Cureus Journal of Computer Science
https://doi.org/10.7759/s44389-026-00053-7

Technical Report

A Federated Learning–Based Intrusion Detection Framework for Blockchain-Enabled Internet of Things (IoT) Supply Chains

Yukta Vishnoi [1], Rupesh Mishra [2]

1. *Computer Engineering, Mukesh Patel School of Technology Management & Engineering, Mumbai, IND*
2. *Computer Engineering, St. Francis Institute of Technology, Mumbai, IND*

Received: February 12, 2026 | Review began: March 02, 2026 | Review ended: April 08, 2026 | Published: April 08, 2026

Abstract

Integrating Internet of Things (IoT) networks in supply chain operations implies the extension of real-time data possibilities along with augmenting the security challenges of cyber-physical nature. This paper proposed an interdisciplinary simulation framework that incorporates decentralized learning-trained deep neural networks for distributed anomaly detection on the IoT devices with a permissioned blockchain layer that secures anomaly recording. Several different simulation scenarios using NS3 and a blockchain simulator under cyber-attack scenarios such as data exfiltration, distributed denial-of-service attack, and malicious device behavior have shown that machine-learning networks do well in threat detection with over 95% accuracy while significantly reducing false positives relative to baseline methods. The blockchain layer contributes to a tamper-proof audit capability and increases supply chain data visibility and traceability for events. The unique contribution is captured in proposing an innovative federated-machine learning framework for detecting anomalies, a blockchain-driven storage layer connecting alerts and trained models to the system, and a comprehensive simulation study revealing an empirical superiority of the proposed system. However, the integration of federated machine learning in blockchain technology may foster response to incidents, adding single-tenancy separation to make the IoT data stream more trustworthy. This study helped in laying the groundwork for the realization of secure and intelligent IoT supply chain network deployments in real-world environments, providing them with solid security and transparency in operations.

Categories: Blockchain and Cryptocurrency, Computational Science and Engineering, IoT Security and Privacy

Keywords: accuracy, federated learning, simulation, supply chains, threat assessment, blockchains, internet of things, security, anomaly detection

Introduction

Recently, supply chain management (SCM) has gained a lot from the use of Internet of Things (IoT) devices, such as radio frequency identification tags and shipment sensors, which allow real-time tracking and visibility [1]. Although the IoT contributes to better operational efficiency, its decentralization and limited resources make it very vulnerable to security threats, such as data corruption, illegal access, and network hacking being the most prevalent ones. Attackers can take advantage of these vulnerabilities by impersonating sensor data or creating false alarms, which can then cause the supply chain to malfunction [2]. The use of blockchain technology has been proposed as a solution to these issues through the creation of a decentralized, unalterable ledger for transactions and device event recording. In blockchain-based supply chains, sensor data can be safely logged to allow traceability, prevent the existence of single points of failure, and create trusted automation through smart contracts [3]. However, blockchain technology cannot automatically detect abnormal behavior or hacking attempts in real-time IoT data streams [4]. Machine learning (ML), especially deep

learning-based intrusion detection systems (IDS), has been successful in spotting anomalous patterns in IoT networks by recognizing normal device and traffic behavior. Moreover, the use of Federated Learning (FL) further increases this ability because it allows IoT devices to work together in training a common model with their respective local data, thus ensuring privacy and preventing the need for central data collection. Previous studies have shown that FL-based IDS have high accuracy in detecting intruders in distributed IoT environments [5-6].

The present study is inspired by these findings and proposes an integrated ML- and blockchain-based security framework for IoT supply chains [7]. In the designed system, the IoT devices use the models trained on FL to detect anomalies, whereas the alerts that are detected and the updates of the model are stored in the blockchain.

This study contributes to the literature by presenting an integrated ML-blockchain architecture, where a federated deep learning method is implemented in the IDS installed on IoT devices, with anomaly alerts and model updates securely stored on a permissioned blockchain. The proposed framework is evaluated through simulations using NS3 and a blockchain simulator under various attack scenarios, demonstrating superior detection accuracy and reduced false positives compared to non-ML baselines. Additionally, the study analyzes the impact of FL rounds, device heterogeneity, and blockchain consensus mechanisms on detection performance and network latency, thereby highlighting the trade-offs relevant for real-world deployment.

