Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

Threats, Problems, and Secure Framework of Aggregation in Federated Learning (FL) in IoT

Gaddapaara Swetha
Research Scholar, Department of CSE
Malla Reddy University
Hyderabad

Dr. J. Pradeep Kumar
Professor, Department of CSE
MallaReddy University
Hyderabad

***Abstract*-Increase in the high rate of Internet of Things (IoT) devices has led to massive volumes of sensitive data which have to be processed by learning structures that are both safe and do not undermine privacy. Federated Learning (FL) is one of the potential solutions that have been identified as a guarantee of training a model without the need to gather the data at a single point. However, FL is vulnerable to different security attacks including poisoning attacks, model inversion, free-riding and unsecured aggregation. In the present study, the shortcomings of FL in the context of IoT environment are discussed and a secure architecture of aggregation is provided in the form of lightweight encryptions, anomaly detection and selection of clients by trust. The simulation of the simulation experiments with simulated data of the IoT indicates that the malicious update resilience is improved and that the model accuracy and the low cost of communication are also high. The proposed solution provides the scalable and secure learning architecture that may be applied to the next-generation IoT applications.**

Keywords- Federated Learning,IoT Security,Secure Aggregation, Adversarial Attacks, Edge Computing, Privacy Preservation.

1.INTRODUCTION

The development of the Internet of Things (IoT) ecosystem has been accelerating dramatically, which leads to the presence of billions of connected devices that constantly produce huge amounts of heterogeneous and sensitive data. The conventional centralized machine learning methods involve consolidation of such data into one server in the cloud that creates serious privacy issues, network constraints and high communication expenses. Federated Learning (FL) has become an exciting alternative paradigm of decentralized learning that allows performing training on global models by using IoT devices without exchanging raw data. FL would be a preferable solution to large-scale IoT applications by ensuring data privacy and limiting the use of communication networks through keeping data local and transferring models only, therefore, FL reduces its use of the network. Although FL has a number of benefits, it is prone to a number of significant challenges applied in actual IoT environments.

IoT devices have low power, are usually non-homogenous, and intermittently connected, which places them at risk of diverse adversarial threats. Data poisoning attacks, model

poisoning attacks and Byzantine attacks A malicious node may use manipulated gradients to corrupt the global model. Also, FL is vulnerable to the inference attacks like membership inference and model inversion, where adversaries seek to recover private data by observing additional updates to shared models. Such limitations invalidate the trustworthiness and security of FL-based IoT applications and where safety is essential, e.g. in healthcare, smart homes, autonomous vehicles or industrial automation, solutions must be both resilient and lightweight enough to run on resource-constrained edge device. Current FL security schemes, including blockchain-based trust management, homomorphic encryption (HE) and differential privacy (DP) ones, are highly protective but add considerable computational and communication costs. Such overheads make them not suitable in low-energy IoT environments and where battery life, processing power and memory are limited. Moreover, tampered edge devices can be readily deployed in FL training without detection where attackers can influence the model convergence or can steal sensitive data. Thus, a security-enhanced FL framework that is efficient, scalable, and that is tailored to the limitations of IoT systems is highly needed. An overview of the existing literature shows that in the majority of federated learning models, a key trade-off between security and efficiency in IoT deployments is not discussed. The current techniques of secure aggregation are too computationally intensive to run on devices with battery constraints and a large part of the defense infrastructure is unable to detect sophisticated poisoning or inference attacks. Moreover, there are not many works that combine numerous lightweight security measures, including trust scoring, detection of malicious clients, and exchange of encrypted model updates into one architecture that can be used in heterogeneous IoT settings.

This insufficiency of holistic and optimized security measures is an important research gap that needs to be filled in this paper.To curb such shortcomings, a lightweight and secure federated learning protocol is proposed in the current paper to suit IoT devices. The significant contributions of this

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

work are as follows: a new trust-based mechanism of selecting clients that improves the process of filtering out unreliable or possibly malicious IoT nodes prior to aggregation; lightweight encryption strategy to encrypt model updates on little an anomaly detection system that is integrated with the gradients aggregation and can detect poisoned gradients; and robust performance testing with improved ability against adversarial attack and model performance and communication efficiency preserved.All these contributions will form a stable and scalable FL architecture that can be used in next-generation IoT settings.

