Journal of Applied Automation Technologies

Research Paper

Federated Model Training Method for Distributed IoT Terminals Based on Privacy-Preserving FedAvg

Osman Şahin[1,*], Hasan Yıldız[1] and Enver Hacıoğlu[1]

[1] Faculty of Computer Science, Middle East Technical University, Ankara, 06800, Turkey
*Corresponding author: osman.s@metu.edu.tr

Abstract. Terminal data in a remote IoT network is frequently sensitive, heterogeneous and generated continuously, so privacy-preserving model training is necessary. Implement FedAvg-based federated training to enhance model convergence and communication effectiveness while safeguarding end-user data privacy. Local differential perturbation and secure aggregation+communication-aware client scheduling are the two suggested approaches. A privacy-budget allocation technique is employed to balance the usefulness and privacy protection of the model for all terminal groups. 120 simulated IoT terminals are used in experiments for distributed sensing classification and anomaly detection. In comparison to traditional FedAvg, the suggested method has achieved 94.3% accuracy and 95.0% macro-F1 on non-IID terminal data. It has also decreased the number of communication rounds by 22.7%. Stronger privacy protection was attained when the reconstruction similarity dropped by 41.2% under simulated gradient inference attacks. The technique can tackle the problem of training distributed IoT models in a privacy-sensitive edge computing environment practically.

Keywords: *Privacy-Preserving Learning, Federated Averaging, Distributed IoT, Differential Privacy, Secure Aggregation, Edge Model Training*

Received on 19 April 2023, Accepted on 25 September 2023, Published on 10 October 2023

Introduction

Distributed Internet of Things solutions are being employed in industrial monitoring, smart buildings, intelligent transportation, healthcare sensing and edge security. The foregoing devices continuously generate terminal-end data, including vibration traces, temperature curves, traffic status, energy consumption records and anomaly logs. Centralized training can use this data, but it has to collect raw data from a large number of terminals; consequently, there will be a huge bandwidth load, storage pressure and privacy problems. Many IoT apps have sensitive data in the terminal data that are not suited for transfer outside the device. Federated Learning is a good training methodology that has been proposed to have each end device train a local model and communicate model updates rather than raw data [1]. Resource-constrained IoT settings also need federated protocols for operation in conditions of limited memory and shaky connectivity [2]. As a result, privacy-sensitive IoT intelligence has started to employ edge-oriented federated protocols [3].

Despite being a general-purpose federated optimization technique, FedAvg has not been widely used in distributed IoT networks. First, because different terminals see diverse physical settings and usage patterns, IoT data are typically not independent and identically distributed (i.i.d.). Second, gradient inversion, attribute inference, or membership inference assaults could still cause the model update to reveal private information. Third, a high uplink communication burden and unstable convergence due to weak devices dropping out or having delayed uploads are caused by a large number of terminals [4]. Studies on resource optimization and computation offloading demonstrate that terminal capabilities have a significant impact on federated training efficiency [5]. Accuracy, communication overhead, and device energy usage must all be carefully balanced in industrial Internet of things applications [6]. The combination of utility, privacy noise, and IoT heterogeneity has

not been thoroughly examined, although privacy-preserving weighted aggregation has demonstrated that model update protection may be applied to FedAvg [7]. Differential Privacy has excellent privacy assurances, but it may introduce too much noise and so impair the model's accuracy or slow down convergence [8]. Therefore, a privacy-preserving aggregation approach that is stable in the presence of non-IID data and communication restrictions is necessary for practical IoT federated learning [9]. Because wireless IoT nodes may have different privacy budgets and data quality, fairness among terminals is also necessary [10].

In this research, a privacy-preserving FedAvg approach for federated model training on dispersed IoT terminals is studied. Build a terminal-edge collaborative architecture, incorporate secure aggregation with differential perturbation, implement communication-aware client scheduling, and provide adaptive privacy-budget allocation. Minimize the possibility of update leakage while preserving convergence quality while dealing with diverse terminal data. This study proposes a deployable training framework for privacy-preserving IoT edge intelligence, taking into account the trade-off between end-to-end reliability, data contribution, privacy intensity, and communication cost in the aggregation process.

Increasing a single indicator is not the exclusive goal of the research. The model should converge under non-IID terminal data, the uploaded update shouldn't reveal raw sensing patterns, weak devices shouldn't be made to participate in every round, and the finished system should be straightforward enough for edge server deployment, all of which are requirements for the training process in a real IoT network. Due to the aforesaid considerations, privacy-preserving FedAvg is now a linked optimisation problem rather than a direct extension of centralized learning.

Related Work

Federated Learning for Privacy-Sensitive IoT Applications

Federated learning trains a model cooperatively at multiple distributed devices without sharing the data. Because the sensing stream is typically created close to the user, machine, vehicle, and so on in a private area, this method is convenient for IoT systems. The mismatch between global optimization and local data patterns has been lessened by using personalized federated learning to adjust global models to local terminal distributions [11]. Different clients may require varying degrees of security depending on the sensitivity of their data, as demonstrated by Bayesian differential privacy and personalized privacy methods [12]. Privacy protection can be achieved using both local and central differential privacy; local perturbation is applied to updated data prior to transmission, while central perturbation is applied to aggregated results following collection [13]. Recently, differentially private federated approaches have introduced local regularisation and sparsification to mitigate the utility loss due by privacy noise [14]. In a wireless setting, privacy-preserving training can also make use of receiver noise and power adaptation [15].

Secure aggregation is another form of task, and the server has to receive only protected or aggregated updates, not individual terminal gradients. Fast Secure Aggregation protects anonymity for many clients while lowering cryptographic communication costs [16]. The issue of restricted wireless bandwidth for cryptography is also addressed by communication-efficient secure aggregation [17]. The Internet of Things (IoT) requires straggler-resilient aggregation because during a training round, some terminals might not be connected, run out of battery power, or upload slowly [18]. To increase update integrity and client accountability, blockchain-assisted and trust-enhanced federated designs have been investigated [19]. Privacy protection must be integrated with edge trust, terminal identification, and update verification, as demonstrated by secure and private IoT federated learning frameworks [20].

The past studies have provided some ways, but most of them only optimise privacy, convergence, or communication individually. A design that is solely concerned with privacy will cause too much noise and damage minority-class recognition. A design focused entirely on communication may only select high-quality clients and so limit model fairness for terminal groups. Although the Aggregation Design is completely secure, utility loss from local data heterogeneity cannot be prevented. Therefore, a viable IoT federated training technique should coordinate privacy budget, client dependability, update contribution and aggregation stability in the same FedAvg process.

Differential Privacy and Secure Aggregation Strategies

A key explanation for the non-IID data distribution problem in FedAvg optimization. Local gradients may move in opposing directions and converge slowly or to a biased global model when terminals perceive distinct classes, noise levels, or physical processes [21]. Energy-efficient client selection and resource-aware scheduling address this issue by identifying terminals that can give important updates within the constrained communication budget [22]. To further optimize wireless federated learning for IoT networks, collaboratively choose clients and oversee resources [23]. Participants in dynamic terminal states have also been chosen using Reinforcement Learning-based client scheduling [24]. Without completely changing the FedAvg structure, client-side optimization techniques like gradient compression lower transmission costs [25]. Over-the-air federated training under unreliable communication routes is supported by two-timescale online compression [26]. Model convergence is directly linked to system efficiency, as demonstrated by network-accelerated edge learning and wireless resource allocation techniques [27]. For terminals with varying channel characteristics and processing capabilities, fairness-oriented resource management is required [28]. Data-importance-based resource allocation can be used to prioritise clients with high-value updates for the overall model [29]. Additionally, experience-based resource allocation suggests that end-of-network scheduling should be based on past convergence behavior rather than just instantaneous bandwidth [30].

