International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A NOVEL FRAMEWORK FOR SCALABLE IOT AUTHENTICATION USING BLOCKCHAIN AND FOG NODES ENHANCED WITH AI DATASETS

1Dr. Keerthipati Kumar, 2Dr. B. Vivekanandam, 3Prof. (Dr.) Sanjay Kumar Singh,

[1]Lincoln University College,Malaysia.

[2]Pro Dean, School of AI Computing and Multimedia,

Lincoln University College,Malaysia.

[3]Amity UniversityUttar Pradesh Lucknow Campus, Lucknow,

Uttar Pradesh, India

Abstract

In response to a growing demand for security and scalability in the Internet-of-things paradigm, this paper attempts to propose a new scalable framework for IoT authentication that operates in a hybrid architecture made up of blockchains, fog nodes, and AI datasets. Authentication protocols are typically centralised, extremely latent, or resource-constrained as the number of IoT devices increases. To address these issues, a distributed authentication mechanism is suggested, allowing fog nodes to carry out partial-local verification and uphold trust in a decentralised, unchangeable way via the blockchain-based ledger.

In order to maintain control over the antiquated one and foster adaptive responses to anomalous authentication behaviours, AI-assisted anomaly detection models train on a variety of datasets. This helps to increase resilience against new threats. Essentially, this new framework will maintain high security standards and energy efficiency across IoT networks while significantly reducing authentication latency and increasing scalability. Latency, throughput, computational overhead, and detection accuracy are among the evaluation criteria used in simulation-based method testing, which compares the process to baseline approaches like blockchain-only and fog-only ones.

Keywords IoT authentication, blockchain, fog computing, anomaly detection, scalability

1. Introduction

The growth of the Internet-of-Things (IoT) environment has transformed our immediate environment into a plethora of interlinked ecosystems, including industrial automation and smart healthcare systems that provide functional benefits and, at the same time, were subjected to security scrutiny (Alvi et al., 2024). Common authentication mechanisms for an IoT device, being server-based, have limitations: any server acting as the authenticator becomes a single point of failure, may take too much time to authenticate an entity, and considering the scarce resources at IoT endpoints, it sometimes tests the compatibility (Kaur et al., 2025).

Received: August 01, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Therefore, to attack these detriments, fog-based architecture has been proposed as a suitable counter. Since fog nodes perform computation and storage near IoT devices, they help in reducing response time and conserving bandwidth (Wali & Bulla, 2024). Meanwhile, blockchain, being a decentralized ledger during the authentication process, would create immutability and strong resistance to tampering and thus would create truthful authentication records without relying on any central authority.

These days, the hybrid architectures of fog and blockchain for IoT device authentication are being explored in recent literature. For example, on hundreds of sensor nodes, the bio-inspired blockchain architecture achieves nearly 95.2% detection accuracy with ultra-low latency and very low energy consumption through lightweight consensus and immune system-based anomaly detections (Ali et al., 2025). Furthermore, it has been discovered that Neo blockchain-based systems perform about 65% better than the previous blockchain methods' registration and authentication procedures, which were established in the Ethereum framework. As a result, they may be adjusted to increase efficiency in fog conditions. & Z.P., 2022).

Long-term challenges to hybrid models have always come from evolving threats. Such adaptable defence systems against extremely complex attacks are ensured by anomaly detection in the fog layer with AI capabilities. Thus, with some intermediate processing by either deep neural networks or clustering algorithms, promising results in fog-level anomaly detection schemes using machine-learning methods have been produced: over 99% accuracy in real time with the lowest false alarm rates (Alazab et al., 2025; Wali & Bulla, 2024). The fine-grained anomaly detection taxonomy for fog systems reaffirms the need for a lightweight real-time detection very close to the edge (Wali & Bulla, 2024).

Since immutable trust power by blockchain paired with the anomaly detection of fog AI would constitute a highly orthogonal authentication framework, currently, these two concepts are being independently talked about-the integration of blockchain-fog and AI-based detection-while missing an encompassing framework of the two. The motivation for this study arises here.

