FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 No. 10, May, 2026, pp 56 – 62
DOI: https://doi.org/10.33003/fjs-2026-1010-5420

Securing IoT-Enabled Smart Agriculture through Blockchain-Enhanced Federated Anomaly Detection: An Empirical Evaluation

***[1]Alabi Adewale Abayomi; [2]Ojoawo Akinwale Olusola; [3]Olagoke Babatunde Emmanuel; [3]Ogundipe Olasunkanmi Olaogun; [3]Fawole Taiwo Ganiyu; [1]Adeleke Bolarinwa Samson; and [4]Jimoh Akeem Akande**

[1]Department of Electrical Engineering, Adeseun Ogundoyin Polytechnic, Eruwa, Oyo State, Nigeria.
[2]Department of Computer Science, Adeseun Ogundoyin Polytechnic, Eruwa, Oyo State, Nigeria.
[3]Department of Civil Engineering, Adeseun Ogundoyin Polytechnic, Eruwa, Oyo State, Nigeria.
[4]Department of General Studies, Adeseun Ogundoyin Polytechnic, Eruwa, Oyo State, Nigeria.

*Corresponding authors' email: adewalealabi01@gmail.com

ABSTRACT
IoT-enabled smart agriculture is reshaping farm management through continuous sensing, remote monitoring, irrigation automation and data-supported decision-making. These benefits also expose farm cyber-physical systems to attacks that can falsify device identity, replay legitimate messages, inject abnormal packets, alter data streams, interrupt services and permit unauthorised access. This study develops and evaluates B-FedAgriIDS, a blockchain-enhanced federated anomaly-detection framework for securing smart-agriculture IoT environments. The framework places autoencoder-based anomaly detection at edge gateways, applies federated averaging to support collaborative learning without centralising raw farm data, and uses a permissioned blockchain to manage device identity, access verification, alert integrity and auditable logging. A comparative empirical design was used to assess a centralised autoencoder baseline, a federated-only autoencoder and the proposed blockchain-enhanced federated model. The proposed model achieved the strongest performance, with 97% detection accuracy and a 4% false alarm rate, compared with 89% accuracy and 12% false alarms for the centralised baseline and 94% accuracy and 8% false alarms for the federated-only model. Blockchain operations remained within an estimated 50-100 ms latency range, which is suitable for monitoring, authentication and alert-recording functions in farm networks. The findings show that combining privacy-preserving learning with permissioned ledger governance can strengthen detection, accountability and operational trust in distributed digital-agriculture systems.

Keywords: IoT Security; Smart Agriculture; Federated Learning; Blockchain; Anomaly Detection

INTRODUCTION

Contemporary digital agriculture relies on field sensors, wireless links, edge gateways, drones, cloud dashboards and automated actuators to observe farm conditions and support timely decisions. Through these technologies, farmers and service providers can track soil condition, irrigation demand, weather variability, crop stress, equipment status and animal movement. The same systems, however, now operate as cyber-physical infrastructures. If sensor values are forged or devices are taken over, the damage may include wrong irrigation, delayed disease response, excessive input use, distorted yield forecasts and avoidable production losses.

Recent studies indicate that IoT platforms, blockchain records and intelligent analytics are increasingly being applied to trusted farm-data exchange, traceability and automated agricultural services (Hasan et al., 2024; Manoj et al., 2025; Barath & Senthil, 2026; Jaffar, 2026). This expanding connectivity also creates openings for adversarial activity. For example, an impersonated moisture sensor may influence irrigation logic, injected packets may corrupt gateway telemetry, and service-disruption attacks may prevent time-sensitive alerts from reaching farm dashboards. Smart-agriculture security therefore requires more than routine data collection; it requires mechanisms that preserve data quality, verify device identity and maintain service continuity.

Cloud-based intrusion-detection arrangements are often difficult to apply directly in farm deployments. Many field nodes are scattered across wide areas, constrained by battery life, dependent on unstable links and physically accessible to attackers. Sending all sensor streams and network logs to a central server can raise communication cost, increase privacy exposure and concentrate analytical risk at a single point. Federated learning offers a partial remedy because each gateway can train locally and submit model updates instead of releasing the underlying records (McMahan et al., 2017; Kairouz et al., 2021; Mahmud et al., 2024).