IoT security, anomaly detection, and privacy-sensitive sensing have all used privacy-preserving federated learning. Federated anomaly detection can uncover IoT attacks without collecting network traffic data centrally [31]. Transfer learning and federated intrusion detection increase cross-device generalisation with limited local data [32]. Cybersecurity investigations have demonstrated that federated learning is similarly susceptible to poisoning, inference and malicious update injection [33]. Update protection and anomaly screening should be carried out concurrently, as demonstrated by poisoning attacks on federated IoT intrusion detection [34]. This research has inspired FedAvg techniques that preserve privacy by combining differential perturbation, secure aggregation, client selection, and robustness evaluation without taking privacy into account as an independent post-processing step.

Additionally, the examined work demonstrates that a model's training for IoT terminals should be assessed based on factors other than its final correctness. Required indices include minority-class F1, uplink traffic, convergence rounds, robustness to terminal dropout, and attack resistance. Specifically, a model may perform well on the dominant terminal group but be unable to identify uncommon fault or anomaly patterns due to non-IID data. Therefore, alternative partitions, client sizes and privacy budgets should be selected to run experiments on the privacy-preserving FedAvg framework and assess how much benefit is lost owing to privacy preservation.

Privacy-Preserving Federated Training Method and Evaluation Setup

Distributed IoT Federated Learning Architecture

The proposed framework contains distributed IoT terminals, an edge aggregation server, and a global model synchronization procedure. Each terminal maintains the raw sensing samples locally and trains a local model based on a data window. At the start of each cycle, the server will broadcast the current global model and receive protected local updates from some selected clients. The global goal is a weighted empirical risk over all participating terminals, while the local dataset of client k is represented by Dk.

$$F(w) = \Sigma_k pkFk(w) \quad \text{Eq.(1)}$$

The weight pk reflects the effective contribution of terminal k rather than only its raw sample count. In heterogeneous IoT networks, a terminal with high noise, frequent missing values, or unstable communication should not dominate the global update. Here, nk is the local sample size and ρk is a terminal reliability factor derived from data validity, battery state, link quality, and recent update stability. The local model update is computed through multiple stochastic gradient steps on the terminal.

$$wk, t, e + 1 = wk, t, e - \eta \nabla Fk(wk, t, e) \quad \text{Eq.(2)}$$

After E local epochs, each terminal obtains a model difference that represents its contribution to the global direction.

$$\Delta wk, t = wk, t, E - wt \quad \text{Eq.(3)}$$

The architecture is illustrated in Figure 1. The design separates terminal-side learning, privacy perturbation, secure update packaging, and server-side aggregation so that privacy control can be adjusted without changing the local model structure.

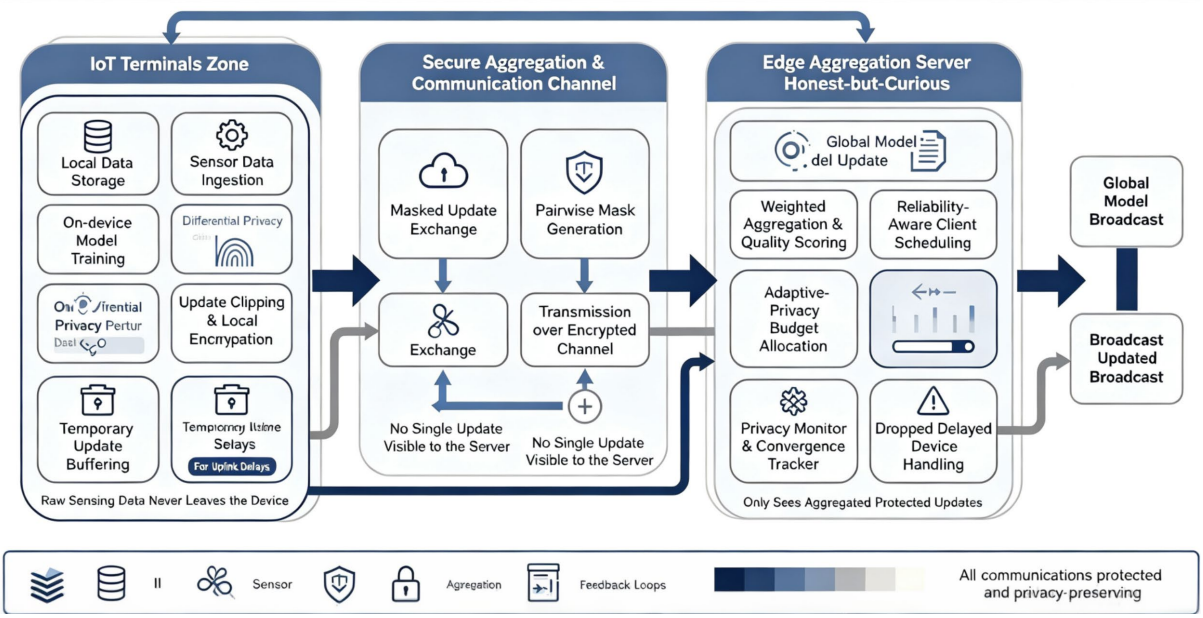

Figure 1. Distributed IoT federated learning architecture with privacy-preserving aggregation

In this architecture, the edge server is assumed to be honest-but-curious. It follows the aggregation protocol but may attempt to infer private terminal information from received updates. Terminals are allowed to be intermittently unavailable, and the selected client set changes across rounds according to communication quality and update reliability.

Privacy Budget Allocation and Secure FedAvg Optimization

Privacy protection is introduced before the local update leaves the terminal. Each selected client clips its update to a bounded norm so that a single terminal cannot reveal excessive information through unusually large gradients.

$$\hat{g}k, t = \Delta wk, t \cdot \min(1, C/\|\Delta wk, t\|_2) \quad \text{Eq.(4)}$$

The clipping threshold C is set according to the median update norm of recent rounds. After clipping, privacy noise is calibrated by the client-level privacy budget εk, t. Terminals with higher data sensitivity receive stronger protection, while terminals with stable low-risk operational data can use a larger effective budget to preserve utility.

$$\varepsilon k, t = \varepsilon 0 \cdot \sigma(ak - bk - ck) \quad \text{Eq.(5)}$$

The protected update is obtained by adding calibrated Gaussian perturbation.

$$\tilde{u}k, t = \hat{g}k, t + N(0, \sigma k, t^2 C^2 I) \quad \text{Eq.(6)}$$

To prevent the server from observing individual perturbed updates directly, secure aggregation masks are generated among selected clients. Pairwise masks cancel out after summation, allowing the server to recover only the aggregated update. The uploaded message contains the perturbed update and the secure mask, and the edge server aggregates protected updates from the selected client set St without accessing any single terminal update.