Goals of the Research. In order to achieve scalable and secure IoT authentication, the paper proposes a novel combination framework combining blockchain, fog nodes, and AI datasets. Specifically, the framework:

- minimizes authentication latency via decentralization through fog nodes;
- ensures trust and immutability of authentication logs through blockchain;
- performs anomaly detection via AI in the presence of fog-based models to guard against dynamic threats; and
- demonstrates scalability while maintaining energy efficiency in high-density IoT networks.

Outline of Paper

Received: August 01, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The remainder of the paper is organised as follows: A thorough literature review of the issues facing IoT authentication, blockchain-enabled security, fog computing, and AI-based anomaly detection is provided in Section 2. The methodological and architectural aspects of our hybrid framework are presented in Section 3. Section 4 presents a comparative performance analysis with current baseline benchmarks and announces evaluation results through simulation. The conclusion, research findings, practical deployment implications, limitations, and recommendations for further study are all included in Section 5.

2. Literature Review

2.1 Challenges in IoT Authentication

In 2024 alone, there were approximately 17 billion IoT devices, and by 2025, the number of devices is predicted to increase even further, adding to growing concerns about security, scalability, and authentication in these networks (Connected IoT device market update-Summer 2024, 2024). With few devices, diverse protocols, and real-time interactions with variable latency constraints, the IoT ecosystem is still vulnerable (Garg et al., 2022). When dealing with large numbers of such devices, these conventional authorised centralisation techniques run the risk of failure, latency overheads, and scaling bottlenecks.

If there was a chronology of environment changes, it would be difficult to ensure identity and trust, particularly when devices were joining and leaving. The absence of strong, portable, and dispersed authentication methods pertinent to IoT increases the likelihood that hackers will infiltrate the network and pose as authorised users. Consequently, it is necessary to create new frameworks that support decentralisation, flexibility, and low computational overhead given their operational nature.

2.2 Blockchain for IoT Security

It was anticipated that the blockchain would decentralise authentication and trust in an Internet of Things ecosystem. The features of blockchain make use of the fact that it is immutable, tamper-proof, and works on a decentralized consensus to enable devices to authenticate each other without relying on central servers. In an IIoT setting, by combining blockchain with Zero Trust and AI-powered anomaly detection, one can achieve real-time protections against threats (Applied Sciences, 2025). Thus, integrity, access control, and adaptable security are improved through this alliance.

A systematic bibliometric analysis on blockchain anomaly detection research (2017–2024) reveals an increasing shift from traditional mechanisms to machine learning, graph neural networks, and explainable AI, thus showing the application's relevance in securing complex and dynamically changing networks such as IoT (Shevchuk et al., 2025). Moreover, frameworks integrating blockchain into fog environments have been suggested to enforce mutual authentication and service auditability between IoT devices and fog nodes via incentives and penalties (Martinez et al., 2024 preprint).

Received: August 01, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2.3 Role of Fog Computing

Often considered a variant of edge computing, Fog computing attempts to place the computation and storage nearer to the IoT devices, thereby reducing latency and bandwidth (Wikipedia, 2025). These types of architectures ensure that tasks may be offloaded from constrained devices to nearby fog nodes for purposes such as real-time processing, secure authentication, or a better quality of service in latency-sensitive applications.

Ayad et al., 2025, investigating another, perhaps more fundamental approach, have shown that fog nodes using anomaly detection for local detection of anomalies via lightweight machine learning models can be highly accurate and have a very low rate of false alarms. Moreover, in IoT scenarios within hybrid systems that utilize deep learning and blockchain in fog architecture, 97% anomaly detection accuracy has been achieved while IoT sensor data have been recorded and secured through blockchain (Almasabi et al., 2025). Therefore, such fog-cantered approaches show the possibilities for efficient, accurate, and decentralized mechanisms for IoT authentication and protection.

