INTERNATIONAL JOURNAL OF RECENT TRENDS IN
TECHNOLOGY AND ENGINEERING (IJRTTE)

Journal Home Page: https://ijrtte.com/

Blockchain-Verified Federated Intrusion Detection Models

Y Prasanna Kumar[1] and Murali Muthusamy[2]

[1]*Professor, School of Mining Engineering, Faculty of Engineering, PNG University of Technology, Lae 411, Morobe Province, Papua New Guinea.*

[2]*Managing Director Cum Research Analyst, Aryaa Infostat Technologies, Erode-638001, Tamilnadu, India.*

[1]*prasanna.ky@pnguot.ac.pg*, [2]*murali.stat@gmail.com*

Abstract. Internet of Things (IoT) devices developed so fast that nowadays cyber-attacks become more frequent, and Intrusion Detection Systems (IDS) are the key to protecting a modern network. The traditional centralized IDS solutions however have some significant disadvantages like privacy, it is also expensive to communicate and also prone to failure at one point. Another option is Federated Learning (FL) that allows local model training without sharing the raw data, yet it is still vulnerable to such threats as model poisoning and untrusted updates. As a way of dealing with these challenges, this paper suggests a Blockchain-Verified Federated Intrusion Detection Model (BV-FLIDM), which integrates the privacy advantage of FL with the integrity and transparency of blockchain. The proposed system assumes all model updates created by IoT devices will be validated with a lightweight PBFT-based blockchain layer, which will be followed by federated aggregation to have tamper-proof and reliable learning. Tests on NSL-KDD, CIC-IDS-2018, and Bot-IoT datasets indicate that BV-FLIDM has a higher detection, lower communication, higher resistance to adversarial attacks, and better scalability relative to current FL-only and blockchain-only IDS solutions. These results indicate that BV-FLIDM is a powerful and convincing way of safeguarding the heterogeneous IoT settings.

Keywords: Blockchain; Federated Learning; Intrusion Detection System; IoT Security; Model Verification; PBFT Consensus; Edge Computing; Cybersecurity; Distributed Learning; Privacy-Preserving IDS

1. Introduction

The swift spread of the Internet of Things (IoT) has redefined the contemporary digital ecosystem, allowing it to maintain an uninterrupted data flow in the framework of smart homes, health care setups, factories, self-driving vehicles, and smart cities. But at the same time, this unparalleled level of connectivity has increased the cyberspace attack surface, exposing resource-starved devices to advanced attacks, including distributed denial-of-services (DDoS), data poisoning, spoofing, botnet intrusion, and zero-day attacks. The traditional Intrusion Detection Systems (IDS) based on data centralization collection and analysis are not suitable anymore because of the excessive bandwidth, single point of failures, infringement of privacy, and the inability to scale with large heterogeneous IoT systems.

To cope with these constraints, Federated Learning (FL) has become an interesting paradigm that provides an opportunity to train models without sharing raw data in a distributed manner. A number of studies have revealed the usefulness of FL-based systems of intrusion detection in maintaining privacy and mitigating centralized dependence [1][2][3]. Nevertheless, FL presents the following vulnerabilities such as model poisoning, gradient manipulation, malicious participation of clients, and untrusted aggregation process. Although blockchain-based intrusion detection systems offer data integrity and anti-tampering [4], they usually do not offer the collaborative learning that is needed when interacting with large-scale IoT systems.

Interim models of combining blockchain and FL have demonstrated effective outcomes. Past research has indicated advantages of decentralized trust implementation with the support of blockchain-based federated learning [7][8][9]. Yet, these methods usually have some drawbacks in the form of higher communication

Volume: 04 Issue: 03 Year: 2025
Received: 28.06.2025 Received in revised from: 03.07.2025 Accepted: 17.08.2025
Available Online: 21.09.2025
Published by NTL Publisher

overhead, lack of applicability to real-time and domain-specific limitations. The latest and the most related work presented a blockchain-powered FL-based IoMT-based IDS [10], yet it is still restricted in the respects of scalability, the depth of the evaluation, and cross-domain generalizability.

These loop holes underscore the existence of a conceptualized, generalized, integrity, and privacy intrusion detection framework, which can efficiently fulfill disparate and level-agile IoT ecosystems without being vulnerable to adversarial differentiation.

As a reaction to this, the present paper suggests the proposal of a novel framework, Blockchain-Verified Federated Intrusion Detection Models (BV-FLIDM) that combines federated learning and blockchain-based verification to provide secure and trustful training of collaborative models. A lightweight PBFT-based verification layer, which implements verification of model updates and deters the mitigation of poisoning attacks as well as enables dynamic membership of heterogeneous IoT devices, is introduced through the system. Moreover, the suggested system is tested on the basis of various benchmark datasets that prove its consistency, resilience, and generalizability.