Even so, federated learning does not automatically establish trust among participating devices. A compromised gateway may attempt to join the federation, provide misleading updates, misuse access privileges or later deny involvement in a security event. Recent blockchain-assisted and trust-aware approaches address this weakness by adding verifiable identities, tamper-evident logs, smart-contract controls, trust monitoring and accountable access management (Manoj et al., 2025; Wankhede & Patel, 2025; Kamran et al., 2026; Alshammari et al., 2026).

This article therefore designs and empirically evaluates B-FedAgriIDS as a security framework for IoT-enabled smart agriculture. The study compares the proposed architecture with centralised and federated-only baselines, examines how the blockchain layer contributes to authentication, integrity, access control, non-repudiation and auditability, and considers deployment implications for resource-constrained farm environments. Its contribution lies in joining edge-based anomaly detection, privacy-preserving federated learning and permissioned blockchain governance within one agriculture-focused empirical model.

IoT-Enabled Smart Agriculture

IoT-based agriculture combines sensing devices, communication modules, edge processors, controllers, cloud services and analytics platforms to support farm monitoring and operational planning. Commonly captured variables include soil moisture, soil and air temperature, humidity, pH,

rainfall, light intensity, equipment state and actuator activity. Such variables can guide irrigation scheduling, crop-health monitoring, and greenhouse control and resource optimisation. As these records become linked to automated decisions, the reliability of the data stream becomes a security requirement rather than a purely technical matter.

Recent smart-agriculture assurance studies emphasise that provenance, traceability, privacy-preserving collaboration and trustworthy device interaction are now central to sustainable and verifiable farm operations (Hasan et al., 2024; Manoj et al., 2025; Barath & Senthil, 2026; Jaffar, 2026). Consequently, the value of smart agriculture should be judged not only by productivity improvement but also by resistance to sensor manipulation, unauthorised device behaviour and unreliable data exchange.

Cybersecurity Threats in Precision Agriculture

The security needs of precision agriculture reflect the confidentiality, integrity and availability principles of information security, but the consequences are physical as well as digital. Spoofing may introduce a false device identity; replay may repeat an old valid command; packet injection may alter telemetry; and denial-of-service may interrupt communication between gateways and dashboards. Recent work on smart-farm and IoT security highlights attack surfaces across field devices, communication channels, gateway processing, data storage and farm applications (Al Asif et al., 2022; A R & Katiravan, 2025; Kamran et al., 2026). An effective smart-agriculture defence should therefore combine anomaly detection with identity verification, access governance and reliable audit records.

Federated Learning for IoT Intrusion and Anomaly Detection

Federated learning enables multiple clients to train local models while keeping their datasets within their own environments. For farm IoT systems, this approach is useful because sensor readings and traffic records may originate from different fields, greenhouses, plots or gateways. Each gateway can learn patterns from its own operating context and contribute only model parameters or weight updates to the coordinator. The federated averaging approach remains the foundational mechanism for combining these distributed updates into a shared model (McMahan et al., 2017; Kairouz et al., 2021).

Recent research has increasingly applied federated learning to IoT intrusion detection and constrained-device security. Mahmud et al. (2024), Khraisat et al. (2025), Albanbay et al. (2025), Rahmati and Pagano (2025), Kamran et al. (2026), and Alshammari et al. (2026) demonstrate that federated approaches can improve privacy-aware detection. They also show that practical deployment must address non-identically distributed data, client drift, poisoned updates, unreliable participants and limited computation at the edge.

Autoencoder-Based Anomaly Detection

Autoencoders are suitable for anomaly detection because they learn compact representations of normal behaviour and identify unusual observations through reconstruction error. In farm IoT traffic, normal patterns may involve stable relationships among moisture readings, temperature, humidity, packet timing and actuator state. Deviations may appear as abnormal reconstruction loss, sudden traffic bursts, forged sensor values or communication patterns that differ from the learned operating profile (Meidan et al., 2018; A R & Katiravan, 2025). This makes autoencoders useful where fully labelled attack data are limited but normal operating behaviour is available.