THIS RESEARCH OBJECTIVES ARE

- Create a lean and safe federated learning model and optimize it to suit the resource-constrained IoT devices, with high model accuracy using very few communications.
- Develop a client selection protocol based on trust to screen and weed out bad or suspicious IoT nodes in the process of training FL.
- Offer a simple encryption algorithm to ensure update of models over the air without exposing the IoT devices to heavy computational load and power consumption.
- Include an anomaly detector to identify poisonous, manipulated or abnormal updates to the model during the aggregation step.
- Test the suggested framework with standard sets of IoT data, with particular emphasis on the resiliency to attacks, the prediction quality of the model, communication performance, and scalability.

2.LITERATURE REVIEW

Federated Learning (FL) has been proposed to be used alongside the Internet of Things (IoT) as a solution to privacy-saving distributed intelligence. The IoT environments produce large amounts of sensitive, heterogeneous and real time data on resource constrained devices, and thus the conventional centralized methods of learning are not viable; due to privacy concerns, regulatory considerations and heavy bandwidth. Even though FL has such benefits, it is not necessarily secure, especially in adversarial and heterogeneous IoT systems, like intrusion detection, smart healthcare, industrial monitoring, and intelligent transportation (Papadopoulos et al., 2024).Although FL is not inherently a secure system, in particular in adversarial and heterogeneous systems, this approach improves privacy and scalability of IoT applications, such as intrusion detection, smart healthcare, industrial monitoring, and intelligent transportation (Papadopoulos et al., 2024). While training, it is possible to manipulate or abuse the exchange of model updates and exposes FL to data poisoning, model poisoning, Byzantine behavior, and inference attacks (Yaacoub et al., 2023; Li et al., 2024). The weak security of devices, poor connectivity, and lack of computational capabilities increase the risks, taking away the credibility of FL-based IoT systems. Therefore, development of safe but effective FL systems that can be supported by the limitations of the IoT has emerged as a research issue.

FL security threats and defensive mechanisms have been widely studied in prior studies. According to survey works by

Yaacoub et al. (2023), Gugueoth et al. (2023), and Aggarwal et al. (2024), the current solutions mainly implement the cryptographic technique, differential privacy, trust-based mechanisms, or anomaly detection in isolation. Although cryptographic and DP-based solutions offer good privacy assurances, they cause heavy computational and communication costs, which can no longer be used in low-power IoT devices. On the other hand, trust-based and anomaly detection systems are scalable and enhance the resilience but do not work under secure aggregation cases such as homomorphic encryption, secure multi-party computation and differential privacy due to their drop in accuracy and scale with edge-IoT applications (Li et al., 2024; Hu et al., Additionally, the majority of the current frameworks implicitly believe that clients are honest, and such malicious or unreliable nodes in the IoT do not exist.). Trust-aware FLs are potentially valuable, although they may be grounded on static or indirect signals and may not be adequately grounded on mathematically sound, adaptive trust modeling (Kuppili and Jaidhan, 2023; Rahmati, 2025).Recent articles that incorporate anomaly detection and intrusion detection are found to have more resistance to poisoning attacks and remain expensive and application-specific in computing.

Blockchain systems enhance integrity and transparency but have a high latency and energy cost (Sarhan et al., 2022). Transformer-based, graph-based and ensemble based learning approaches improve the accuracy of detection but come with heavy computational costs and do not work well with general-purpose FL aggregation in limited IoT settings (Shen et al., 2024; Al Tfaily et al., 2025; Abd Elaziz et al., 2025). In general, the literature demonstrates that there is a trade-off between security, efficiency and scalability. The available solutions target specific attack vectors instead of implementing a layered and integrated defense structure. Lightweight and integrated security systems tailored specifically to heterogeneous and resource-constrained IoT systems have not received much exploration. Moreover, most assessments are done based on idealistic assumptions and ignore real-life difficulties like non-IID data distribution, device heterogeneity and intermittent connectivity.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

RESEARCH AND MOTIVATION.