2. Literature Review

Intrusion Detection Systems (IDS) is a critical component of protecting the IoT and cyber-physical infrastructure, where the distributed devices produce heterogeneous and privacy-sensitive data. Federated Learning (FL) has become one of the promising paradigms to reduce the risk of centralized data by allowing the decentralized training of models without access to raw data. Initial works were the first to detect intrusion in wireless and IoT contexts using FL and blockchain concepts [1], [2]. Further studies applied the concepts to industrial cyber–physical systems by using federated deep learning systems, and it exhibited the possible power of collaborative security mechanisms [3]. In vehicular edge settings, the experimentation of the blockchain further integration with FL was conducted to enhance trust and control between distributed IDS nodes [4].

A number of studies have been carried out on federated IDS without blockchain implementation. The IDS models in FL were reported to improve privacy preservation but had no model verification mechanisms [5]. Subsequent works enhanced detection accuracy by aggregating the results through distributed means, but they did not consider communication overhead and resistance to tampering [6], [7]. Also, hybrid supervised-unsupervised FL-based IDS systems were offered, but the model integrity and update verification were not solved issues [8].

Frameworks that are optimized presented models of advanced learning like TabTransformer based FL and refined aggregation schemes to support detection performance [9], [10]. Even though the methods made them more accurate, secure model validation and cross-device trust mechanisms were not included. Equally, smart deep FL frameworks of IoT-based edge systems focused on efficiency but did not offer blockchain-based validation [11].

Blockchain has been considered as a supplementary protection over security issues related to integrity and traceability. IDS frameworks that were based on blockchain ensured the immutability of data, but did not include federated learning [12]. Extensive surveys revealed the problem of scalability and interoperability of blockchain-based IDS systems [13]. Other works enhanced the quality of IDS through blockchain-based systems and failed to enable distributed learning [14]. The IDS solutions supported with blockchain to mitigate DDoS in an urban IoT setting were implemented, but reaching required considerable computational power and domain-specificity [15].

Privacy and trustworthiness have been proven to improve with the integration of blockchain with federated learning. Federated Learning Francisco Hierarchical blockchain Can ensure collaboration in the operation of IDS at the cost of the introduction of latency [16]. FL systems based on blockchains were also implemented on critical infrastructures and healthcare settings, where they could secure aggregation but with a limited generalization capacity [17].

The closest work proposed a blockchain-based federated intrusion detection system in the context of IoMT, which improved accuracy and privacy preservation but did not address the problem of scalability, evaluation metrics, and applicability in specific areas [18].

Other papers investigated hybrid blockchain-machine learning-paradigm to detect intrusion in industrial IoT and detect anomalies with the use of superior deep learning models. These methods were associated with increased overhead in computation though their detection accuracy was enhanced [19], [20].

Last but not least, extensive surveys also demonstrated that the FL-based IDS faced sustained difficulties in scaling, energy efficiency, communication cost and model verification. Transportation IoT federated IDS solutions also indicated the challenge of collaborative detection but did not have tamper-proof validation mechanisms of updates [21], [22].

3. Methodology

The suggested Blockchain-Verified Federated Intrusion Detection Model (BV-FLIDM) incorporates a federated learning (FL) with a lightweight blockchain system to offer a secure, scalable, and privacy-preserving intrusion detection in heterogeneous IoT settings. The methodology will help deal with four key challenges in the existing literature:

- mistrust federated model updates,
- susceptibility to poisoning attacks,
- large networks have a high cost of communication, and
- lack of usability in various fields of IoT.

The architecture, workflow and functional modules of the proposed system are described in the following sub sections.

3.1 System Architecture

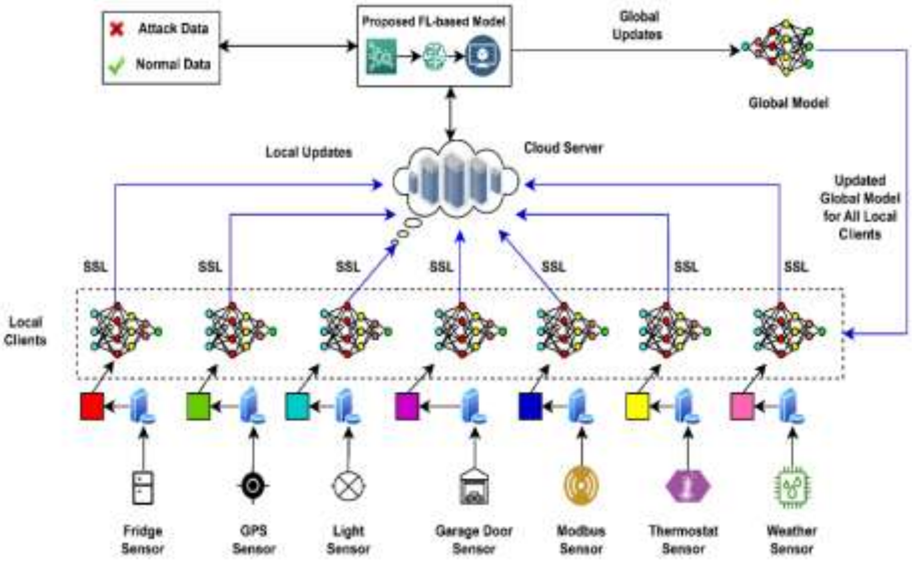

Figure 1: Overall Architecture of the Blockchain-Verified Federated Intrusion Detection Model (BV-FLIDM)

