FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 No. 10, May, 2026, pp 63 – 68
DOI: https://doi.org/10.33003/fjs-2026-1010-5418

Empirical Evaluation of a Blockchain-Enhanced Federated Learning and Trust-Aware Security Framework for IoT-Enabled Smart Agriculture

***[1]Alabi Adewale Abayomi, [2]Ojoawo Akinwale Olusola, [3]Olagoke Babatunde Emmanuel, [3]Ogundipe Olasunkanmi Olaogun, [3]Fawole Taiwo Ganiyu 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
Internet of Things (IoT)-based farming systems now link field sensors, edge gateways, irrigation devices and analytics dashboards into continuous decision-support networks. This connectivity improves monitoring and resource use, but it also creates new security weaknesses in farm operations. False sensor identities, replayed messages, injected packets, denial-of-service traffic and unauthorised gateway activity can corrupt the data used for irrigation, crop surveillance and farm planning. This study evaluates a hybrid security framework that combines federated autoencoder anomaly detection, permissioned blockchain authentication and dynamic trust-based device governance for smart agriculture. In the framework, edge gateways learn from local agricultural and network-traffic streams without transferring raw farm data to a central repository, while the blockchain layer records device enrolment, access-control activities, model-update events and verified alerts. The trust module converts repeated abnormal behaviour into operational responses such as watch-listing, restriction, quarantine and retraining. Evaluation was conducted with agricultural sensor streams and IoT attack scenarios involving spoofing, replay, packet injection and DDoS behaviour. The proposed framework achieved 97% detection accuracy, reduced false alarms to 4% and maintained blockchain transaction latency within 50-100 ms. The results indicate that privacy-preserving learning, auditable identity control and trust-aware response can jointly improve cybersecurity resilience in IoT-enabled smart agriculture.

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

INTRODUCTION

Smart agriculture increasingly depends on connected devices that collect, transmit and analyse field information in near real time. Soil-moisture probes, temperature and humidity sensors, pH meters, weather stations, drones, irrigation actuators, farm gateways and cloud dashboards now operate as interlinked cyber-physical components. These tools improve decisions about water use, crop stress, disease monitoring and equipment status. Recent studies also show that IoT and blockchain are being used to build traceable agricultural data services, trusted device interactions and privacy-conscious digital farm platforms (Hasan et al., 2024; Manoj et al., 2025; Jaffar, 2026). However, greater connectivity also increases exposure to cyber manipulation. A forged sensor reading may trigger wrong irrigation; a spoofed gateway may falsify operational records; a replay attack may reuse old control messages; and DDoS traffic may delay time-sensitive farm alerts.

Traditional security arrangements are difficult to apply directly in this setting. A centralised intrusion-detection server requires large volumes of farm data to leave the local environment, which may increase privacy risk, bandwidth cost and dependence on one point of failure. Recent work on IoT security indicates that federated learning can limit raw-data movement, while blockchain mechanisms can improve authentication, provenance and tamper resistance (Khraisat et al., 2025; Wankhede & Patel, 2025; Sathyabama & Katiravan, 2025). Signature-based detection also remains weak against unknown or evolving attacks, and many low-power field sensors cannot support heavy cryptographic or machine-learning workloads. A practical design must therefore move intensive security functions to gateways and administrative nodes while preserving the responsiveness of field devices.

This article evaluates a blockchain-enhanced federated learning framework with trust-aware governance for IoT-enabled smart agriculture. In the proposed design, edge gateways train anomaly-detection models with local sensor and traffic data and share only model updates for aggregation. A permissioned blockchain layer verifies device identity, records access-control decisions and preserves audit trails for security events. The trust-governance component then links detection outcomes to operational control by updating device-level trust scores, restricting suspicious devices, quarantining repeatedly abnormal nodes and initiating retraining when network behaviour changes. This integration follows the recent direction of AgriFLChain and AgriChain-FL-type models, which combine decentralised learning with blockchain-backed trust for smart-agriculture environments (Manoj et al., 2025; Barath & Senthil, 2026; Jaffar, 2026).