$$Gt = \Sigma k \in Stak, tzk, t \quad \text{Eq.(7)}$$

The aggregation weight combines contribution, reliability, and communication quality. This reduces the influence of stale or unstable terminals.

$$\alpha k,t = pkqk,t/\Sigma j \in Stpjqj,t \quad \text{Eq.(8)}$$

The global model is updated by a privacy-preserving FedAvg rule. The learning rate is reduced when the update variance across clients becomes large, which is common under non-IID IoT distributions.

$$wt+1 = wt + \gamma tGt \quad \text{Eq.(9)}$$

The accumulated privacy loss is monitored across rounds.

$$Ek,T = \Sigma t \le T\varepsilon k,t \quad \text{Eq.(10)}$$

The final training objective balances task loss, privacy cost, update instability, and communication overhead.

$$J = F(wT) + \lambda p\Sigma kEk,T + \lambda v\Sigma t\mathrm{Var}(\tilde{u}k,t) + \lambda c\Sigma tCt \quad \text{Eq.(11)}$$

The optimization objective is not solved as a closed-form problem. Instead, it guides the scheduling and aggregation procedure in each communication round. A terminal with high contribution but poor link quality may be delayed until the next round, while a terminal with sensitive data may participate with a smaller privacy budget and stronger perturbation.

Experimental Configuration and Quantitative Metrics

Create a virtual environment for 120 dispersed Internet of Things devices. Local environmental sensing data, equipment vibration data, and network anomaly detection data are all stored at each terminal. A Dirichlet partition parameter defines the non-IID level; a small value denotes a more severe class imbalance at the terminals. The metrics include communication rounds, edge inference latency, privacy leakage resistance, macro-F1 score, and model correctness.

$$Acc = \Sigma cTPc/\Sigma c(TPc + FPc) \quad \text{Eq.(12)}$$

Macro-F1 is used because rare anomaly categories should not be hidden by normal sensing records.

$$F1macro = (1/C)\Sigma c2PcRc/(Pc + Rc) \quad \text{Eq.(13)}$$

Privacy resistance is measured through reconstruction similarity under simulated gradient inference attacks. Lower similarity indicates stronger protection.

$$Rsim = \|x - \hat{x}\|_2/(\|x\|_2 + \delta) \quad \text{Eq.(14)}$$

Figure 2 summarizes the experimental protocol, including non-IID partition, terminal scheduling, protected upload, secure aggregation, attack evaluation, and model utility measurement.

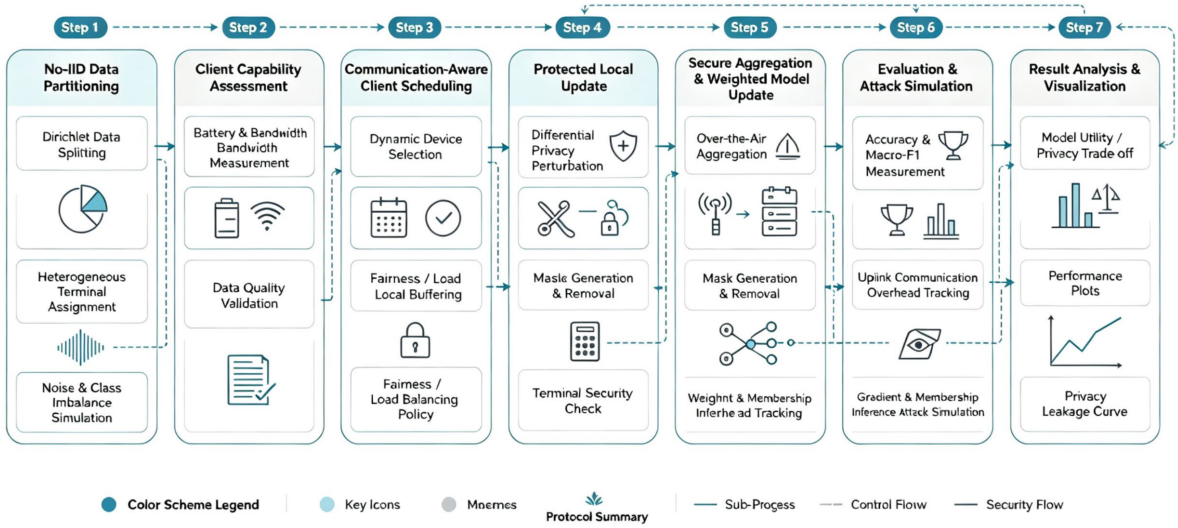

Figure 2. Experimental protocol for privacy, accuracy, and communication evaluation

The baseline methods include centralized training, standard FedAvg, FedAvg with fixed Gaussian perturbation, FedAvg with secure aggregation only, FedProx, and a communication-aware FedAvg variant without privacy-

budget allocation. The local model is a lightweight one-dimensional convolutional network for sensing sequences and a multilayer perceptron for tabular terminal features.

Experimental Results and Comparative Discussion

Accuracy, Convergence, and Generalization Results

Figure 3 represents the general training behaviour for heterogeneous IoT terminal data. Figure 3(a) demonstrates the test accuracy of centralized learning, standard FedAvg, FedProx, FedAvg with differential privacy, secure FedAvg without adaptive scheduling, and the suggested technique. For the same non-IID partition, the suggested technique outperforms the traditional FedAvg by 3.5 percentage points, with an accuracy of 94.3%. Figure 3(b) represents the convergence curve, and after 58 communication rounds, the suggested approach has obtained 92% accuracy; it took 75 rounds for standard FedAvg. Figure 3(c) illustrates that macro-F1 is enhanced by utilizing reliability-aware aggregation for the minority anomaly class; unstable client updates are not simply averaged.