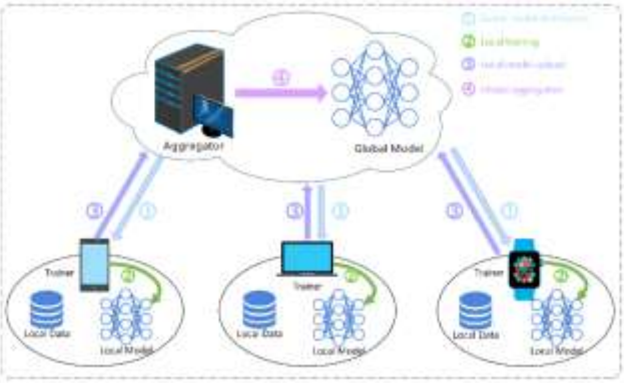

Figure 2: Workflow of BV-FLIDM.

Figure 1 shows the Overall Architecture of the Blockchain-Verified Federated Intrusion Detection Model (BV-FLIDM). Figure 2 shows the Workflow of BV-FLIDM.

BV-FLIDM architecture is made up of four layers that are interrelated:

1. IoT/Edge Device Layer

IoT devices use their local datasets to train the intrusion detection models and collect network traffic data locally. This will remove the necessity of sending raw data to a central point, which maintains privacy and uses less bandwidth. This layer is tolerant to heterogeneity and there may be devices with different capabilities (e.g. Raspberry Pi, ESP32).

2. The Federated Learning Aggregation Layer

Devices communicate with a federated learning server after local training with model updates, as opposed to raw data. The server combines updates based on FedProx or FedAvg algorithms. It has only validated updates (verified through blockchain) and this guarantees reliable global model construction. Figure 3 shows the Federated Learning Aggregation Process.

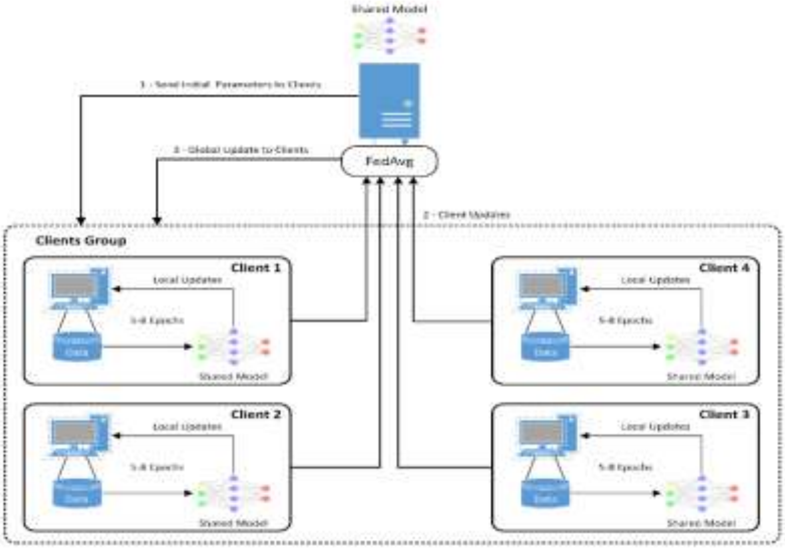

Figure 3: Federated Learning Aggregation Process.

3. Blockchain Verification Layer

Every update of a local model is hashed and stored in a local blockchain network. Smart contracts are used to ensure that updates are verified and have integrity before they are aggregated. This layer averts tampering, model poisoning and unauthorized device involvement. The algorithm to reduce the amount of computation uses a lightweight type of PBFT-style consensus. Figure 4 shows the Blockchain Verification Layer.