Technical Report

Literature review

Blockchain technology has been thoroughly studied to enhance SCM systems' data integrity, traceability, and transparency [1]. Earlier studies have pointed out that data can be electronically unchangeable and can be reached by various parties through consensus mechanisms [2]. In addition, smart contracts can play a role in secure automation and access control within the supply chain [3]. Although some blockchain SCMs have been implemented in the food, drug, and logistics sectors, which have improved the monitoring and auditing of products, these systems still rely heavily on trusted data inputs and do not provide any means to actively detect anomalies at the IoT layer. Because IoT devices are heterogeneous and have limited resources, the marriage of IoT and blockchain is advantageous for data integrity but also poses issues [5].

Researchers have indicated that IoT devices may be prone to physical and software attacks, leading to concerns regarding the level of trust in decentralized systems [6]. The distribution of authentication and logging may help avoid losing total control; however, solutions based exclusively on blockchain do not analyze the data and depend on off-chain security mechanisms to protect them from intrusions [7]. This shortcoming indicates the need for security techniques based on ML. ML, especially deep learning, applied in IDS has already been recognized as a powerful method for the protection of IoT networks through the acceptance of normal traffic and device patterns [8]. Different models, such as CNNs, RNNs, and autoencoders, have been used to spot unauthorized access and data injection as part of the anomalies. FL is a new trend in the field of IoT security that provides the advantages of distributed model training along with data privacy [9]. The above-mentioned points direct further discussions about the inadequacies of communication, scalability, and consensus latency in systems with high trustworthiness and security capabilities. One of the most common approaches to assess the impact of new technologies in combination with IoT/ML and blockchain is simulation-based evaluation, owing to the very high costs of real-world deployment [10]. Among the most widely used are NS-3 and BlockSim, which serve to model the behavior of the IoT network and the consensus mechanism of the blockchain, respectively [11]. Previous studies have simulated various IoT security protocols and lightweight blockchain operations; however, comprehensive simulation-based evaluations of federated ML-driven intrusion detection integrated with blockchain for IoT supply chains are still very limited.

The literature highlights several key points about blockchain technology, which provides enhanced transparency and trust: it does not inherently support automatic anomaly detection; ML, particularly FL, proves to be highly effective for intrusion detection in IoT environments but remains underexplored; furthermore, comprehensive cross-domain simulation studies that integrate IoT, blockchain, and ML applications are still limited in number [12-13].

How to cite this article:
Vishnoi Y, Mishra R (April 08, 2026) A Federated Learning–Based Intrusion Detection Framework for Blockchain-Enabled Internet of Things (IoT) Supply Chains. Cureus J Comput Sci 3 : es44389-026-00053-7. DOI https://doi.org/10.7759/s44389-026-00053-7

This study fills the gaps mentioned above by proposing and testing a federated ML-augmented blockchain framework for secure IoT-enabled supply chain networks.

Methodology

The framework being suggested is based on a four-layer architecture.