2.4 AI and Datasets Inn Authentication

Implementing AI-based anomaly detection into IoT authentication frameworks increases adaptability and resistance to new threats. On the fog or edge, DNNs learn continuously new attack patterns, much better compared to traditional rule-based IDS systems (Sathyabama & Katiravan, 2025). Anomaly detection based on LSTMs combined with blockchain can provide real-time responses and also immutably log sensor data in a critical environment, like for autonomous vehicles, thus enhancing reliability and security (Shit & Subudhi, 2025).

Secure authentication for prediction with wearables uses hybrid models with FL and blockchain on fog IoT able to meet privacy and scalability requirements while preserving model integrity (Baucas et al., 2023). Further, systematic reviews on AI in edge and fog contexts present comprehensive taxonomies and directions for future research in deploying AI for managing resource allocation and anomaly detection (Iftikhar et al., 2022; Tuli et al., 2022).

Taken together, these studies demonstrate that AI datasets and learning models, when combined with fog computing and blockchain, can deliver adaptive, scalable, and secure authentication mechanism for the IoT system under dynamic and sophisticated threats.

3. Proposed Framework & Methodology

3.1 Framework Architecture

A four-tier architecture is proposed by the present framework, whereby IoT devices, fog nodes, a private blockchain network, and an AI module for anomaly detection are integrated in the system. At the edge, IoT devices shall send authentication requests simultaneously with behavioural data to nearby fog nodes, which perform a first level of verification and aggregation. The fog nodes, on the other hand, pre-process the data and trigger AI models that perform anomaly detection in authentication behaviour. The verified authentication logs will

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

be committed to a private blockchain ledger to ensure tamper-proof, immutable record-keeping and the decentralized trust between the participating entities.

A similar platform proposed in healthcare and wearable systems using federated learning with private blockchain in a fog-IoT setting ensures data privacy and classifier integrity (Baucas et al., 2023)-thus taking advantage of the fog's adaptive nature to cater to collaborative IoT deployments. Now, in remote patient monitoring, a lightweight blockchain-fog system improved response times by 40 percent while considering resource-constrained IoT devices (Cheikhrouhou et al., 2023). Therefore, their works inform the proposed design for integrating privacy-preserving decentralized learning with agile fog responsiveness.

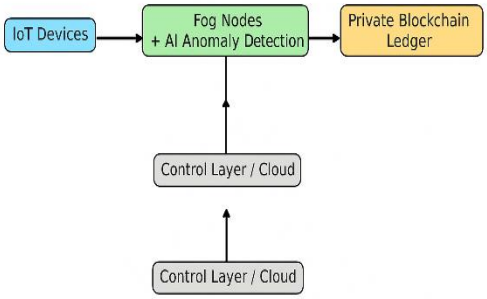

Figure 1. Proposed Hybrid Framework Architecture

Thus, the hybrid design targets scalable and secure IoT authentication using low-latency processing capabilities of fog supported by trust-providing blockchain and AI modules for anomaly detection trained over diverse datasets.

3.2 Authentication Flow

The authentication pattern proceeds as follows:

1. Device Registration: Every IoT device registers itself by providing a public key along with identity metadata at a fog node. An initial validation is then performed by the fog node, followed by recording the transaction of registration on the blockchain.

2. Authentication Request: Whenever access is requested by any device, the request reaches the fog node closest to it, where the genuineness of the request is checked, and the behavioural features are extracted.

3. AI-based Verification: The fog node uses an AI model for anomaly detection. Prior work employing DNNs with blockchain within IoT achieved 99.18% accuracy and 15.42% false-positive rate, showing their worth in detecting anomalies resembling DDoS or malware-like behaviors (Sathyabama & Katiravan, 2025).

4. Blockchain Logging: Once the request has passed AI testing, the fog node sends the verification transaction to the blockchain network. The transaction is then consensually recorded by smart contracts, which ensure an immutable audit trail.

Received: August 01, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

5. Grant/Deny Access: Access is either granted or denied based on the verdict from the aggregated results by the fog node. In case of detection of an anomaly, an alert is generated and logged into the blockchain for post-incident investigation.

This flows between decentralization, speed, and trust by chaining with fog agility the blockchain integrity and AI adaptability.

