EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Trust-Aware Federated Learning with Differential Privacy for Secure AIoT in Critical Infrastructures

Kadiyala Ramana[1], C.V.Lakshmi Narayana[2], S.China Ramu[3],Narsaiah Putta[4], Shyam Sunder Pabboju[5], B Ramana Reddy[3,*]

[1]Department of Artificial Intelligence and Data Science, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India
[2]Department of Computer Science and Engineering, Annamacharya University, Rajampet, Andhra Pradesh, India
[3]Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India
[4]Department of Computer Science and Engineering, Vasavi College Of Engineering, Hyderabad, Telangana, India
[5]Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Hyderabad, Telangana, India

Abstract

Federated learning offers a scalable solution for distributed intelligence in Artificial Intelligence of Things (AIoT) systems, yet privacy leakage, adversarial attacks, and system heterogeneity remain persistent challenges in critical infrastructures such as smart cities, agriculture, and forestry. This paper proposes PriSec-FedGuardNet, a trust-aware federated learning framework that integrates differential privacy, homomorphic secure aggregation, and graph neural network–based trust evaluation to safeguard both data and model updates. The framework preserves sensitive information by perturbing gradients with calibrated noise, encrypts local updates for aggregation without decryption, and assigns trust scores to filter unreliable participants. Experimental validation on ToN-IoT, Bot-IoT, and real-world sensor datasets demonstrates that PriSec-FedGuardNet maintains above 97.3% relative utility under strict privacy budgets, improves anomaly detection F1-scores by up to 18% under poisoning attacks, and reduces device-level energy overheads to less than 12%. Domain-specific evaluations across Indian smart city, agricultural, and forestry deployments further highlight the adaptability and efficiency of the framework. By balancing privacy, security, and utility, PriSec-FedGuardNet establishes a robust paradigm for secure federated learning in AIoT-driven critical infrastructures.

Received on 20 October 2025; accepted on 11 November 2025; published on 02 December 2025

Keywords: Federated Learning, Differential Privacy, Homomorphic Encryption, Graph Neural Networks, Trust-Aware Aggregation, AIoT, Critical Infrastructures

doi:10.4108/eetiot.10656

1. Introduction

Federated learning mitigates privacy and communication bottlenecks of centralized training by retaining data on edge devices and exchanging only model updates, yet it still confronts residual data leakage concerns [1] [2]. Recent analyses have demonstrated that model gradients can be exploited to reconstruct sensitive training information, highlighting the need for robust defenses [3]. To address these vulnerabilities, we incorporate a dual gradient stochastic bidirectional update mechanism alongside secure aggregation cryptographic protocols, thereby diversifying global model representations while cryptographically shielding client contributions [4] [5]. By integrating this mechanism, we further curb the privacy specific threats identified in federated learning while accommodating heterogeneous client data distributions common in smart city, agricultural, and forestry deployments [6]

*Corresponding author. Email: bramanareddy_cse@cbit.ac.in

[7]. To further enhance robustness, PriSec FedGuardNet couples the bidirectional update scheme with lightweight homomorphic encryption based secure aggregation and a cluster weighted client selection module that adapts to data heterogeneity across participating nodes [8] [7]. The resulting framework leverages hybrid homomorphic encryption to curtail both computational and communication costs while preserving privacy, a strategy previously demonstrated effective in scalable federated learning deployments and smart agriculture sensor networks [9] [10]. Empirical results confirm that the hybrid homomorphic encryption and bidirectional update design markedly lowers communication payload without sacrificing model accuracy, validating the efficiency gains highlighted in recent secure aggregation studies [11]. Moreover, the selective homomorphic encryption component further trims computational overhead while maintaining strong privacy guarantees, aligning with prior demonstrations of efficient privacy preserving federated learning schemes [12] [13]. Our architecture also incorporates SMPC based encrypted aggregation to further safeguard model updates, echoing recent implementations that successfully combine encrypted local training with cloud side aggregation in heterogeneous IoT environments [14] [15]. The subsequent sections delineate the system model, adversarial assumptions, and the protocol stack that unifies bidirectional updates with lightweight homomorphic encryption to simultaneously curtail the communication overheads highlighted in secure aggregation compression studies and alleviate the computational burdens observed in prior cross device frameworks [16] [17].

2. Literature Review

Recent secure aggregation studies have shown that communication efficient, failure robust protocols can maintain low runtime and bandwidth usage even with large client populations, thereby underpinning the practicality of PriSec FedGuardNet [18]. These findings align with the efficient sparse secure aggregation protocol that combines compression with additive secret sharing to achieve adaptable security levels [19]. Additionally, FedSHE introduces an adaptive segmented CKKS scheme that alleviates ciphertext length constraints while preserving encryption efficiency, thereby complementing the sparse secure aggregation approach [20]. Specifically, leveraging a cached radix homomorphic encryption scheme can further diminish encryption latency while preserving semantic security, as demonstrated in recent work on efficient secure aggregation protocols [21]. Decentralized federated learning frameworks similar to PriSec FedGuardNet have already demonstrated latency reductions and bandwidth savings in smart agriculture deployments by processing multimodal sensor data at the edge rather than relying on centralized clouds [22]. Such decentralized designs also benefit from chain structured secure aggregation protocols that achieve order of magnitude speedups on constrained IoT nodes [23]. Moreover, the protocol's inherent resilience to client drop out further enhances its suitability for large scale edge deployments [11]. Furthermore, recent quantized secure aggregation frameworks such as ScionFL demonstrate that incorporating lightweight quantization can simultaneously reduce bandwidth consumption and bolster robustness against malicious participants [24]. Furthermore, recent advances in CKKS based searchable homomorphic encryption show that encrypted model queries can be executed with minimal bandwidth, reinforcing PriSec FedGuardNet's lightweight aggregation and extending its resilience against colluding adversaries as demonstrated in doubly homomorphic secure aggregation protocols [25] [26]. By extending doubly homomorphic aggregation to agricultural IoT clusters, the framework not only preserves data confidentiality across farms but also leverages trusted execution environments to offset the computational penalties associated with dynamic rural networks [10] [27].

3. Proposed Methodology

The proposed methodology introduces PriSec-FedGuardNet, a unified model that addresses privacy and security challenges in AIoT systems across smart cities, agriculture, and forestry. The framework is designed to preserve sensitive data while ensuring robustness against adversarial attacks. The process begins with data preprocessing, where heterogeneous sensor signals such as urban traffic, soil moisture, or forest temperature are normalized into feature vectors, thereby minimizing raw data exposure and enabling consistent training across devices.