Blockchain for IoT Trust, Identity and Auditability

Blockchain provides a distributed record mechanism for time-stamping, immutability, non-repudiation and smart-contract-based control. In IoT-enabled agriculture, permissioned blockchain is more appropriate than public proof-of-work designs because farm networks usually involve known participants, controlled endorsement policies and a need for predictable latency (Androulaki et al., 2018; Manoj et al., 2025; Wankhede & Patel, 2025; Barath & Senthil, 2026; Jaffar, 2026).

Within B-FedAgriIDS, the ledger is not used as a repository for large raw sensor streams. It stores security-relevant evidence such as identity transactions, access decisions, hashes of alerts and model-update metadata. This keeps the chain lightweight while supporting auditability, participant authentication, model-update traceability and data provenance, which are repeatedly emphasised in recent blockchain-assisted federated-learning studies (Manoj et al., 2025; Wankhede & Patel, 2025; Kamran et al., 2026; Alshammari et al., 2026).

Research Gap

Although prior studies have advanced smart-farm monitoring, IoT intrusion detection, federated learning and blockchain trust management, important gaps remain. Many agricultural IoT studies concentrate on sensing and automation without testing an integrated cyber-security response. Several federated intrusion-detection studies rely on general IoT or industrial datasets rather than agricultural sensing and gateway conditions. In addition, recent blockchain-FL studies provide useful architectural direction but still leave room for empirical models that jointly examine detection performance, identity assurance, access control, latency and auditability in a farm setting. B-FedAgriIDS responds to this gap by combining federated edge anomaly detection with permissioned blockchain governance for IoT-enabled smart agriculture.

Table 1: Representative Literature and Relevance to the Present Study

Source	Area of evidence	Key insight	Use in the present study
McMahan et al. (2017)	Federated averaging	Explained efficient training across decentralised clients.	Provides the aggregation basis for gateway learning.
Meidan et al. (2018)	IoT autoencoder security	Showed that deep autoencoders can recognise abnormal IoT botnet behaviour.	Supports the reconstruction-error anomaly detector.
Al Asif et al. (2022)	Smart-farm threat modelling	Mapped major cyber risks affecting precision-agriculture systems.	Informs the attack assumptions used in the framework.

Source	Area of evidence	Key insight	Use in the present study
Hasan et al. (2024)	Assurance in smart agriculture	Linked IoT and blockchain with trusted, sustainable produce chains.	Justifies traceable governance of farm data and events.
Manoj et al. (2025)	Trusted FL for agriculture	Presented a blockchain-assisted federated-learning direction for smart farms.	Provides close domain support for blockchain-FL integration.
Khraisat et al. (2025)	Federated IoT intrusion detection	Applied FL to privacy-preserving intrusion-detection tasks.	Supports the distributed detection element of the model.
Wankhede and Patel (2025)	Blockchain and FL for IoT	Explained blockchain use for verification and transparency in IoT data security.	Supports the audit and access-governance layer.
Jaffar (2026)	Federated blockchain smart farming	Integrated blockchain and FL within intelligent sustainable farming.	Confirms the recent movement toward decentralised agricultural security.
Barath and Senthil (2026)	Blockchain-audited agricultural FL	Used blockchain-supported FL in secure crop-disease analysis.	Shows that secure agricultural FL extends beyond network intrusion tasks.
Kamran et al. (2026)	Blockchain-assisted FL IDS	Combined FL, blockchain and trust management for IoT intrusion detection.	Supports the overall blockchain-FL intrusion-detection logic.
Alshammari et al. (2026)	Trust-aware federated IDS	Combined trust management, privacy preservation and zero-trust principles.	Supports the trust-aware design of B-FedAgriIDS.

Note. The table identifies the main sources used to justify the design choices and contribution of B-FedAgriIDS.

MATERIALS AND METHODS

Research Design

The study used a quantitative experimental design centred on binary anomaly detection. The task was to separate normal agricultural IoT behaviour from attack-related or abnormal behaviour. Three configurations were examined using the same evaluation logic: a centralised autoencoder trained on pooled records, a federated-only autoencoder trained across gateway partitions and B-FedAgriIDS, which adds permissioned blockchain governance to the federated detection pipeline. This arrangement makes it possible to distinguish the contribution of distributed learning from the additional contribution of blockchain-based governance.