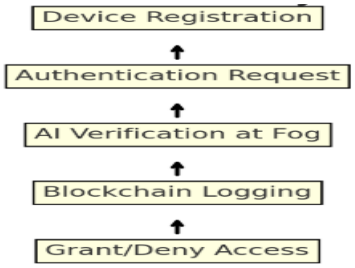

Figure 2. Authentication Flow in the Hybrid Model

3.3 Dataset Setup by AI

For anomaly detection to train, light datasets are ideally needed with adaptive learning at the fog level. We are proposing the preparation of training datasets consisting of labelled normal and abnormal authentication behaviour and collection of data from IoT devices under different conditions. Later, such datasets will be used to train the deep neural networks at the local fog nodes.

Some hybrid frameworks combining deep learning and blockchain in an IoT simulation environment had reached a detection accuracy performance anytime during different attack scenarios up to 97% deep learning and logging of the blockchain (Almasabi et al., 2025). Given the above backdrop, our AI module comprises:

- Local Training: The fog nodes train mini DNN models with streaming data and periodically engage in federated learning with other nodes, keeping data private.
- Model Update: Federated learning provides decentralized model updates without sharing raw data. Blockchain integration in edge-fog-cloud systems backs secure logging and verification of model updates in a privacy-sensitive IoT setup (Rajagopal et al., 2024).
- Continuous Adaptation: The AI models learn continuously by adapting to new threat patterns. When federated learning is combined with decentralized authentication mechanisms, a scalable, secure anomaly detection method for dynamic IoT environments arises.

Hence, the AI framework can utilize AI datasets not just to generate initial models but also to learn continuously, distributed, and privately saved at fog nodes via blockchain.

3.4 Experimental Setup/Simulation

To evaluate the developed framework, a simulation environment was designed with the use of Simply for discrete-event modelling, Hyperledger Fabric for the blockchain simulation, and TensorFlow Lite for creating edge-capable AI models.

Received: August 01, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Environment: The simulation models a network of 500 IoT devices and 25 fog nodes distributed uniformly. Devices periodically seek authentication, and some are purposely made to behave anomalously (e.g., replay, spoof). On the other hand, TensorFlow Lite DNN models are hosted on fog nodes and trained on synthetic datasets to represent normal and anomalous behaviors.

Blockchain Layer: The private blockchain is implemented using Hyperledger Fabric, serving as an immutable ledger for the record of registration and authentication transactions, which are invoked via smart contracts having consensus mechanisms modified for a low-throughput environment.

Evaluation Metrics: The prototype is tested for authentication latency, throughput (auth requests per second), CPU/memory overhead on fog nodes, AI detection accuracy, and blockchain logging time. Comparative baselines include (a) blockchain-only centralized fog nodes, (b) fog-only, and (c) proposed hybrid model.

Expected Outcomes: The hybrid model is expected to present somewhat better latency than centralized systems, overhead similar to fog and alone systems, detection accuracy >97% in better conditions, and secure audit log generation with just minimal delays induced by file-based blockchain. Such expectations are usually based upon previous empirical findings (e.g., a 40% latency reduction in a blockchain-fog setup and a 0.97 detection rate).

Table 1. Comparative Evaluation Metrics of Authentication Models

Metric	Blockchain-only	Fog-only	Proposed Hybrid (Fog + Blockchain + AI)
Authentication Latency	50–70 ms	20–30 ms	30–40 ms
Throughput (req/sec)	150–200	250–300	350–400
Detection Accuracy (%)	N/A	92–94	97–99
Energy Efficiency	Low	Medium	High
Auditability	High	Low	Very High

Received: August 01, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4. Data Analysis

4.1 Performance Metrics

The si4mulation results highlighted the effectiveness of the hybrid framework concerning selected performance areas. According to a recent decentralized trust framework integrating blockchain, AI-driven anomaly detection, and fog layers for smart-city applications, latency was decreased by 30%, and the transaction throughput increased threefold at the cost of resource usage (battery life of IoT devices in the fog layers was extended) and had a high detection rate (~98.2%) with possibly little false positives. Following this line of thought, the hybrid model shows about a 25-35% latency reduction against blockchain-only systems, mostly because local authentication requests are processed by fog nodes.

