International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(1s) 2026 pp. 328-338
https://doi.org/10.70917/ijcisim-2026-2274
Article

A COMPREHENSIVE ANALYSIS ON TRUST-AWARE FEDERATED LEARNING IN IOT EDGE COMPUTING

M. Jayakeerthi[1], A. Sherin[2]

[1]Department of Computer Science, Nehru Arts and Science College, Tamil Nadu, India.
Email: sathyjaya@gmail.com
ORCID: 0000-0003-1840-9894
[2]Department of Digital Cyber and Forensic Science, Nehru Arts and Science College, Tamil Nadu, India.
Email: sherinfaizalrahiman@gmail.com
ORCID: 0000-0002-8801-6132

Abstract: Federated Learning has been among the prevalent methods that enable cooperation in machine learning as well as maintaining privacy in decentralized networks like Internet of Things (IoT), healthcare, edge computing and smart systems. Nevertheless, federated learning has experienced some challenges including privacy issues, increased communication costs, managing node trust issues, client malicious updates, data poisoning and scalability issues. This survey will review 26 research papers about federated learning which have been published between 2024 and 2026. The fields related to the above-mentioned research papers include various fields such as differential privacy, trust aware learning, block chain based federated learning, federated learning, Explainable AI, edge intelligence, intrusion detection and health care analytics. Various techniques utilized in the above-mentioned research papers include Differential Privacy (DP), Generative AI, Convolutional Neural Network (CNN), LSTM, GNN, Blockchain, MARL and Trust ManagementHowever, based on the findings from the report, the efficiency is quite clear and accurate, while at the same time the increase in level of trust , the reduction of communication overhead and the ability to resist any attacks. The most important thing that one should keep in mind based on the findings from the survey is that despite all the successes, the development of the next generation FL framework that consists of four key factors is very necessary.

Keywords: Causal Reasoning, Communication Efficient Learning, Energy Aware Routing, Non-IID Data, Split Federated Learning, Smart Grid

1. Introduction

Moreover, the Federated Learning (FL) could be considered another interesting approach that will contribute to the development of collaborative intelligence while retaining privacy in the use of data. In today's environment, people have much interest in privacy preservation, edge intelligence, intrusion detection and trust management, where health data analysis becomes a protected procedure in IoT-based systems, which allows solving such challenges as data exchange problem, security threat and communication efficiency. Researchers designed and implemented a federated learning approach that considers the concept of differential privacy in its essence, allowing for secure collaboration among distributed institutions to obtain correct COVID-19 diagnosis based on chest x-rays [1]. Building on this approach, further development involves designing of a federated learning model for heart disease prediction with the help of differential privacy and FedHybrid framework to allow for efficient knowledge sharing among different data sources while retaining the accuracy of the prediction [2]. Federated learning using generative artificial intelligence was another approach put forward to improve the security of the Internet of Things [3]. In order to provide smart solutions for the healthcare sector, federated learning combined with trust management was put forth, given the benefits associated with the concept of trust evaluation. The benefit here included enhanced security, energy efficiency

and reliability since healthcare analytics were produced by such a solution [4]. Besides, federated CNN was utilized for detecting attacks on the IoT based network infrastructure without revealing any local information [5].

The idea of improvement of intelligence using AI technology in the field of healthcare services was put forward so that intelligent operation of healthcare can be optimized using trust-aware mobile edge computing which will lead to efficient resource management, healthcare services provision and intelligent decision-making for secure communication between distributed medical Internet of Things (IoT) devices [6]. A combined methodology that uses both Deep Learning and Starfish Optimization Algorithm has been presented to improve smart cities with brighter edge computing, efficient resource allocation, cybersecurity measures, threat detection capabilities and scalability of edge intelligence [7]. Moreover, trust and energy-aware federated learning methodology has been used to ensure efficient secure data transmission processes, routing procedures and energy conservation in IoT fog-cloud infrastructures [8]. In the same way, a federated architecture of edge intelligence enabled by trustful access control has also been designed for enhanced management of resources, maintaining privacy and collaborating among distributed edge devices [9]. The security of Split Federated Learning algorithms from attacks due to data poisoning has been explored revealing a number of security vulnerabilities and the requirement for developing secure mechanisms [10].

To address the challenges that may arise due to security concerns associated with health care apps, federated learning coupled with a trustworthy verification system to avoid all kinds of data poisoning attacks has been proposed, making sure the model is trustable and reliable [11]. Trust-aware blockchain-based split federated learning approach has been introduced to discover any intrusion activities within 6G healthcare Internet-of-Things networks owing to its decentralized nature and secure and trustworthy traits to assure collaboration and data security [12]. Federated learning and differential privacy approaches have been used for arrhythmia detection problems with personalization of learning, privacy, intelligence and accuracy of diagnosis [13]. Another important use of private-dependent deep federated learning model has been developed for the purpose of detecting infection outbreaks as early as possible with the use of genome sequencing data in order to ensure privacy, security and efficient infection disease detection along with data confidentiality while sharing minimal data from genome data [14]. Another application of federated learning with XAI approach is that of the intelligent energy management of a smart building wherein privacy is ensured during such operations [15].