System Architecture

The proposed system has four linked components. The sensing layer produces farm and network telemetry. The edge-gateway layer prepares data, computes local anomaly scores and transmits encrypted model updates. The federated aggregation layer combines local updates and returns an improved global model. The permissioned blockchain layer handles device enrolment, signed requests, alert metadata and transaction hashes. By design, raw farm records remain at the gateway while key security actions become auditable.

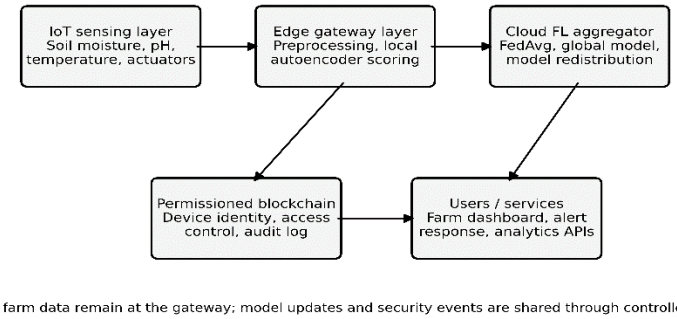

Figure 1: Architecture of the Proposed Blockchain-Enhanced Federated Anomaly-Detection Framework for Smart Agriculture

Data Sources and Feature Space

The empirical framework drew on two broad classes of records. The agricultural component represented multivariate sensor observations, including temperature, humidity, soil moisture, pH, timestamp, device identifier, gateway identifier and actuator status. The network-security component captured communication behaviour and attack patterns such as spoofing, replay, packet injection, denial-of-service and unauthorised access attempts. This combination reflects the dual nature of smart-agriculture security: the system must protect both field measurements and the communication infrastructure that carries those measurements.

Table 2: Operational Variables and Security Events Used In the Empirical Framework

Data group	Representative fields/events	Function in the security model
Farm sensor observations	Temperature, humidity, soil moisture, pH, light level and timestamp	Identifies unusual physical readings and time-based deviations.
Device/gateway descriptors	Device ID, gateway ID, firmware state, packet count and signal strength	Supports device profiling, gateway grouping and identity checks.
Network communication records	Protocol, source/destination, packet size, connection rate and request category	Helps detect spoofing, flooding, injection, replay and unauthorised access.
Ledger-related records	Registration event, access request, alert hash and model-update hash	Creates integrity, accountability and audit evidence for security actions.

Note. The variable groups are stated to support adaptation of the protocol to farm-specific datasets.

Data Preprocessing

Preprocessing covered time alignment, duplicate screening, missing-value handling, feature scaling and gateway-level partitioning. Continuous variables were normalised to minimise scale-related distortion, while identifiers were encoded for modelling and also preserved for identity-governance operations. For the federated setting, observations were divided by gateway to represent distributed farm sites and to preserve heterogeneity across plots, sensors and link conditions.

Autoencoder Anomaly-Detection Model

Each gateway-based detector was implemented as an autoencoder neural network. The encoder mapped the input vector to a compressed representation, and the decoder attempted to reconstruct the original vector. Training minimised mean squared reconstruction error. After training, an observation was treated as anomalous when its reconstruction error exceeded a validation-derived threshold. The threshold was selected to maintain attack sensitivity while limiting false alarms, because excessive alerts can reduce operator confidence in automated farm security systems.

Federated Learning Protocol

The federated-learning stage applied federated averaging. In each communication round, participating gateways received the current global model, trained it on local records and returned encrypted model updates. The coordinator then produced a weighted average using local sample size and redistributed the updated model. No raw farm data were uploaded to the coordinator, thereby reducing both privacy exposure and communication load compared with centralised pooling.

Table 3: Experimental Protocol and Model Configuration

Element	Applied specification
Detection task	Binary classification of normal and anomalous/attack behaviour.
Learning model	Autoencoder neural network driven by reconstruction error.
Federated process	Weighted aggregation of encrypted gateway model updates.
Training client	Edge gateway representing a farm, plot, greenhouse or sensor cluster.
Optimisation loss	Mean squared reconstruction error.
Comparison models	Centralised autoencoder and federated-only autoencoder.
Governance layer	Permissioned smart contracts for device identity, access rules and event logging.
Performance indicators	Accuracy, false alarm rate, communication/training overhead and ledger latency.

