Federated Learning with Differential Privacy for Intrusion Detection in Internet of Flying Things: A Robust Approach

Vivian Ukamaka Ihekoronye, Dong-Seong Kim, Jae Min Lee
Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea
(ihekoronyevivian)@gmail.com,(dskim, ljmpaul)@kumoh.ac.kr

***Abstract*—In recent times, Federated Learning (FL) has emerged as a decentralized framework for intelligent knowledge sharing, demonstrating a degree of privacy preservation in safeguarding users' sensitive information across various cyber-physical networks like the Internet of Flying Things (IoFT) network. Nevertheless, there exists a vulnerability wherein adversaries can deduce clients' gradient or parameter updates to compromise privacy. This vulnerability is particularly concerning due to the clients' utilization of cybersecurity models aimed at securing the network against cyber intrusions and attacks. This study investigates the utilization of Gaussian and Laplace differential privacy (DP) mechanisms by clients during local training to obfuscate their model parameters, thereby mitigating the risk of data leakage. Extensive simulations utilizing the edge-IIoT dataset, validate the effectiveness of perturbing client models, in terms of upholding privacy and enhancing global model performance. Thus, demonstrating significant global model accuracy of 90%, specifically with the introduction of Laplace noise outperforming an unperturbed global model in a scalable network.**

***Index Terms*—Cybersecurity, Differential Privacy, Drone Network Security, Federated Learning, Internet of Flying Things, Intrusion Detection**

I. Introduction

Over the past decade, unmanned aerial vehicles (UAVs), commonly known as drones, have witnessed significant adoption in both civilian and military operations, owing to advancements in drone manufacturing technology and cost reduction [1]. Moreover, drones, being highly mobile and flexible Internet of Things (IoT) devices, are capable of functioning as aerial base stations, providing computational services within IoT networks. Thus, the integration of drones into the IoT network is referred to as the Internet of flying things (IoFT). The IoFT network enables drones to be equipped with adequate sensors, communication, and intelligent data processing capabilities to expand the functionality of real-time applications, such as security surveillance, key infrastructure monitoring [2], precision farming, disaster management, etc. Nevertheless, security issues have become a daunting challenge in the IoFT network, due to the susceptibility of IoT devices and systems to cyber threats. To promote security in this network, intrusion detection systems (IDS) based on artificial intelligence (AI) techniques are employed for detecting cyber attacks [3].

In the design of conventional AI-based IDS for IoFT networks, UAVs serve as relay nodes responsible for gathering data from the heterogeneous IoT devices within the network and transmitting these data either in real-time or periodic batches to a centralized data center in the cloud for processing and analysis. Consequently, machine learning (ML) models are leveraged to learn normal network patterns enabling the detection of anomalous deviations that could potentially pose threats to the network's security [4]. However, the continuous data transmission inherent in conventional IDS can lead to high communication costs and exacerbate the susceptibility to potential attacks. Which can be heightened in resource-constrained networks like the IoFT. Also, the sensitive data of users and industries are not preserved, since data privacy is not guaranteed in such cloud-centric frameworks [5].

Federated Learning (FL), is an emerging privacy-preserving computing paradigm that enables collaborative training of ML algorithms across distributed IoT devices [6],. Moreover, the IoT environment is highly susceptible to diverse types of attacks, therefore, the collaborative knowledge-sharing offered by the FL scheme is a plausible solution to promote privacy and security [7]. In the FL training process, edge devices or clients utilize their local data to train a shared global model and subsequently transmit only their model parameters to a parameter server for the global model aggregation. This approach minimizes the risk of private data leakage since only the clients' model parameters are transferred to a central server while the data remains locally. Nevertheless, one of the major privacy challenges encountered in FL is the potential of adversarial nodes to infer clients' model updates to launch various attacks like spoofing, malware injections, man-in-the-middle (MITM) attacks, and denial of service (DoS) attacks [8]. To address these privacy concerns in FL, various privacy-preserving techniques such as Secure Multiparty Computation (SMC), Homomorphic Encryption (HE), and Differential Privacy (DP) can be employed [9]. However, DP, specifically local DP (LDP) is the commonly used privacy-preserving technique in FL due to the computational complexity of other techniques [10].