The study contributes in four ways. First, it develops a four-layer security architecture for distributed smart-agriculture deployments. Second, it describes an empirical anomaly-detection pipeline based on autoencoder learning and federated aggregation. Third, it introduces trust-aware governance as a post-detection response mechanism rather than ending the process at intrusion classification. Fourth, it compares a centralised baseline, a federated-only design and the proposed FL-blockchain-trust configuration using detection accuracy, false alarm rate, overhead and latency indicators.

IoT-Enabled Smart Agriculture

IoT-enabled agriculture uses distributed sensing, machine-to-machine communication, edge or cloud analytics and automated actuation to support farm management. Its value comes from converting heterogeneous field data into

dependable decisions on irrigation, disease monitoring, fertiliser application and equipment control. Recent work on smart-agriculture assurance emphasises that trusted data provenance, traceability and secure communication are part of the reliability of the agronomic decision itself, not merely additional technical features (Hasan et al., 2024; Jaffar, 2026). Smart-farm environments are often geographically dispersed, exposed to weather and physical tampering, and populated by devices with unequal computation, memory and energy capacity. These conditions make a uniform security design impractical. Gateways may run analytics and communicate with a ledger, whereas many field sensors can only perform lightweight authentication and basic reporting. Recent smart-agriculture and federated-blockchain studies therefore favour gateway- or edge-centred security, where capable nodes handle model updates, ledger interaction and policy enforcement (Albanbay et al., 2025; Barath & Senthil, 2026). This study follows that approach by placing the heaviest security tasks at gateways and blockchain nodes rather than on constrained sensors.

Cybersecurity Threats in Smart Agricultural IoT

Agricultural IoT systems face threats such as device spoofing, replayed commands, packet injection, eavesdropping, malware, unauthorised access, data tampering and DDoS attacks. The consequences are serious because the systems directly influence physical farming actions. Altered measurements or blocked communication can produce excessive irrigation, missed disease alerts, wrong chemical application or malfunctioning equipment (Roman et al., 2013; Al Asif et al., 2022).

The adopted threat model is based on confidentiality, integrity and availability. Confidentiality concerns the protection of farm-production and business records. Integrity concerns the trustworthiness of sensor, gateway and control data. Availability concerns the continuous accessibility of monitoring and control services. The framework also assumes a zero-trust posture: devices are not trusted simply because they have joined the network; they must be authenticated, monitored continuously and downgraded or revoked when their behaviour becomes suspicious.

Federated Learning for IoT Anomaly Detection

Federated learning is appropriate for IoT security because it supports joint model training without moving raw data from each local environment. In this study, every gateway learns from its own farm and network streams, while a coordinator aggregates model updates and returns an improved global model. Recent IoT intrusion-detection studies report that this approach can preserve data locality while maintaining collaborative attack-learning capacity across distributed clients (Khraisat et al., 2025; Albanbay et al., 2025; Rahmati & Pagano, 2025).

Autoencoder anomaly detection is used because many IoT attacks appear as departures from normal communication or sensor behaviour. The model compresses normal patterns into a latent representation and reconstructs the original input. Observations with reconstruction errors above a selected threshold are treated as suspicious. Recent IoT cybersecurity literature continues to support deep-learning anomaly detection for DDoS, spoofing, malware and other abnormal traffic patterns, particularly when combined with decentralised or tamper-resistant security layers (Sathyabama & Katiravan, 2025; Rahmati & Pagano, 2025).

Blockchain for Authentication, Integrity and Non-Repudiation

In this study, blockchain is treated as a permissioned security and audit layer rather than as a cryptocurrency system. Known farm administrators, gateways and authorised service nodes participate in identity verification, event validation and record keeping. Recent blockchain-assisted federated learning studies describe blockchain as useful for authenticating participants, recording model updates, preserving provenance and improving auditability in IoT and smart-agriculture systems (Manoj et al., 2025; Wankhede & Patel, 2025; Jaffar, 2026). Smart contracts define how devices are enrolled, how access requests are checked, how alerts are logged and how compromised devices are revoked.