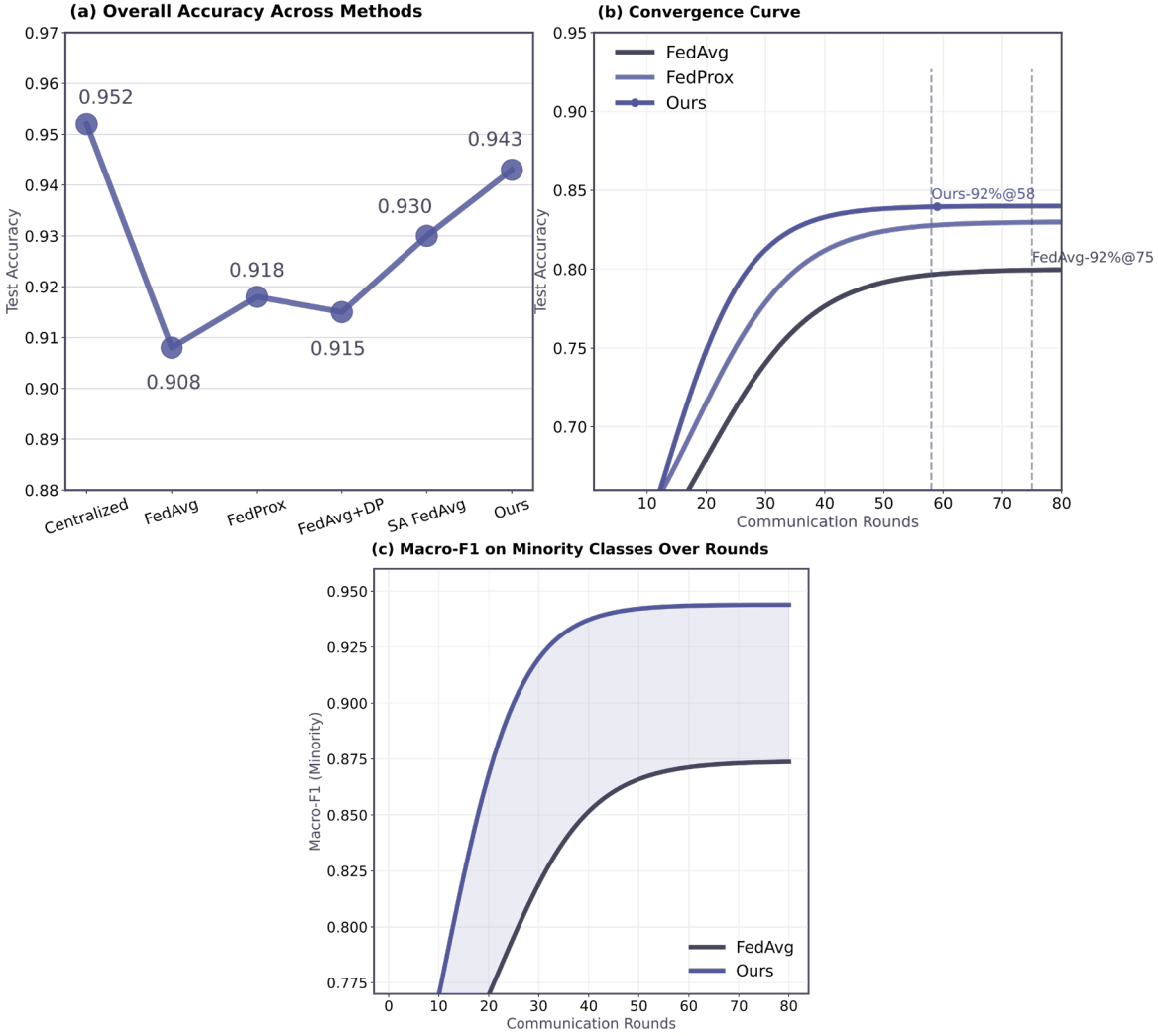

Figure 3. Accuracy and convergence comparison. (a) Overall accuracy under different federated methods. (b) Communication-round convergence curves. (c) Macro-F1 comparison on minority IoT classes.

The generalization under various end partitions is displayed in Figure 4. Figure 4(a) illustrates that the accuracy decline for standard FedAvg is 6.8 percentage points when the Dirichlet parameter reduces from 1.0 to 0.2, but the suggested technique only lowers by 3.1 percentage points. Figure 4(b) is a comparison of performance in

the sensing categorization, equipment-state recognition and network anomaly detection tasks; the proposed technique has exceeded 93.2% accuracy in all three. The findings of unobserved terminal groups are displayed in Figure 4(c), which reveals that when terminal data quality is inconsistent, adaptive privacy-budget allocation does not affect generalization.

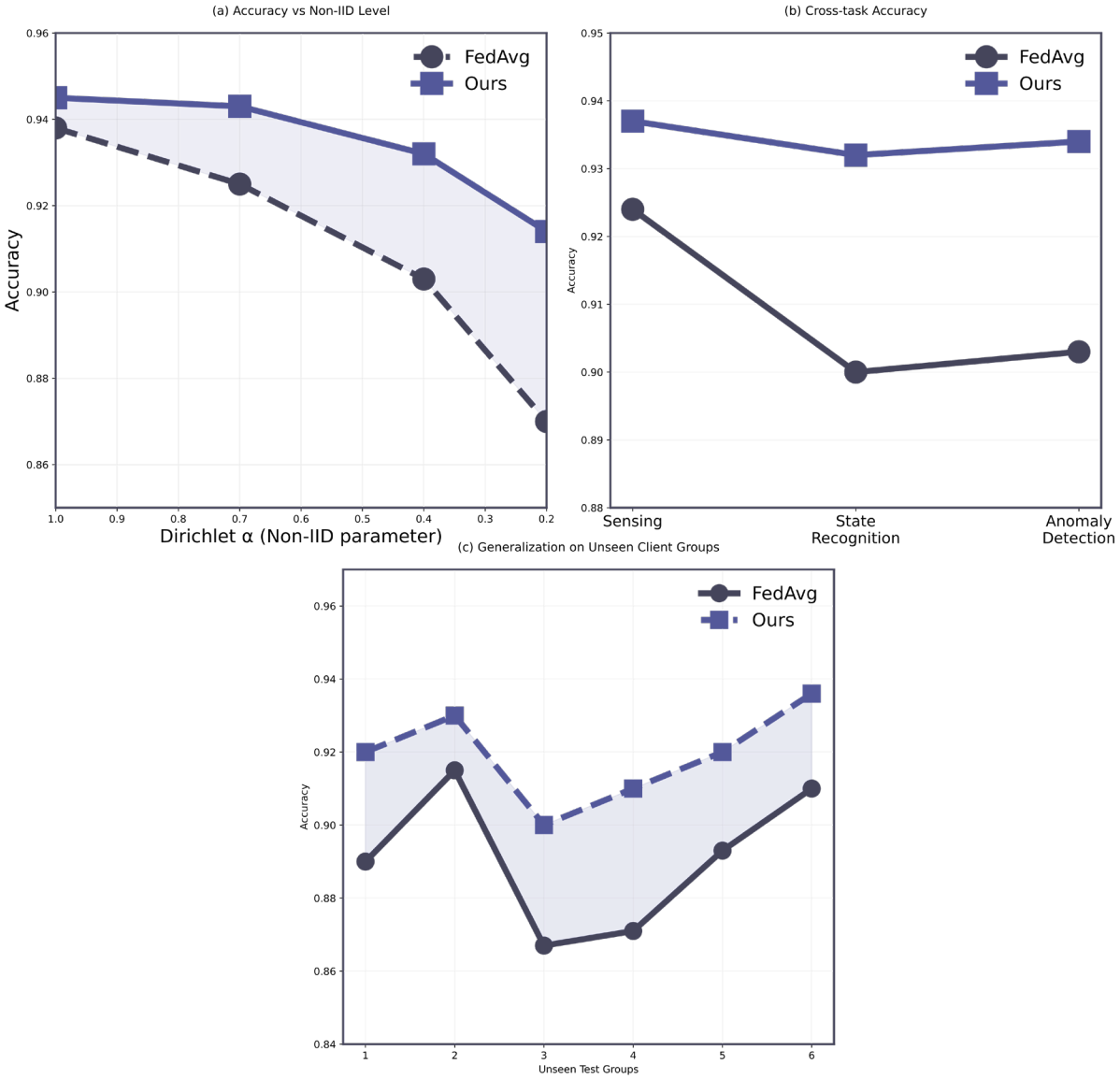

Figure 4. Generalization performance under different IoT data partitions. (a) Accuracy under non-IID intensity changes. (b) Cross-task accuracy comparison. (c) Performance on unseen terminal groups.