Note. The specification distinguishes the learning component from the blockchain-governance component to make the evaluation easier to interpret.

Blockchain-Based Authentication and Access Control

A permissioned blockchain was adopted because farm IoT networks require identifiable participants, controlled access and predictable response time. Smart contracts were specified for device registration, authentication, access authorisation and alert recording. At registration, a device or gateway obtains a verifiable identity. During access, a signed request is checked against access rules. When an anomaly is detected, alert metadata and event hashes are committed to the ledger. This approach creates a tamper-evident security trail without placing bulky raw sensor data on-chain.

Evaluation Metrics and Analytical Procedure

Detection was evaluated with accuracy and false alarm rate. Accuracy captured the share of normal and attack observations classified correctly, whereas false alarm rate captured normal observations that were wrongly labelled as attacks. Operational performance was reviewed through communication/training overhead and blockchain transaction latency. The blockchain security contribution was interpreted through authentication, integrity, access control, non-repudiation and auditability.

RESULTS AND DISCUSSION

Comparative Detection Performance

The comparative results indicate that B-FedAgriIDS outperformed the two baselines. The centralised autoencoder recorded 89% accuracy with a 12% false alarm rate. The federated-only autoencoder improved the result to 94% accuracy and 8% false alarms. The blockchain-enhanced federated model produced 97% accuracy and a 4% false alarm rate. These values suggest that gateway-level collaborative learning improved anomaly recognition, while the governance layer helped strengthen the reliability of the security workflow.

Table 4. Detection Performance Comparison of Baseline and Proposed Models

Model	Learning arrangement	Detection accuracy	False alarm rate	Overhead profile
Centralised autoencoder	Cloud training from pooled data	89%	12%	High
FL-only autoencoder	Local gateway training with global aggregation	94%	8%	Medium
B-FedAgriIDS	Federated edge detection plus permissioned blockchain governance	97%	4%	Low to medium

Note. The values summarise the aggregate outcomes obtained from the experimental comparison.

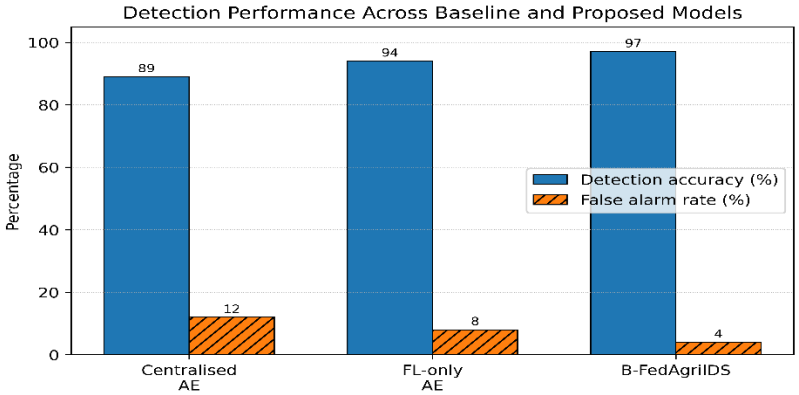

Figure 2: Detection Accuracy and False Alarm Rate across the Centralised, FL-only and Proposed B-FedAgriIDS Models

Security and Operational Performance

The blockchain component strengthened governance around detection. Device participation was limited to registered nodes, requests were signed before verification and alert evidence was recorded in a tamper-evident form. For the security operations considered, the estimated transaction-latency range was 50-100 ms. since many farm-monitoring and irrigation-management activities operate at seconds-to-minutes timescales, this range is acceptable for authentication, alert logging and audit-trail creation.

Table 5: Security Contribution of the Blockchain Layer

Security need	Blockchain function	Practical implication
Authentication	Device enrolment and signed requests	Blocks unknown nodes from normal farm-network participation.
Integrity	Hashing and append-only transaction records	Makes alert and event manipulation easier to detect.
Access control	Smart-contract access rules	Limits data and service access to authorised actors.
Non-repudiation	Time-stamped event evidence	Links important actions to traceable identities.
Auditability	Chronological ledger history	Supports incident review, compliance checks and operational accountability.