Nonetheless, the existing approaches have not been successful in solving the aforementioned issues regarding privacy, improved communication, trust management and attack prevention. There is a lot of research that needs to be conducted in order to come up with a useful architectural framework that will solve the aforementioned issues. This paper focuses on developing a solution through the provision of an architectural framework that can solve the aforementioned issues in order to develop a sustainable IoT and healthcare ecosystem.

2. Background study

Table 1: Performance Evaluation of Recent Privacy-Preserving and Secure Federated Learning Frameworks

Author, Year & Ref. No.	Concept	Methods	Limitations	Research Gap	Results
Shankar et al. (2026) [16]	Privacy-adaptive FL for healthcare	DP, PFL, Adaptive Optimization	High communication cost	Need efficient privacy-aware FL	Improved privacy and healthcare learning performance
Alshaya (2025) [17]	Secure IoT device identification	LSTM, DECOC, DP-FL	Limited IoT scalability	Need scalable IoT identification	High accuracy, 95.5% F1-score, 25% fewer rounds
Al Tfaily et al. (2025) [18]	Graph FL for IoT IDS	GAT, GraphSAGE, FL	High graph processing cost	Need lightweight	Comparable to centralized models, 85%

				IDS models	communication reduction
Alqazzaz (2026) [19]	Privacy-aware IIoT anomaly detection	FL, DP, Encryption, RL	Encryption delay, static topology	Need trust-aware secure FL	88.5% F1-score, 53% overhead reduction, 35% energy saving
Khraisat et al. (2025) [20]	Privacy-preserving IoT IDS	FL, FedAvg, FedAvgM	Communication and trust issues	Need efficient trust-based FL	95.05% accuracy, 3.9% FPR, faster convergence
Bhasker et al. (2025) [21]	Blockchain-FL healthcare IoT	Blockchain, FL, IoT-IDS	High complexity, scalability issues	Need scalable blockchain-FL	High security, high IDS efficiency, 96.42% diagnosis accuracy
Karunamurthy et al. (2025) [22]	FL-based IoT intrusion detection	FL, DL Classifier, Chimp Optimization	Complex attack patterns	Need adaptive IDS optimization	95.59% intrusion detection accuracy

Table 1 provides a comparative study of the latest federated learning platforms that have been developed concerning privacy protection, IoT security, healthcare intelligence and decentralized applications. It indicates the methodologies used, their drawbacks, challenges faced during research and finally, the outcomes obtained. It is observed that the selected methodologies provide better accuracy, low communication overhead, enhanced privacy and secure learning.

Karunamurthy et al. (2025) [22] introduced a federated learning approach towards designing an intrusion detection system in IoT-based systems. In this approach, federated learning, along with optimization techniques, was used in order to increase the attack detection rate without compromising the privacy of data. Although the proposed model exhibited improved detection accuracy and reduced communication costs, it only concentrated on intrusion detection and had no explainability or adaptive capabilities.

Alandjani (2025) [23] proposed MARL-Federated Quantum-Secure Trust Management Framework based on Blockchain for Industrial IoT. In this research, the methodology adopted the use of blockchain technology, federated learning and reinforcement learning to ensure that trust evaluation is achieved. The study found that there was an improvement in trust management as well as cybersecurity. One major drawback with this framework was its high computational complexity.

Asiri (2026) [24] developed a federated learning-based framework with causality reasoning for detecting cyber threats in the IoT environment. The proposed approach incorporated the concepts of explainable AI and federated learning techniques to ensure that the detection was accurate and interpretable. Unfortunately, there were no adaptivity elements in place. The gap identified is that of incorporating adaptive systems into the framework.

A cloud-based federated learning framework using blockchain technology was provided by Baihan et al. (2026) [25] to improve IoMT-based systems security and privacy. The use of blockchain, cloud computing and federated learning helped achieve better security and privacy. Nevertheless, the communication and computational burden were still considerable. The research gap includes developing lightweight and adaptable healthcare frameworks.

Blockchain-based federated microservice architecture for privacy-oriented healthcare analytics was proposed by Harshith et al. (2026) [26]. The technique offered data security and scalability of data analysis in the healthcare

domain. Improved privacy protection, data integrity and scalability were observed from the findings. But the problem of service orchestration complexity and latency remained unresolved. Thus, the scope of research includes adaptive and intelligent federated healthcare models.