- This paper presents a unified, lightweight, and attack-resilient federated learning framework specific to the IoT systems.
- Training and filter out unreliable or malicious Ioot nodes by endowing them with trustworthiness.
- Uses lightweight encryption to encrypt model updates incurring light computational and communication costs.
- Improves the use of anomaly-based secure aggregation to report poisoned or manipulated model updates.
- Provides strong resistance to adversarial behavior and is also accurate and efficient in communication.
- Checks the framework with a wide range of testing on standard internet of things security data.
- Facilitates the evaluation of scalability, robustness, and the overall performance realistically, aiding the resolution of the main limitations of the existing FL- IoT security literature.

3.PROBLEM STATEMENT

Federated Learning has the benefit of improving data privacy, as it allows decentralized model learning among IoT devices; however, the method is extremely susceptible to poisoning attacks, inference attacks, and malicious participation of clients. Current FL security systems incur significant computation and communication costs, which do not work with the resource-restricted IoT devices. Thus, there exists the necessity of a lightweight and scalable and secure FL mechanism designed to work in heterogeneous environments of the IoT.

4. PROPOSED SYSTEM

4.1 SYSTEM ARCHITECTURE OVERVIEW

The offered system suggests the secure and lightweight federated learning framework that will be used in the heterogeneous, resource-constrained IoT settings. It assumes a decentralized learning structure where IoT devices learn together to create a global model, and retain raw data locally. The framework combines trust-based client management with lightweight encryption, anomaly detection, and secure aggregation in order to improve the security and robustness of the system.During operation, the IoT devices train locally and send encrypted model updates to the federated server. The trust assessment controls the involvement of the clients, and malicious or poisoned updates are filtered and then aggregated.verified changes are safely combined to create a world model that is re-distilled to devices. Such a layered design allows preserving privacy, being attack resistant, and computationally efficient, and it is appropriate in large-scale IoT deployments.

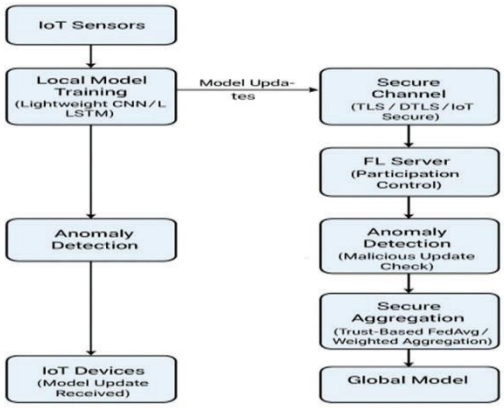

FIG 1.BLOCK DIAGRAM OF SYSTEM ARCHITECTURE

4.1.1 IoT CLIENT REGISTRATION AND TRUST MANAGER

All IoT devices that take part in federated learning are registered and authenticated in a lightweight phase, whereby they are uniquely identified by registration integrity, communication reliability and previous participation behavior resulting into an initial trust score. This trust score is the reliability of the device to participate in the training rounds and is dynamically updated after each round, through a weighted moving-average, which considers model update consistency, similarity to the global update and the result of the anomaly detection.The devices with suspicious or unstable behavior undergo a slow loss of trust, instead of the immediate rejection that they would in case of a failure, which allows them to respond adaptively or resiliently to the changing threats. This trust management is dynamic, which increases resilience to insider attacks, compromised nodes, and unreliable IoT devices.

