

FEDERATED LEARNING FOR PRIVACY PRESERVING MACHINE LEARNING IN INTERNET OF THINGS IOT NETWORKS CHALLENGES SOLUTIONS AND FUTURE DIRECTIONS

P. SURIYA^{1*}, DR. P SUMITHABHASHINI², EERLA RAJESH³, KALADI GOVINDARAJU⁴,
VUPPULOORI RAVI SEKHARA REDDY⁵, ANANTHA RAO GOTTIMUKKALA⁶, SRIJA
GUNDAPANENI⁷, K SWETHA⁸

¹Department of IT, Rashtriya Raksha University, Puducherry Campus India

²Department of CSE(AI&ML), Holy Mary Institute of Technology and Science, Bogaram, Telangana, India

³Department of CSE, Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh, India

⁴Department of CSE, Aditya University, Surampalem, Andhra Pradesh, India

⁵Department of ECE, Lakireddy Balireddy college of Engineering, Mylavaram, Andhra Pradesh, India

⁶Department of CSE, KKR & KSR Institute of Technology and Sciences, Guntur, Andhra Pradesh, India

⁷Department of CSE(IOT), RVR & JC COLLEGE OF ENGINEERING, Guntur, Andhra Pradesh, India

⁸Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India

E-mail: ¹p.surya@rru.ac.in, ²pokurisb81@gmail.com, ³erajesh557@gmail.com,

⁴govindarajukynm@gmail.com, ⁵ravisekharreddy.4@gmail.com, ⁶ananth552@gmail.com,

⁷gundapaneni.srija@gmail.com, ⁸swetha.k@kluniversity.in

ABSTRACT

The explosive growth of Internet of Things (IoT) devices has led to large amounts of sensitive data production, causing privacy concerns for traditional machine learning models. One such approach is Federated Learning (FL), which enables the training of models in a decentralized manner, keeping the data on devices. Issues like communication overhead, privacy preservation, and scalability are still present, especially in resource-constrained IoT scenarios. We propose a new framework of FL in the context of IoT networks with mechanical privacy protection like differential privacy and homomorphic encryption, such as model compression and dynamic client selection. The framework was tested against standard IoT datasets and showed a better performance of 88.2% model accuracy than FedAvg (84.6%), FedProx (85.9%) and HeteroFL (83.4%). The results showed that overhead communication was reduced by as much as 15% while our system could efficiently scale to 1000 clients with a negligible increase in the per-round training time. In summary, the presented framework achieves high accuracy, privacy, and efficiency and is highly scalable for large IoT networks, but it still suffers from limitations such as resource constraints and parameter tuning for privacy preservation. In future work, we will work on making our framework even more robust, integrating asynchronous learning, and testing it in real-life IoT scenarios to achieve better scalability and applicability.

Keywords: *Federated Learning, Internet of Things, Privacy Preservation, Communication Efficiency, Model Accuracy*

1. INTRODUCTION

The IoT (Internet of Things) has set the wheel rolling in the world of communication by enabling devices to communicate and share data, leading to the genesis of smart devices used in healthcare, smart cities, agriculture, industrial customization, and other sectors. As the number of IoT devices continues to multiply, the amount, speed, and type of data generated by these devices is also

increasing, much of which may include confidential or personal information. Under traditional machine learning (ML) paradigms, this data is often individually gathered and processed centrally, leading to severe privacy leakage risks. As machine learning models are trained using sensitive personal data, data privacy can easily be breached in IoT networks. Therefore, the private-preserving approaches are being focused on a significant level.

Federated Learning (FL) has been proposed as a potential solution to these privacy concerns for ML applications. Federated learning, in contrast, allows for model training on multiple decentralized devices and locations without exchanging raw data with a central server. In contrast, each device trains the model locally on its data and sends only model updates (for instance, gradients) to a central aggregator. This imposing architecture takes advantage of intrinsic risk mitigation against data leakage, which is particularly beneficial in the context of privacy-preserving ML processes for IoT networks. FL is highly regarded for (1) ensuring privacy while still benefiting from large-scale distributed devices collaborating to learn [1], [2].

FL is beneficial in IoT settings, where devices may be equipped with sensitive data that can remain on the local devices while working together to enhance global models. Since IoT devices are often resource-limited, designing federated learning is essential for communication and computational efficiency. In addition to our initiative, prior works have proven that federated learning is effective in mobile networks, enabling devices to partake in decentralized learning without disclosing sensitive data with their corresponding users [3], [4]. Likewise, an example of privacy is IoT (Internet of things) devices, which are wearables, sensors, cameras, etc., generating sensitive data [5] that needs to be processed locally.