The blockchain layer supports the framework by excluding unauthorised devices, preserving tamper-resistant evidence of access and alert events, and linking security decisions to verifiable identities. Its use is limited to capable gateway and administrative nodes so that low-power sensors are not burdened with ledger operations. Recent studies also show that lightweight permissioned designs are more appropriate for agricultural and IoT deployments than public-chain consensus approaches that add high delay and computational cost (Barath & Senthil, 2026; Jaffar, 2026).

Trust-Aware Device Governance

Detection alone is insufficient in an operational farm network. After an anomaly is observed, the system must decide whether the device should continue normal operation, be monitored more closely, lose privileges or be isolated. The trust-aware layer addresses this need by assigning each device a dynamic score derived from authentication behaviour, conformity with learned patterns, frequency of anomalies and past response history. Stable devices retain higher trust, whereas repeatedly abnormal devices are downgraded or quarantined.

This trust mechanism links machine-learning output with enforceable security policy. Instead of applying only a binary allow-or-block decision, it creates graduated responses. A single unusual packet may lead to enhanced monitoring, while repeated deviations from a critical irrigation controller may lead to quarantine and a blockchain-recorded revocation event.

Prior studies have examined IoT anomaly detection, blockchain access control and federated learning as separate research streams. More recent work is moving toward integrated designs that join federated intelligence, blockchain verification and edge deployment for IoT and smart-agriculture security (Manoj et al., 2025; Wankhede & Patel, 2025; Barath & Senthil, 2026; Jaffar, 2026). The remaining gap is the limited empirical attention to smart-agriculture frameworks that add device-governance logic after detection. This study addresses that gap by evaluating a combined approach that preserves data privacy through federated training, secures identity through a permissioned ledger and translates detection evidence into trust-based response.

MATERIALS AND METHODS

Research Design

A comparative empirical design was used. Three configurations were assessed: a centralised anomaly-detection model, a federated-learning-only model and the proposed blockchain-enhanced federated learning framework with trust-aware device governance. The comparison used detection accuracy, false alarm rate, precision, recall, F1-score, training/communication overhead and blockchain latency. This design separates the effect of decentralised

learning from the additional security value introduced by blockchain authentication and trust scoring.

Proposed System Architecture

The architecture has four coordinated layers. The sensing layer contains soil-moisture, temperature, humidity and pH sensors, crop-monitoring nodes and irrigation actuators. The edge-intelligence layer performs local preprocessing, anomaly detection and federated-client training. The blockchain layer manages device identities, signed access requests, smart-contract rules and immutable event records. The trust-governance layer updates device scores and activates warnings, restrictions, quarantine or retraining when suspicious behaviour persists.

Figure 1 illustrates the data and control flow across the four layers. Raw sensor and traffic data remain at the gateway level; the federated coordinator receives model updates rather than farm records; the blockchain layer verifies identities and records security events; and the trust layer converts anomaly evidence into response actions.

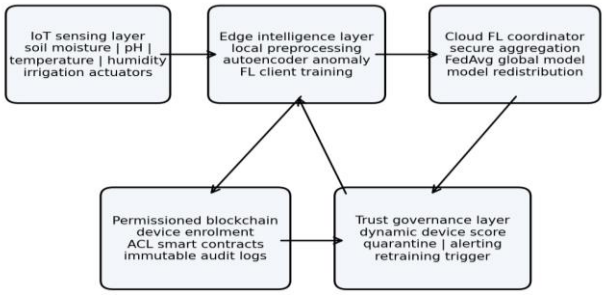

Figure 1: Architecture of the Blockchain-Enhanced Federated Learning and Trust-Aware Security Framework for Smart Agriculture

Dataset and Attack Scenarios

The evaluation used agricultural sensor streams together with IoT network-traffic records. The sensor component represented field variables such as temperature, humidity, soil moisture, pH and sensor status. The traffic component represented normal gateway communication and attack behaviour. Spoofing, replay, packet injection and DDoS scenarios were included because they target identity, message integrity and service availability in smart-agriculture networks.

For transparency, the empirical assessment was organised around normal and attack-labelled records, preprocessing logs and model-training settings. These supporting materials should be retained by the authors and supplied to reviewers or readers on reasonable request to strengthen reproducibility.