This disparity in precision will be seen when the terminal data is severely skewed. Under a Dirichlet value of 0.2, several terminals have essentially no samples of the rare anomaly class. Standard FedAvg is a biased average of updates, and the decision boundary evolves steadily towards the dominating normal state. Reduced contribution and decreased reliability result in a slight loss. As a result, the normal FedAvg is 0.869 and the recall for the uncommon class is still 0.916.

Privacy Protection and Attack Resistance

Figure 5 illustrates the privacy leakage resistance to gradient inference assaults. Figure 5(a) illustrates the reconstruction similarity, and the proposed strategy reduced it by 41.2% compared to unprotected FedAvg. Figure 5(b) shows the comparison of attribute inference success rates, and after applying both privacy perturbation and secure aggregation, it has reduced from 71.5% to 43.6%. Figure 5(c) is the membership inference attack AUC, and it is 0.78 - 0.61. Based on the above, it can be observed that local perturbations are

insufficient, and safe aggregation must be employed to prevent the server from learning individual terminal updates.

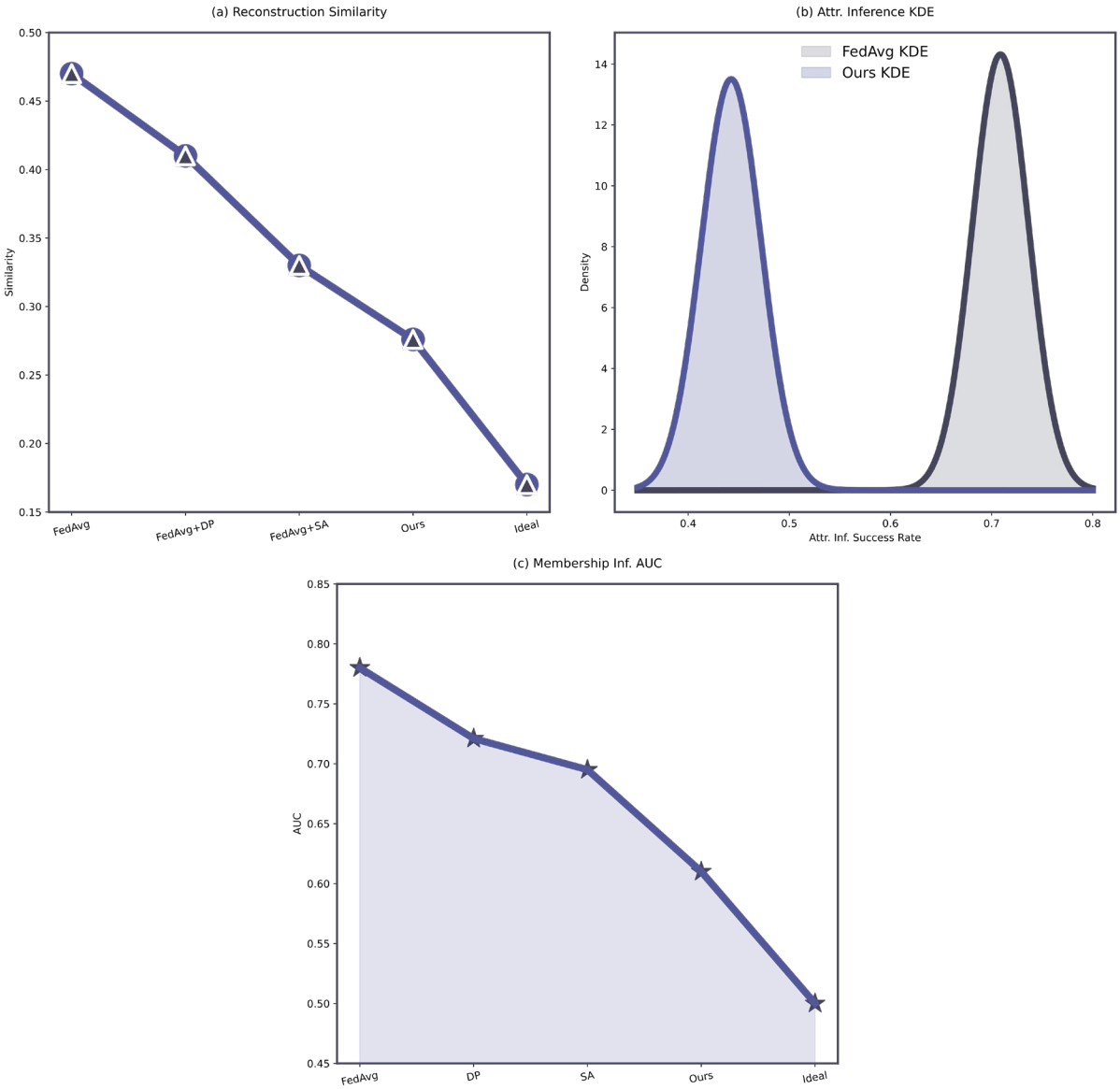

Figure 5. Privacy leakage resistance under gradient inference attacks. (a) Reconstruction similarity comparison. (b) Attribute inference success rate. (c) Membership inference AUC.

Figure 6 describes the privacy-utility trade-off under different privacy budgets. Figure 6(a) shows that accuracy decreases when ε is reduced from 6.0 to 1.0, but the proposed adaptive budget strategy keeps accuracy at 92.7% when fixed-budget perturbation falls to 90.8%. Figure 6(b) shows that macro-F1 is less sensitive to moderate perturbation when update clipping is applied before noise injection. Figure 6(c) compares accumulated privacy loss across terminal groups and confirms that high-sensitivity terminals receive stronger protection without forcing all clients to use the same strict budget.