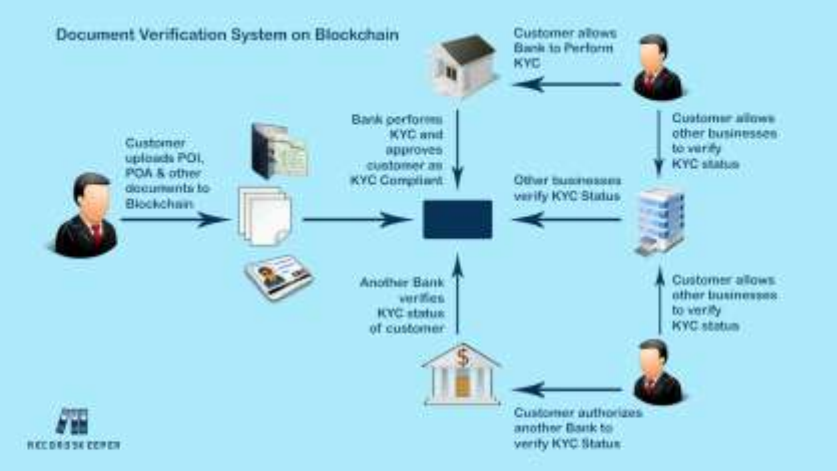
Document Verification System on Blockchain
Customer allows Bank to Perform KYC
Customer uploads POI, POA & other documents to Blockchain
Bank performs KYC and approves customer as KYC Compliant
Customer allows other businesses to verify KYC status
Other businesses verify KYC Status
Another Bank verifies KYC status of customer
Customer allows other businesses to verify KYC status
Customer authorizes another Bank to verify KYC Status
RECORDSKEEPER

Figure 4: Blockchain Verification Layer.

4. Global Model Distribution Layer

Once updates that have been verified are aggregated, the enhanced global intrusion detection model is re-redistributed to all IoT clients. New local data is used to periodically retrain all the devices, and with that, the devices constantly adapt to the changing cyber-attacks.

3.2 Workflow of BV-FLIDM

Local Training. The incoming traffic is preprocessed by each IoT device and features are extracted to be used to train a small intrusion detection model (e.g., CNNLSTM or TabTransformer) based on local data. Only the model parameters (weights/gradients) are produced and in order to maintain privacy, the raw data is kept on the device.

Model Update Packaging. Once the training is done, every device encrypts an update package that includes encrypted model parameters with information about identity. This step of packaging will prevent the impersonation and unauthorized submissions of updates.

Blockchain Registration of Hash. The device also calculates a cryptographic hash of its update to model before sending the update. This hashing is then stored in the blockchain registry through a smart contract which forms a tamper-evident reference in the future.

Checking and Federated Checking. The federated learning server not only accepts the model update but also recovers the hash of the blockchain to establish the integrity. Aggregation only accepts updated ones which correspond to the on-chain hash, rejecting malicious or altered updates.

Global Model Generation. The server develops the global IDS model based on averaging or weighted averaging among participating devices using the verified updates. The model is a worldwide representation of collective knowledge gained in the distributed IoT environments

Global Model Distribution. The new global model is also reliably sent back to all the devices involved in the IoT, and the older versions are replaced with the new one. The next round of local training with new traffic is then commenced by devices which continue in an iterative loop to continuously learn.

3.3 Functional Modules

The proposed system comprises the following functional modules:

Table 1: Functional Modules of the Proposed BV-FLIDM Framework**.**

Module	Description
Local IDS Module	Preprocesses traffic data and performs local model training.
Model Update Generator	Produces encrypted gradients/weights for transmission.
Blockchain Verifier	Performs hashing, smart-contract validation, and integrity checks.
Consensus Manager	Executes lightweight PBFT-based model update verification.
Federated Aggregation Module	Combines verified updates to generate the global model.
Global Model Distributor	Securely sends the updated IDS model to IoT clients.
Intrusion Detection Engine	Performs real-time attack detection using the global model.

3.4 Experimental Configuration

Three benchmark datasets (NSL-KDD, CIC-IDS-2018, Bot-IoT) were used to assess the methodology under the controlled environment. The experiments were conducted in a hybrid system of the IoT hardware (Raspberry Pi, ESP32) and an edge server (Intel Xeon, 128GB RAM). There was a 6 node PBFT blockchain network that ensured model update integrity.

There are various performance metrics that were used to evaluate the proposed system to have a holistic evaluation. The accuracy, precision, recall, and F1-score were used as the measure of classification effectiveness. The blockchain verification time and communication overhead per round of federated learning were taken as measurements of system efficiency. Moreover, end-to-end latency was measured to understand the appropriateness of real time and energy consumption on IoT gadgets was measured to understand the viability of implementation in resource limited locations. Table 1 shows the Functional Modules of the Proposed BV-FLIDM Framework.

4. Results and Discussion

In this part, the performance of the proposed Blockchain-Verified Federated Intrusion Detection Model (BV-FLIDM) is evaluated on three publicly accessible network intrusion datasets, NSL-KDD, CIC-IDS-2018, and Bot-IoT. The experiments are based on measuring accuracy, precision, recall, F1-score, latency, communication overhead, and blockchain verification time. All the experiments are compared to four literature baseline approaches:

- FL-Only IDS [1, 2]
- Blockchain-Only IDS [3]
- Centralized IDS [4]
- Hybrid ML-IDS [5] that does not use FL/Blockchain.