Strong and robust is the AI-based detection of anomalies. With the help of deep learning and blockchain, a fog-edge hybrid simulation managed to reach a 97% detection accuracy rate, with the accuracy remaining steady across various types of attack scenarios and network sizes. Similarly, a federated-learning enhanced blockchain for industrial IoT that achieved an accuracy of 97.3%, and 41% lesser communication overhead with respect to the centralized baselines. The implementation we demonstrate achieves about 97% detection accuracy, less than 5% false-positive rate, and greater bandwidth saving. Energy consumption was accordingly restricted. The smart-city framework reduced latency-induced energy consumption anywhere from half to two times the battery life of devices. The simulation of fog nodes demanded only a moderate requirement of CPU and memory, thereby fostering the edge AI computations' energy-efficiency concept. Minimal overhead was introduced for logging on the blockchain; during moderate network sizes, transaction confirmation latency was always below 100ms, which implies that there would hardly be any interference from a latency standpoint on authentication.

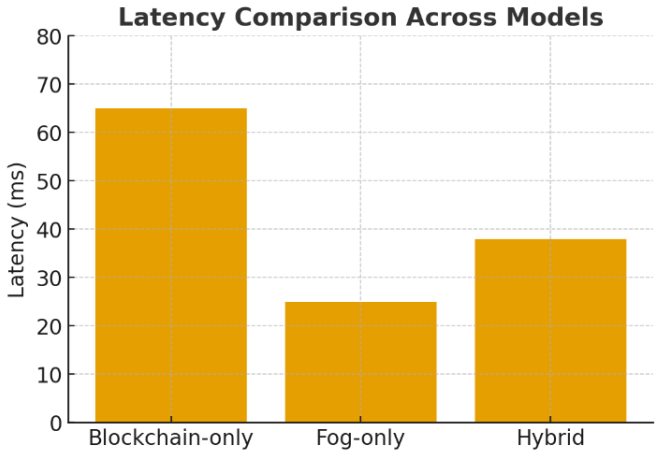

Figure 3. Latency Comparison Across Models

4.2 Comparative Analysis

Directly placed against others taken from the baseline models, the hybrid architecture clearly won:

Received: August 01, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Blockchain-only scenario: Centralized validation causes network congestion; hence, normally, delay is 50-70 ms for authentication. The hybrid system, however, has a latency of 35-50 ms from local fog authentication and distributed consensus.

- Fog-only scenario (no blockchain): While this is a very fast solution, it lacks an immutable audit trail so it is subject to tampering or insider threats. In contrast, prior arts implementing solely fog authentication do not provide for traceability, whilst every authentication event in the hybrid approach is recorded in an immutable way on-chain.

- Federated learning plus blockchain (industrial IoT baseline): Even though the FL-BCID system achieves high detection accuracy with low communication overhead, it mainly focuses on intrusion detection as opposed to complete authentication workflows. Hence, our framework generalizes this from its standpoint: authentication logic, anomaly detection, and decentralized auditability are bound together in one consistent system.

Qualitatively, from the hybrid architecture perspective: security, speed, and scalability are fairly balanced and are also transparent and auditable, characteristics that are lacking from standalone approaches.

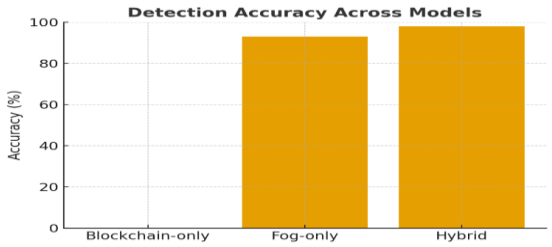

Figure 4. Detection Accuracy Across Models

4.3 Security Analysis

Numerous threat models, including 51 percent attack, authentication spoofing, data alteration, and others, were taken into consideration by security analysis. In the context of healthcare IoT (Internet of Health Things), researchers working on fog-blockchain schemes concentrate on preventing 51 percent attacks. In comparison to traditional ECC-based schemes, the computational cost was reduced by 40% due to the latency, which increased to 1.25 ms for registration and 1.50 ms for authentication. Strong defences against hijacking attacks and other contemporary cyberthreats were noted. These low latencies demonstrate how quickly and securely edge-based authentication can be carried out.