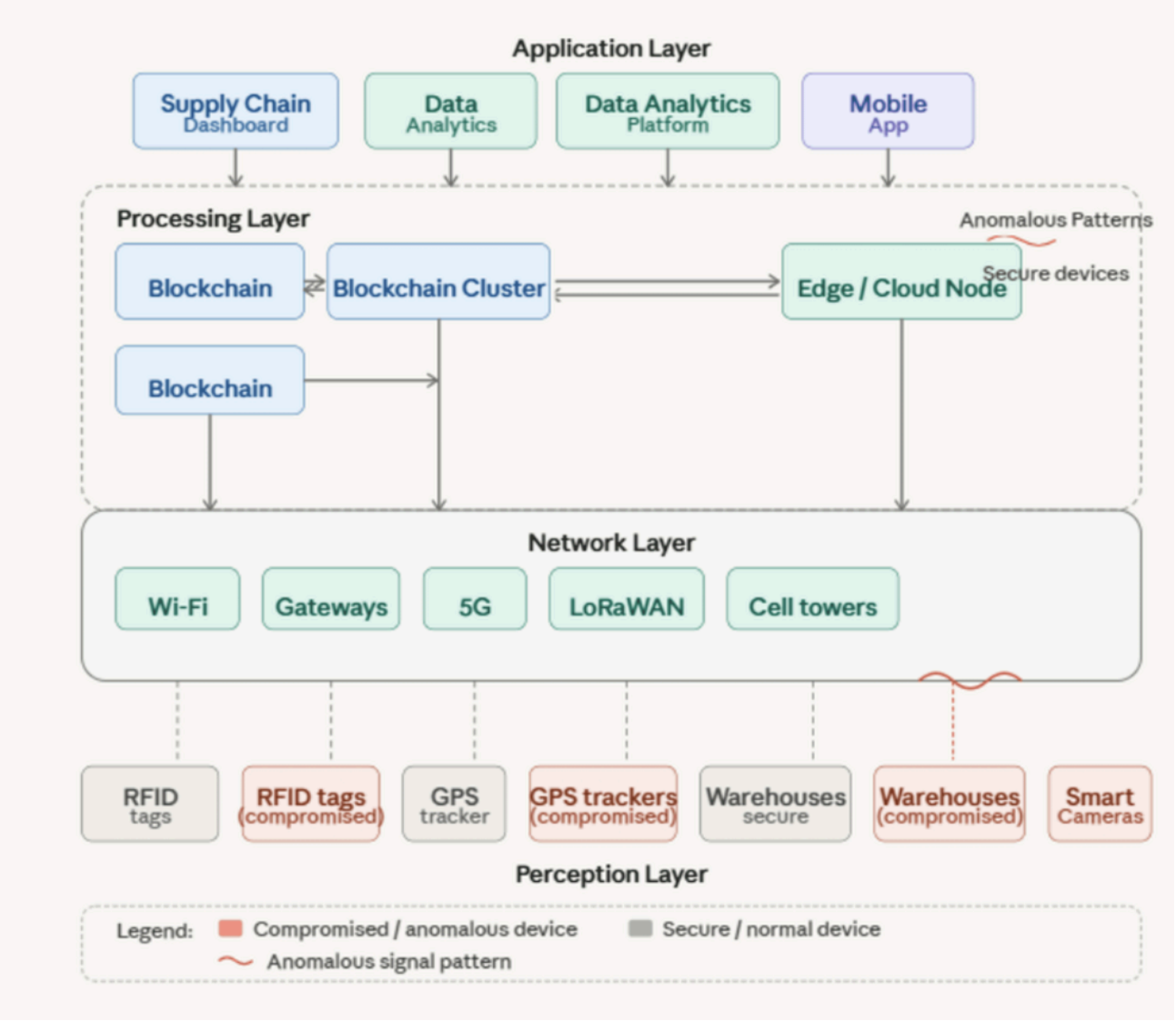

FIGURE 1: Four layers of an IoT-enabled supply chain network

IoT, Internet of Things; GPS, Global Positioning System; RFID, Radio-Frequency IDentification

Four typical layers of an IoT-enabled supply chain network, as shown in Figure *1*, include the Perception Layer, which comprises the IoT sensors and devices attached to the supply chain assets; the Network Layer, responsible for providing wireless connectivity through IoT gateways; the Processing Layer, consisting of edge and cloud nodes that support FL and blockchain services; and the Application Layer, which offers monitoring and control interfaces to the supply chain stakeholders. Time-series data, such as location, temperature, and device logs, are generated by IoT devices. Local lightweight anomaly detection models operate on devices, while only anomaly alerts and model updates are sent to the processing layer, where they are validated and recorded on a permissioned blockchain [14]. At the edge of each IoT

device, a specific anomaly detection model is run, which is designed with a gated recurrent unit (GRU) neural network, as it is suitable for the temporal nature of the IoT data streams [15]. FL is used for the global model's training in partnership with other devices without the necessity for publishing any raw data.

