoT environments. This framework delivers AES-256 level security with an O(n) complexity through a lightweight multi-key management scheme that combines Diffie-Hellman key exchange with SHA3-256 hashing; furthermore, it employs hardware-accelerated AES-CTR encryption and homomorphic MAC techniques to detect weight tampering in real time. In experiments utilizing the NIH Chest X-ray dataset—which evaluated various architectures including ViT, ResNet-50, and MobileNet—LMSA demonstrated that it maintains predictive accuracy comparable to centralized learning while incurring negligible memory overhead relative to model size. Consequently, LMSA provides a practical foundation for enabling secure and efficient collaborative learning among distributed healthcare institutions, allowing them to comply with strict regulations—such as HIPAA—at low computational and communication costs.

In the paper by Lo et al. [8], a novel dynamic trust evaluation framework is proposed to address the recent surge in IoT security threats, serving as an alternative to conventional static risk assessment models. This system combines **unsupervised learning (K-means clustering)** with decision tree algorithms to detect unknown attack patterns and precisely analyze the behavioral characteristics of devices. Furthermore, by integrating Zero-Knowledge Proofs and a Zero Trust architecture, the framework is designed to disallow any implicit trust between devices, mandating rigorous trust verification prior to any data exchange. Simulation results based on actual device interactions demonstrated high classification accuracy, achieving rates of 98.96% for normal behavior and 95.39% for anomalous behavior. Consequently, this framework offers an effective solution for establishing an adaptive security system within the complex and ever-evolving IoT landscape.

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

References

1. Alharbi M, Haseeb K, Humayun M. AI-driven SDN and blockchain-based routing framework for scalable and trustworthy AIoT networks. Comput Model Eng Sci. 2025;145(2):2601–16. doi:10.32604/cmes.2025.073039.
2. Baek S, Jeon J, Jeong B, Jeong Y. Hybrid meta-heuristic feature selection model for network traffic-based intrusion detection in AIoT. Comput Model Eng Sci. 2025;145(1):1213–36. doi:10.32604/cmes.2025.070679.
3. Ullah S, Wu J, Kamal MM, Mohamed HG, Sheraz M, Chuah TC. MBID: a scalable multi-tier blockchain architecture with physics-informed neural networks for intrusion detection in large-scale IoT networks. Comput Model Eng Sci. 2025;144(2):2647–81. doi:10.32604/cmes.2025.068849.
4. Yu S, Won Y. Port-based pre-authentication message transmission scheme. Comput Model Eng Sci. 2025;143(3):3943–80. doi:10.32604/cmes.2025.064997.
5. Tan Q, Li Y, Shin B. Defending against backdoor attacks in federated learning by using differential privacy and OOD data attributes. Comput Model Eng Sci. 2025;143(2):2417–28. doi:10.32604/cmes.2025.063811.
6. Alahmari S, Alkharashi A. Privacy-aware federated learning framework for IoT security using chameleon swarm optimization and self-attentive variational autoencoder. Comput Model Eng Sci. 2025;143(1):849–73. doi:10.32604/cmes.2025.062549.
7. Park H, Lee J. LMSA: a lightweight multi-key secure aggregation framework for privacy-preserving healthcare AIoT. Comput Model Eng Sci. 2025;143(1):827–47. doi:10.32604/cmes.2025.061178.
8. Lo N, Lin K, Chang C, Chang C, Tran L. Constructing a dynamic trust assessment mechanism combining zero knowledge proof with unsupervised learning. Comput Model Eng Sci. 2026. doi:10.32604/cmes.2026.077316.