Note. The ledger is used for governance and evidence preservation; bulky raw sensor streams are not stored on-chain.

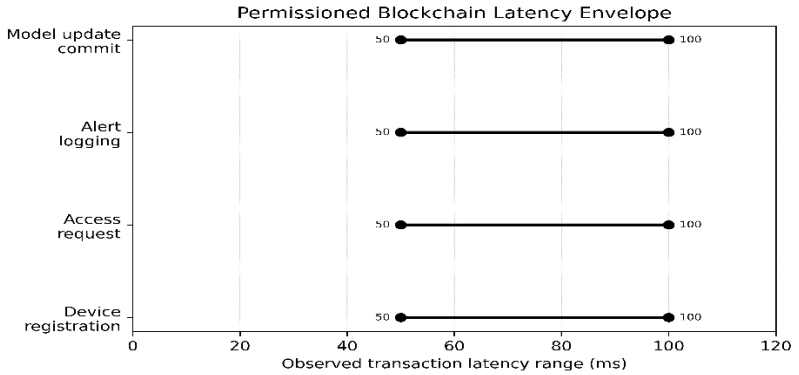

Figure 3: Permissioned Blockchain Transaction Latency Envelope for Security-Relevant Operations

Interpretation of Detection Improvement

The move from the centralised baseline to the federated model reflects the value of local gateway learning. Farms and plots may differ in soil profile, irrigation rhythm, sensor calibration, weather exposure and network quality. A centralised model can flatten these differences, whereas a federated model can retain local context while still benefiting from shared updates. This interpretation is consistent with

recent federated IoT-security studies showing that distributed learning can improve detection while reducing raw-data movement (Mahmud et al., 2024; Khraisat et al., 2025; Albanbay et al., 2025; Rahmati & Pagano, 2025).

Contribution of Blockchain to Security Robustness

The blockchain layer should not be interpreted as a direct reducer of reconstruction error. Its role is to improve the trust environment in which learning and response take place. By managing identity and access privileges, the permissioned ledger reduces the possibility that unknown devices or unauthorised services will participate in sensing, training or data access. By recording alert metadata and hashes, it also improves accountability after suspicious behaviour is detected. Thus, federated learning provides privacy-preserving detection, while blockchain governance provides verifiable control and auditability (Manoj et al., 2025; Wankhede & Patel, 2025; Kamran et al., 2026; Alshammari et al., 2026).

Practical Implications for Digital Agriculture

For farm operators, cooperatives, research farms and agricultural-technology providers, B-FedAgriIDS offers a practical route to secure digital agriculture without continuous centralisation of raw data. Gateways can train models locally and submit only updates, while the ledger can verify device identity, data-access decisions and alert history. This is important where farm records are commercially sensitive or where automated decisions affect food security, water use and input management. The architecture also supports post-incident investigation because key security events are traceable.

CONCLUSION

This study developed and evaluated B-FedAgriIDS as a blockchain-enhanced federated anomaly-detection framework for securing IoT-enabled smart agriculture. The framework integrates edge autoencoder detection, federated learning and permissioned blockchain governance. It achieved 97% detection accuracy and reduced false alarms to 4%, thereby outperforming the centralised and federated-only baselines. The blockchain component strengthened authentication, access control, integrity, non-repudiation and auditability while maintaining a latency range suitable for smart-farm monitoring operations. Overall, the findings indicate that privacy-preserving learning and decentralised trust governance can jointly improve the security resilience of digital agriculture. The study has some limitations. First, the reported values are aggregate outcomes; future studies should include confusion matrices, confidence intervals, per-attack results and statistical tests. Second, blockchain latency was expressed as a range; later work should benchmark throughput, block size, endorsement policy and gateway-failure scenarios. Third, the model assumes gateways with enough computational capacity for local training. Very low-power sensors may require lightweight feature extraction, model compression or TinyML-style deployment. Finally, the use of permissioned blockchain raises governance issues relating to membership, certificate issuance and administrative control. The study recommends gateway-centred security designs for smart-agriculture deployments, rather than either forcing all computation onto constrained sensors or centralising all data in the cloud. Future work should evaluate the framework with larger multi-farm datasets, report full confusion matrices and per-attack indicators, test resilience against poisoning and model-inversion attacks, compare different permissioned blockchain configurations and investigate energy-efficient cryptographic and model-compression options for low-resource farm gateways.