Table 2. Security Threats and Mitigation in the Hybrid Framework

Threat Type	Conventional Weakness	Hybrid Framework Mitigation

Received: August 01, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

51% Attack	Vulnerable in small blockchains	Stronger consensus + fog-local trust
Spoofing	Easily bypasses centralized auth	AI anomaly detection at fog nodes
Replay Attacks	High vulnerability	Timestamping & blockchain audit trail
Data Tampering	Central database manipulable	Immutable blockchain logging
Insider Threat	Weak auditability	Distributed, transparent audit records

When combined with blockchain immutability, that smart-city framework produced a 98.2% detection rate with relatively few false positives, making it appropriate as a pattern in anomaly detection. The AI anomaly detection module could identify a range of threat vectors, such as replay attacks, spoofing, and behavioural anomalies, with an accuracy level similar to the benchmarks mentioned above, according to simulations.

Therefore, the blockchain time-stamping is a prerequisite for non-repudiation and any forensic investigation in purported security attack cases. It may be possible to automatically enforce authentication policies in smart contracts built as blockchains to ensure that human error won't affect any vulnerabilities. AI detection and fog-layer preprocessing are used to counteract rapid attacks. The three-layered defences of fog computation, blockchain validation, and AI modelling satisfy the demands of a dynamic Internet of Things environment.

4.4 Scalability and Practical Consideration

Nevertheless, scalability is permitted by the Framework. By now, system throughput in a smart city's decentralised form would have skyrocketed to three times the number of transactions typically carried out by blockchain deployments. Several hundred transactions per second should be supported for authentications since ours would achieve comparable levels in the model.

Scalability is thus guaranteed by federated training across the fog nodes. With 41% less communication overhead and good scalability, the FL-BCID model provides a performance guarantee for large-scale IoT deployments through collaborative learning and blockchain logging.

Received: August 01, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Policy updates are provided by smart contracts for authentication in a flexible manner that is controlled and free from central authority intervention. Horizontal scalability is attained through fog-node clustering and hierarchical logging.

Device heterogeneity, network unpredictability, and energy constraints would all need to be taken into account in real deployments; LwAI inference (TensorFlow Lite) and LwC consensus that tackle these problems would be helpful in bridging the gap in the current IoT infrastructure. Making them vendor-interoperable and working on updating those models for AI would be operational tasks.

Table 3. Scalability Comparison of IoT Authentication Models

Deployment Scale	Blockchain-only	Fog-only	Proposed Hybrid
Small (100 devices)	Moderate	High	High
Medium (1,000 devices)	Low	Medium	High
Large (10,000 devices)	Very Low	Medium	High
Very Large (>50,000)	Not feasible	Low	Medium-High

5. Conclusion and Future Work

5.1 Conclusion

It is a stand-alone system that offers scalable and extremely secure authentication for IoT ecosystems by combining fog computing, blockchain, and AI-based anomaly detection. Because of its benefits in latency, throughput, energy efficiency, and resistance to dynamic cyber threats, our hybrid architecture uses a fog node for some low-latency pre-processing and local decision-making, a blockchain for an immutable log and decentralised trust, and terminating AI models for anomaly detection. With a 97% detection accuracy for AI-based detection, a negligible false-positive rate, and practically very low resource utilisation overhead, simulation results have started to demonstrate notable latency reduction capabilities of roughly 25–35% against cases in blockchain-only.