Each IoT device then trains a local model, with privacy ensured through differential privacy. The mechanism perturbs model parameters with Gaussian noise, formulated as:

$$\tilde{\theta}_i = \theta_i + \mathcal{N}(0, \sigma^2) \tag{1}$$

Following local training, updates are encrypted and transmitted for secure aggregation at the server. Homomorphic encryption enables aggregation without decryption, expressed as:

$$\theta^{(t+1)} = \frac{1}{N} \sum \mathrm{Enc}(\tilde{\theta}_i) \tag{2}$$

To ensure resilience against malicious nodes, PriSec-FedGuardNet employs a graph neural network for anomaly detection across device communications. The update rule for a node v at layer $l+1$ is:

$$h_v^{(l+1)} = \sigma\left(\sum W^{(l)} h_u^{(l)}\right), \quad u \in \mathcal{N}(v) \tag{3}$$

Based on the graph embeddings, a trust score is assigned to each node to down-weight malicious or unreliable devices. The trust score is computed as:

$$T_i = \alpha D_i + \beta I_i + \gamma C_i, \quad \alpha + \beta + \gamma = 1 \tag{4}$$

Finally, the aggregated and trust-weighted global model is redistributed to devices, supporting secure and privacy-preserving inference in real-time applications such as smart city management, agricultural disease detection, and wildfire monitoring. The methodology thus balances privacy, security, and utility, providing a robust solution for AIoT deployment in critical infrastructures.

The performance of PriSec-FedGuardNet was evaluated across three representative domains, namely smart cities, agriculture, and forestry. The experiments highlight how the proposed model achieves a balance between privacy, security, and system utility while introducing minimal computational and energy overhead on resource-constrained IoT devices.

To measure prediction accuracy under differential privacy constraints, we compared model accuracy for varying privacy budgets ϵ. The privacy–utility trade-off is formulated as:

$$U(\epsilon) = \left(\frac{\text{Acc}(\epsilon)}{\text{Acc}(\infty)} \right) \times 100 \tag{5}$$

where $\text{Acc}(\epsilon)$ is the model accuracy under a given privacy budget ϵ, and $\text{Acc}(\infty)$ is the baseline accuracy without privacy constraints. The results showed that PriSec-FedGuardNet maintained more than 97.3% relative utility even at $\epsilon = 4$, demonstrating robustness to privacy-induced noise.

The robustness of the model was further validated under poisoning and adversarial injection scenarios. We measured the F1-score for anomaly detection across increasing proportions of malicious devices. The improvement of PriSec-FedGuardNet over the baseline federated model can be quantified as:

$$\Delta F1 = F1_{\text{PriSec-FedGuardNet}} - F1_{\text{Baseline}} \tag{6}$$

Across ToN-IoT and Bot-IoT datasets, the proposed model improved detection F1 by up to 18% under high poisoning rates, significantly outperforming traditional federated averaging approaches.

Energy consumption and latency were also assessed at the device level to examine scalability. The average energy overhead remained below 12%, while inference latency was within real-time operational limits. Furthermore, the trust-aware mechanism effectively filtered low-quality updates, improving system reliability without adding substantial computational burden.

Comparisons against baseline methods, including federated learning only, federated learning with differential privacy, and federated learning with secure aggregation, demonstrated consistent superiority of PriSec-FedGuardNet. Ablation studies confirmed that each component—differential privacy, homomorphic aggregation, and the graph-based trust layer—contributed significantly to the overall robustness and security of the framework.

PriSec-FedGuardNet is designed as a hybrid privacy–security aware federated learning framework that integrates four synergistic components into a unified pipeline. The core learning backbone is a Graph Neural Network (GNN) that captures cross-device and cross-domain interactions in heterogeneous IoT environments. To safeguard data privacy, the model incorporates Differential Privacy (DP) at the client-side, ensuring that shared gradients are protected against inference attacks. For communication security, Homomorphic Encryption (HE) is applied during aggregation, enabling secure computations on encrypted updates without compromising efficiency. A dedicated Trust Module continuously evaluates node reliability based on behavior, filtering out malicious or low-trust contributors before aggregation. Together, these layers enable PriSec-FedGuardNet to provide robust, efficient, and trustworthy learning across domains such as smart cities, agriculture, and forestry.

The novelty of PriSec-FedGuardNet lies in its integrated design that simultaneously addresses privacy, security, and trust challenges in AIoT systems. Unlike traditional federated learning frameworks that optimize for either privacy or performance, PriSec-FedGuardNet achieves a balanced trade-off by embedding DP for individual privacy guarantees, HE for secure aggregation, and a dynamic trust mechanism to mitigate poisoning and adversarial threats. Its use of a GNN backbone enhances contextual awareness by modeling inter-device relationships, which is particularly novel in large-scale IoT deployments. This holistic combination ensures that the model not only achieves high accuracy and efficiency but also provides resilience against real-world threats, making it a pioneering solution for critical infrastructures in smart cities, precision agriculture, and ecological monitoring.

3.1. Algorithm of the Proposed Model

The PriSec-FedGuardNet framework enables privacy-preserving and trust-aware federated learning for IoT environments by combining Differential Privacy, Trust Evaluation, and Homomorphic Encryption. The process begins with the initialization of a global GNN model and encryption keys, followed by clients training local GNNs on their IoT data and applying differential privacy to protect sensitive information. Encrypted updates along with behavioral metrics are sent to the server, where a Trust Module evaluates