FL is executed in numerous rounds, where at each round, the IoT gadgets achieve in-house local training using that data only to give the updates of the model weights. These local updates are sent to aggregator nodes linked to a blockchain system, where safe aggregation awaits. By learning collaboratively, this approach helps to keep data privacy intact. The global model becomes generated for all participating devices, thus allowing them to jump into the next round of training. With collaborative learning, above approaches improve anomaly detection accuracy. Here is a simplified algorithm to illustrate a single FL training round used for decentralized anomaly detection. Algorithm given below provides an overview of a single FL training round that is applied for the purpose of distributed anomaly detection. The pseudocode for one FL round is shown below:

Mathematical Formulation of Federated Learning:

Let there be N IoT devices, each having local dataset D_i.

The global objective is to minimize:

$$F(w) = \sum_{i=1}^{N} \left(\frac{|D_i|}{|D|} \right) F_i(w)$$

where, w represents global model parameters, and $F_i(w)$ is the local loss function at device i.

Local update at each device:

$$w_i^{(t+1)} = w^t - \eta \nabla F_i(w^t)$$

Global aggregation:

$$w^{(t+1)} = \sum_{i=1}^{N} \frac{|D_i|}{|D|} w_i^{(t+1)}$$

Algorithm 1: Federated Learning-Based Anomaly Detection

Input: Initial global model w^0

Output: Updated global model w^T

1. Initialize global model w^0
2. For each round $t = 0$ to $T–1$ do:
3. For each device $i \in \{1,2, ..., N\}$ in parallel:
4. Receive global model w^t
5. Train model on local dataset D_i
6. Compute updated weights $w_i^{(t+1)}$
7. Send model updates to blockchain network
8. End for
9. Aggregate updates:
10. $w^{(t+1)} = \sum_{i=1}^{N} \frac{|D_i|}{|D|} w_i^{(t+1)}$
11. Store updated model on blockchain
12. Broadcast $w^{(t+1)}$ to all devices
13. End for

How to cite this article:
Vishnoi Y, Mishra R (April 08, 2026) A Federated Learning–Based Intrusion Detection Framework for Blockchain-Enabled Internet of Things (IoT) Supply Chains. Cureus J Comput Sci 3 : es44389-026-00053-7. DOI https://doi.org/10.7759/s44389-026-00053-7

This approach now extends to adopting FedAvg by default and for all standard model training.

To gain the trust of users and have the ability to audit activities carried out on the system, a permissioned blockchain is set up at the processing layer. The blockchain stores the hash values of the updates made to the global model, authentication records of devices, and alerts regarding anomalies generated by devices connected to the Internet. Smart contracts perform the functions of identity management and access control, making it possible for only those devices that have been granted permission to send updates and alerts. A low-latency consensus protocol, such as Practical Byzantine Fault Tolerance (PBFT) or Raft, is utilized to facilitate consortium-based supply chain scenarios. By combining FL and blockchain, the system not only gains but also retains the non-repudiable recording of security events and distributed intrusion detection, which is highly resilient. The suggested framework is evaluated through a simulation, where NS-3 is applied for modelling IoT network behavior, and a custom-made blockchain simulator is used for ledger operations. The simulated environment comprises IoT devices capable of producing both normal and malicious traffic patterns, and a small number of devices are attacked using techniques such as data spoofing and abnormal traffic injection. Important simulation parameters, including but not limited to network size, attack rate, ML model configuration, and blockchain consensus settings, are compiled in Table *1*. Under various circumstances, performance measures such as detection accuracy, false positive rate, block latency, and network speed were tracked and documented.

Parameter	Value
Number of IoT devices	50 (uniformly placed in area)
Data sampling rate	1 Hz (one packet/second per device)
Attack injection rate	5% of packets are malicious
Wireless protocol	IEEE 802.11n (Wi-Fi)
Blockchain network size	5 validator nodes (permissioned consortium)
Consensus mechanism	PBFT with block time ~2 sec
ML model type	GRU with 2 hidden layers (10 units each)
Feature vector length	20 (statistical & flow features from traffic)
FL rounds	30 rounds per epoch
Learning rate	0.01
Epochs per round	5

TABLE 1: Summary of important simulation parameters

FL, Federated Learning; GRU, Gated Recurrent Unit; IoT, Internet of Things; ML, Machine Learning; PBFT, Practical Byzantine Fault Tolerance