LDP is employed in the IoFT network and other wireless networks to safeguard users' sensitive data. By adding noise to clients' training data or model parameters, the contribution of individual clients' data is obfuscated with randomized noise, rendering it difficult for attackers to infer specific client information. Several works have utilized LDP to achieve pri-

vacy preservation in FL [8]–[12], employing the probabilistic distribution of the DP mechanism. A novel noise additive DP mechanism based on differentiated noise perturbation was proposed in [8]. To reduce the loss of model performance, the proposed algorithm analyzes the weight of each client's update and compares the value with the weight of the global model parameter before adding noise to the model parameter. Also, [9] designed a privacy defense mechanism that intuitively perturbs gradients to compensate for the risk of information leakage in FL and to enhance the accuracy performance of the clients' models. In [11], the authors presented a secure DP that leverages an exchange protocol to secure clients transmitted weights and a decentralized FL setting to curb the failure risk of single-point systems.

Amidst the contributions of existing works, there is still a lack of investigation into the impact of the variants of statistical LDP on the baseline federated averaging (FedAVG) algorithm, especially in the security domain of the IoFT network. Therefore, this study presents a comprehensive evaluation of Laplacian and Gaussian noise perturbation techniques, which are integrated during the local training of the FL-based IDS to secure and guarantee privacy in the IoFT network.

The following are the contributions of this study:

1) The implementation of FL-based intrusion detection framework to secure the IoFT network from adversarial threats and attacks.
2) The perturbation of the clients' model updates with calibrated noise before updating the parameter server. Hence safeguarding the leakage of the users' sensitive information from malicious nodes.
3) The investigation of the impact of Gaussian and Laplace DP techniques on the performance of federated averaging aggregating algorithm, while analyzing the trade-off between utility (global model performance) and privacy, considering varying client sizes, privacy budgets, and batch sizes.

The rest of this article is structured as follows: The proposed federated learning privacy-preserving framework is captured in Section II, Results and Performance Evaluation is discussed in Section III, while Section IV captures the Conclusion.

II. Privacy-Preserving Federated Learning

In the scope of the Internet of Flying Things (IoFT) network, drones assume the role of aerial access points and edge servers, employed for operating ML-enabled intrusion detection models (IDMs), thus, fostering secure communication between IoT devices and the core network infrastructure. The interaction between drones and other IoT devices in the IoFT network is facilitated by a diverse array of communication mediums, encompassing Bluetooth, Zigbee, Wi-Fi, and advanced cellular networks (4G/5G). Leveraging FL techniques, the heterogenous data generated from IoT devices, including packets, logs, and network activities, is seamlessly relayed to the drones for localized model training. FL's decentralized and collaborative learning paradigm not only preserves user data privacy but also emerges as a potent defense mechanism against cyberattacks. By distributing model training across devices, FL minimizes the concentration of sensitive data in a central repository, thereby reducing the risk of data breaches and unauthorized access. Furthermore, as an extra layer of resilience against potential threats, noise is judiciously added to the model parameters during local training. This strategy not only enhances privacy preservation but also serves as a proactive measure to thwart potential privacy infringements arising from adversaries or cyberattacks. In summation, the fusion of Federated Learning with the IoFT network architecture stands as a promising strategy to mitigate cyberattacks, fortify security measures, and uphold the sanctity of data privacy in the ever-evolving digital landscape.