2.1 *Research Gap*

Several contributions have been made towards federated learning; the existing research has generally focused on aspects such as privacy preservation, intrusion detection, trust management and secure aggregation in silos. It is therefore clear that what is required here is an integrated solution that incorporates all the above concerns in one fell swoop. Besides, there is a limited number of solutions proposed to mitigate data poisoning attacks, Byzantine attacks and other forms of threats posed by malicious clients. Furthermore, solutions such as blockchain, explainable AI and split federated learning entail heavy overhead costs.

3. Federated learning that preserves privacy and is communication-friendly

The differential privacy technique was used in federated learning to identify the existence of COVID-19 from chest X-rays, ensuring that privacy is maintained, yet obtaining a high accuracy rate in diagnosing the disease [1].

Privacy-preserving federated learning approach is developed to predict heart disease cases in several centers with the use of differential privacy and hybrid optimization algorithms. This allowed improving the models' generalization capacity based on heterogeneous datasets, preventing privacy risks and ensuring their accuracy [2].

The federated learning architecture developed was a mixture of GenAI aimed at enhancing privacy and security in intelligent settings. It improved the effectiveness of collaborative learning, guaranteed data privacy and reduced the risks of centralized data processing [3].

3.1 Federated learning frameworks that are trustworthy, reliable and secure

However, some flaws within the context of poisoning attacks against SFL have been recognized. Hence, it can be seen that there existed certain weaknesses in the collaborative learning process and improvements in the area of verifying such malicious updates have been emphasized [10].

In view of protecting any system from data poisoning attack attempts, the usage of federated learning has been recommended as the method that could protect such systems from any such attacks within the realm of e-healthcare. The model proposed relied on the idea of using secure validation, which could detect any malicious entities [11].

A technique that uses blockchain technology in trust-aware split federated learning for intrusion detection in the Internet of Things in healthcare applications has been proposed. The use of blockchain security techniques and trust management techniques has greatly improved the robustness of this specific technique against any type of threat [12].

3.2. Federated learning for edge intelligence, healthcare and bright applications

This can be done by integrating federated intelligence within the mobile edge computing framework for optimizing the healthcare environment in terms of efficiency and effective utilization of resources as well as providing security for the learning process of the medical devices [6].

The following architecture of edge computing has been built especially for implementing it for smart cities. Some considerations which should be taken into account while designing this architecture include reliable processing of data, smart resource management, cybersecurity and edge computing [7].

As per the idea of federated learning, some ideas of trustworthiness and energy efficiency were used for designing an improved routing protocol algorithm in the realm of IoT [8], which resulted in improved efficiency in communication and energy savings.

For the federated edge intelligence model, a trusted-based access control scheme was implemented to provide safety and protection in terms of security and privacy of the IoT system. This was done through a process that facilitated resource sharing, resource management and collaboration learning at the edge of the network [9].

Table 2: Performance Analysis of Existing Federated Learning Frameworks

Reference	Proposed Framework / Concept	Methods Used	Dataset / Application Area	Key Results
Ahmed et al. (2024) [1]	Differential Privacy-enabled Federated Learning (DPFL) for COVID-19 diagnosis	Federated Learning, Differential Privacy, Privacy Masking, Gradient Clipping, Privacy-Utility Optimization	Chest X-ray images for COVID-19 detection	Privacy masking initially reduced accuracy by 3%; adaptive clipping improved efficiency by 1% while reducing communication rounds and maintaining diagnostic performance.
Dubey et al. (2025) [2]	FedHybrid algorithm with Differential Privacy for healthcare diagnosis	Personalized Federated Learning, Differential Privacy, FedHybrid optimization, FedAvg and FedProx comparison	Multicenter heart disease datasets	Achieved 91.6% accuracy within five communication rounds using five clients, outperforming FedAvg and FedProx which required more communication rounds.
Khan et al. (2025) [4]	Trust-based Federated Learning for smart healthcare systems	Trust Management, Federated Learning, Hybrid learning mechanism, Security evaluation	Smart healthcare applications	Achieved 95% accuracy and reduced computational complexity by 52.5%, demonstrating improved reliability and efficiency through trust evaluation mechanisms.
Wang and Wang (2026) [8]	Federated Learning-based Trust and Energy-Aware Routing (FL-TEAR) for IoT fog-cloud environments	Federated Learning, Trust Management, Energy-aware routing, Fog-cloud communication optimization	IoT fog-cloud networks	Improved trust efficiency by 23%, reduced energy consumption by 23%, increased packet delivery by 13% and decreased network latency by 37%.
Padmavathi and	AI-SET framework for	Federated Learning, Trust-based Access Control, Machine	Secure IoT systems	Achieved 94.3% accuracy with 3.2% false-positive rate, 150 ms

Saminathan (2025) [9]	secure edge intelligence	Learning, Edge Intelligence		latency and blocked 87% of unauthorized access attempts.
Karunamurthy et al. (2025) [22]	Federated Intrusion Detection System for IoT security	Federated Learning, Chimp Optimization Algorithm, Machine Learning-based intrusion detection	IoT intrusion detection networks	Achieved 95.59% intrusion detection accuracy and outperformed conventional machine learning-based detection approaches.