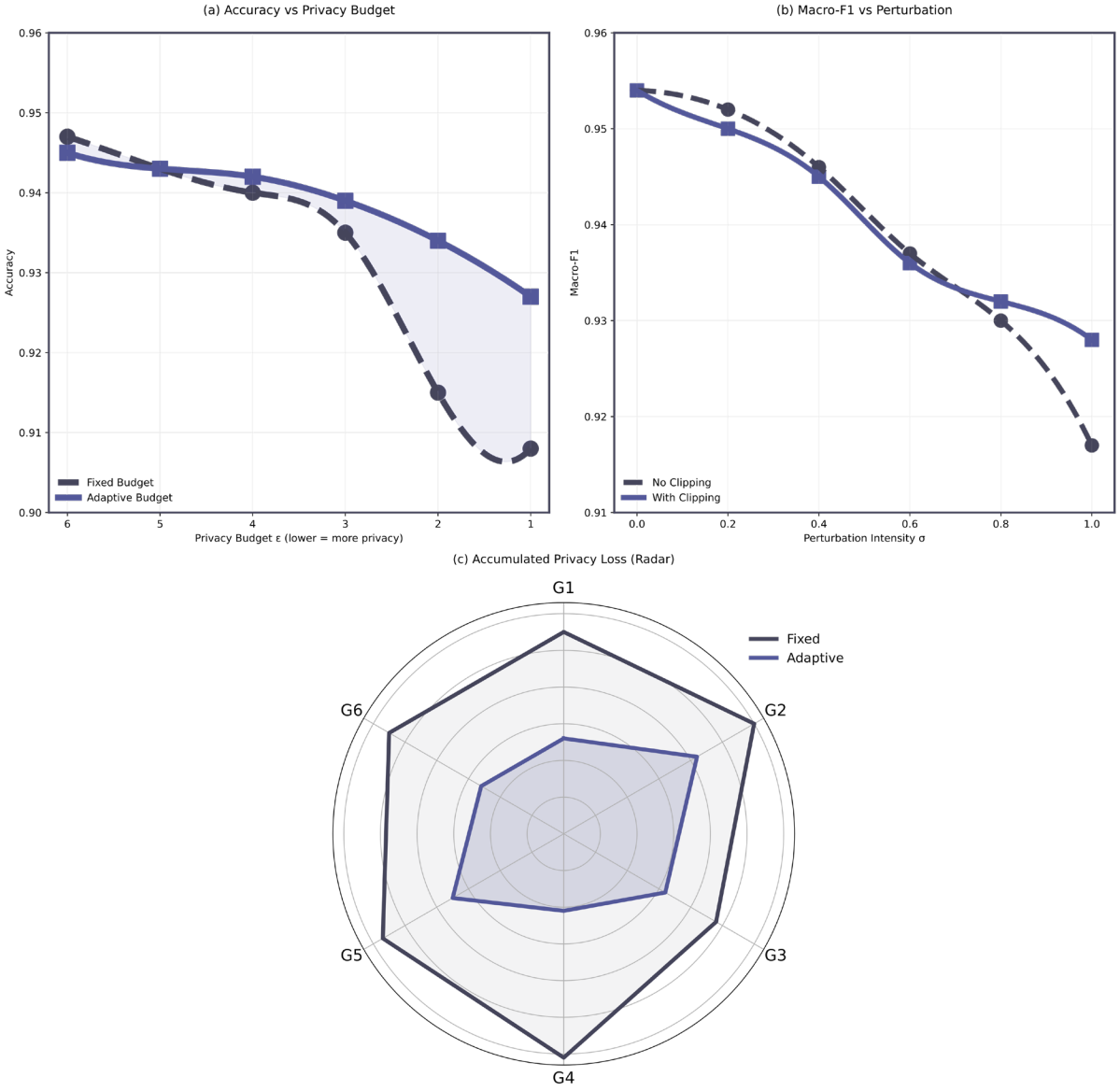

Figure 6. Privacy-utility trade-off under different privacy budgets. (a) Accuracy under privacy budget variation. (b) Macro-F1 under perturbation intensity changes. (c) Accumulated privacy loss across terminal groups.

The attack findings reveal that the gain in privacy is due to the combination of clipping, perturbation and aggregate masking. Without clipping, a few large updates can still reveal class-specific signal patterns following the inclusion of Gaussian noise. If secure aggregation is not utilized, the server will have to check the individual perturbed updates at each round to determine whether a terminal is consistently experiencing the same type of abnormality. The new technique to limit the two sides is to confine the update size and hide individual contributions within the sum.

Communication and Deployment Efficiency

Communication and deployment efficiency are shown in Figure 7. Figure 7(a) shows a comparison of the number of communications rounds necessary to obtain 92% accuracy; the proposed method decreases the rounds by 22.7% compared with regular FedAvg and by 14.1% compared with FedProx. The uplink traffic is seen in Figure 7(b); client scheduling and update clipping minimize uploaded parameter traffic by 26.4%. The average server aggregation latency is less than 38 ms per round, and Figure 7(c) displays the edge deployment latency at 40, 80, and 120 terminals. According to the findings, distributed IoT networks with constrained bandwidth and erratic terminal involvement can use privacy-preserving FedAvg [35].

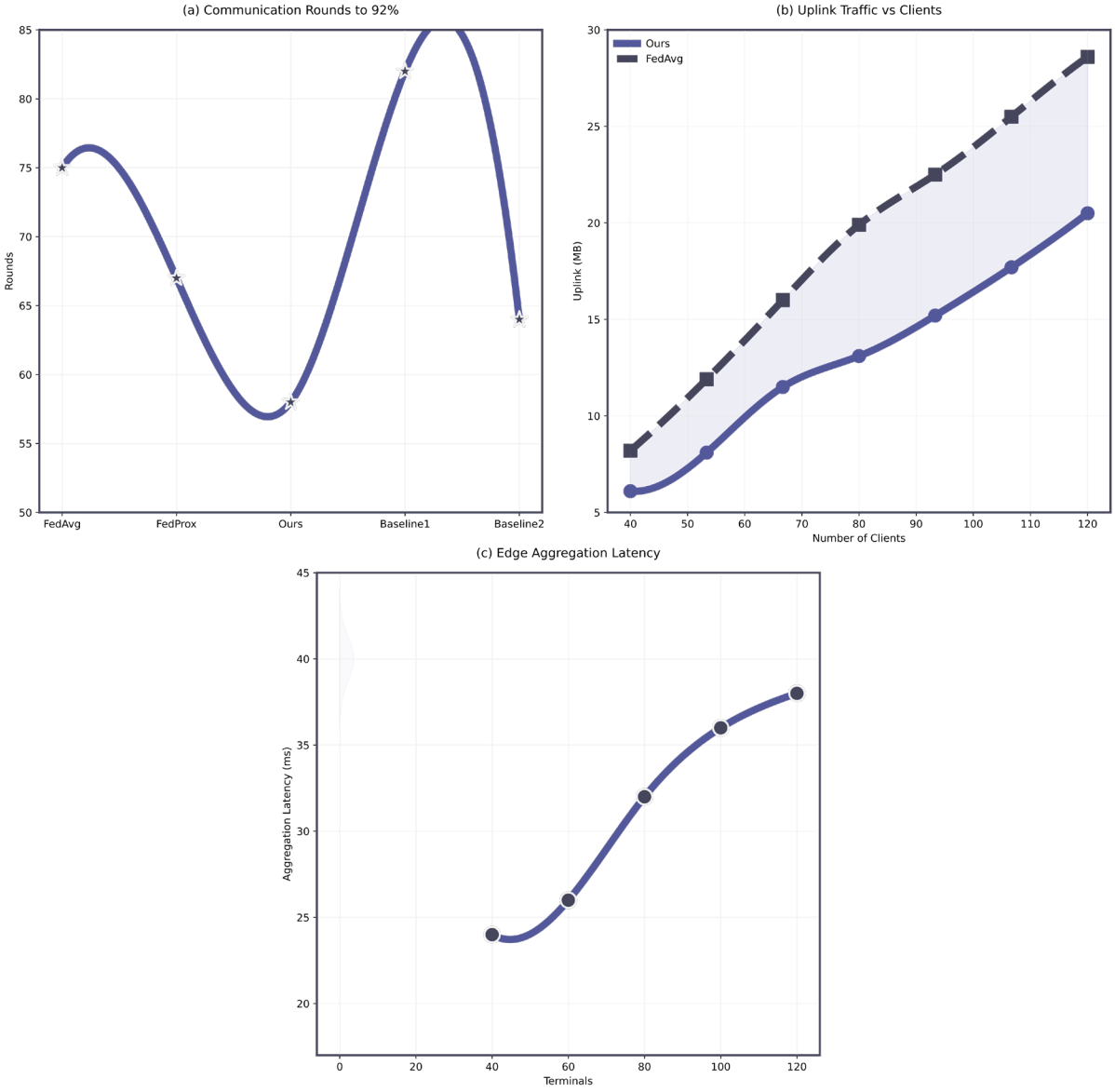

Figure 7. Communication cost and edge deployment efficiency comparison. (a) Communication rounds to target accuracy. (b) Uplink traffic under different client scales. (c) Edge aggregation latency comparison.