Detection Model

How to cite this article:
Vishnoi Y, Mishra R (April 08, 2026) A Federated Learning–Based Intrusion Detection Framework for Blockchain-Enabled Internet of Things (IoT) Supply Chains. Cureus J Comput Sci 3 : es44389-026-00053-7. DOI https://doi.org/10.7759/s44389-026-00053-7

The model for detecting anomalies is built on a deep neural network that is GRU-based and specifically designed for sequential IoT data. In this process, statistical features are extracted over short time windows and used as the model input. The GRU layers learn the temporal dependencies, and a fully connected layer outputs an anomaly score. The Adam optimiser and binary cross-entropy loss were used to train the model. When the output score exceeds a certain limit, an anomaly is marked, and an alert is logged onto the blockchain. The experimental evaluation revealed that the supervised GRU model exhibited higher detection accuracy than the unsupervised alternatives.

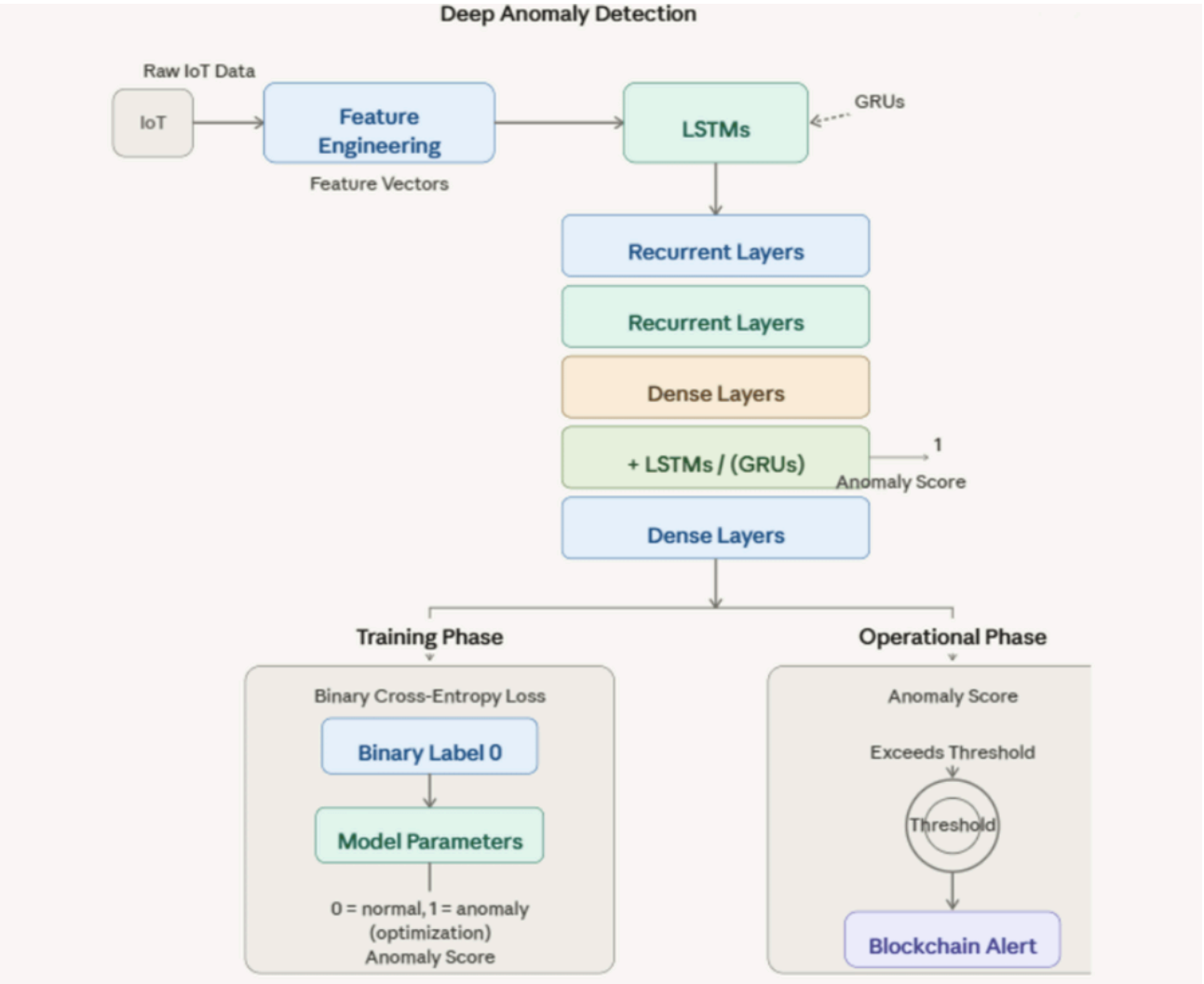

FIGURE 2: Anomaly detection using a deep learning pipeline

GRU, Gated Recurrent Unit; IoT, Internet of Things; LSTM, Long Short-Term Memory

In Figure *2*, unprocessed IoT data (e.g., traffic flow statistics) were transformed into feature vectors, which were then processed via recurrent and dense layers to produce an anomaly score. The anomaly detection model employs a GRU network to detect temporal patterns in the data streams of IoT devices. Initially, the raw data from the sensors and traffic statistics are converted into feature vectors, which are passed through the recurrent and dense layers, where the anomaly scores are produced. The model is trained in a supervised manner using normal and attack data marked with labels and is deployed on nearby IoT devices, where the identified anomalies are sent to the blockchain for auditability.

Dataset and Feature Engineering

How to cite this article:
Vishnoi Y, Mishra R (April 08, 2026) A Federated Learning–Based Intrusion Detection Framework for Blockchain-Enabled Internet of Things (IoT) Supply Chains. Cureus J Comput Sci 3 : es44389-026-00053-7. DOI https://doi.org/10.7759/s44389-026-00053-7

The research used the NS-3 simulation environment to create a synthetic dataset because real-world IoT security datasets for blockchain-based supply chain systems are not available. The dataset contains network traffic data that two groups of 50 IoT devices transmitted through a wireless network during normal operations and security attack tests. The data instance represents a time window that shows aggregated network traffic statistics.