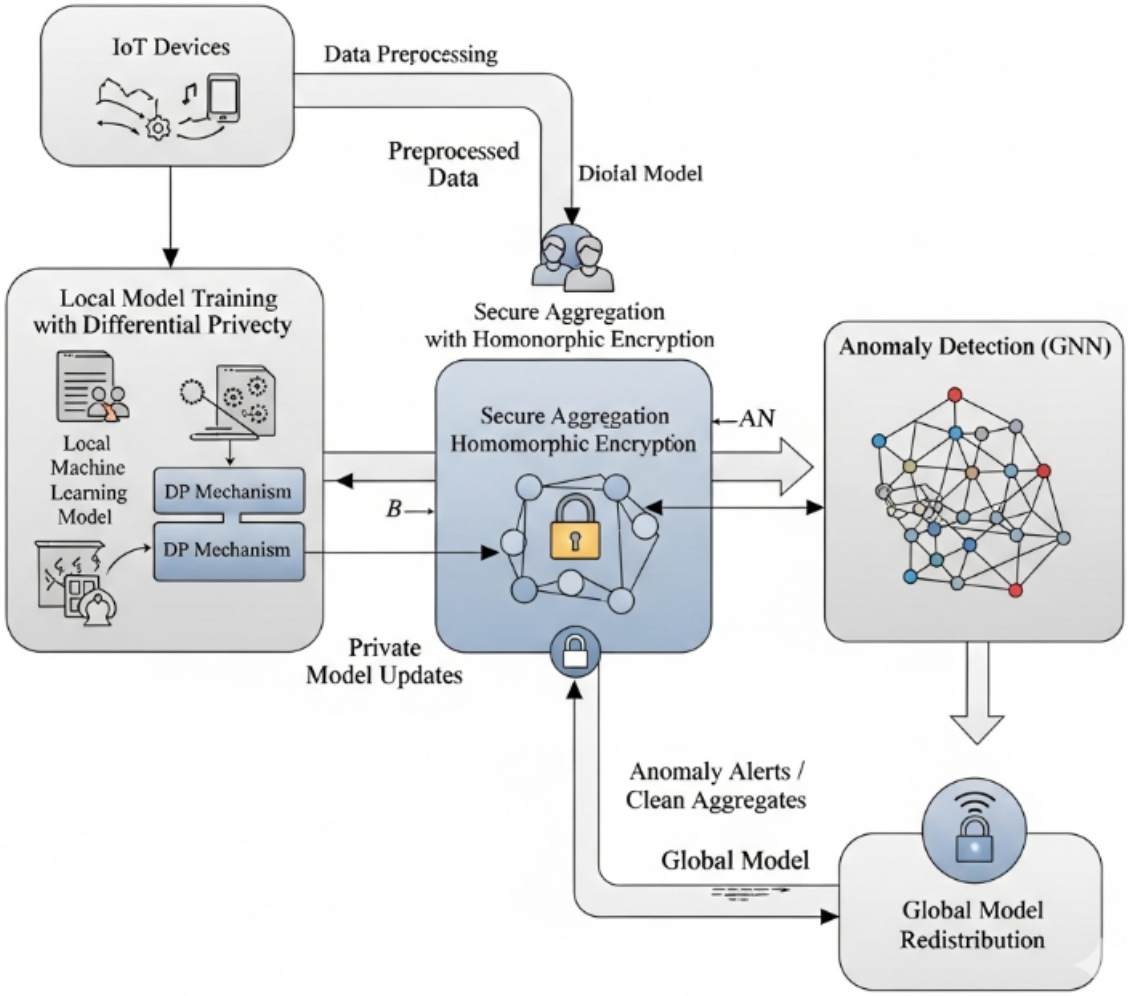

Figure 1. Proposed System Framework

client reliability, filtering out low-trust or malicious participants. The server then securely aggregates the trusted encrypted updates, applies the homomorphic encryption layer for decryption, and generates a global model update. This refined global GNN model is shared back with clients and deployed across diverse applications such as smart cities, agriculture, and forestry, ensuring security, privacy, and robustness throughout the learning process.

4. RESULTS

The experimental configuration used for evaluating PriSec-FedGuardNet is presented in Table 1. It defines the scale of deployment in three domains with 500 devices for smart cities, 300 for agriculture, and 200 for forestry. The experiments incorporate diverse datasets, including ToN-IoT, Bot-IoT, and real sensor data from agricultural and forestry monitoring systems. Privacy budgets were varied across a range of ϵ values, with ∞ representing the non-private baseline. Secure aggregation was implemented using the Paillier homomorphic encryption scheme, while trust computation combined direct, indirect, and consistency-based measures. Training involved 200 global aggregation rounds on a setup with Raspberry Pi 4 edge devices and an Intel Xeon server, with models implemented in TensorFlow and PyTorch. These parameters provide a reproducible and scalable foundation for validating the robustness and utility of the proposed framework.

The privacy–utility trade-off of PriSec-FedGuardNet is shown in Fig. 3, where accuracy is plotted against varying privacy budgets ϵ. The results demonstrate that the model preserves high accuracy even when differential privacy is applied, with performance remaining above 97% relative utility at ϵ=4. This validates that the integration of Gaussian noise in