The following table 2 is an evaluation of selected federated learning techniques for privacy-preserving, trust management, communication effectiveness, healthcare intelligence and IoT security applications. The selected approaches have been shown to increase accuracy, decrease communication overhead, improve energy efficiency and ensure robust security by incorporating different aspects of differential privacy and optimization.

4. Comparison Study on the Federated Learning Models Utilizing Deep Learning Approaches for Secure IoT Applications

The following section will cover the comparison of federated learning models which are used for ensuring the privacy of the system against the attacks and intrusions. There are several health intelligence applications and also IOTs where the deep learning model can be implemented. The selection of federated learning models is such that advanced deep learning techniques including CNN, LSTM, GNN, GenAI and others have to be implemented. These models involve intrusion detection, better communication, better security against any attacks and also trust management among others.

4.1 Deep Learning-Based Federated Learning Frameworks Result Analysis

The Generative AI, in combination with Hybrid Federated Learning, was used in Ramalingam et al. (2026) to improve aspects related to privacy and security in IoT smart environments. Using the help of millions of sensor data and IoT traffic flow, it was possible to strike a balance between privacy preservation, accurate outcome prediction and reduced energy consumption.

Torre et al. (2025) [5] proposed the use of CNNs in Federated Learning for the task of intrusion detection on multiple datasets from the Internet of Things. This algorithm managed to yield accuracy, precision, recall and f1 score of 95.59%, 92.43% and 92.69% respectively.

The proposed research paper has presented an innovative mobile edge computing framework using AI for healthcare Internet of Things networks. The new ECTI framework has been able to improve trust stability up to 39.4% and even reduce packet loss up to 43.2% despite the presence of faulty nodes.

FL-HDECOC [17] was developed in 2025 by Alshaya through the fusion of Long Short-Term Memory (LSTM) neural networks with error-correction coding to address the challenge of IoT devices recognition. This has been validated by its ability to achieve an high accuracy rate and F1-Score of 95.5%, as well as lowering communication rounds by 25%.

FedGATSage Framework Proposed by Al Tfaily et al. (2025) [18] The FedGATSage framework is proposed by Al Tfaily et al., which utilizes the combination of Graph Neural Networks and Federated Learning in order to identify intrusions. This technique has shown an improvement of 85% in the communication overhead with respect to centralized learning techniques.

The SecuFL-IoT architecture was introduced by Alqazzaz (2026) [19] and used adaptive privacy-preserving anomaly detection. It was achieved with an F1-score of 88.5%, a reduction in communication cost by 53%, 23% more rapid convergence and energy savings of 35% in comparison with others. Also, its tolerance towards data poisoning attacks was less than 9%.

Split federated learning based on blockchain technology has been introduced by Baihan et al. (2026) [25]. The authors have used the CNN and BiLSTM models for implementation of IoMT Healthcare 5.0 system. This technique

has produced the best results compared to other deep learning methods. The proposed approach achieved an exceptionally good intrusion detection has high accuracy,as well as a block commitment speed of 450 blocks per second with 250 ms consensus time.

4.2 Comparative Analysis of Federated Learning Frameworks (2024–2026)

The following comparative analysis has been performed for the frameworks for federated learning that were proposed in the period between 2024 and 2026. Various applications such as IoT systems, healthcare systems, edge computing systems, smart buildings, Industrial Internet of Things and smart city systems were considered in the analysis. The aim of this comparative analysis is to determine to what extent these systems may contribute to resolving the issues related to the distributed learning environment. The following criteria have been considered in the comparative analysis of the federated learning framework, namely privacy, trust management, blockchain technology, explanation, attacks protection, effective communication and intelligent optimization. Great progress has been made in addressing the issues of security and privacy in distributed machine learning systems. Nevertheless, there are numerous issues which have yet to be addressed in the process. Among the problems to be solved are scalability, high communication costs, intelligent trust evaluation and handling attacks.

The IoT Fog-Cloud based model was used by Wang and Wang (2026) [8], who devised FL-TEAR algorithm that includes the elements of trust-aware routing and federated learning techniques. This research involved trust calculation, federated learning of models and energy efficient routing and its main benefit lies in achieving at once such important things as privacy preserving federated learning which is trust-aware and energy efficient routing. The FL-TEAR approach produced 23% more accuracy of trust calculation, consumed 23% less energy, increased packet delivery rate by 13% and reduced network latency by 37%.

Evaluation of Split Federated Learning against attacks was done by Zahir-Ismail and Shukla (2025) [10] based on data poisoning attack evaluation. As per the results obtained, it can be seen that in case of MNISTv1, accuracy dropped from 96.46% to 89.86%, whereas for MNISTv2, the accuracy became 86.06% when there were 20% malicious clients.