Feature Extraction

The simulated IoT traffic produced 20 extracted features, which enabled the network analysis of both statistical and behavioral network characteristics. The following features were selected:

1. Packet size (mean)
2. Packet size (variance)
3. Flow duration
4. Packet inter-arrival time (mean)
5. Packet inter-arrival time (variance)
6. Number of packets per flow
7. Number of bytes per flow
8. Packet rate (packets per second)
9. Byte rate (bytes per second)
10. Source IP frequency
11. Destination IP frequency
12. Protocol type (TCP/UDP/ICMP)
13. Connection state duration
14. Retransmission count
15. Error packet rate
16. Dropped packet count
17. Forward packet count
18. Backward packet count
19. Flow idle time
20. Flow active time

The selected features enable researchers to identify temporal patterns and analyze communication patterns while they detect IoT traffic anomalies.

Feature Preprocessing

The feature extraction process required several steps, which needed to be completed before the model training could begin:

- Missing values (if any) were handled using zero imputation.
- The researchers applied Min-Max scaling to all numerical features, which resulted in values between 0 and 1.
- The research team used one-hot encoding to transform categorical features, which included protocol type.
- The researchers used fixed time windows to create feature vectors, which enabled them to study how time patterns in data developed.
- The process of feature selection eliminated redundant features and highly correlated features, which improved model performance by decreasing unwanted data.

Simulated Attack Types

The proposed system tested its strength against various cyber-attacks, which were performed on the IoT network through multiple attack methods.

How to cite this article:
Vishnoi Y, Mishra R (April 08, 2026) A Federated Learning–Based Intrusion Detection Framework for Blockchain-Enabled Internet of Things (IoT) Supply Chains. Cureus J Comput Sci 3 : es44389-026-00053-7. DOI https://doi.org/10.7759/s44389-026-00053-7

Results

The experimental setup was implemented using an NS-3-simulated IoT network comprising 50 devices communicating over IEEE 802.11n, where synthetic traffic data with a 5% attack injection rate was generated to model both normal and malicious behaviour. A GRU-based FL model was trained over 30 rounds using 20 extracted traffic features, while anomaly alerts and model updates were securely recorded on a permissioned blockchain employing PBFT consensus with five validator nodes.