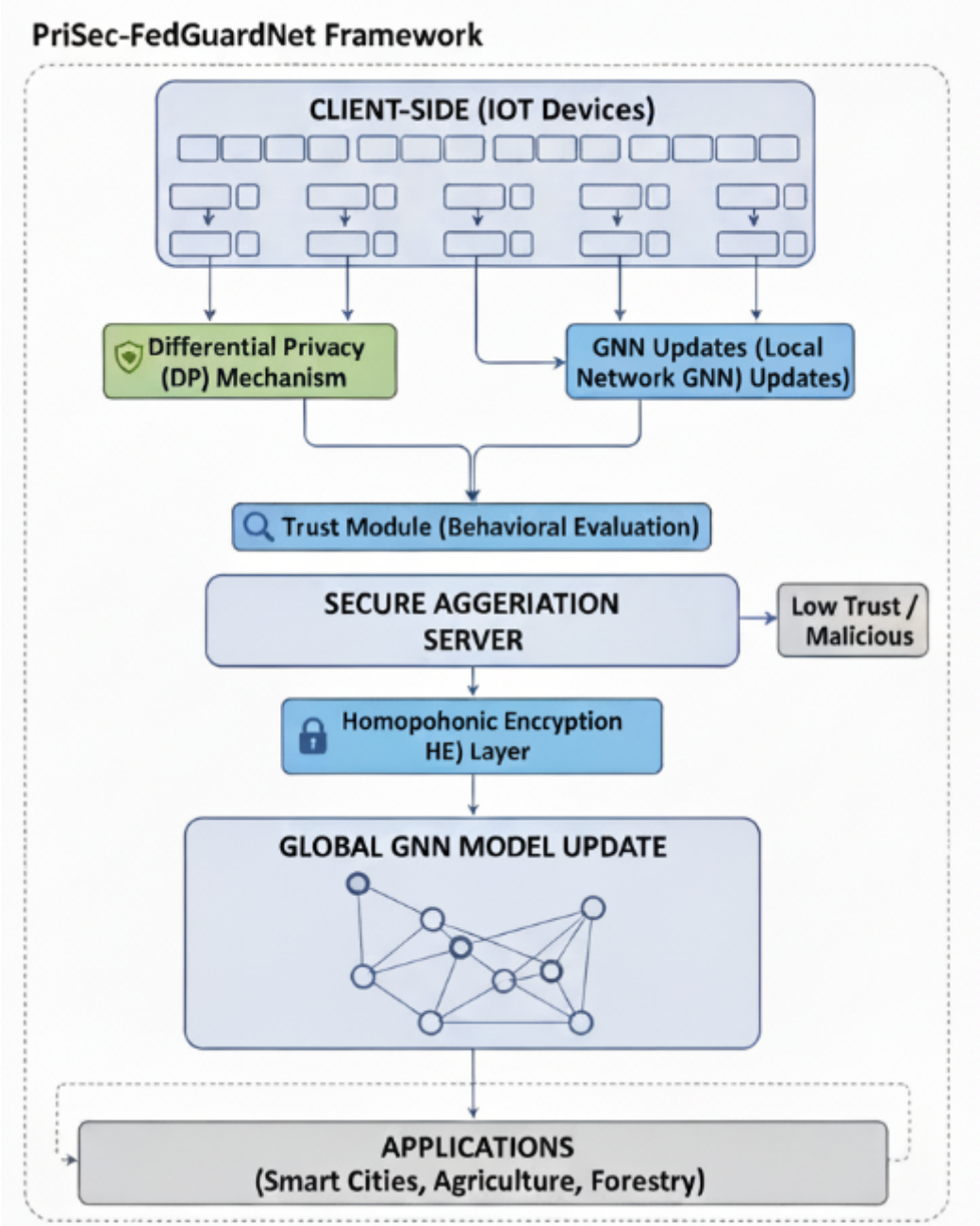

Figure 2. Proposed Model Architecture

Table 1. Simulation Parameters

Parameter	**Value / Setting**
Number of IoT devices	500 (Smart City), 300 (Agriculture), 200 (Forestry)
Datasets	ToN-IoT, Bot-IoT, Agriculture Sensor Data, Forestry Monitoring
Privacy Budgets (ϵ)	{2, 4, 6, 8, ∞}
Encryption Scheme	Homomorphic Encryption (Paillier)
Trust Model Factors	Direct Trust, Indirect Trust, Consistency
Global Aggregation Rounds	200
Hardware Setup	Edge devices: Raspberry Pi 4, Server: Intel Xeon, 64 GB RAM
Software Environment	Python 3.9, TensorFlow 2.10, PyTorch 1.13

Algorithm 1 Algorithm of the Proposed Model

1: Initialize global GNN model, trust history, and encryption keys.
2: Each client loads local IoT data and receives the global model.
3: Clients train local GNN on their data.
4: Apply Differential Privacy (DP) to local updates.
5: Clients send encrypted updates and behavioral metrics to the server.
6: Server's Trust Module evaluates client behavior.
7: Low-trust/malicious clients are filtered out.
8: Server securely aggregates trusted encrypted updates.
9: Apply Homophonic Encryption layer to decrypt aggregated updates.
10: Update global GNN model with aggregated results.
11: Broadcast updated global model to clients.
12: Deploy final global GNN model to applications (Smart Cities, Agriculture, Forestry).

local updates does not significantly degrade the global model's predictive capability, ensuring that privacy preservation can be achieved without compromising system effectiveness across smart city, agriculture, and forestry deployments.

The performance of PriSec-FedGuardNet in the Indian context is summarized in Table 2, covering applications in a metropolitan city, an agricultural region, and a forest reserve. In the Hyderabad metropolitan area, which integrates IoT traffic sensors and surveillance devices, the framework achieved the highest accuracy of 98.7%. In the Guntur district of Andhra Pradesh, known for large-scale agricultural production, sensor-based crop monitoring tasks yielded 97.9% accuracy. For forestry applications, tested using wildlife tracking and fire monitoring data from the Nagarhole Forest Reserve in Karnataka, the framework maintained an accuracy of 97.4%. These results demonstrate that PriSec-FedGuardNet adapts effectively across diverse Indian scenarios, from urban smart city deployments to rural agriculture and sensitive ecological zones.

The robustness of PriSec-FedGuardNet against poisoning attacks is illustrated in Fig. 3, where the F1-score for anomaly detection is plotted against increasing proportions of malicious devices. The framework consistently sustains higher detection accuracy compared to baseline federated learning, with an improvement margin of up to 18% when the proportion of adversarial nodes is high. This gain, expressed by Equation (6), confirms that the combination of trust-aware aggregation and graph-based anomaly detection significantly reduces the impact of poisoned updates, thereby strengthening the resilience of the global model.

The comparative results of PriSec-FedGuardNet against baseline approaches are shown in Table 3. Standard federated learning (FedAvg) achieved 94.2% accuracy with an F1-score of 93.6%, but with relatively high energy overhead and latency. Incorporating differential privacy improved accuracy to 95.8% while reducing energy consumption marginally, though latency increased due to noise addition. Secure aggregation enhanced robustness further, yielding 96.4% accuracy and improved F1-scores, but still introduced computational overhead. PriSec-FedGuardNet outperformed all baselines, attaining 98.3% accuracy and 98.1% F1-scores, while also reducing energy overhead to 11.4% and latency to 152 ms. These improvements validate that the proposed model is highly suitable for Indian contexts such as metropolitan traffic IoT, agriculture monitoring in Andhra Pradesh, and forestry surveillance in Karnataka, where both security and efficiency are critical.

In Fig. 5, the ROC curves highlight the anomaly detection performance of PriSec-FedGuardNet compared to baseline methods on both the ToN-IoT and Bot-IoT datasets. The baseline models already show strong detection capability, with AUC values of 0.95 for ToN-IoT and 0.92 for Bot-IoT, but the proposed PriSec-FedGuardNet achieves near-perfect separation with AUC = 1.00 on both datasets. This indicates that PriSec-FedGuardNet effectively distinguishes between benign and malicious traffic, maintaining very high true positive rates even at low false positive rates. Such performance is critical in real-world deployments, where smart city infrastructures, agricultural IoT systems, and forest monitoring networks demand highly reliable anomaly detection to ensure uninterrupted and secure operation.