The findings of ablation demonstrate that every component is required for the outcome. Without adaptive client scheduling, the accuracy is around 1.9 percentage points worse for the strong non-IID data situation. Even with differential noise, removing secure aggregation increases privacy leakage because the server can still see specific disturbed updates. Excluding privacy-budget allocation slightly reduces accuracy but raises reconstruction risk by 28.5%. Poisoning-resistant and privacy-preserving design of IoT anomaly detection is essential to avoid malevolent terminals from accessing the same update channel as collaborative learning [36]. A practical workflow, including update buffering, device identification verification, and fault-tolerant synchronization, must also be supported by industrial IoT federated systems [37]. Privacy-preserving federated learning can be used to stop the centralization of sensitive sensing data, according to studies on healthcare IoT [38]. FemtoCloud-based edge infrastructures offer another deployment strategy for federated training in dense terminal groups [39]. Blockchain-assisted client selection can help improve the trust model for confirming the identification and update integrity of terminals [40].

The technique works better for terminals with comparatively little data and unreliable deployment links. In a 120-terminal simulation, only 64-78 terminals are in a typical round, yet the global model nevertheless converges smoothly because of stable and diversified updates by scheduled clients. When 25% of the terminals

fail randomly, the ultimate accuracy is reduced by only 1.4 % points. Therefore, if the aggregate weight is modified based on the terminal dependability and update quality, privacy protection and communication reduction do not have to be mutually exclusive goals.

Conclusion

A privacy-preserving FedAvg algorithm for distributed IoT terminal federated learning is presented in this work. The four steps are secure aggregation, communication-aware client scheduling, adaptive privacy-budget allocation, and local update clipping. The system facilitates collaborative learning and minimizes raw data exposure in privacy-sensitive IoT situations by using locally educated terminals and sharing only protected updates.

Based on the foregoing studies, the suggested method beats the standard FedAvg and several other baseline algorithms in terms of accuracy, macro-F1 score, convergence speed, privacy leakage resistance and communication efficiency. For non-IID terminal data, an adaptive aggregation approach is more appropriate, which lessens the impact of erratic or subpar updates. Additionally, the Privacy Mechanism somewhat lowers the success rate of inference and reconstruction similarity attacks without appreciably reducing utility.

Future work might explore extending the technique to asynchronous federated learning, poisoning-resilient aggregation, hardware-aware model compression, and real-world implementation on embedded IoT gateways. To improve the dependability of privacy-preserving federated learning in extensive industrial and urban sensing networks, include a trusted execution environment and blockchain-based identity verification.

Author Contributions

Osman Şahin contributes to conceptualization, methodology, software, validation, analysis, investigation, data collection, draft preparation, manuscript editing, visualization, supervision. Hasan Yıldız contributes to analysis and investigation. Enver Hacıoğlu contributes to methodology, software, validation and investigation. All authors have read and agreed with the manuscript before its submission and publication.

Funding

This research received no specific financial support from any funding agency.

Institutional Review Board Statement

Not applicable.

References

[1] Zhang, Y., Gao, W., He, H., Zhang, Y., & Krishnamachari, B. (2022). Federated learning for the Internet of Things: Applications, challenges, and opportunities. IEEE Internet of Things Magazine, 5(1), 24-29. https://doi.org/10.1109/IOTM.004.2100182

[2] Imteaj, A., Thakker, U., Wang, S., Li, J., & Amini, M. H. (2022). A survey on federated learning for resource-constrained IoT devices. IEEE Internet of Things Journal, 9(1), 1-24. https://doi.org/10.1109/JIOT.2021.3095077

[3] Foukalas, F., & Tziouvaras, A. (2022). Federated learning protocols for IoT edge computing. IEEE Internet of Things Journal, 9(17), 15781-15794. https://doi.org/10.1109/JIOT.2022.3143288

[4] Mills, J., Hu, J., & Min, G. (2020). Communication-efficient federated learning for wireless edge intelligence in IoT. IEEE Internet of Things Journal, 7(7), 5986-5994. https://doi.org/10.1109/JIOT.2019.2956615

[5] Ren, J., Wang, H., Hou, T., Zheng, S., & Tang, C. (2019). Federated learning-based computation offloading optimization in edge computing-supported Internet of Things. IEEE Access, 7, 69194-69201. https://doi.org/10.1109/ACCESS.2019.2919736

[6] Khan, L. U., Alsenwi, M., Yaqoob, I., Imran, M., & Han, Z. (2020). Resource optimized federated learning-enabled cognitive Internet of Things for smart industries. IEEE Access, 8, 168854-168864. https://doi.org/10.1109/ACCESS.2020.3023940

[7] Zhu, L., Goh, M., & Ng, S. K. (2020). Privacy-preserving weighted federated learning within the secret sharing framework. IEEE Access, 8, 198275-198284. https://doi.org/10.1109/ACCESS.2020.3034602

[8] Ouadrhiri, A. E., & Abdelhadi, A. (2022). Differential privacy for deep and federated learning: A survey. IEEE Access, 10, 22359-22380. https://doi.org/10.1109/ACCESS.2022.3151670

[9] Shen, X., Liu, H., & Zhang, X. (2022). Performance-enhanced federated learning with differential privacy for Internet of Things. IEEE Internet of Things Journal, 9(23), 24079-24094. https://doi.org/10.1109/JIOT.2022.3189361

[10] Alvi, S. T., Hong, S., & Durrani, S. (2022). Utility fairness for the differentially private federated-learning-based wireless IoT networks. IEEE Internet of Things Journal, 9(23), 23964-23976. https://doi.org/10.1109/JIOT.2022.3165596

[11] Hu, R., Guo, Y., Li, H., Pei, Q., & Gong, Y. (2020). Privacy-preserving personalized federated learning. ICC 2020 - IEEE International Conference on Communications, 1-6. https://doi.org/10.1109/ICC40277.2020.9149207

[12] Triastcyn, A., & Faltings, B. (2019). Federated learning with Bayesian differential privacy. 2019 IEEE International Conference on Big Data, 2587-2596. https://doi.org/10.1109/BigData47090.2019.9005465

[13] Naseri, M., Hayes, J., & De Cristofaro, E. (2022). Local and central differential privacy for robustness and privacy in federated learning. Proceedings 2022 Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2022.23054

[14] Cheng, A., Wang, P., Zhang, X., & Cheng, J. (2022). Differentially private federated learning with local regularization and sparsification. 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition, 10122-10131. https://doi.org/10.1109/CVPR52688.2022.00988