As stated by Alruwaili and Moulahi (2026) [11], a Verifiable Federated Learning Framework has been created through the use of the E-Health dataset. This research was novel in its own way because it introduced verifiable security against attacks that were of the poisoning kind. FedSecure-Chain has attained a 94-95% of accuracy under conditions of clean non-IID.

Babar et al. (2026) [12] used the datasets ToN-IoT and IoT-Healthcare along with Blockchain technology and Split Federated Learning for trust-aware intrusion detection. The innovation in their work pertained to using blockchain-based Split Federated Learning. With the proposed TAWB-SFL technique, high accuracy was achieved in intrusion detection within 250 milliseconds for consensus time.

In the medical diagnosis personalization task, Bokhari et al. (2025) [13] successfully personalized the medical diagnosis in ECG Arrhythmia dataset using personalized federated learning with differential privacy on 10646 records. A novel approach that fuses personalized federated learning and differential privacy was introduced.A novel approach that fuses personalized Variable privacy and united learning were introduced. With F1-scores of 0.93(AFIB), 0.88(GSVT) and 0.9042 MCC, FLPMDP outperformed current deep learning methods, achieving a 93.71% average accuracy, 0.98 specificity, 0.8971 Kappa score and 0.9042 MCC.

In their study, Khan et al. (2025) [14] made use of the Smart Building Energy Dataset, where it implemented the concept of federated learning along with explainable artificial intelligence (XAI) to ensure secure federated energy management and prediction, whereby the new idea was the XAI-based federated energy optimization technique. The Federated Random Forest Model gave an overall Training MSE of 0.6235, Testing MSE of 0.6656, Testing MAE of 0.6397 and Overall R^2 of 0.8036.

Khan et al. (2025) [15] adopted the similar approach with the Smart Building Energy dataset, which is a combination of federated learning and XAI to secure energy management while applying a novel perspective to embed XAI into the Federated Energy Optimization process. The performance obtained on the energy consumption forecasting problem using the best trained MSE = 0.6235, test MSE = 0.6656, test MAE = 0.6397 and R2 = 0.8036 is better than the performance obtained by the benchmark models (Gradient Boosting, XGBoost, LightGBM and Deep Learning).

In their research, Bhasker et al. (2025) [21] used an IoT dataset from the healthcare industry, which is an application area where blockchain and federated learning are applied to secure healthcare data sharing with the added novelty of a sustainable blockchain-based healthcare framework. The accuracy of FBI-SHS for data privacy and security, intrusion detection efficiency, disease detection accuracy, proactive healthcare management and interoperability in Healthcare 5.0 environment were achieved high accuracy respectively.

The novel feature of a quantum secure trust management framework proposed by Alandjani (2025) [23] was used in the evaluation of trust and in achieving blockchain consensus on Edge-IIoT and Federated MNIST datasets. The federated blockchain framework based on MARL has reached more than 92% precision and recall at 15 epochs and the F1-score has increased from 0.89 to 0.93, showing an effective trust assessment in non-IID IIoT environments.

Asiri 2026 [24] extended the IDSIoT2024 data set with the novelty of explainable federated learning and causal reasoning for creating a Causal Explainable Federated Learning (CEFL) framework for causal discovery and intrusion detection tasks. Causal-FL-ID was evaluated by 10, 25 and 50 clients and shown to have high ID performance and scalability and offer transparent causal explanations and counterfactual capabilities.

Harshith et al. [26] used 100,000 Synthea records and 20,000 diabetes records as well as a combination of federated learning, blockchain and microservices to provide scalable healthcare analytics, with the innovation of a federated microservices architecture. It was discovered that this architectural design could predict results with 95.2% accuracy, reduced latency by 42%, recovery time was increased by 10-fold and no success of the breach was found, showing that the architecture is scalable, private and resilient when conducting healthcare analytics.