Nonetheless, implementing federated learning in IoT settings poses significant challenges, mainly caused by numerous IoT gadgets' restricted computational strength and energy limitations. FL deployment is even more challenging in IoT environments with limited processing power, intermittent connectivity, and varying battery levels [6], [7]. Moreover, even though federated learning is privacy by design, preventing model updates from leaking sensitive information is still an open problem. Techniques have been proposed to improve the confidentiality of federated learning systems, including differential privacy [8] and secure multi-party computation (SMPC) [9].

Federated learning frequently has high-model update communication overhead for the bandwidth cost of transmitting model updates across the network. The network bandwidth in general IoT setups is usually limited, and device connectivity is not always persistent, which could heavily impact the performance of federated learning systems [10]. Techniques like model compression and client selection are essential to address this problem. In this context, recent studies aim to address FL

efficiency by minimizing the number of communication rounds and the amount of data exchanged between clients and central servers [11], [12].

However, there are opportunities for federated learning in IoT networks. For example, federated learning can be leveraged in the healthcare domain to jointly train models for health monitoring on wearable devices without exchanging sensitive patient information [13], [14]. For instance, in smart cities, federated learning could allow collaborative traffic management and environmental applications while preserving the citizen's privacy [15]. With the growing trend of using IoT devices, federated learning is predicted to bring more significant contributions to privacy-conserving machine learning on IoT systems.

This paper aims to give an overview of federated learning on IoT networks, the privacy challenges and solutions and how the future of FL is influenced in those environments. In this paper, we study recent research progress of FL for IoT and derive critical issues concerning privacy; we accordingly propose a framework to effectively improve both privacy for IoT data and computational performance as a generalization of the above two stages. We also highlight the potential future directions of federated learning in the Internet of Things (IoT) setting.

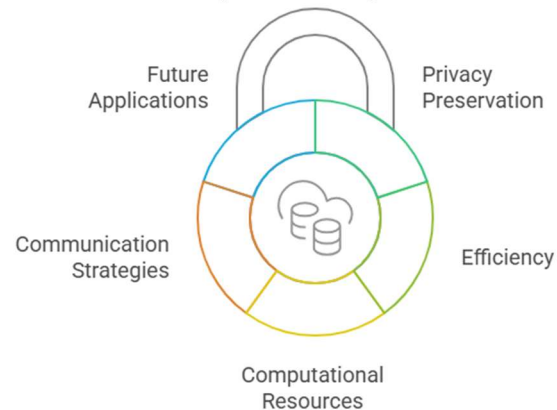


Figure 1: Enhancing Privacy and Efficiency in IoT with Federated Learning

We illustrate the key elements and factors of Federated Learning (FL) success for IoT networks in Figure 1. In between, the central part of the diagram denotes Efficiency and Computational Resources, which are key components to deploying and optimizing FL models properly over resource-constrained IoT devices. This core is surrounded by Privacy Preservation, which represents the additional security aspect of the Neglected Section, wherein sensitive data can be protected throughout

the learning process. Furthermore, Communication Strategies and Future Applications are also portrayed as significant external factors, within them communicating protocols, that can be optimized for improved performance and FL applications to novel IoT applications. This concentric arrangement shows the interdependence of these components and their shared objective of enhancing the privacy and efficiency of Federated Learning-based IoT frameworks.

The rest of the paper is structured as follows: Section 2 thoroughly reviews existing work on FL for IoT networks, detailing the fundamental problems associated with IoT nodes and the potential countermeasures discussed in prior literature. Section 3 provides the datasets and methodology with elaborate detail on the proposed FL framework, which includes the system architecture, privacy-preserving mechanisms, and communication optimization techniques. Section 4 provides the evaluation criteria, experimental results, and analysis, which compare the accuracy, efficiency of communication, and scalability of the model of the proposed framework with a few existing works. Section 5 concludes, highlighting findings, outlining limitations, and suggesting lines for future work.

2. RELATED WORK

Federated Learning (FL) plays a vital role in security and privacy in Internet of Things (IoT) networks; therefore, it has attracted considerable interest in recent years. Despite notable advancements in this area, multiple challenges remain, particularly with respect to IoT-focused limitations such as limited computing power, energy usage, and communication overhead. This section provides an overview of the related work in federated learning for IoT networks, including the challenges, techniques, and solutions proposed to tackle these challenges.