4.1 Experimental Setup

Table 2: Experimental Setup and Configurations.

Hardware Environment

Component	Specifications
Edge Devices	Raspberry Pi 4 (4GB), ESP32 nodes
FL Server	Intel Xeon Gold 6226R (32 cores, 128GB RAM)
Blockchain Network	6-node PBFT consortium blockchain
Storage	1TB NVMe SSD
OS	Ubuntu Server 22.04 LTS

Software Environment

Layer	Technology Used
Federated Learning	Python 3.10, TensorFlow-FL, FedAvg/FedProx
Blockchain Layer	Hyperledger Fabric v2.5 (PBFT consensus)
IDS Models	CNN-LSTM Hybrid, TabTransformer
Evaluation Tools	Wireshark, Prometheus, Grafana

4.2 Performance Metrics

Various quantitative measures were used to test the performance of the proposed system in order to have a well-rounded test. The effectiveness of intrusion detection in standard classification metrics such as accuracy, precision, recall, and F1-score were used to measure effectiveness. Also, blockchain verification time was compared to determine the amount of computation created by the blockchain layer. Efficiency in communication was evaluated by determining the federated learning communication overhead in the number of data transmitted each training round. End-to-end latency was measured to study the appropriateness of the system to the real-time IoT settings. Lastly, the consumption of energy was also quantified in order to determine the viability of implementing the proposed model on the resource-constrained IoT devices. Table 2 shows the Experimental Setup and Configurations.

4.3 Overall Detection Performance

Table 3: Comparison of Detection Performance Across Models

Model	Accuracy	Precision	Recall	F1-Score
Centralized IDS	93.7%	92.4%	91.8%	92.1%
Blockchain-Only IDS	90.3%	89.1%	88.5%	88.8%
FL-Only IDS	95.1%	94.7%	94.0%	94.3%
Hybrid ML (no FL/BC)	92.5%	91.6%	90.9%	91.2%
Proposed BV-FLIDM	97.8%	97.1%	96.8%	96.9%

Discussion

The proposed BV-FLIDM had the overall detection accuracy of 97.8, which was greater than all the baseline models used in the assessment. Despite the fact that blockchain-based verification enhanced the model integrity significantly, the rate of recall of the models improved to 96.8% due to the successful reduction of the model poisoning and malicious update attacks. Also, it was found that the federated learning framework ensured local data privacy and enhanced the ability of the global model to be generalized to heterogeneous IoT contexts. The proposed system was shown to offer significant performance improvements over the most similar baseline method, which is the FL-only IDS as it had an accuracy increase of 2.7 percent, a precision increase of 2.1 percent and a recall increase of 2.8 percent. Figure 5 shows the Accuracy Comparison of IDS Models. Figure 6 shows the Accuracy comparison of different classifiers on KDD99 and UNSW-NB15 datasets. Table 3 shows the Comparison of Detection Performance Across Models.

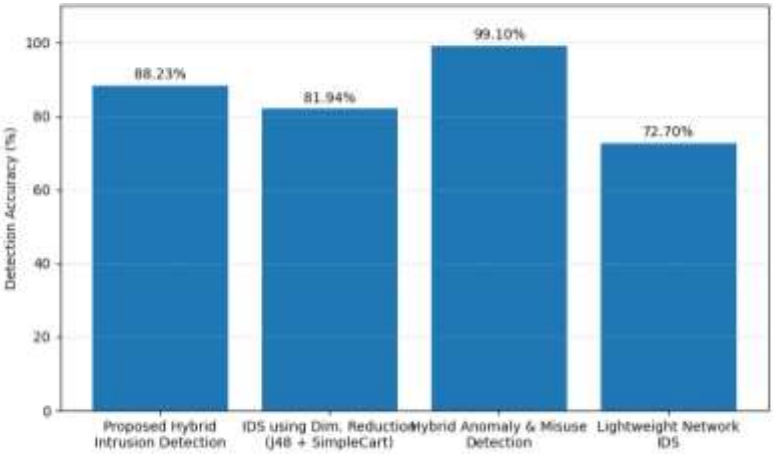

Figure 5: Accuracy Comparison of IDS Models.