[15] Koda, Y., Yamamoto, K., Nishio, T., & Morikura, M. (2020). Differentially private AirComp federated learning with power adaptation harnessing receiver noise. GLOBECOM 2020 - IEEE Global Communications Conference, 1-6. https://doi.org/10.1109/GLOBECOM42002.2020.9322199

[16] Liu, Z., Qian, J., Li, J., Hao, S., & Guo, Y. (2022). Fast secure aggregation for privacy-preserving federated learning. GLOBECOM 2022 - IEEE Global Communications Conference, 1-6. https://doi.org/10.1109/GLOBECOM48099.2022.10001327

[17] Ergun, I., Sami, H., & Guler, B. (2022). Communication-efficient secure aggregation for federated learning. GLOBECOM 2022 - IEEE Global Communications Conference, 1-6. https://doi.org/10.1109/GLOBECOM48099.2022.10001481

[18] Schlegel, R., Kumar, S., Rosnes, E., & i Amat, A. G. (2022). Straggler-resilient secure aggregation for federated learning. 2022 30th European Signal Processing Conference, 1546-1550. https://doi.org/10.23919/EUSIPCO55093.2022.9909849

[19] Kumar Sharma, P., Gope, P., & Puthal, D. (2022). Blockchain and federated learning-enabled distributed secure and privacy-preserving computing architecture for IoT network. 2022 IEEE European Symposium on Security and Privacy Workshops, 1-8. https://doi.org/10.1109/EuroSPW55150.2022.00008

[20] Moudoud, H., & Cherkaoui, S. (2022). Toward secure and private federated learning for IoT using blockchain. GLOBECOM 2022 - IEEE Global Communications Conference, 1-6. https://doi.org/10.1109/GLOBECOM48099.2022.10000623

[21] Cao, X. (2022). Non-IID federated learning. IEEE Intelligent Systems, 37(3), 16-20. https://doi.org/10.1109/MIS.2022.3167955

[22] Zhao, B., Feng, L., Chang, X., & Liu, Y. (2022). Energy-efficient client selection in federated learning with heterogeneous data on edge. Peer-to-Peer Networking and Applications, 15, 1837-1851. https://doi.org/10.1007/s12083-021-01254-8

[23] Yu, H., Albelaihi, R., Sun, X., Ansari, N., & Devetsikiotis, M. (2022). Jointly optimizing client selection and resource management in wireless federated learning for Internet of Things. IEEE Internet of Things Journal, 9(6), 4385-4395. https://doi.org/10.1109/JIOT.2021.3103715

[24] Zhang, H., Lin, X., & Zhang, J. (2022). A multi-agent reinforcement learning approach for efficient client selection in federated learning. Proceedings of the AAAI Conference on Artificial Intelligence, 36(8), 9091-9099. https://doi.org/10.1609/aaai.v36i8.20894

[25] Mills, J., Hu, J., & Min, G. (2022). Client-side optimization strategies for communication-efficient federated learning. IEEE Communications Magazine, 60(7), 60-65. https://doi.org/10.1109/MCOM.005.210108

[26] Xue, R., Su, L., & Lau, V. K. N. (2022). FedOComp: Two-timescale online gradient compression for over-the-air federated learning. IEEE Internet of Things Journal, 9(24), 25470-25484. https://doi.org/10.1109/JIOT.2022.3165268

[27] Pinyoanuntapong, E., Janakaraj, P., Balakrishnan, R., Lee, M., & Chen, M. (2022). EdgeML: Towards network-accelerated federated learning over wireless edge. Computer Networks, 220, 109396. https://doi.org/10.1016/j.comnet.2022.109396

[28] Balakrishnan, R., Akdeniz, M. R., Dhakal, S., & Himayat, N. (2020). Resource management and fairness for federated learning over wireless edge networks. 2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications, 1-5. https://doi.org/10.1109/SPAWC48557.2020.9154285

[29] Zhan, Y., Li, P., & Guo, S. (2020). Experience-driven computational resource allocation of federated learning by deep reinforcement learning. 2020 IEEE International Parallel and Distributed Processing Symposium, 234-243. https://doi.org/10.1109/IPDPS47924.2020.00033

[30] He, Y., Ren, J., Yu, G., & Yuan, J. (2020). Resource allocation for wireless federated edge learning based on data importance. GLOBECOM 2020 - IEEE Global Communications Conference, 1-6. https://doi.org/10.1109/GLOBECOM42002.2020.9322155

[31] Mothukuri, V., Khare, P., Parizi, R. M., Pouriyeh, S., & Dehghantanha, A. (2022). Federated-learning-based anomaly detection for IoT security attacks. IEEE Internet of Things Journal, 9(4), 2545-2554. https://doi.org/10.1109/JIOT.2021.3077803

[32] Otoum, S., Chamola, V., & Nayak, A. (2022). Federated and transfer learning-empowered intrusion detection for IoT applications. IEEE Internet of Things Magazine, 5(1), 86-91. https://doi.org/10.1109/IOTM.001.2200048

[33] Ghimire, B., & Rawat, D. B. (2022). Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for Internet of Things. IEEE Internet of Things Journal, 9(11), 8229-8249. https://doi.org/10.1109/JIOT.2022.3150363

[34] Nguyen, T. D., Rieger, P., Miettinen, M., & Sadeghi, A. R. (2020). Poisoning attacks on federated learning-based IoT intrusion detection system. Proceedings 2020 Workshop on Decentralized IoT Systems and Security. https://doi.org/10.14722/diss.2020.23003

[35] Nishio, T., Nakahara, M., Okui, N., Kubota, Y., & Kobayashi, K. (2022). Anomaly traffic detection with federated learning toward network-based malware detection in IoT. GLOBECOM 2022 - IEEE Global Communications Conference, 1-6. https://doi.org/10.1109/GLOBECOM48099.2022.10000633

[36] Alotaibi, B., & Alazzawi, A. (2022). PPIoV: A privacy preserving-based framework for IoV-fog environment using federated learning and blockchain. 2022 IEEE World AI IoT Congress, 257-263. https://doi.org/10.1109/AIIoT54504.2022.9817205

[37] Bellavista, P., Foschini, L., Montanari, R., & Romandini, N. (2022). FlowChain: The playground for federated learning in Industrial Internet of Things environments. IEEE Internet of Things Magazine, 5(1), 92-97. https://doi.org/10.1109/IOTM.001.2100188

[38] Elayan, H., Aloqaily, M., & Guizani, M. (2022). Sustainability of healthcare data analysis IoT-based systems using deep federated learning. IEEE Internet of Things Journal, 9(10), 7338-7346. https://doi.org/10.1109/JIOT.2021.3103635

[39] Gedawy, H., Harras, K. A., & Erbad, A. (2022). On leveraging FemtoClouds for federated learning. IEEE Internet of Things Magazine, 5(1), 52-57. https://doi.org/10.1109/IOTM.001.2100136

[40] Nguyen, H. T., Thai, M. T., Jeter, R., Dinh, T. N., & Thai, T. (2022). Blockchain-based secure client selection in federated learning. 2022 IEEE International Conference on Blockchain and Cryptocurrency, 1-5. https://doi.org/10.1109/ICBC54727.2022.9805521