Preprocessing and Feature Engineering

Preprocessing involved normalising sensor readings so that variables measured on different scales did not dominate the learning process. Missing, extreme or implausible readings were marked before training. Network features were derived from packet frequency, transmission intervals, source identity, request type, failed authentication attempts and abnormal burst patterns. The feature set was designed to capture both agronomic behaviour and cyber-communication behaviour.

Federated Autoencoder Anomaly Detection

At each gateway, a local autoencoder was trained on normal operating patterns from the available farm and network data. The encoder learned a compact representation of input behaviour, and the decoder attempted to reconstruct the original input. Reconstruction error served as the anomaly signal: records with errors above the calibrated threshold were flagged. The gateway retained raw data locally and sent encrypted model updates to the federated coordinator.

Federated aggregation followed the standard weighted averaging principle. For K gateways, the contribution of each local model was weighted by the number of observations available at that gateway before updating the global model for the next round. This procedure supports collaborative learning across distributed farms while limiting exposure of raw data (McMahan et al., 2017; Kairouz et al., 2021).

Permissioned Blockchain and Smart Contracts

The permissioned blockchain was positioned at edge-server and administrative-node level. Smart contracts handled device registration, access verification, security-event recording and revocation. When a device joined the network, it received a unique identifier and credential; access requests were signed, validated and logged; and verified anomaly alerts or quarantine decisions were written to the ledger. This placement reflects recent evidence that blockchain-supported federated learning is most practical when ledger tasks are assigned to capable nodes rather than low-power sensors (Manoj et al., 2025; Wankhede & Patel, 2025; Jaffar, 2026).

Trust-Scoring Model

The trust-governance module translates detection evidence into security policy. Each device is assigned a score T_i within the interval 0 to 1. The score reflects authentication reliability, behavioural consistency, anomaly frequency and previous response history.

The simplified update rule is: T_i(t) = alpha T_i(t-1) + beta A_i(t) + gamma B_i(t) - delta E_i(t). In this expression, A_i represents successful authentication behaviour, B_i represents conformity with the anomaly detector, E_i represents recent security events, and alpha, beta, gamma and delta are policy weights. Devices above the acceptance threshold operate normally; devices in the warning range are monitored or rate-limited; and devices below the quarantine threshold are isolated and recorded on the blockchain.

Evaluation Metrics

The evaluation metrics were detection accuracy, false alarm rate, precision, recall, F1-score, communication/training overhead and blockchain transaction latency. Accuracy represents the share of normal and attack cases classified

correctly. False alarm rate represents benign cases wrongly labelled as attacks. Blockchain latency represents the time required to validate and record a relevant security transaction. Training and communication overhead were compared qualitatively as high, medium or low according to the cost profile of each configuration.

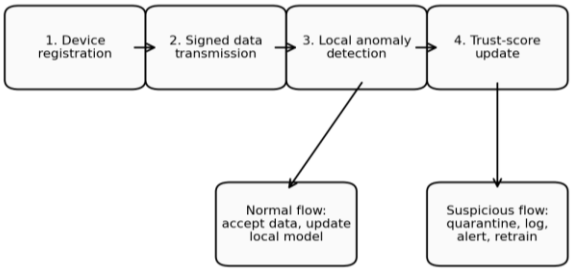

Figure 2: Workflow for Device Registration, Anomaly Detection, Trust-Score Update and Security Response

RESULTS AND DISCUSSION

The comparative results show how the three evaluated configurations performed under the selected metrics. The centralised baseline is used to show the cost of relying on one data-collection point. The federated-only model shows the effect of distributed learning. The proposed model then adds blockchain authentication and trust-aware governance to evaluate whether detection and response can be improved without unacceptable latency.