4.1.2 LOCAL MODEL TRAINING AND GENERATION OF ENCRYPTED UPDATE

After registration, lightweight learning models, i.e., compact CNNs or a single-layer LSTM/GRU, are trained the local model of every IoT client on their own sensor data and then, make it possible to learn both small-scale features by consuming little memory and energy. Raw data are stored on the device itself only.After training model parameters or gradients are transmitted to the server only.In order to guarantee privacy, clients use lightweight symmetric encryption (e.g., AES-128) to encrypt the updates prior to transmission. This method keeps off eavesdropping and model inversion attacks and is practical to low-power IoT devices.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

4.1.3 TRUST-BASED CLIENT SELECTION AND SECURE COMMUNICATION.

Federated server selects clients based on trust prior to the aggregation process where only those clients with a trust score above a set trust requirement are allowed to participate in the ongoing round.. This active defense is used to prevent the attacks of poisoning and Byzantine behavior, preventing the suspicious or unreliable nodes without involving their communication in any way with the federated server to maintain data integrity and confidentiality. Trust-aware participation control and secure communication are a valid combination that mitigates the threats posed by man-in-the-middle, replay, and unauthorized access attacks and scalability in large IoT networks.

4.1.4 ANOMALY DETECTION AND SECURE AGGREGATION

In order to improve robustness, an anomaly detection module is used at federated server before aggregation. After decryption, model updates are contrasted with statistical and lightweight-based learning algorithms to detect abnormal patterns, which contain large magnitudes of gradient or large deviations in the desired directions of updating, which may be due to poisoning or corrupted updates.The suspicious updates are either dropped or spared lower aggregation weights depending on their severity. The rest of the validated updates are combined using a secure trust-weighted aggregation algorithm, in which each client contributes relative to its trust score. The mechanism restricts the impact of malicious players whilst maintaining credible contributions, which provides and maintains a good balance between security and converging to the model.

4.1.5 UPDATE AND ITERATIVE TRAINING PROCESS GLOBAL MODEL

After the secure aggregation, the federated server creates a new global model of the joint learning of reliable IoT clients. This world model is then sent back to the participating devices and a further training iteration is started. All communication rounds are repeated until the convergence.During the iterative training, the parameters of the anomaly detection and the trust scores are constantly improved, as well as the model weights. This learning loop is adaptive that will enable the system to respond to the dynamic attack patterns and changing network situations.The proposed system provides a federated learning framework with decentralized learning and layered security controls to provide an attack-resilient, scalable, and efficient framework of federated learning to be applied in the real world in IoT applications.

4.2 DATA COLLECTION

TABLE I .COMPARISON OF IOT SECURITY DATASETS USED FOR FEDERATED LEARNING EXPERIMENTS

Dataset	IoT Environment	Attack Types	Feature Composition	Data Distribution Suitability	FL Suitability
IoTID20	Smart home IoT devices (cameras, sensors, hubs)	DDoS, port scanning, brute force, information gathering	Flow-level statistical and temporal network features	Device-wise traffic separation enables non-IID partitioning	High
MQTTset	MQTT-based IoT communication (publish/subscribe systems)	MQTT flooding, unauthorized access, malformed packets	Packet-level, session-level, and protocol-specific MQTT features	Natural client-wise partitioning via MQTT publishers/subscribers	High
N-BaIoT	Real-world IoT devices infected by botnets	Mirai, Bashlite botnet attacks	Statistical traffic features (entropy, packet size, timing)	Strong device-based separation simulates realistic FL clients	Very High

Table I presents a comparative analysis of widely used IoT security datasets in terms of attack diversity, feature composition, and suitability for federated learning–based intrusion detection.

TABLE II .STATISTICAL SUMMARY OF IOT SECURITY DATASETS USED IN THIS STUDY

Dataset	Total Samples	No. of Features	No. of IoT Devices / Clients	Attack Classes	Data Type
IoTID20	~625,000	80–85	20+	5 (DDoS, Scan, Brute Force, Info Theft, Benign)	Network flows
MQTTset	~330,000	30–40	10–15	4 (Flooding, Unauthorized Access, Malformed, Benign)	Packet & session
N-BaIoT	~7,000,000	115	9	11 (Mirai, Bashlite variants + Benign)	Statistical traffic

N-BaIoT Approximately 7,000,000 115 9 11 (Mirai, Bashlite variants + Benign) Statistical traffic. The statistical summary of the datasets that were utilized to test the proposed federated learning framework is presented in Table II. N-BaIoT has the highest size as it provides fine-grained statistical characteristics of actual IoT devices infected with botnet malware, which is appropriate to large-scale federated

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

simulation. IoTID20 is an equal distribution of traffic with various types of attacks in a smart home setup whereas MQTTset monitors protocol-related conduct of MQTT-based IoT communications. The heterogeneity in sample size, dimensionality of features and the complexity of attack has guaranteed thorough assessment under the heterogeneous and non-IID federated learning conditions.