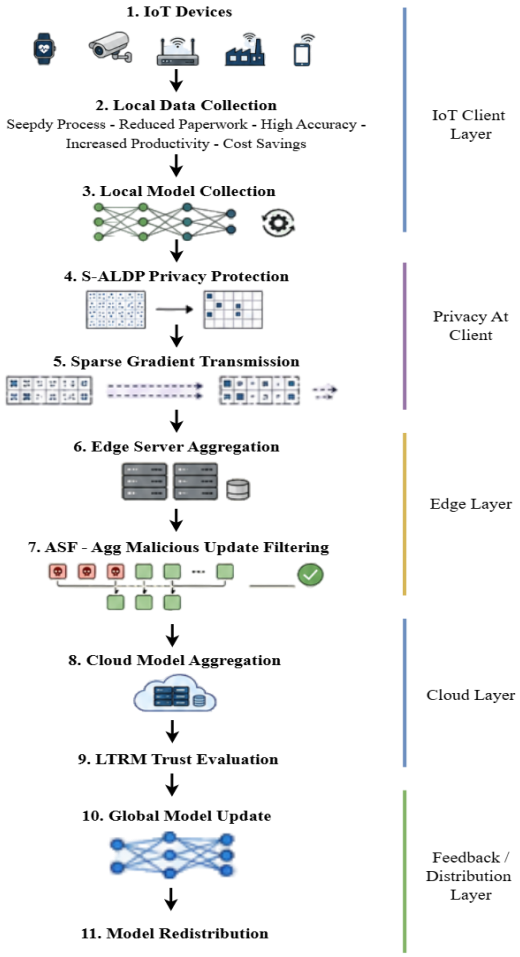

Figure 1: Secure and Adaptive Lightweight Differential Privacy Federated Learning Framework for IoT Environment

Figure 1 represents the S-ALDPF framework, which is built to address issues related to privacy preservation within IoT networks. Under this architecture, the process initiates with the distributed IoT nodes training models using their local data but without sending any raw data to others. Following that, local updates on the model training are protected by the adaptive differential privacy technique before their communication. To minimize communication costs, the sparse gradient transmission mechanism is adopted, transferring only meaningful updates. Afterward, the created model updates are aggregated at both the edge and cloud levels using the ASF-Agg algorithm that was introduced. The main reason behind developing such an algorithm lies in its role in detecting and filtering any malicious or abnormal model updates. Further, the reputation management scheme determines the level of trust of each client during each federated learning round. Finally, the aggregated global model will be transmitted back to all IoT participants.