The proposed architecture was assessed with two references: a central IDS that is not blockchain-based and a blockchain system that does not use ML-based detection. Detection performance results are presented in Table *2*. The proposed federated GRU-based IDS achieved 95.2% detection accuracy with a 3.8% false positive rate, demonstrating the best performance compared to the centralized ML baseline, which had 87.3% accuracy, and the blockchain-only system, which lacked detection capability. This progress highlights the effectiveness of distributed learning in detecting various attack patterns in IoT devices.

System	Detection Accuracy	False Positive Rate
Centralized ML (ANN)	87.30%	9.50%
Federated GRU (proposed)	95.20%	3.80%
Blockchain only	No IDS	No IDS

TABLE 2: Anomaly detection performance

ANN, Artificial Neural Network; GRU, Gated Recurrent Unit; IDS, Intrusion Detection System; ML, Machine Learning

The results of the blockchain latency and throughput are shown. The average finalization delay of the block was approximately 2-3 seconds using a permissioned blockchain with PBFT consensus and five validator nodes, and the throughput was 10-15 TPS. This performance can facilitate the updates of the FL model as well as the alerting of anomalies without affecting the training time or the network operation.

Impact of System Parameters

The sensitivity analysis indicated that the higher the number of IoT devices, the better the detection accuracy, which was mainly due to the diversity of data; however, the communication overhead was nearly linear to the device count. Making shorter block intervals led to a reduction in the aggregation latency but an increase in the validator workload, hence the trade-off between the system's responsiveness and the consumption of its resources. The system stability was maintained through variations in the conditions.

Discussion

The proposed framework combines the highest detection accuracy of existing IDS solutions with an additional feature of auditability using blockchain logging. The results were obtained from a simulated environment, but they still point to the possibility of integrating FL with blockchain to secure IoT-enabled supply chain networks in the future. The challenges of adversarial FL participants and real-world deployments must be addressed in future research.

How to cite this article:
Vishnoi Y, Mishra R (April 08, 2026) A Federated Learning–Based Intrusion Detection Framework for Blockchain-Enabled Internet of Things (IoT) Supply Chains. Cureus J Comput Sci 3 : es44389-026-00053-7. DOI https://doi.org/10.7759/s44389-026-00053-7

Conclusions

In this study, a simulation-based study of an IoT-enabled supply chain architecture that combines federated deep learning and blockchain is presented. The FL aspect of the proposed framework allows for privacy-preserving, distributed anomaly detection at the network edge while at the same time ensuring secure logging of security events and model updates through a permissioned blockchain. Simulation results reveal that the hybrid method yields excellent threat detection accuracy (over 95%) and incurs only a negligible amount of communication and consensus overheads. The combination of localized intelligence and distributed trust results in a substantial increase in both security and efficiency in the operation of IoT-based supply chains. The next stage will involve creating a prototype of the framework for actual IoT deployments and testing it with different learning models and consensus mechanisms to further increase scalability and resilience. This study is a step towards durable, intelligent supply chain systems that are resistant to evolving cyber-physical threats.

Additional Information

Author Contributions

All authors have reviewed the final version to be published and agreed to be accountable for all aspects of the work.

Concept and design: Yukta Vishnoi, Rupesh Mishra

Acquisition, analysis, or interpretation of data: Yukta Vishnoi

Drafting of the manuscript: Yukta Vishnoi

Critical review of the manuscript for important intellectual content: Yukta Vishnoi, Rupesh Mishra

Supervision: Yukta Vishnoi

Disclosures

Human subjects: All authors have confirmed that this study did not involve human participants or tissue. **Animal subjects:** All authors have confirmed that this study did not involve animal subjects or tissue. **Conflicts of interest:** In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there are no other relationships or activities that could appear to have influenced the submitted work.

Data Availability Statements

The data supporting this study were synthetically generated using a simulation-based IoT network environment.