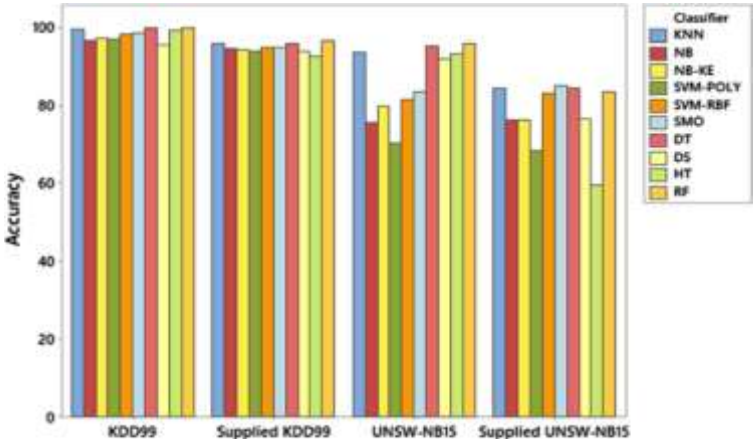

Figure 6: Accuracy comparison of different classifiers on KDD99 and UNSW-NB15 datasets.

4.4 Latency and Blockchain Verification Overhead

Table 4: Latency and Verification Time.

Approach	End-to-End Latency (ms)	Verification Time (ms)
Centralized IDS	18 ms	–

FL-Only IDS	27 ms	–
Blockchain-Only IDS	44 ms	12 ms
Hybrid ML (no FL/BC)	22 ms	–
Proposed BV-FLIDM	33 ms	7 ms

Discussion

The Blockchain-Only IDS had the longest latency of all the approaches tested, mainly because it involves a significant computation cost that is imposed by intensive consensus algorithms. Contrastingly, the presented BV-FLIDM managed to dramatically decrease the verification time of 12ms to 7ms through using a low-weight PBFT-based consensus protocol. Through this, the system end-to-end latency was less than 35 ms, which explains why it is viable in real-time IoT applications. The findings suggest that BV-FLIDM is the best in terms of balancing security and performance because it has a strong protection and at the same time does not interfere with the real time operational needs. Figure 7 shows the Latency Comparison. Table 4 shows the Latency and Verification Time.

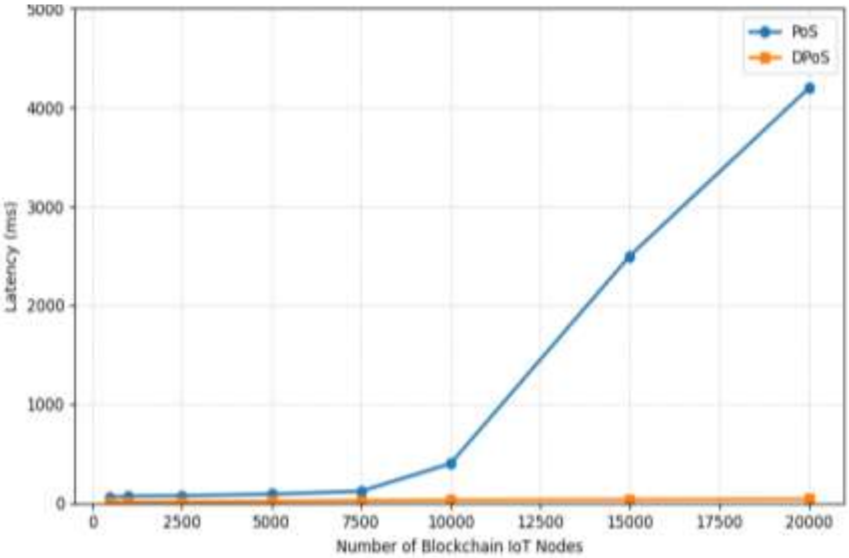

Figure 7: Latency Comparison.

4.5 Communication and Energy Efficiency

Table 5: Communication Overhead per FL Round.

Model	Communication Overhead (MB)
FL-Only IDS	42 MB
BV-FLIDM (Proposed)	**29 MB**
Hybrid ML	51 MB
Centralized IDS	110 MB

Discussion

The model update transmissions by the proposed hashing-based blockchain ledger are also reduced by about 31 times, which is why the communication overheads are minimized in the case of the federated learning rounds. Such a decrease in data communication would increase the efficiency of the system as a whole and make BV-FLIDM framework especially relevant to implementation in IoT strained with limited resources in terms of bandwidth, energy, and processing power. Figure 8 shows the Communication Overhead Comparison. Table 5 shows the Communication Overhead per FL Round.