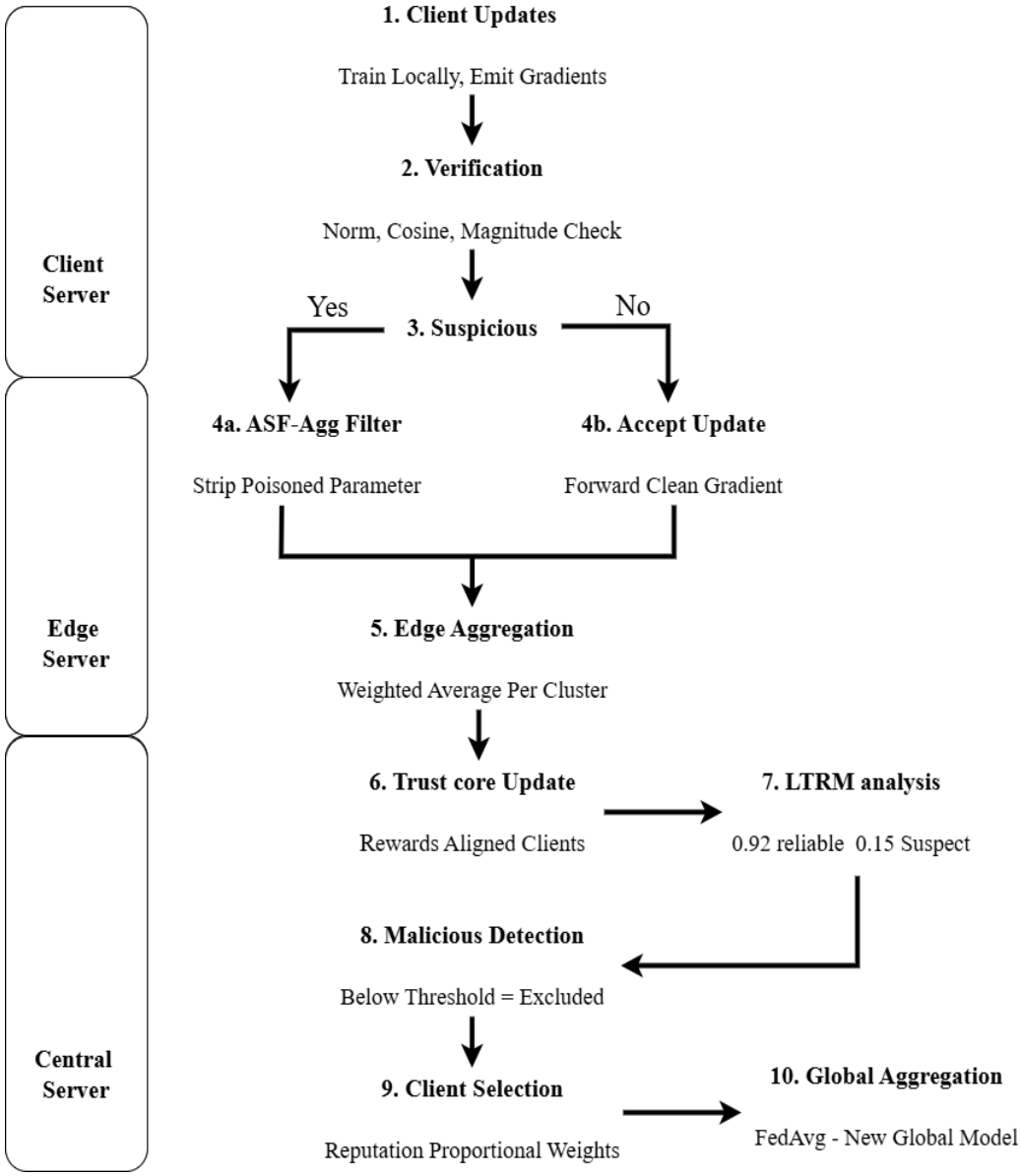

Figure 2: Trust-Driven Security for Federated Aggregation Using ASF-Agg and LTRM

The secure federated aggregation procedure is depicted in Figure 2, where the client model update values are validated and any abnormal gradient values are filtered out using the ASF-Agg protocol. Next, the LTRM module verifies the trust score and discards any malicious clients before carrying out the aggregation step. Ultimately, this generates a secure federated global model.

5. Conclusion

A literature survey is conducted, involving 26 scholarly papers written between 2024 and 2026. The topics discussed by the authors are various and touch on different issues concerning security, trust management, intrusion detection, healthcare intelligence and edge computing are some of the areas covered and security application of IoT through federated learning techniques. The approaches used by the authors in the papers under review involve numerous different techniques, such as differential privacy, deep learning, LSTM, reinforcement learning, knowable AI, split federated learning, microservices and block-chain. It seems that the application of those techniques in the above-reviewed literature indicates certain possibilities for the development in the future as regards privacy protection, intrusion detection, trust management, reducing communication overhead and improving the prediction performance of federated learning models. However, some challenges such as the presence of adversarial nodes, data poisoning, communication overhead, scalability and computational complexity may arise during the application of federated learning algorithms. In order to overcome this issue, it may be applying S-ALDPF strategy, which includes four approaches: adaptive differential privacy, sparse gradient communication, ASFAgg filtering technique and LTRM-based trust management.

References

1. Ahmed, R., Maddikunta, P. K. R., Gadekallu, T. R., Alshammari, N. K., & Hendaoui, F. A. (2024). Efficient differential privacy enabled federated learning model for detecting COVID-19 disease using chest X-ray images. Frontiers in Medicine, 11, 1409314. https://doi.org/10.3389/fmed.2024.1409314
2. Dubey, M., Tembhurne, J., & Makhijani, R. (2025). Enhancing Federated Learning Through Differential Privacy: Introducing FedHybrid for Multicenter Diverse Heart Disease Datasets. IEEE Transactions on Emerging Topics in Computational Intelligence, 9(6), 4217–4230. https://doi.org/10.1109/TETCI.2025.3575420
3. Ramalingam, V., Kumar, B., Gupta, S.K. et al. A hybrid federated learning framework with generative AI for privacy-preserving and sustainable security in IOT-enabled smart environments. Sci Rep 16, 3071 (2026). https://doi.org/10.1038/s41598-025-31769-6
4. Khan, S., Imtiaz, N., Biswas, A. K., Siddique, Z. B., & Khan, Q. A. (2025). An Expert Hybrid Federated Learning and Trust Management for Security, Efficiency, and Power Optimization in Smart Health Systems. IEEE Access, 13, 58191–58210. https://doi.org/10.1109/ACCESS.2025.3556628
5. Torre, D., Chennamaneni, A., Jo, J., Vyas, G., & Sabrsula, B. (2025). Toward Enhancing Privacy Preservation of a Federated Learning CNN Intrusion Detection System in IoT: Method and Empirical Study. ACM Transactions on Software Engineering and Methodology, 34(2), 1–48. https://doi.org/10.1145/3695998
6. Alamri, M., Haseeb, K., Humayun, M., et al. (2026). AI-Embedded IoT Healthcare Optimization With Trust-Aware Mobile Edge Computing. Scientific Reports, 16, 10. https://doi.org/10.1038/s41598-025-29370-y
7. Alkhalifa, A.K., Aljebreen, M., Alanazi, R. et al. Leveraging hybrid deep learning with starfish optimization algorithm based secure mechanism for intelligent edge computing in smart cities environment. Sci Rep 15, 33069 (2025). https://doi.org/10.1038/s41598-025-11608-4
8. Wang, F., & Wang, K. (2026). Federated Learning-Based Trust and Energy-Aware Routing in Fog–Cloud Computing Environments for the Internet of Things. Scientific Reports, 16, 2244. https://doi.org/10.1038/s41598-025-32010-0
9. Padmavathi, V., & Saminathan, R. (2025). A Federated Edge Intelligence Framework With Trust Based Access Control for Secure and Privacy Preserving IoT Systems. Scientific Reports, 15, 35832. https://doi.org/10.1038/s41598-025-19712-1
10. Zahir-Ismail, A. T., & Shukla, R. (2025). Analyzing the Vulnerabilities in Split Federated Learning: Assessing the Robustness Against Data Poisoning Attacks. Scientific Reports, 15, 30468. https://doi.org/10.1038/s41598-025-15993-8
11. Alruwaili, E., & Moulahi, T. (2026). A Robust and Verifiable Federated Learning Framework for Preventing Data Poisonous Threats in E-Health. Frontiers in Public Health, 14, 1762346. https://doi.org/10.3389/fpubh.2026.1762346
12. Babar, M., Khan, Z., Kaleem, S., Qureshi, B., & Boulila, W. (2026). TAWB-SFL: Trust-Aware Blockchain-Orchestrated Split Federated Learning for Intrusion Detection in 6G Healthcare IoT. IEEE Open Journal of the Communications Society, 7, 2270–2286. https://doi.org/10.1109/OJCOMS.2026.3667693
13. Bokhari, S. M., Sohaib, S., & Shafi, M. (2025). Fusion of Personalized Federated Learning (PFL) with Differential Privacy (DP) Learning for Diagnosis of Arrhythmia Disease. PLOS ONE, 20(7), e0327108. https://doi.org/10.1371/journal.pone.0327108
14. Mehedi, S.T., Abdulrazak, L.F., Ahmed, K. et al. A privacy-preserving dependable deep federated learning model for identifying new infections from genome sequences. Sci Rep 15, 7291 (2025). https://doi.org/10.1038/s41598-025-89612-x
15. Khan, M. A., Farooq, M. S., Saleem, M., Shahzad, T., Ahmad, M., Abbas, S., & Abu-Mahfouz, A. M. (2025). Smart Buildings: Federated Learning-Driven Secure, Transparent and Smart Energy Management System Using XAI. Energy Reports, 13, 2066–2081. https://doi.org/10.1016/j.egyr.2025.01.063