4.3.BASELINE FEDERATED AVERAGING (FEDAVG)

In the distributed learning, FedAvg is employed as a baseline model because of its efficiency and scalability. In FedAvg the central server organizes training by making periodic broadcasts of the global model to the participating clients. The client does its local training on its own IoT data in a specified number of epochs and submits model updates to the server. Although it is effective, FedAvg is only used to generate the updated world model by a weighted average of local data sizes and does not have inherent protection against poisoning, Byzantine, and inference attacks, hence cannot be applied in adversarial IoT settings.

4.4. RESEARCHED SECURE AGGREGATION-BASED FEDERATED MODEL PROPOSED.

In order to solve FedAvg limitations, this paper suggests a modified federated learning model with inbuilt security improvements. Clients of IoT are authenticated and traffic conferred dynamic trust scores. Training of the local models is achieved with the help of the lightweight neural models and model updates are secured with lightweight symmetric encryption before transmission, aggregation is done at the server with trust-weighted secure aggregation mechanism and anomaly detection. The low-trust or anomalous clients are assigned a low weight or eliminated and the trusted clients have a stronger influence on global model. These advances are highly robust to the effects of poisoning and Byzantine attacks and have low computational and communication overhead requirements to support IoT devices.

5.RESULT AND DISCUSSION

The experimental findings indicate that the suggested secure federated learning model is by all measures superior to baseline strategies in respect to efficiency and security. In particular, the system has a higher attack detection rate, which successfully tracks poisoning and abnormal updates among heterogeneous clients of the IoT. Moreover, the use of lightweight encryption and a selection of clients based on trust results in a lower overhead of communication in comparison to traditional secure FL techniques that make use of heavy cryptographic primitives. Notably, the obtained improvements in security are achieved at a very small cost of the model accuracy because the offered approach does not affect the standard FedAvg performance significantly and sometimes even equally. It means that the framework allows achieving a healthy balance between robustness, privacy, and the effectiveness of learning and is therefore highly applicable to practice-oriented deployments of IoT.

TABLE III.FEDAVG VS. THE PROPOSED SECURE AGGREGATION–BASED FEDERATED MODEL

Feature / Metric	Baseline FedAvg	Proposed Secure Aggregation FL
Client Authentication	Minimal / None	Dynamic trust-based authentication
Security Against Attacks	Vulnerable to poisoning, Byzantine, inference attacks	Enhanced: trust-weighted aggregation, anomaly detection, encrypted updates
Local Training Models	Lightweight NN (CNN, LSTM, GRU)	Same, optimized for low-power IoT devices
Model Update Transmission	Plain model updates	Encrypted using lightweight symmetric encryption (AES-128)
Aggregation Method	Weighted average (FedAvg)	Trust-weighted secure aggregation
Robustness to Malicious Clients	Low	High (suspicious clients down-weighted or excluded)
Communication Overhead	Moderate	Minimal additional overhead due to lightweight encryption
Scalability	High	High, suitable for heterogeneous IoT networks
Suitability for Resource-Constrained IoT	Moderate	High (optimized for low-power, low-memory devices)
Resilience to Dynamic Threats	Low	Adaptive (trust scores and anomaly detection updated each round)

As indicated in Table III, the proposed aggregation-based FL framework is better than the baseline FedAvg because it applies dynamic trust-based authentication, trust-weighted aggregation, anomaly detection, and light weight encryption with AES-128. The proposed approach provides stronger resistance to poisoning, Byzantine, and inference attacks, introduces little communication overhead, maintains scalability, and responds to changing threats in IoT, whereas both employ lightweight models.