Table 1: Threat Classes and Security Functions Addressed by the Proposed Framework

Threat class	Risk in smart agriculture	Detection/control mechanism	Security property
Spoofing	False device identity or forged sensor source	Blockchain identity and signed access request	Authentication
Replay	Reuse of previously valid messages to manipulate farm actions	Timestamping, challenge-response and immutable event log	Integrity
Packet injection	Manipulated readings or command messages	Autoencoder anomaly detection and trust-score downgrade	Integrity
DDoS	Service disruption at gateway or dashboard	Traffic anomaly detection and quarantine rules	Availability
Data tampering	Incorrect irrigation, disease or resource decision	Ledger-backed event audit and anomaly evidence	Integrity/non-repudiation

Table 2: Comparative Detection Performance of Evaluated Security Configurations

Model configuration	Accuracy	False alarm rate	Precision	Recall	F1-score
Centralized anomaly detector	89%	12%	0.88	0.89	0.88
Federated-learning only	94%	8%	0.93	0.94	0.93
Proposed FL-blockchain-trust framework	97%	4%	0.96	0.97	0.96

Note. The values summarise the comparative experimental outcomes for the three evaluated security configurations. Accuracy and false alarm rate are the principal indicators used for model comparison.

Table 2 shows that the proposed framework produced the best detection profile. The centralised model achieved 89% accuracy and 12% false alarms. The federated-only model improved accuracy to 94% and lowered false alarms to 8%, indicating that collaborative edge learning improved detection while reducing raw-data dependence. The complete FL-blockchain-trust framework achieved 97% accuracy and 4% false alarms, suggesting that identity assurance, auditable logging and trust-based response improved both detection reliability and operational filtering.

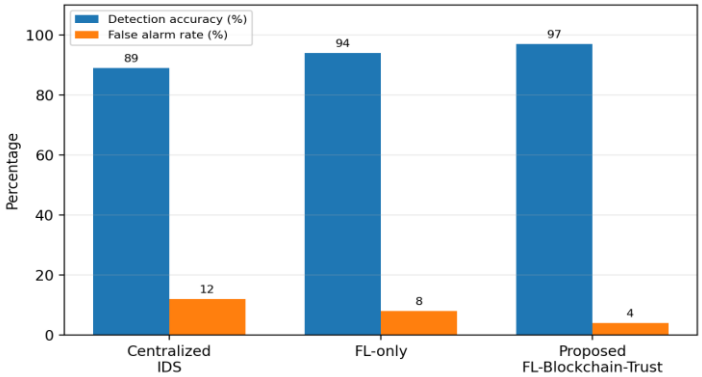

Figure 3: Detection Accuracy and False Alarm Rate across Centralised, Federated-Only and Proposed Configurations

Table 3: Operational Overhead and Blockchain Latency Profile

Configuration	Training overhead	Communication exposure	Auditability	Latency implication
Centralized model	High	High raw-data exposure	Low	No ledger latency but higher privacy risk
FL-only model	Medium	Model updates only	Medium	No blockchain latency
Proposed framework	Low-to-medium	Model updates plus signed events	High	50-100 ms per recorded security transaction

Note. The blockchain latency range reflects the reported transaction-latency profile of the permissioned ledger layer.

The latency result suggests that the blockchain component is acceptable for the security functions evaluated in this study. Device enrolment, access verification, anomaly logging and audit-trail creation do not normally require the same ultra-low latency as emergency closed-loop control. Keeping blockchain operations at gateway and administrative nodes also avoids placing heavy computation directly on field sensors.

Table 4: Trust-Score Decision Policy Used For Device Governance

Trust-score range	Device status	System action	Blockchain record
0.80-1.00	Trusted	Accept data and continue monitoring	Routine event log
0.60-0.79	Watch-listed	Increase monitoring and rate-limit suspicious bursts	Warning log
0.40-0.59	Restricted	Require re-authentication and reduce privileges	Access-control log
Below 0.40	Quarantined	Isolate device, alert administrator and trigger retraining	Revocation/quarantine log

Note. Thresholds are policy-adjustable and should be calibrated according to farm risk tolerance and device criticality.

The results indicate that distributed intelligence can strengthen IoT-enabled smart-agriculture security. The improvement from 89% accuracy in the centralised model to 94% in the federated-only model shows the value of training across edge gateways without moving raw records to a single server. This finding is consistent with recent federated-learning intrusion-detection studies, which report that distributed clients can share model knowledge while preserving local traffic and sensor data (Khraisat et al., 2025; Albanbay et al., 2025; Rahmati & Pagano, 2025).