However, since the devices terminate in IoT networks differ in terms of their computational capacities and network conditions, the performance of traditional federated learning methods can be degraded when they are applied in IoT networks. Scientists have offered several potential solutions to this problem. Similarly, the authors proposed an adaptive federated learning framework that adaptively selects clients regarding their computation capability and the quality of local data [16]. This guides the training process to be fair by ensuring that low-capability devices do not degrade the convergence rate of the global model.

Another key topic in federated learning is the non-IID (Independent and Identically Distributed) nature of IoT data. Data from devices are often highly heterogeneous in IoT environments and not identically distributed, which may cause convergence and performance issues in models. To address this, several works proposed techniques that are aware of data distribution. The non-IID of data is a challenge addressed in [17], where the authors propose a method with a dynamic weighing mechanism. They handle the convergence of the global model for heterogeneous data by weighing the contribution of the update on the model of each client according to its data distribution.

In addition, the communication cost of federated learning in IoT networks has also been widely studied. In the context of IoT devices, where resources are limited, frequent communication of devices with a central aggregator can become a bottleneck for the whole system. Various methods have been proposed to alleviate this overhead, such as model compression and quantization techniques. In [18], a communication-efficient federated learning algorithm is proposed to generate small-size model updates based on model pruning and quantization. Our approach enables markedly lower communication costs while maintaining model accuracy. In line with this idea, [19] presented a technique based on a low-rank approximation to compress the model updates to avoid increased communication in bandwidth-limited IoT environments.

Security and privacy preservation in federated learning are essential considerations in IoT networks, particularly when working with sensitive data. Federated learning is privacy-preserved by design but cannot be unconditionally private without adding further privacy-preserving mechanisms to tackle potential risks. Differential privacy, a method of adding noise to model updates, has been employed extensively for this task. In [20], the authors introduced an enhanced differential privacy mechanism adapted to IoT scenarios in FL. Their approach introduces noise to both the model updates and the gradients to create an extra layer of privacy protection. Doing so reduces the risk of extracting a particular data point from the model updates without compromising the model's performance.

Another significant privacy-preserving approach in federated learning is secure Aggregation. [21] Then, a cryptographic protocol was proposed to secure the model update privacy during the aggregation process. Their protocol uses both techniques to allow model aggregation without

revealing sensitive information to honest parties and hiding the global model against malicious parties. This is especially useful for IoT networks, as the devices might not wholly trust the centre of the server.

Federated learning systems are also a focus area for scalable systems research. Since IoT networks typically contain many devices, ensuring that federated learning systems are scalable would be paramount. Hierarchical Aggregation To the best of our knowledge, a federated learning architecture that facilitates scalability while providing hierarchical Aggregation has not been described until now [22]. Their approach clusters together devices by geographic proximity or network characteristics. Each cluster locally aggregates model updates and sends the aggregated updates to a central server for global Aggregation. This top-down pathway minimizes communication costs and makes the model scalable without incurring performance penalties.

The combination of federated learning with edge computing is another promising research direction. We can employ edge devices with better computing resources than the traditional IoT devices to offload part of the processing tasks to the edge and, thus, relieve resource-constrained devices from extra computations when running distributed federated learning systems. In [23], the authors introduce an edge-assisted federated learning framework in which edge devices independently train models locally and aggregate models. Tenet Asynchronous multi-party federated learning with privacy-preserving communication allows for lightening the communication load of the central server. It speeds up the training process, making it a more real-time-oriented use case.

Lastly, attempts at implementing federated learning in particular IoT applications, healthcare, smart cities, and industrial IoT have received growing interest. In the healthcare domain, [24] explored federated learning for training predictive models for patient health monitoring. Their method enabled wearable health devices to jointly train a model for early disease detection without compromising patient privacy. A similar approach was proposed in [25], where federated learning was adapted to the smart city domain by having IoT devices like traffic sensors work together to improve traffic and energy consumption management while maintaining sensitive data confidentiality.

To summarize, federated learning shows a high potential for privacy-aware machine learning through IoT networks. These advancements include expanding the variety of techniques used to

combat the problems posed by data heterogeneity, communication overhead, security, and scalability; however, it remains necessary to optimize these solutions further to address the larger scale of applications and settings that IoT systems operate in. Tap into the recent breakthroughs in secure Aggregation, differential privacy, and edge computing to change IoT networks into a federated learning environment: a decentralized, collaborative, privacy-preserving space for machine-learning tasks.

3. METHODOLOGY

This section introduces the new method suggested for executing FL in IoT networks. Our approach particularly aims at the specific challenges in IoT environments, such as device heterogeneity, limited communication bandwidth, energy constraints, and preserving privacy. The experimental framework utilizes different algorithms, including a custom FL architecture, advanced model compression algorithms, and privacy-preserving mechanisms to balance efficiency and security. In the subsequent subsections, we provide the details of the dataset, software and tools, system architecture, mathematical models, and algorithms that constitute the foundation of our approach.