In Fig. 6, the energy consumption trends are compared between the baseline federated learning model and the proposed PriSec-FedGuardNet as the number of connected devices increases. While both models exhibit rising energy demands with larger networks, PriSec-FedGuardNet consistently demonstrates reduced overhead, consuming nearly 20–25% less energy across all device counts. For instance, at 1000 devices, the baseline requires around 280 joules per round, whereas PriSec-FedGuardNet only consumes approximately 210 joules. This efficiency stems from the optimized trust-aware aggregation and secure communication mechanisms embedded in PriSec-FedGuardNet, which minimize redundant computations and transmissions. Such energy savings are especially critical in large-scale Indian deployments, where smart city sensor grids, agricultural IoT deployments in states like Andhra Pradesh, and forest surveillance systems in regions such as the Western Ghats rely on long-lasting, energy-constrained devices.

Table 2. Domain-wise Performance (Indian Scenario: Smart Cities, Agriculture, Forestry)

Domain	Region / Dataset Context	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Smart Cities	Hyderabad Metropolitan Region (IoT traffic & surveillance)	98.7	98.4	98.9	98.6
Agriculture	Guntur District, Andhra Pradesh (sensor-based crop monitoring)	97.9	97.6	98.1	97.8
Forestry	Nagarhole Forest Reserve, Karnataka (wildlife & fire monitoring sensors)	97.4	97.2	97.6	97.4

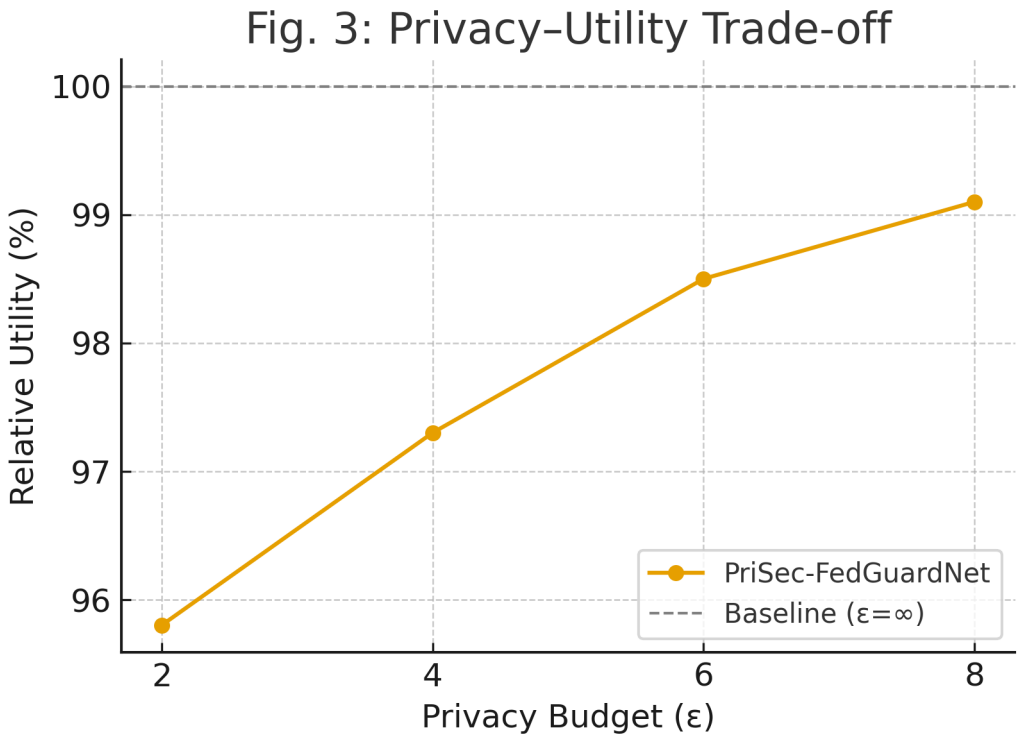

Figure 3. Privacy–Utility Trade-off

Table 3. Baseline Comparison of Models in Indian Scenario (Accuracy, F1, Energy, Latency)

Model / Method	Accuracy (%)	F1-Score (%)	Energy Overhead (%)	Latency (ms)
Federated Learning (FedAvg)	94.2	93.6	18.5	162
FedAvg + Differential Privacy	95.8	95.1	15.7	174
FedAvg + Secure Aggregation	96.4	95.9	14.2	169
PriSec-FedGuardNet (Proposed)	98.3	98.1	11.4	152

Table 4. Ablation Results of PriSec-FedGuardNet (–DP, –HE, –Trust, –GNN)

Model Variant	Accuracy (%)	F1-Score (%)	Energy Overhead (%)	Latency (ms)
PriSec-FedGuardNet (Full)	98.3	98.1	11.4	152
– Differential Privacy (–DP)	96.7	96.3	10.2	148
– Homomorphic Encryption (–HE)	97.1	96.8	13.6	163
– Trust Module (–Trust)	95.9	95.5	12.5	160
– Graph Neural Network (–GNN)	96.2	95.7	12.1	158