In the IoFT network, drones act as aerial access points/edge servers for communication between IoT devices and the core network, employing diverse communication mediums such as Bluetooth, Zigbee, Wi-Fi, and cellular networks (4G/5G). Leveraging the training techniques of Federated Learning, heterogeneous data from IoT devices, including packets, logs, and network activities, is transmitted to the drones for localized model training. FL's decentralized and collaborative learning paradigm not only preserves user data privacy but also emerges as a potent defense mechanism against cyberattacks. By distributing model training across devices, FL minimizes the concentration of sensitive data in a central server, thereby reducing the risk of data breaches and unauthorized access. Furthermore, as an extra layer of resilience against potential threats, noise is proactively added to the model parameters during local training. This strategy not only enhances privacy preservation but also serves as a proactive measure to thwart potential privacy infringements arising from internal adversaries (malicious participating clients/ honest-but-curious parameter server) and any external adversarial nodes.

A. Federated Averaging

Consider that the parameter server (a central aggregator) coordinates the training processes amongst the distributed clients (K) in the network. It is important to note that clients herein represent the drones that perform local training with the heterogenous data generated by the different IoT devices in the IoFT network. Let P_i be the private dataset owned by client i denoted as K_i, while D is the total data samples of all the clients. Therefore the federated knowledge-sharing process in the IoFT network as captured in Fig. 1 involves the following steps:

Step 1: The parameter server initializes the global model parameter W_R (including learning rate, batch size, and number of epochs for a neural network).

Step 2: The initial global model parameter is broadcast to a random number of selected clients f from the set of K clients, based on a predefined client selection approach (e.g. the drone's computational resource).

Step 3: Upon receiving the initial parameter of the global model W_R, the clients utilize their private data P_i to train the global model with the objective of minimizing the local loss function $L_i(P_i, w_i)$. Furthermore, leveraging a specific

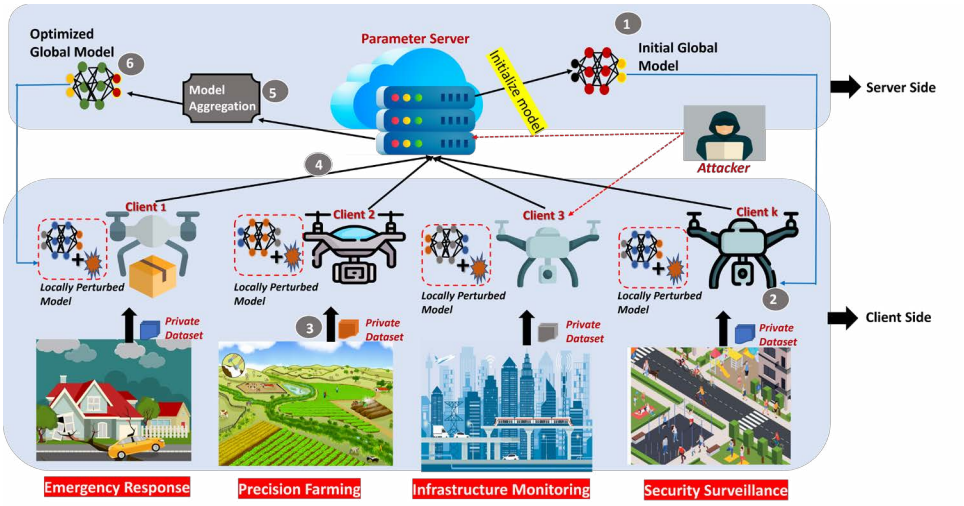

Fig. 1. Proposed Privacy-Preserving FL-Based Intrusion Detection Model for IoFT Network

differential privacy mechanism (either Gaussian or Laplacian DP mechanism), the clients anonymize the computed model parameter.

Step 4: Each participating client's resultant anonymized parameter is transmitted back to the parameter server.