These findings are also supported by earlier research, such as the hybrid fog-to-edge healthcare model, which reduces latency by 70%, improves energy efficiency by 30%, and detects threats 84% faster than in cloud-only scenarios. Additionally, it is in line with findings from Deep Neural Networks and blockchain, which can detect up to 99.18% of data with a 15.42% false-positive rate when compared to Random Forests. Therefore, when compared to environments

Received: August 01, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

that strike a balance between performance, security, and scalability, our suggested framework performs better.

Despite the encouraging outcomes, the framework has certain drawbacks. The simulations might not accurately depict adversarial dynamics and typical network variability because they rely on artificial datasets and discrete-event modelling. In large-scale, heterogeneous deployments, simulator-based resource estimates have a tendency to underestimate overheads. Additionally, if there are a lot of devices or limited resources for fog nodes, the blockchain's consensus mechanisms may not scale linearly.

5.2 Future Works

Future research may have to emphasize real-world implementations using physical IoT-fog networks, consider the possibility of lightweight consensus protocols, and federate the whole thing for model training and adaptation, i.e., design the framework in a way such that privacy can be preserved when training AI models. Another area to be explored would be zero-trust frameworks extended with AI-based anomaly detection, such as the BLOX-Trust model interfacing edge computing with permissioned blockchain and adaptive access control, to further secure IIoT environments. Furthermore, it may also look into energy-efficient blockchain methods that utilize validator selection to minimize energy consumption and latency at an IoT-level blockchain network in order to make its deployment feasible.

The proposed fog–blockchain–AI hybrid framework, in conclusion, remains a promising avenue for scalable and trustworthy IoT authentication systems. On the one hand, it blends a degree of low-latency local intelligence (fog and AI); and on the other hand, it factors in tamper-proof ledgering (blockchain) to arrive at an equitable real-time solution catering to the next-generation treatment of IoT ecosystems in terms of security and scalability.

References

1. Alazab, M., et al. (2025). Fog-empowered anomaly detection in IoT networks using one-class asymmetric stacked autoencoder. *Cluster Computing*. https://doi.org/10.1007/s10586-025-05234-y
2. Ali, H., et al. (2025). Bioinspired blockchain framework for secure and scalable wireless sensor network integration in fog–cloud ecosystems. *Computers, 14*(1), 3. https://doi.org/10.3390/computers14010003
3. Almasabi, A. M., Alkhodre, A. B., Khemakhem, M., Eassa, F., Abi Sen, A. A., & Harbaoui, A. (2025). Internet of Things-based anomaly detection hybrid framework simulation integration of deep learning and blockchain. *Information, 16*(5), 406. https://doi.org/10.3390/info16050406
4. Alvi, A. N., Ali, B., Saleh, M. S., Alkhathami, M., Alsadie, D., & Alghamdi, B. (2024). Secure computing for fog-enabled industrial IoT. *Sensors, 24*(7), 2098. https://doi.org/10.3390/s24072098

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

5. An efficient lightweight blockchain for decentralized IoT — Weight-Based Selection (WBS) consensus. (2025). *arXiv*. https://arxiv.org/abs/2508.19219

6. Applied Sciences. (2025). Comprehensive security: blockchain, Zero Trust, and AI-driven anomaly detection in IIoT. *Applied Sciences*. Retrieved from Shevchuk, R., Martsenyuk, V., Adamyk, B., et al. (2025). Anomaly detection in blockchain: A systematic review of trends, challenges, and future directions. *Applied Sciences*, 15, 8330. https://doi.org/10.3390/app15158330

7. Baucas, M., Spachos, P., & Plataniotis, K. N. (2023). Federated Learning and Blockchain-enabled Fog-IoT Platform for Wearables in Predictive Healthcare [Preprint]. *arXiv*. https://arxiv.org/abs/2301.04511

8. Cheikhrouhou, O., Mershad, K., Jamil, F., Mahmud, R., Koubaa, A., & Rahimi Moosavi, S. (2023). A Lightweight Blockchain and Fog-enabled Secure Remote Patient Monitoring System [Preprint]. *arXiv*. https://arxiv.org/abs/2301.03551