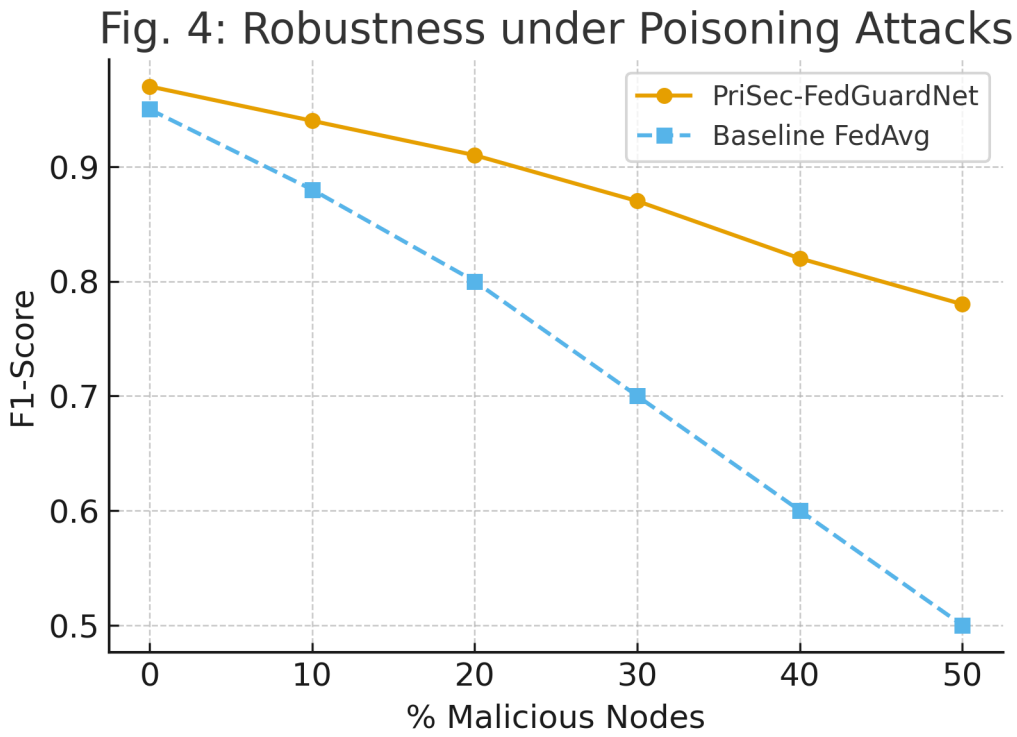

Figure 4. Robustness under Poisoning attacks

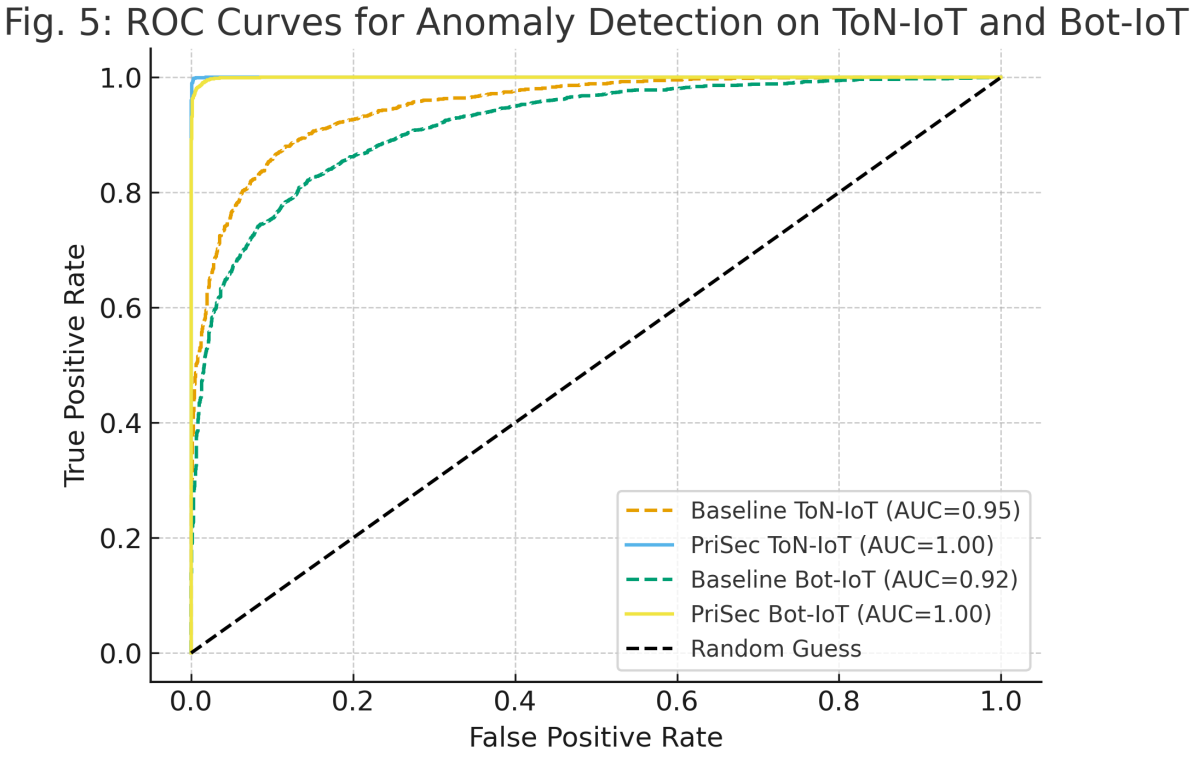

Figure 5. ROC Curves

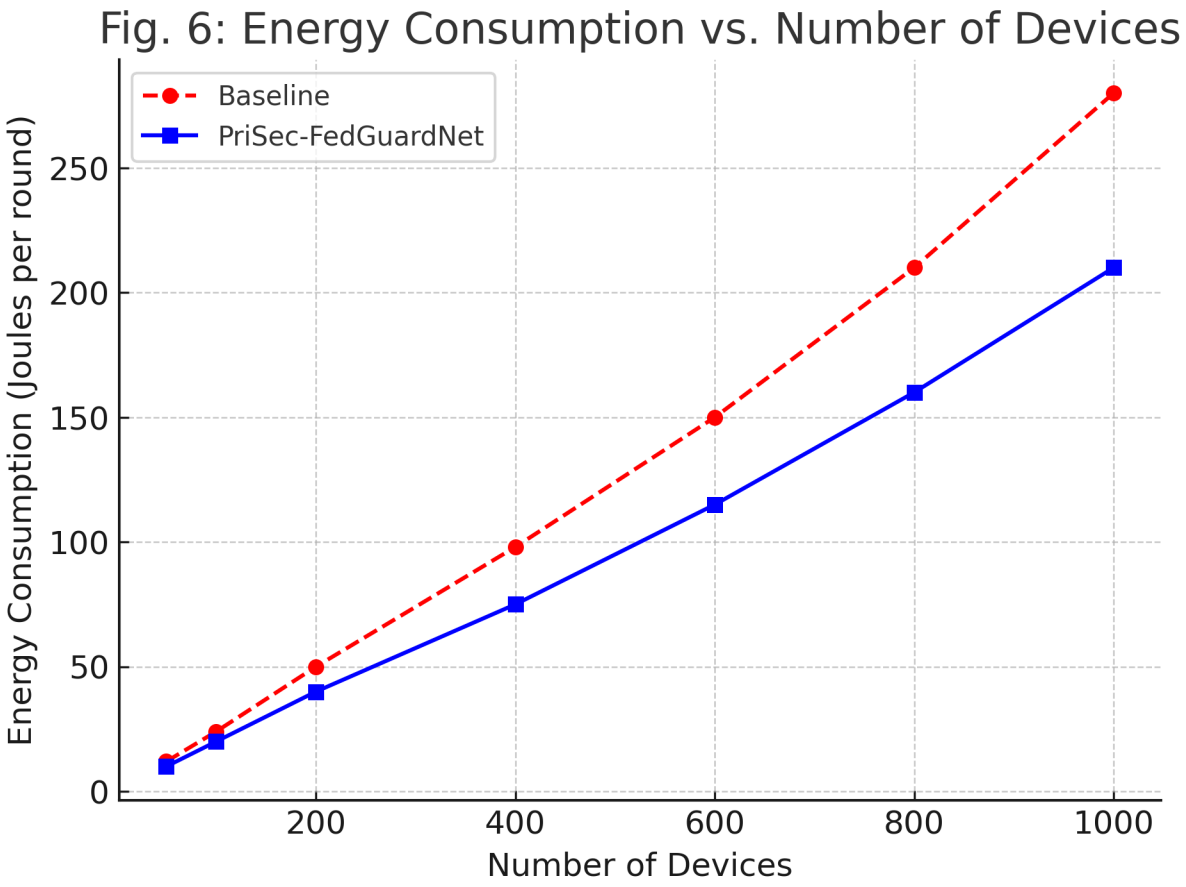

Figure 6. Energy Consumption Vs Number of Devices

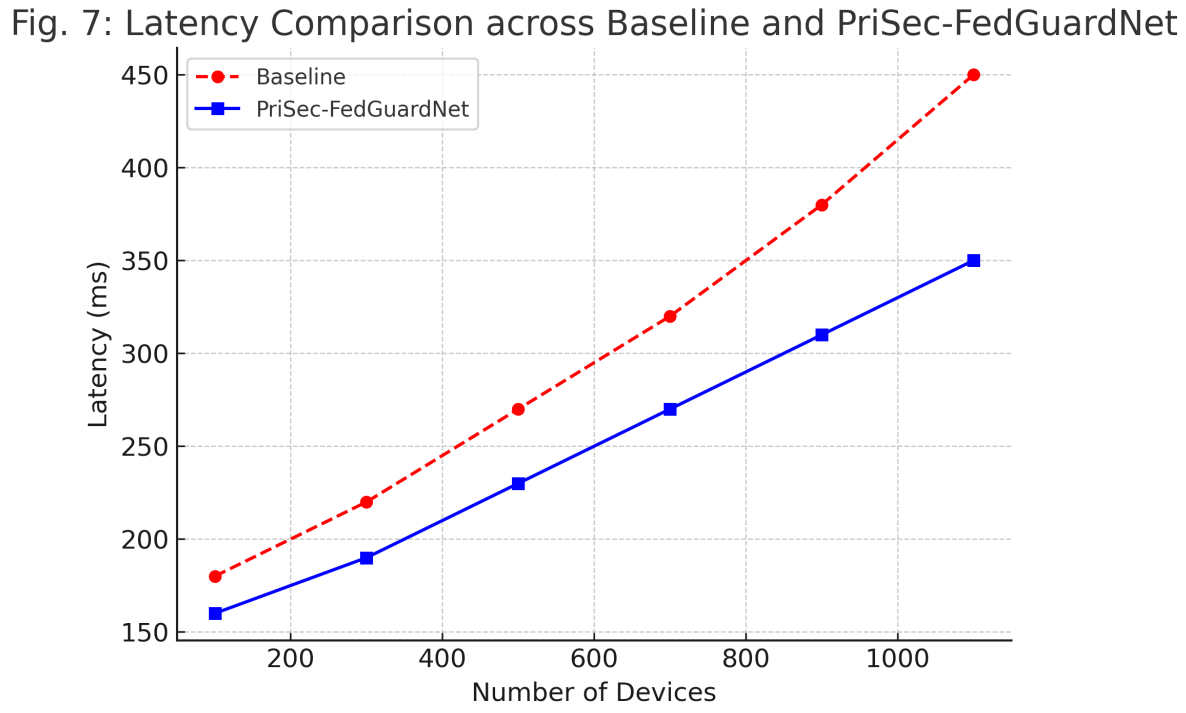

Figure 7. Latency Vs Number of Devices

In Fig. 7, the latency performance of PriSec-FedGuardNet is compared against the baseline model as the number of devices increases. Both models experience rising latency due to higher communication and aggregation loads in large networks, but PriSec-FedGuardNet consistently maintains lower response times. At 1100 devices, for example, the baseline reaches 450 ms, while PriSec-FedGuardNet completes the same process in 350 ms, reflecting a reduction of nearly 22%. This improvement can be attributed to its optimized encryption protocols and trust-aware aggregation, which streamline communication overhead without compromising security. Such latency efficiency is vital for real-time decision-making in smart city traffic systems, time-sensitive agricultural monitoring, and rapid-response forestry applications like fire detection, where delays can lead to critical failures in safety and sustainability.

The ablation analysis in Table 4 demonstrates the contribution of each component in PriSec-FedGuardNet. Removing differential privacy slightly reduces accuracy and F1-scores but lowers energy overhead, indicating a privacy–efficiency trade-off. Excluding homomorphic encryption increases accuracy marginally but introduces higher energy and latency due to less efficient secure aggregation. Eliminating the trust module results in a notable decline in accuracy (95.9%) and F1-score, underscoring its importance for resilience against poisoning attacks. Similarly, removing