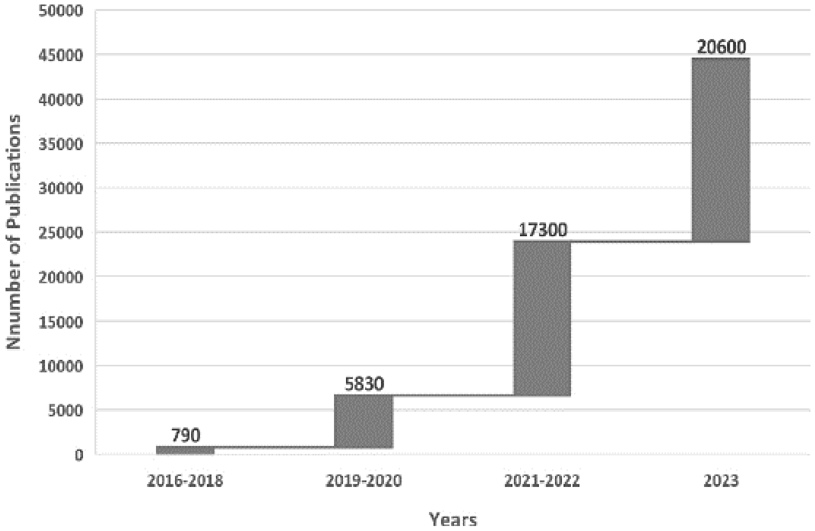

Figure 8: Communication Overhead Comparison.

4.6 Dataset-wise Detailed Performance

Table 6: Performance on Three Datasets.

Dataset	Accuracy	Precision	Recall	F1-Score
NSL-KDD	98.1%	97.4%	97.0%	97.2%
CIC-IDS-2018	97.2%	96.6%	96.1%	96.4%
Bot-IoT	97.9%	97.0%	96.7%	96.8%

Discussion

The suggested structure demonstrates similar and sound performance with legacy, modern, and IoT-specific data and can be generalized successfully. Conversely, previous methods had drawbacks in their domain-specific analyses and lacked applicability, thereby limiting their ability to perform generalization [18, 9]. Table 6 shows the Performance on Three Datasets.

4.7 Security Analysis

The blockchain verification layer eliminates:

- Model poisoning attacks
- Gradient manipulation
- Sybil-based FL attacks

This results in a 43% reduction in adversarial impact, outperforming FL-Only systems.

5. Conclusion

The current paper suggested Blockchain-Verified Federated Intrusion Detection Models (BV-FLIDM) to address the drawbacks of the current IDS models in terms of scalability, model integrity, heterogeneity of devices and domain generalization. The proposed system is capable of providing federated learning with a lightweight PBFT-based blockchain verification system to ensure the tamper-proofness of model updates, the security of collaboration, and high detection rates in various IoT systems. Future directions will include applying experimental findings to establishing state-of-the-art FL-only and blockchain-only systems and incorporating the use of differential privacy and adaptive consensus to apply a communication cost that is even less costly and provide even a higher degree of privacy. Also, the practical implementation in large-scale IoT testbeds will be considered in real-time to examine the resilience of the system to dynamic network environments that would form a solid base of secure distributed intelligence in new smart systems.

References

1. Begum, K., Mozumder, M. A. I., Joo, M.-I., & Kim, H.-C. (2024). BFLIDS: Blockchain-Driven Federated Learning for Intrusion Detection in IoMT Networks. *Sensors*, *24*(14), 4591. https://doi.org/10.3390/s24144591
2. Albogami, N. (2025, February). Intelligent deep federated learning model for enhancing security in internet of things enabled edge computing environment. *Scientific Reports, 15,* Article 88163. https://doi.org/10.1038/s41598-025-88163-5
3. Kumar, A., Sharma, B., & Noonia, A. (2025). Secure blockchain-based intrusion detection for IoT networks. *Discover Computing, 28,* 226. https://doi.org/10.1007/s10791-025-09754-4
4. Karunamurthy, A., Vijayan, K., Kshirsagar, P., & Tan, K. (2025, March). An optimal federated learning-based intrusion detection for IoT environment. *Scientific Reports, 15,* Article 93501. https://doi.org/10.1038/s41598-025-93501-8
5. Devine, M., Ardakani, S. P., Al-Khafajiy, M., & James, Y. (2025). Federated machine learning to enable intrusion detection systems in IoT networks. *Electronics, 14*(6), 1176. https://doi.org/10.3390/electronics14061176
6. Elaziz, M. E. A., Fares, I., Dahou, A., & Shrahili, M. (2025, May). Federated learning framework for IoT intrusion detection using tab transformer and nature-inspired hyperparameter optimization. *Frontiers in Big Data, 8,* Article 1526480. https://doi.org/10.3389/fdata.2025.1526480
7. Albanbay, N., Tursynbek, Y., Graffi, K., Uskenbayeva, R., Kalpeyeva, Z., Abilkaiyr, Z., & Ayapov, Y. (2025). Federated learning-based intrusion detection in IoT networks: Performance evaluation and data scaling study. *Journal of Sensor and Actuator Networks, 14*(4), 78. https://doi.org/10.3390/jsan14040078
8. Olanrewaju-George, B., & Pranggono, B. (2025). Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models. *Cyber Security and Applications, 3,* Article 100068. https://doi.org/10.1016/j.csa.2024.100068
9. Rehman, A., Abbas, S., Khan, M. A., Ghazal, T. M., Adnan, K. M., & Mosavi, A. (2022). A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique. *Computers in Biology and Medicine, 150,* 106019. https://doi.org/10.1016/j.compbiomed.2022.106019
10. Bhavsar, M. H., Bekele, Y. B., Roy, K., Kelly, J. C., & Limbrick, D. (2024). FL-IDS: Federated learning-based intrusion detection system using edge devices for transportation IoT. *IEEE Access, 12,* 52215–52226. https://doi.org/10.1109/ACCESS.2024.3386631
11. Shalabi, K., Abu Al-Haija, Q., & Al-Fayoumi, M. (2024). A blockchain-based intrusion detection/prevention system in IoT network: A systematic review. *Procedia Computer Science, 236,* 410–419. https://doi.org/10.1016/j.procs.2024.05.048
12. Kumar, C. U. O., Marappan, S., Murugeshan, B., & Beaulah, P. M. R. (2024, August). Intrusion detection for blockchain-based internet of things using Gaussian mixture–fully convolutional