Step 5: Based on the averaging principles of FedAVG employed by the parameter server, the server aggregates the updates from K clients to obtain an optimized global model.

$$W_{R+1} = \frac{1}{K}\sum_{i=1}^{K} w_i \tag{1}$$

Step 6: The new optimized global model is sent to a subset of clients for another round of training, iterating over multiple rounds of steps 3 to 5 until the global model converges giving a desirous performance. Therefore, the federated optimization problem can be formulated as:

$$w^* = argmin \sum_{i=1}^{K} L_i(P_i, w_i) \tag{2}$$

where w^* is the global loss function that solves the optimization problem of finding the optimal model parameters.

B. Local Differential Privacy (LDP)

A significant merit of the FL approach is that the clients' private data remains at the edge, while only their model updates are transmitted after training, hence, achieving a certain level of data privacy. However, inference attacks can be launched on clients' updates to infer the training data of specific users. Therefore, LDP is implemented as an additional defense layer to secure clients' sensitive data from inference attacks against malicious clients or a hones-but-curious parameter server. By implementing LDP, each client during training adds random noise to their model updates (as discussed in Step 3) before transmitting the resultant perturbed model to the parameter server for aggregation, to preempt data compromise. Definition 1 (Neighboring Datasets): Let the domain of all datasets in the IoFT network be denoted as P^n. Datasets P, $P^{'}$, where P, $P^{'} \in P^n$, are considered neighbors if they differ in a single entry.

Definition 2 (Mechanism): A mechanism M is a specific algorithm that adds noise to a dataset so that the privacy of individual data points is preserved. The mechanism M takes a dataset P as input and produces a randomized output Q.

Definition 3 (Differential Privacy): A mechanism M satisfies (ϵ)-DP if for any pair of neighboring datasets P and $P^{'}$, and any subset S of the mechanism's output space, the given probability is well defined:

$$Pr[M(P) \in S] \leq e^{\epsilon} Pr[M(P') \in S] \tag{3}$$

In other words, there is an inconsequential difference to an output when a mechanism M is applied to P and P', satisfying the differential privacy property. ϵ is the privacy budget that guarantees the level of privacy protection. A smaller value of ϵ provides a stringent privacy guarantee, which helps to limit the influence of any individual data point on the output. It is important to note that there is often a trade-off between privacy and utility (global model performance) when DP is implemented in the FL setting. As the addition of more noise (smaller value of ϵ) strengthens privacy, invariably limiting the potential for inference attacks. However, this can decrease the predictive capability of the global model, because excessive noise can obscure important learning patterns. Therefore, allocating the right amount of the privacy budget ϵ, that guarantees optimal data privacy and global model performance should be considered. The overall privacy-preserving FL-based algorithm is highlighted in Algirthm 1

C. Noise Additive DP Mechanisms

Gaussian and Laplace distributions are widely recognized as the primary noise additive mechanisms that inject random noise into data or computation outputs. These mechanisms serve the purpose of enhancing privacy and mitigating the potential exposure of sensitive information. Thus, the clients

Algorithm 1 Federated Averaging with Differential Privacy. K is the total number of clients, β the batch size, E number of epochs, p data sample, η learning rate and ϵ privacy guarantee

Procedure: Server Executes
Initialize Global Model Parameter W_G
Initialize privacy parameters ϵ

for *each federal round R = 1, 2, ...* **do**
  $F_R \leftarrow$ (random selection of F clients)
  for *each client* $k \in F_R$ *in parallel* **do**
    $W_{R+1}^k \leftarrow \text{ClientUpdate}(K, W_R, \epsilon, \delta)$
  end
  $W_{R+1} \leftarrow \sum_{k=1}^{K} \frac{p_k}{p} \cdot W_{R+1}^k$
end
Procedure: Client Update (k, w, ϵ)
$\beta \leftarrow$ (split p_i into mini-batches of size β)
for *each local epoch i from 1 to E* **do**
  for *batch* $b \in \beta$ **do**
    $w \leftarrow w - \eta \cdot \nabla l(w, b)$
  end
  Add the (ϵ)-DP mechanism to the local model weights w
  $w \leftarrow Q(w)$
end
return $Q(w)$ to server

perturb their model updates before sending them to the parameter server, to guard against privacy leakage.