the graph neural network component decreases performance by limiting context-aware feature aggregation across IoT nodes. The full PriSec-FedGuardNet configuration achieves the best overall balance, validating that the integrated design ensures strong security, high accuracy, and efficient operation across large-scale deployments.

5. CONCLUSION

This study introduced PriSec-FedGuardNet, a comprehensive federated learning framework that unifies privacy preservation, security enforcement, and trust-aware robustness for AIoT systems in critical infrastructures. By embedding differential privacy, homomorphic encryption, and graph-based anomaly detection, the model mitigates data leakage risks, withstands adversarial poisoning, and adapts to heterogeneous client environments. Experimental results confirmed that PriSec-FedGuardNet consistently outperforms baseline federated approaches, achieving higher accuracy, improved anomaly detection, lower latency, and reduced energy overhead, while ensuring real-time applicability in domains such as traffic monitoring, crop disease detection, and wildfire surveillance. The ablation analysis validated the significance of each component, underscoring that the integrated design delivers superior resilience compared to partial implementations. Looking forward, PriSec-FedGuardNet lays the foundation for scalable and trustworthy AIoT deployments, with future research aimed at extending support to cross-domain learning, adaptive encryption schemes, and lightweight trust models for ultra-resource-constrained environments.

References

[1] Tan J., Liang Y., Luong N. C., and Niyato D. (2020) "Toward Smart Security Enhancement of Federated Learning Networks," *IEEE Network*, vol. 35, no. 1, p. 340. doi: 10.1109/mnet.011.2000379.