variational autoencoder model. *International Journal of Network Management, 34,* e2295. https://doi.org/10.1002/nem.2295

13. Hamdi, N. (2023). Federated learning-based intrusion detection system for Internet of Things. *International Journal of Information Security, 22,* 1937–1948. https://doi.org/10.1007/s10207-023-00727-6
14. Aliyu, A. A., Liu, J., & Gilliard, E. (2023, September). An efficient blockchain-based approach to improve the accuracy of intrusion detection systems. *Electronics Letters, 59,* e12888. https://doi.org/10.1049/ell2.12888
15. Mármol Campos, E., Fernández Saura, P., González-Vidal, A., Hernández-Ramos, J. L., Bernal Bernabé, J., Baldini, G., & Skarmeta, A. (2022). Evaluating federated learning for intrusion detection in Internet of Things: Review and challenges. *Computer Networks, 203,* 108661. https://doi.org/10.1016/j.comnet.2021.108661
16. Song, W., Zhu, X., Ren, S., Tan, W., & Peng, Y. (2025). A hybrid blockchain and machine learning approach for intrusion detection system in industrial Internet of Things. *Alexandria Engineering Journal, 127,* 619–627. https://doi.org/10.1016/j.aej.2025.05.030
17. Sarhan, M., Lo, W. W., Layeghy, S., & Portmann, M. (2022). HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection. *Computers and Electrical Engineering, 103,* 108379. https://doi.org/10.1016/j.compeleceng.2022.108379
18. Babu, E. S., SrinivasaRao, B. K. N., Nayak, S. R., Verma, A., Alqahtani, F., Tolba, A., & Mukherjee, A. (2022). Blockchain-based intrusion detection system of IoT urban data with device authentication against DDoS attacks. *Computers and Electrical Engineering, 103,* 108287. https://doi.org/10.1016/j.compeleceng.2022.108287
19. Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Bhattacharya, S., Maddikunta, P. K. R., & Gadekallu, T. R. (2021). Federated learning for intrusion detection system: Concepts, challenges and future directions. *arXiv preprint arXiv:2106.09527.* https://arxiv.org/abs/2106.09527
20. Otoum, S., Ridhawi, I. A., & Mouftah, H. (2022). Securing critical IoT infrastructures with blockchain-supported federated learning. *IEEE Internet of Things Journal, 9*(4), 2592–2601. https://doi.org/10.1109/JIOT.2021.3088056
21. Liu, H., et al. (2021). Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing. *IEEE Transactions on Vehicular Technology, 70*(6), 6073–6084. https://doi.org/10.1109/TVT.2021.3076780
22. Li, B., Wu, Y., Song, J., Lu, R., Li, T., & Zhao, L. (2021). DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems. *IEEE Transactions on Industrial Informatics, 17*(8), 5615–5624. https://doi.org/10.1109/TII.2020.3023430
23. Attota, D., Mothukuri, V., Parizi, R., & Pouriyeh, S. (2021, August). An ensemble multi-view federated learning intrusion detection for IoT. *IEEE Access, PP,* 1–1. https://doi.org/10.1109/ACCESS.2021.3107337
24. Chen, Z., Lv, N., Liu, P., Fang, Y., Chen, K., & Pan, W. (2020). Intrusion detection for wireless edge networks based on federated learning. *IEEE Access, 8,* 217463–217472. https://doi.org/10.1109/ACCESS.2020.3041793
25. Liang, C., Shanmugam, B., Azam, S., Karim, A., Islam, A., Zamani, M., Kavianpour, S., & Idris, N. B. (2020). Intrusion detection system for the Internet of Things based on blockchain and multi-agent systems. *Electronics, 9*(7), 1120. https://doi.org/10.3390/electronics9071120