1) Gaussian Mechanism [13]: Given a client's local model parameter w_R^i, the Gaussian mechanism can be implemented to perturb w by the addition of Gaussian noise u sampled from a Gaussian distribution with mean 0 and scale parameter σ ($n \sim N(0, \sigma^2)$) determined by the sensitivity (Δ) of the function and the privacy budget ϵ. Therefore, the addition of artificial Gaussian noise $n \sim N(0, \sigma^2)$ from a chosen noise scale $\sigma \geq c\Delta w/\epsilon$. c is the constant represented as $c \geq \sqrt{2ln(1.25/\delta)}$ for $\epsilon \in (0, 1)$. Note that Δ quantifies the maximum amount of noise that can be added to the client's update to obfuscate its contribution while achieving a desired level of privacy. Mathematically expressed as:

$$\Delta = \max_{\substack{P,P' \\ \|P-P'\|_1=1}} \|w'(P) - w'(P')\|$$

where P and P' are neighboring datasets that differ in a single entry ($\|P - P'\|_1 = 1$). $w'(P)$ is the perturbed model parameter computed with P. $w'(P')$ is the perturbed model parameter computed with P' and $\|.\|$ is the L_1 norm that measures the absolute difference between two vectors.

2) Laplace Mechanism [8]: Satisfies ϵ-DP and adds noise to a client's update from the Laplace distribution to enhance data privacy preservation. The Laplace Mechanism M given a function f: $P^n \rightarrow Y$, where Y is the set of possible outputs, is defined as:

$$M(P) = f(P) + Lap(\frac{\Delta f}{\epsilon}) \quad (4)$$

where Δf is the sensitivity of the function f

D. Learning Algorithm, Dataset Description, and Experimental Setup

We envisioned that each client in the network is equipped with a cybersecurity deep neural network (DNN) model that enables them to intelligently detect the emerging cyber-attacks peculiar to the IoT environment. To this effect, a lightweight DNN model comprising an input layer (64 neurons, representing the input features), 2 hidden layers (each stacked with 128 neurons), and an output layer of 6 neurons (representing the target classes of 5 attack and 1 benign label) was utilized as the shared model collaboratively optimized by the clients during the FL process for enhanced security in the IoFT network. Moreover, the ReLU activation function was applied to introduce non-linearity in the hidden layers, while the categorical cross-entropy loss function and the Adam optimizer were employed to address the requirements of the multi-class classification task.

Furthermore, we utilized the edge-IIoT dataset [14], a real-world dataset containing recent attacks such as MITM, DoS/DDoS, malware injections, information gathering, and injection attacks which constitute the major five classes of attacks in the dataset, to evaluate the performance of the proposed FL-based privacy-preserving IDM. After data preprocessing (the detailed preprocessing procedures can be gotten in [14]), 64 input features and 6 target classes containing a total of 152,196 instances were the final datasets used for the experiment, which was further split into 70:20:10, as the training, testing, and validation set respectively. Lastly, the experiment was done using $Flower$ federated framework on Google Colaboratory with Python 3.9.7.

III. Result Discussion and Performance Evaluation

The impact of both the Gaussian and Laplace mechanisms for varying privacy budget ϵ was investigated on the performance of the FedAVG aggregating algorithm, based on the Accuracy, Recall, Precision, and F1-Score evaluation metrics. On the one hand, the accuracy performances of FedAVG for both mechanisms given batch sizes 32 and 16 with a learning rate of 0.001, a local epoch of 5, client size K of 15, and communication rounds of 10, are displayed in Fig. 2. Also, we investigated the performance of FedAVG without the addition of noise.