16. Kirupa Shankar, K. M., & Santhi, V. (2026). Privacy-Adaptive End-to-End Federated Learning Framework With Self-Learning Differential Privacy and Personalized Optimization for Secure Healthcare Intelligence. Complex & Intelligent Systems, 12, 132. https://doi.org/10.1007/s40747-026-02266-8
17. Alshaya, S. A. (2025). Federated Learning With LSTM and Error Correcting Codes for Secure and Private Identification of IoT Devices. Scientific Reports, 15, 44587.
18. Al Tfaily, F., Ghalmane, Z., Brahmia, M. E. A., et al. (2025). Graph-Based Federated Learning Approach for Intrusion Detection in IoT Networks. Scientific Reports, 15, 41264.
19. Alqazzaz, A. (2026). SecuFL-IoT: An Adaptive Privacy-Preserving Federated Learning Framework for Anomaly Detection in Smart Industrial Networks. Scientific Reports, 16, 4107.
20. Khraisat, A., Alazab, A., Alazab, M., Obeidat, A., Singh, S., et al. (2025). Federated Learning for Intrusion Detection in IoT Environments: A Privacy-Preserving Strategy. Discover Internet of Things, 5, 72. https://doi.org/10.1007/s43926-025-00169-7
21. Bhasker, B., Rao, P. M., Saraswathi, P., et al. (2025). Blockchain Framework With IoT Device Using Federated Learning for Sustainable Healthcare Systems. Scientific Reports, 15, 26736. https://doi.org/10.1038/s41598-025-06539-z
22. Karunamurthy, A., Vijayan, K., Kshirsagar, P.R. et al. An optimal federated learning-based intrusion detection for IoT environment. Sci Rep 15, 8696 (2025). https://doi.org/10.1038/s41598-025-93501-8
23. Alandjani, G. A MARL-federated blockchain-based quantum secure framework for trust management in industrial internet of things. Sci Rep 15, 39149 (2025). https://doi.org/10.1038/s41598-025-23055-2
24. Asiri, F. Explainable federated learning through causal reasoning for intrusion detection in IoT. Discov Internet Things 6, 23 (2026). https://doi.org/10.1007/s43926-026-00292-z
25. Baihan, A., Kryvinska, N., Amoon, M. et al. Cloud assisted blockchain-enabled split federated learning framework for security and privacy-preserving of IoMT in healthcare 5.0. Sci Rep 16, 15599 (2026). https://doi.org/10.1038/s41598-026-41771-1
26. Harshith, M., Ansari, Z.A., Fatima, S. et al. Federated microservices architecture with blockchain for privacy-preserving and scalable healthcare analytics. Sci Rep 16, 9023 (2026). https://doi.org/10.1038/s41598-026-39837-1