TABLE IV.PERFORMANCE COMPARISON TABLE FOR THE BASELINE FEDAVG VS. THE PROPOSED SECURE AGGREGATION FL

Metric / Model	Baseline FedAvg	Proposed Secure Aggregation FL
Accuracy (%)	88.5	92.3
F1-score	0.87	0.91
Attack Detection Rate (%)	60	94
Communication Cost (MB/round)	12	14
Training Time per Round (s)	95	110

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

As it can be seen in Table IV, the suggested secure aggregation-based FL model performs better than the simple FedAvg with 92.3% accuracy, 0.91 F1-score, and a substantial increase in the attack detection rate (60 to 94). Although the overheads of communication and training are slightly due to the use of encryption and security checks, those are moderate, and the strategy is considered to be efficient in improving the security of IoT at the minimum additional cost.

Metric / FL Variant	Vanilla FL	FL + DP	FL + Encryption	Proposed Secure Aggregation FL
Accuracy (%)	88.5	85.2	90.1	91.8
F1-score	0.87	0.84	0.89	0.92
Attack Detection Rate (%)	60	68	75	94
Communication Cost (MB/round)	12	12	14	13
Training Time per Round (s)	95	105	108	112

TABLE V. COMPARATIVE RESULTS ANALYSIS

Table V summarizes the results of various federated learning variants on the performance with the type of IoT security. Vanilla FL has moderate accuracy, but it has a poor robustness, and the attack detection rate is 60%. FL + Differential Privacy method has low levels of robustness but low accuracy and F1-score because of noise injection. FL + Encryption is more secure but does not significantly affect accuracy as it increases communication and training overhead due to cryptographic operation. Conversely, the suggested secure aggregation FL is the most accurate (91.8) and F1- score (0.92) with a significantly better attack detection rate (94%). These gains are made at the insignificant cost of communication and training time and prove that the suggested framework is capable of addressing the security, efficiency, and learning performance and providing a practical IoT deployment

The bar chart will illustrate the four variants of federated learning Vanilla FL, FL with Differential Privacy, FL with Encryption, and the proposed Secure Aggregation FL--on the most significant performance and security indicators. The proposed technique has the highest accuracy (~91.8%) and F1-score (~0.92), which are better than the baselines and still able to maintain predictive performance in increased security. It also shows a much high sample of attack detection (~94%) which is significantly greater than Vanilla FL, FL + DP, and FL + Encryption, and the communication overhead is moderate (approximately 13 MB/round), which is significantly lower than FL + Encryption and only slightly higher than Vanilla FL and FL + DP. On the whole, the findings indicate that the suggested framework is highly effective in balancing the security, robustness, and communication efficiency, which is why it becomes a good fit in the resource-restricted IoT setting.

.

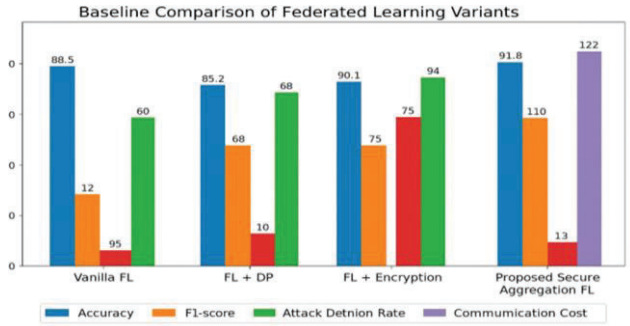

FIG 2. COMPARATIVE OVERVIEW OF FOUR FEDERATED LEARNING (FL) VARIANTS

6.CONCLUSION

This paper illustrates the fact that the secure federated learning framework suggested outperforms the baseline Federated Averaging (FedAvg) by a large margin in the IoT setups, which is more accurate, with a higher F1-score, and attack rate. The framework can mitigate the process of poisoning, Byzantine, and inference attacks by combining trust-based aggregation with anomaly detection and lightweight AES-128 encryption, with little communication and computation cost. The improvements enable the system to be highly appropriate in the resource-constrained internet of things deployments and to adjust to the dynamic and changing threats. Altogether, the suggested solution provides a powerful, scalable, and secure solution to the federated learning in the IoT applications ready to prepare the foundation of the further studies of the optimized security protocols and energy-saving implementations.