Theoretically, a smaller value of ϵ provides stringent privacy preservation but at a trade-off of the utility (global model performance). However, from Fig. 2, considering both Gaussian and Laplace DP mechanisms, the addition of noise enhanced the accuracy of the global model in the detection of attacks. For instance, when ϵ = 0.3 with the addition of the Gaussian noise @ β = 32, the global model recorded increased accuracy

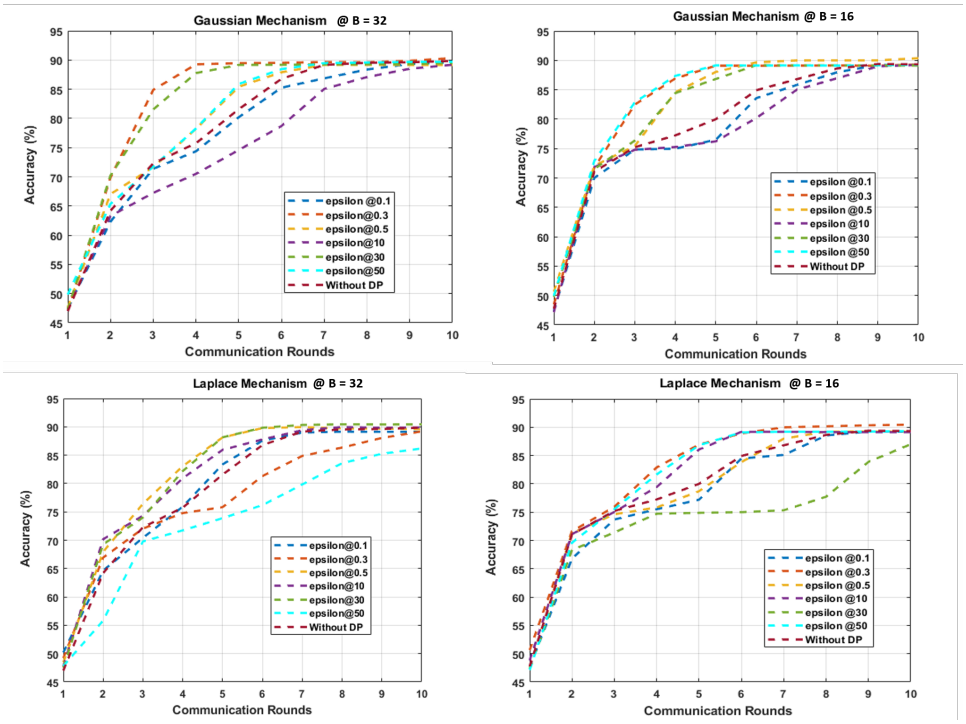

Fig. 2. Accuracy Performances of FedAVG Based on Gaussian and Laplace Mechanisms For Varying ϵ values and Batch-sizes When Client Size $K = 15$

of almost 90% within rounds 1 through 5. Similarly, for scenarios of all ϵ values and without DP given $\beta = 16$, a steady accuracy above 70% was recorded during rounds 1 and 2. However, given the predefined communication rounds, the convergence of the global model reaches optimal when $\epsilon = 0.3$, 0.5, and 50. The same effective global model performance is recorded with the addition of Laplace Noise for the different ϵ values when compared with the absence of the perturbation mechanisms.

This could be explained by recent research validating that the addition of gradient noise to stochastic gradient descent algorithms given a carefully calibrated noise threshold can improve the performance of the model [10]. Therefore, the proposed privacy-preserving FL-based IDM guarantees privacy and effectively secures the IoFT network even for the most stringent value of ϵ (lower) and the most lenient value of ϵ (higher).

On the other hand, to ascertain the robustness of the proposed model in guaranteeing data privacy whilst still securing the network given the imbalance in the class distribution of the dataset, the precision, recall, and F1-score metrics were evaluated and recorded in Table I. As highlighted in Table I, the addition of Gaussian noise requires a smaller value of ϵ to achieve optimal performance (for both batch sizes). In contrast, the Laplace mechanism requires a higher value of ϵ to achieve optimal performance. In essence, the integration of Gaussian noise into the clients' updates not only guarantees to safeguard the privacy of confidential information in the IoFT network but also enhances robust security against cyberattacks, based on the hyperparameters and the dataset utilized.