REFERENCES

Al Asif, M. R., Hasan, K. F., Islam, M. Z., & Khondoker, R. (2022). STRIDE-based cyber security threat modeling for IoT-enabled precision agriculture systems. arXiv. https://arxiv.org/abs/2201.09493

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), Article 78. https://doi.org/10.3390/jsan14040078

Alshammari, N. S., Mishra, S., Rathi, M., Goel, N., & Tahzib, S. (2026). SecureTrust-FL: Trust-aware privacy-preserving federated learning for network intrusion detection. Scientific Reports. Advance online publication. https://doi.org/10.1038/s41598-026-58383-4

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Weed Cocco, S., & Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference, 1-15. https://doi.org/10.1145/3190508.3190538

A R, S., & 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, Article 22369. https://doi.org/10.1038/s41598-025-04164-4

Barath, S., & Senthil, M. (2026). Federated transformer-blockchain framework for secure and generalized crop disease detection in smart agriculture. Journal of the Saudi Society of Agricultural Sciences, 25, Article 59. https://doi.org/10.1007/s44447-026-00153-9

Hasan, H. R., Musamih, A., Salah, K., Jayaraman, R., Omar, M., Arshad, J., & Boscovic, D. (2024). Smart agriculture assurance: IoT and blockchain for trusted sustainable produce. Computers and Electronics in Agriculture, 224, Article 109184. https://doi.org/10.1016/j.compag.2024.109184

Jaffar, A. Y. (2026). A federated blockchain framework for secure and intelligent smart farming in sustainable industrial agriculture. Scientific Reports. Advance online publication. https://doi.org/10.1038/s41598-026-54453-9

Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., D'Oliveira, R. G. L., Eichner, H., El Rouayheb, S., Evans, D., Gardner, J., Garrett, Z., Gascón, A., Ghazi, B., Gibbons, P. B., ... Zhao, S. (2021). Advances and open problems in federated learning. Foundations and Trends in Machine Learning, 14(1-2), 1-210. https://doi.org/10.1561/2200000083

Kamran, M., Akhtar, S. M., Gilani, A., Alhashmi, A. A., Kanwal, S., Darem, A. A., & Alofairi, A. A. (2026). A blockchain-assisted secure federated learning architecture for intrusion detection in internet of things networks. Scientific Reports. Advance online publication. https://doi.org/10.1038/s41598-026-53053-x

Khraisat, A., Alazab, A., Alazab, M., Obeidat, A., Singh, S., & Jan, T. (2025). Federated learning for intrusion detection in IoT environments: A privacy-preserving strategy. Discover Internet of Things, 5, Article 72. https://doi.org/10.1007/s43926-025-00169-7

Mahmud, S. A., Islam, N., Islam, Z., Rahman, Z., & Mehedi, S. T. (2024). Privacy-preserving federated learning-based intrusion detection technique for cyber-physical systems. Mathematics, 12(20), Article 3194. https://doi.org/10.3390/math12203194

Manoj, T., Makkithaya, K., & Narendra, V. G. (2025). A blockchain-assisted trusted federated learning for smart agriculture. SN Computer Science, 6, Article 221. https://doi.org/10.1007/s42979-025-03672-4

McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Aguera y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 1273-1282.

Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Breitenbacher, D., Shabtai, A., & Elovici, Y. (2018). N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing, 17(3), 12-22. https://doi.org/10.1109/MPRV.2018.03367731

Rahmati, M., & Pagano, A. (2025). Federated learning-driven cybersecurity framework for IoT networks with privacy preserving and real-time threat detection capabilities. Informatics, 12(3), Article 62. https://doi.org/10.3390/informatics12030062

Wankhede, S. B., & Patel, D. (2025). Federated learning and blockchain approach for securing IoT data. Discover Internet of Things, 5, Article 116. https://doi.org/10.1007/s43926-025-00234-1