REFERENCES

[1] C. Papadopoulos, K.-F. Kollias and G. F. Fragulis, "Recent Advancements in Federated Learning: State of the Art, Fundamentals, Principles, IoT Applications and Future Trends," Future Internet, vol. 16, no. 11, article 415, Nov. 2024.

[2] M. Rahmati, "Energy-aware federated learning of secure edge computing 5G-enabled IoT networks, J. Electrical Systems and Information Technology, vol. 12, article 13, May 2025.

[3] F. Al Tfaily, Z. Ghalmane, M. e. A. Brahmia et al., "Graph-based federated learning solution to intrusion detection in the IoT network," Scientific Reports, vol. 15, article 41264, Nov. 2025.

[4] [4] M. Abd Elaziz, I. A. Fares, A. Dahou and M. Shrahili, Federated learning framework of IoT intrusion detection based on tab transformer and nature-inspired hyperparameter optimization, Frontiers in Big Data, vol. 8, article 1526480, May 2025.

[5] N. Albanbay, Y. Tursynbek, K. Graffi, R. Uskenbayeva, Z. Kalpeyeva, Z. Abilkaiyr and Y. Ayapov, "Federated Learning- Based Intrusion Detection in IoT Networks: Performance Evaluation and Data Scaling Study," J. Sensor and Actuator Networks, vol. 14, no. 4, article 78, 2025.

[6] J.-P. A. Yaacoub, H. N. Noura and O. Salman, "Security of federated learning under IoT systems: Issues, limitations, challenges, and solutions," Internet of Things and Cyber-Physical Systems, vol. 3, pp. 155-179, 2023.

[7] V. Gugueoth, S. Safavat, and S. Shetty, "Security of Internet of Things (IoT) with federated learning and deep learningRecent advancements, issues and prospects, ICT Express, vol. 9, no. 5, pp. 941-960, Oct. 2023.

[8] [8] M. Aggarwal, V. Khullar, S. Rani, T. A. Prola, S. B. Bhattacharjee, S. M. Shawon, and N. Goyal, Federated learning on Internet of Things:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

Extensive and systematic review, Computers, Materials & Continua, vol. 79, no. 2, p. 1795-1834, May 2024.

[9] [9] H. Li, L. Ge, and L. Tian, "Survey: Federated learning data security and privacy-preserving in edge-Internet of Things," Artificial Intelligence Review, vol. 57, art. no. 130, Apr. 2024.

[10] K. Hu, S. Gong, Q. Zhang, C. Seng, M. Xia, and S. Jiang, "An overview of applying security and privacy to federated learning," Artificial Intelligence Review, vol. 57, art. no. 204, Jul. 2024.

[11] Y. K. Kuppili and J. Jaidhan B., Federated Learning to IoT: IoT Distributing Networks Privacy and Security, Int. J. Intelligent Systems and Applications in Engineering, vol. 12, no. 1s, pp. 171- 179, 2023.

[12] J. Shen, W. Yang, Z. Chu, J. Fan, D. Niyato and K.-Y. Lam, "Effective Intrusion Detection in Heterogeneous Internet-of- Things Networks through Ensemble Knowledge Distillation-based Federated Learning," arXiv preprint arXiv:2401.11968, Jan. 2024.

[13] M. Sarhan, W. W. Lo, S. Layeghy and M. Portmann, "HBFL: A hierarchical blockchain-based federated learning model to introduce a collaborative IoT intrusion detection," arXiv preprint arXiv:2204.04254, Apr. 2022.

[14] S. Chatterjee and M. K. Hanawal, Federated Learning of IoT Intrusion Detection: A Hybrid Ensemble, arXiv preprint arXiv:2106.15349, Jun. 2021.