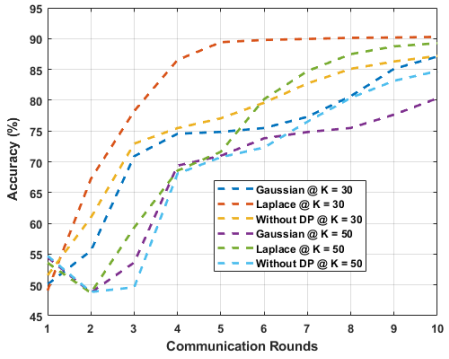

Fig. 3. Accuracy Performance of FedAVG when Perturbed with Different DP Mechanisms Vs Without DP given $\epsilon = 0.5$, $\beta = 16$ @ $K = 30$ and 50

Lastly, we investigated the impact of the noise perturbation mechanisms on a scalable network for fixed ϵ value of 0.5, $\beta = 16$ considering an increased K of 30 and 50 and compared with when no LDP was implemented. The accuracy performance for this simulated scenario is displayed in Fig. 3. As depicted in Fig. 3, the accuracy performance of the global model was optimized when Laplace noise was added to the local updates of the clients, despite the increase of client size. Moreover no significant difference in the accuracy when Gaussian noise was integrated when compared with when no noise was added, especially @ $K = 30$. Since the global model obtained accuracy performance of above 80%, specifically from rounds 8 to 10.

TABLE I
AVERAGE ATTACK DETECTION PERFORMANCE OF FEDAVG WHEN PERTURBED WITH GAUSSIAN AND LAPLACE MECHANISMS BASED ON VARYING PRIVACY BUDGETS

Epsilon	**Gaussian Mechanism @ B = 32**			**Laplace Mechanism @ B = 32**		
	Prec.(%)	**Rec.(%)**	**F1-Score (%)**	**Prec.(%)**	**Rec.(%)**	**F1-Score (%)**
0.1	72.71	74.96	68.78	73.69	75.01	69.70
0.3	**80.40**	72.62	**71.88**	70.55	76.13	68.45
0.5	74.22	74.80	70.08	77.29	73.69	71.03
10	70.62	**75.84**	67.20	75.90	74.39	70.75
30	77.61	73.52	71.69	**79.35**	66.51	**71.06**
50	75.51	74.54	70.25	67.87	**76.50**	65.78
Epsilon	**Gaussian Mechanism @ B = 16**			**Laplace Mechanism @ B = 16**		
0.1	71.84	76.09	69.29	71.85	75.78	69.14
0.3	76.92	74.04	**72.05**	**78.05**	74.09	**71.54**
0.5	**78.47**	74.19	71.82	72.77	75.71	69.80
10	71.10	**76.16**	68.99	75.01	74.93	71.01
30	75.43	74.85	71.54	67.84	**77.68**	66.48
50	77.08	74.05	72.33	75.28	74.67	70.97

IV. Conclusion

This study implemented a Federated Learning (FL) framework to enhance cybersecurity in the Internet of Flying Things (IoFT) network. The FL approach facilitates collaborative training of a shared cybersecurity model among clients (edge devices), aiming to optimize the global model's robustness in detecting attacks while upholding data privacy. Despite this, the potential risk for adversarial nodes to perform inference attacks on clients' updates can not be overlooked. To preempt such risks, local differential privacy utilizing Gaussian and Laplace noise was adopted as a proactive defense layer, effectively mitigating these attacks and preserving privacy. Comprehensive simulation experiments validated the proposed method's robustness, displaying the global model's capacity to attain optimal performance across varying epsilon values, thus ensuring privacy and security in the IoFT network. In the future, we will investigate the impact of advanced aggregation algorithms and differential privacy mechanisms, analyzing the interplay among privacy, communication costs, and utility.