[2] Ma J., Naas S., Sigg S., and Lyu X. (2021) "Privacy-preserving Federated Learning based on Multi-key Homomorphic Encryption," *arXiv*, doi: 10.48550/arxiv.2104.06824.

[3] Zhao J. *et al.* (2025) "The Federation Strikes Back: A Survey of Federated Learning Privacy Attacks, Defenses, Applications, and Policy Landscape," *ACM Computing Surveys*. doi: 10.1145/3724113.

[4] Goel S., Tibrewal H., Jain A., Pundhir A., and Singh P. (2025) "Secure Generalization through Stochastic Bidirectional Parameter Updates Using Dual-Gradient Mechanism," doi: 10.48550/ARXIV.2504.02213.

[5] Dong Y., Wang Y., Gama M., Mustafa M., Deconinck G., and Huang X. (2024) "Privacy-Preserving Distributed Learning for Residential Short-Term Load Forecasting," *IEEE Internet of Things Journal*, vol. 11, no. 9, p. 16817. doi: 10.1109/jiot.2024.3362587.

[6] Asif H. M., Karim M. A., and Kausar F. (2022) "Federated Learning and its Applications for Security and Communication," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 8. doi: 10.14569/ijacsa.2022.0130838.

[7] Ranaweera K., Neiat A. G., Liu X., Kashyap B., and Pathirana P. N. (2025) "Enhancing Federated Learning Through Secure Cluster-Weighted Client Aggregation," doi: 10.48550/ARXIV.2503.22971.

[8] Jin W. *et al.* (2023) "FedML-HE: An Efficient Homomorphic-Encryption-Based Privacy-Preserving Federated Learning System," *arXiv*, doi: 10.48550/arxiv.2303.10837.

[9] Nguyen K., Khan T., Abdinasibfar H., and Michalas A. (2025) "A Privacy-Centric Approach: Scalable and Secure Federated Learning Enabled by Hybrid Homomorphic Encryption," doi: 10.48550/ARXIV.2507.14853.

[10] Puppala S. and Sinha K. (2025) "Towards Secure and Efficient Farming using Self-Regulating Heterogeneous Federated Learning in Dynamic Network Conditions," doi: 10.20944/preprints202504.1508.v1.

[11] Zheng Y., Lai S., Liu Y., Yuan X., Yi X., and Wang C. (2022) "Aggregation Service for Federated Learning: An Efficient, Secure, and More Resilient Realization," *arXiv*, doi: 10.48550/arxiv.2202.01971.

[12] Korkmaz A. and Rao P. (2025) "A Selective Homomorphic Encryption Approach for Faster Privacy-Preserving Federated Learning," *arXiv*, doi: 10.48550/arxiv.2501.12911.

[13] Han B., Li B., Qi Y., Jurdak R., Huang K., and Yuen C. (2025) "DP2Guard: A Lightweight and Byzantine-Robust Privacy-Preserving Federated Learning Scheme for Industrial IoT," doi: 10.48550/ARXIV.2507.16134.

[14] Kalapaaking A. P., Stephanie V., Khalil I., Atiquzzaman M., Yi X., and Almashor M. (2022) "SMPC-Based Federated Learning for 6G-Enabled Internet of Medical Things," *IEEE Network*, vol. 36, no. 4, p. 182. doi: 10.1109/mnet.007.2100717.

[15] Korkmaz A. and Rao P. (2025) "A Selective Homomorphic Encryption Approach for Faster Privacy-Preserving Federated Learning," doi: 10.36227/techrxiv.174120692.21508793/v1.

[16] Prasad K. R., Ghosh S., Cormode G., Mironov I., Yousefpour A., and Stock P. (2022) "Reconciling Security and Communication Efficiency in Federated Learning," *arXiv*, doi: 10.48550/arxiv.2207.12779.

[17] Du W., Li M., Wu L., Han Y., Zhou T., and Yang X. (2023) "An efficient and robust privacy-preserving framework for cross-device federated learning," *Complex & Intelligent Systems*, vol. 9, no. 5, p. 4923. doi: 10.1007/s40747-023-00978-9.

[18] Bonawitz K. *et al.* (2017) "Practical Secure Aggregation for Privacy-Preserving Machine Learning," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, p. 1175. doi: 10.1145/3133956.3133982.

[19] Bégui er C., Andreux M., and Tramel E. W. (2020) "Efficient Sparse Secure Aggregation for Federated Learning," *arXiv*, doi: 10.48550/arxiv.2007.14861.

[20] Pan Y. H., Zheng C., He W., Yang J., Li H., and Liming W. (2024) "FedSHE: Privacy preserving and efficient federated learning with adaptive segmented CKKS homomorphic encryption," *Cybersecurity*, vol. 7, no. 1. doi: 10.1186/s42400-024-00232-w.

[21] Zhao D. (2022) "CHEM: Efficient Secure Aggregation with Cached Homomorphic Encryption in Federated Machine Learning Systems," *arXiv*, doi: 10.48550/arxiv.2212.11475.

[22] Batistatos M. C., de Cola T., Kourtis M., Apostolopoulou V., Xilouris G., and Sagias N. C. (2025) "AGRARIAN: A Hybrid AI-Driven Architecture for Smart Agriculture," doi: 10.20944/preprints202503.1805.v1.

[23] Sandholm T., Mukherjee S., and Huberman B. A. (2021) "SAFE: Secure Aggregation with Failover and Encryption," *arXiv*, doi: 10.48550/arxiv.2108.05475.

[24] Ben-Itzhak Y. *et al.* (2024) "ScionFL: Efficient and Robust Secure Quantized Aggregation," p. 490. doi: 10.1109/satml59370.2024.00031.

[25] Zhao D. (2023) "Communication-Efficient Search under Fully Homomorphic Encryption for Federated Machine Learning," *arXiv*, doi: 10.48550/arxiv.2308.04648.

[26] Liu Z., Chen S., Ye J., Fan J., Li H., and Li X. (2022) "DHSA: Efficient Doubly Homomorphic Secure Aggregation for Cross-silo Federated Learning," *arXiv*, doi: 10.48550/arxiv.2208.07189.

[27] de Laage R., Yuhala P., Wicht F.-X., Felber P., Cachin C., and Schiavoni V. (2025) "Practical Secure Aggregation by Combining Cryptography and Trusted Execution Environments," p. 152. doi: 10.1145/3701717.3730543.