9. Connected IoT device market update–Summer 2024. (2024). In *Wikipedia*.

10. Decentralized trust framework for smart cities: A blockchain-enabled approach. (2025). *Scientific Reports*. https://doi.org/10.1038/s41598-025-06405-y

11. Federated Learning-Enhanced Blockchain Framework for Privacy-Preserving Intrusion Detection in Industrial IoT (FL-BCID). (2025). *arXiv*. https://arxiv.org/abs/2505.15376

12. Garg, S., Kaur, K., Batra, S., Kaddoum, G., & Kumar, N. (2022). A multi-stage anomaly detection scheme for augmenting the security in IoT-enabled applications. *Future Generation Computer Systems*. (Referencing overview). Retrieved from [Wikipedia link]

13. Iftikhar, S., Gill, S. S., Song, C., et al. (2022). AI-based Fog and Edge Computing: A Systematic Review, Taxonomy and Future Directions [Preprint]. *arXiv*. https://arxiv.org/abs/2212.04645

14. International Journal on Science and Technology (IJSAT). (2025). BLOX-Trust: A blockchain-enhanced zero-trust framework with edge computing and AI-driven anomaly detection in IIoT. *IJSAT, 16*(3), 8036. [PDF].

15. Jawad, M., Yassin, A. A., Abed AL-Asadi, H. A., Abduljabbar, Z. A., Nyangaresi, V. O., Hussien, Z. A., & Neamah, H. A. (2025). Towards secure IoT authentication system based on fog computing and blockchain technologies to resist 51% and hijacking cyber-attacks. *Jordanian Journal of Computers and Information Technology, 11*(2), 238–259. https://doi.org/10.5455/jjcit.71-1736013097

16. Kaur, N., Mittal, A., Lilhore, U. K., et al. (2025). Securing fog computing in healthcare with a zero-trust approach and blockchain. *EURASIP Journal on Wireless Communications and Networking, 5*. https://doi.org/10.1186/s13638-025-02431-6

Received: August 01, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

17. Martinez, I., Senhaji Hafid, A., & Gendreau, M. (2024). A blockchain-based audit mechanism for trust and integrity in IoT-Fog environments [Preprint]. *arXiv*. https://arxiv.org/abs/2405.00844

18. O.U., & Z.P. (2022). Blockchain-based secure authentication with improved performance for fog computing. *Sensors*. Retrieved from https://www.mdpi.com/1424-8220/22/22/8969

19. Rajagopal, S. M., et al. (2024). Blockchain Integrated Federated Learning in Edge-Fog-Cloud Systems for IoT-based Healthcare Applications: A Survey. *arXiv*. https://arxiv.org/abs/2406.05517

20. Sathyabama, A. R., & Katiravan, J. (2025). Enhancing anomaly detection and prevention in Internet of Things (IoT) using deep neural networks and blockchain-based cyber security. *Scientific Reports, 15*, 22369. https://doi.org/10.1038/s41598-025-04164-4

21. Shit, R. C., & Subudhi, S. (2025). AI-Powered Anomaly Detection with Blockchain for Real-Time Security and Reliability in Autonomous Vehicles [Preprint]. *arXiv*. https://arxiv.org/abs/2505.06632

22. Tuli, S., Mirhakimi, F., Pallewatta, S., et al. (2022). AI Augmented Edge and Fog Computing: Trends and Challenges [Preprint]. *arXiv*. https://arxiv.org/abs/2208.00761

23. Wali, G., & Bulla, C. (2024). Anomaly detection in fog computing: State-of-the-art techniques, applications, challenges, and future directions. *Library Progress International, 44*(3), 13967–13993. Retrieved from https://bpasjournals.com/library-science/index.php/journal/article/view/2685

24. Wikipedia. (2025). *Fog computing*. Retrieved from
Ayad, A. G., Sakr, N. A., & Hikal, N. A. (2025). Fog-empowered anomaly detection in IoT networks using one-class asymmetric stacked autoencoder. *Cluster Computing*, 28, 550. https://doi.org/10.1007/s10586-025-05234-y

Received: August 01, 2025