Acknowledgment

This work was supported by Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (MEST)(2018R1A6A1A03024003) and the Ministry of Science and ICT (MSIT), Korea, under the Innovative Human Resource Development for Local Intellectualization support program (IITP-2023-2020-0-01612) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

References

[1] C. Zhu, X. Zhu, J. Ren, and T. Qin, "Blockchain-Enabled Federated Learning for UAV Edge Computing Network: Issues and Solutions," *IEEE Access*, vol. 10, pp. 56 591–56 610, 2022.

[2] S. O. Ajakwe, V. U. Ihekoronye, D.-S. Kim, and J.-M. Lee, "ALIEN: Assisted Learning Invasive Encroachment Neutralization for Secured Drone Transportation System," *Sensors*, vol. 23, no. 3, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/3/1233

[3] V. U. Ihekoronye, S. O. Ajakwe, D.-S. Kim, and J. M. Lee, "Cyber Edge Intelligent Intrusion Detection Framework For UAV Network Based on Random Forest Algorithm," in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, 2022, pp. 1242–1247.

[4] Y. Qu, H. Dai, Y. Zhuang, J. Chen, C. Dong, F. Wu, and S. Guo, "Decentralized Federated Learning for UAV Networks: Architecture, Challenges, and Opportunities," *IEEE Network*, vol. 35, no. 6, pp. 156–162, 2021.

[5] N. Mohammadi, J. Bai, Q. Fan, Y. Song, Y. Yi, and L. Liu, "Differential Privacy Meets Federated Learning Under Communication Constraints," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22 204–22 219, 2022.

[6] U. I. Vivian, I. N. Cosmas, D.-S. Kim, and J.-M. Lee, "DATA-FedAVG: Delay-Aware Truncated Accuracy-Based Federated Averaging for Intrusion Detection in UAV Network," *The Journal of Korean Institute of Communications and Information Sciences*, vol. 48, no. 6, pp. 648–668, 2023.

[7] B. Ghimire and D. B. Rawat, "Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8229–8249, 2022.

[8] L. Han, D. Fan, J. Liu, and W. Du, "Federated Learning Differential Privacy Preservation Method Based on Differentiated Noise Addition," in *2023 8th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA)*, 2023, pp. 285–289.

[9] J. Wang, S. Guo, X. Xie, and H. Qi, "Protect Privacy from Gradient Leakage Attack in Federated Learning," in *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*, 2022, pp. 580–589.

[10] P. Ruzafa-Alcázar, P. Fernández-Saura, E. Mármol-Campos, A. González-Vidal, J. L. Hernández-Ramos, J. Bernal-Bernabe, and A. F. Skarmeta, "Intrusion Detection Based on Privacy-Preserving Federated Learning for the Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1145–1154, 2023.

[11] O. Friha, M. A. Ferrag, M. Benbouzid, T. Berghout, B. Kantarci, and K.-K. R. Choo, "2DF-IDS: Decentralized and Differentially Private Federated Learning-Based Intrusion Detection System for Industrial IoT," *Computers Security*, vol. 127, p. 103097, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S016740482300007X

[12] R. Hu, Y. Guo, E. P. Ratazzi, and Y. Gong, "Differentially Private Federated Learning for Resource-Constrained Internet of Things," 2020.

[13] Z. Yu, J. Hu, G. Min, Z. Wang, W. Miao, and S. Li, "Privacy-preserving federated deep learning for cooperative hierarchical caching in fog computing," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22 246–22 255, 2022.

[14] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-iiotset: A new comprehensive realistic cyber security dataset of iot and iiot applications: Centralized and federated learning," 2022. [Online]. Available: https://dx.doi.org/10.21227/mbc1-1h68