The empirical findings support the claim that distributed intelligence improves IoT-enabled smart-agriculture security. The improvement from 89% to 94% after federated training demonstrates that collaborative edge learning can outperform a purely centralised baseline while reducing raw-data exposure. This result is consistent with recent federated-learning intrusion-detection studies, which show that distributed IoT devices can contribute model updates without surrendering local traffic or sensor records to a central server (Khraisat et al., 2025; Albanbay et al., 2025; Rahmati & Pagano, 2025).

The further improvement to 97% accuracy and 4% false alarms shows that detection quality is also affected by identity management and response governance. Blockchain improves the auditability of device identities, model-related events and security actions, while the trust score determines whether a suspicious device should remain active, be monitored, lose privileges or be quarantined. Recent smart-agriculture and IoT studies similarly argue that federated learning should be complemented by verification and provenance mechanisms when multiple devices or organisations participate in learning (Manoj et al., 2025; Wankhede & Patel, 2025; Barath & Senthil, 2026; Jaffar, 2026).

The framework is especially relevant to agriculture because many farm devices are deployed in open fields or remote locations where physical inspection is limited. An attacker may not need to compromise the cloud platform if a field sensor, gateway or irrigation controller can be spoofed or tampered with. Combining behavioural modelling, verified device identity and immutable logging reduces the likelihood that a compromised node will continue to influence farm decisions unnoticed. This position aligns with recent smart-farming blockchain studies that emphasise trust, traceability and verifiable provenance in agricultural digitalisation (Hasan et al., 2024; Manoj et al., 2025; Jaffar, 2026).

Blockchain latency of 50-100 ms is reasonable for the monitored security transactions because logging, enrolment and access verification are not as delay-sensitive as direct emergency control. The ledger layer should nevertheless remain permissioned and lightweight. Recent agricultural blockchain-federated frameworks also recommend low-latency or lightweight consensus to avoid unnecessary processing and energy burdens in smart-farm environments (Barath & Senthil, 2026; Jaffar, 2026). Public blockchain designs are therefore less suitable for this use case.

The main limitation is reproducibility documentation. Although the summary metrics are strong, reviewers may still request raw datasets, hyperparameter settings, train-test partitions, confusion matrices, smart-contract logic and hardware specifications. Trust thresholds may also require recalibration across farms, crops and sensor types. Future studies should test adaptive thresholds and reinforcement-learning-based trust tuning under seasonal and multi-farm conditions.

CONCLUSION

This study evaluated a blockchain-enhanced federated learning and trust-aware security framework for IoT-enabled smart agriculture. The framework targets three connected problems in farm-IoT security: centralised data exposure, weak assurance of device identity and the absence of structured response after anomaly detection. Federated autoencoder learning allows gateways to learn abnormal sensor and traffic behaviour without centralising raw farm data. Permissioned blockchain supports device enrolment, access-control enforcement, immutable event records and non-repudiation. Trust-aware governance then converts anomaly evidence into watch-listing, restriction, quarantine and retraining decisions. This design reflects the recent research direction in which federated learning, blockchain verification and edge governance are combined to improve privacy, auditability and resilience in IoT and smart-agriculture environments (Wankhede & Patel, 2025; Barath & Senthil, 2026; Jaffar, 2026). The proposed framework achieved 97% detection accuracy, reduced the false alarm rate to 4% and maintained blockchain latency within 50-100 ms. these outcomes indicate that combining federated learning, permissioned blockchain and trust scoring can improve confidentiality, integrity, availability and operational resilience in smart-agriculture systems. The study

recommends gateway-centred security architectures for smart-agriculture deployments, rather than placing excessive computation on constrained field sensors. Farm operators should maintain verifiable device registries, enforce signed access requests, monitor behavioural trust scores and preserve tamper-resistant logs of critical security events. Further research should evaluate the framework with larger multi-farm datasets, include energy-consumption analysis, test adaptive trust thresholds and publish benchmark smart-agriculture cybersecurity datasets for reproducible comparison.

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

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. 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., Gascon, 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

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

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.

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

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks, 57(10), 2266-2279. https://doi.org/10.1016/j.comnet.2012.12.018

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

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