Acknowledgements

The authors have not employed any Generative AI tools during the preparation of this article.

References

1. Ehsan I, Khalid MI, Ricci L, Iqbal J, Alabrah A, Ullah SS, Alfakih TM: A conceptual model for blockchain-based agriculture food supply chain system. Scientific Programming. 2022, 2022:1-15. 10.1155/2022/7358354
2. Reddy SS, Jahnavi S, Manjunath DR: Enhancing data security and traceability in supply chain management using blockchain technology. Journal of Cyber Security in Computer System. 2024, 3:11-24. 10.46610/jcscs.2024.v03i03.002

3. Stefanescu D, Montalvillo L, Urbieta A, Galán-García P, Unzilla Galan JJ: Smart contract powered framework for the next generation Industry 4.0 business model. Distributed Ledger Technologies: Research and Practice. 2024, 3:1-24. 10.1145/3686167

4. Habibullah SM, Sikder MA, Tanha NI, Sah BP: A review of blockchain technology's impact on modern supply chain management in the automotive industry. Global Mainstream Journal of Innovation, Engineering & Emerging Technology. 2024, 3:13-27. 10.62304/jieet.v3i3.163

5. Du M, Wang K, Liu Y, Qian K, Sun Y, Xu W, Guo S: Spacechain: a three-dimensional blockchain architecture for IoT security. IEEE Wireless Communications. 2020, 27:38-45. 10.1109/MWC.001.1900466

6. Asaithambi S, Ravi L, Kotb H, et al.: An energy-efficient and blockchain-integrated software defined network for the industrial Internet of Things. Sensors. 2022, 22:7917. 10.3390/s22207917

7. Prasada P, Prasad DS: Blockchain-enhanced machine learning for robust detection of APT injection attacks in the cyber-physical systems. International Journal of Computational and Experimental Science and Engineering. 2024, 10:799-810. 10.22399/ijcesen.539

8. Odeh A, Abu Taleb A: Ensemble-based deep learning models for enhancing IoT intrusion detection. Applied Sciences. 2023, 13:11985. 10.3390/app132111985

9. Senol NS, Baza M, Rasheed A, Alsabaan M: Privacy-preserving detection of tampered radio-frequency transmissions utilizing federated learning in LoRa networks. Sensors. 2024, 24:7336. 10.3390/s24227336

10. Sawarkar AD, Hazari AD: IoT forensic cyber activities detection and prevention with automated machine learning model. Journal of Sensors, IoT & Health Sciences. 2024, 2:1-15. 10.69996/jsihs.2024006

11. Ngoupayou Limbepe Z, Gai K, Yu J: Blockchain-based privacy-enhancing federated learning in smart healthcare: a survey. Blockchains. 2025, 3:1. 10.3390/blockchains3010001

12. Sowmya G, Sridevi R, Rao KSS, Shiramshetty SG: Integrating AI, ML, blockchain, and IoT for end-to-end supply chain optimization. Strategic Innovations for Dynamic Supply Chains. 2024, 123-146. 10.4018/979-8-3693-3575-8.ch006

13. Nandanwar H, Katarya R: Privacy-preserving data sharing in blockchain-enabled IoT healthcare management system. The Computer Journal. 2025, 68:1657-1681. 10.1093/comjnl/bxaf065

14. Rahmati M, Pagano A: Federated learning-driven cybersecurity framework for IoT networks with privacy preserving and real-time threat detection capabilities. Informatics. 2025, 12:62. 10.3390/informatics12030062

15. Addula SR, Meesala MK, Ravipati P, Sajja GS: A hybrid autoencoder and gated recurrent unit model optimized by Honey Badger Algorithm for enhanced cyber threat detection in IoT networks. Security and Privacy. 2025, 8:e70086. 10.1002/spy2.70086

How to cite this article:
Vishnoi Y, Mishra R (April 08, 2026) A Federated Learning–Based Intrusion Detection Framework for Blockchain-Enabled Internet of Things (IoT) Supply Chains. Cureus J Comput Sci 3 : es44389-026-00053-7. DOI https://doi.org/10.7759/s44389-026-00053-7