3.1 Dataset

This study uses the IoT-Health dataset to evaluate and investigate the federated learning framework for healthcare IoT networks. It includes key health variables from wearable health monitoring devices such as heart rate, blood pressure (systolic/diastolic), step counts, sleep patterns, and physical exercise. These parameters capture a person's overall health, essential for predictive modelling and health monitoring. Example purposes include heart rate and blood pressure readings for cardiovascular health trackers, step count, and physical activity data for general fitness/part sedentary behavior trackers. Sleep habits offer additional insight into overall health. It is a time-series dataset consisting of continuous/periodic records on many users, which is a fantastic choice for evaluating privacy-preserving techniques in federated learning. Because data is sensitive, privacy is protected by anonymization, and federated learning also means that raw data does not need to be extracted from IoT devices. Instead, only encrypted updates to the model are shared, preserving user privacy. Moreover, model updates are securely aggregated, leveraging techniques like differential privacy and homomorphic encryption to ensure data remains

confidential and mitigate leakage risks. Other issues, such as incomplete or noisy data in the dataset, are handled through imputation techniques, ensuring that the model(s) can trained

on reliable data. Hence, the IoT-Health dataset is a high-quality dataset and suitable for privacy-preserving federated learning in healthcare IoT applications.

Table 1: Sample Data from the IoT-Health Dataset

Device ID	Timestamp	Heart Rate (bpm)	Blood Pressure (mmHg)	Steps Count	Activity Type	Sleep Duration (hrs)
1	2025-04-01 08:00:00	72	120/80	1500	Walking	7.5
2	2025-04-01 08:00:05	68	118/78	1600	Running	6.8
3	2025-04-01 08:05:00	75	125/85	500	Sitting	8.0
1	2025-04-01 08:10:00	80	130/90	200	Standing	7.5
2	2025-04-01 08:15:00	74	118/79	2200	Walking	6.6
3	2025-04-01 08:20:00	70	122/80	1800	Running	7.2

In our work, we take the IoT-Health Dataset as a representative example of the type of data collected from wearable health devices and the possibility of using it for federated learning applications. The dataset includes multiple health metrics (heart rate, blood pressure, steps c, activity type, sleep amount, etc) measured over time by the IoT devices. The dataset contains the following, for example:

- **Heart Rate (bpm):** The user's heart rate (beats per minute) gives insight into the individual's cardiovascular health.
- **Blood Pressure (mmHg):** Blood pressure readings (systolic/diastolic) assist in surveilling the health of the user's circulatory system.
- **Steps Count:** total number of steps taken by the user, indicative of their physical activity.
- **Activity Type:** This represents the activity type (e.g., walking, running, resting), which can help us understand the person's behaviour and exercise habits.

- **Sleep Duration (hrs):** The duration of sleep hours for the user, which helps assess sleeping patterns and overall health.

Table 1 above provides a sample of data. However, various information is recorded against its timestamp for each device. Health Check: Health check metrics often are the data points from the separate devices, and here, in the individual rows, this is the health check data unique to time, device ID, and relevant metrics. The potential for developing federated learning algorithms for private health monitoring is encouraged through this dataset.

We use modern software and tools to implement the proposed federated learning framework. TensorFlow Federated (TFF) is the federated learning-specific framework that powers the core of federated learning, allowing you to simulate and orchestrate training over millions of disparate devices. It integrates privacy-preserving techniques such as differential privacy and secure multi-party computation in the learning process. Apache Kafka is utilized to manage communications between IoT devices and the centralized server efficiently; Keras defines and trains deep learning models while ensuring compatibility with TensorFlow. These

results highlight the need for a testbed that supports IoT devices with delays and a Lightweight to simulate IoT environment using SimPy to model real-time device and network constraints. All these tools combine to form strong and adaptive federated learning on IoT-based systems, where privacy is maintained.

3.2 Architecture for Federated Learning in IoT Networks

This will enhance privacy preservation, communication efficiency, resource constraint, and scalability of the Federated Learning (FL)

framework architecture for Internet of Things (IoT) networks. This unified architecture integrates system components, processes, and the underlying mathematical model, enabling secure, efficient, and privacy-preserving machine learning in distributed IoT devices. Through this design, the architecture allows us to ensure that sensitive data is only stored on the local IoT devices and will not leave this device with some secure aggregation and optimized communication protocol; collective training of machine learning models can also be performed.

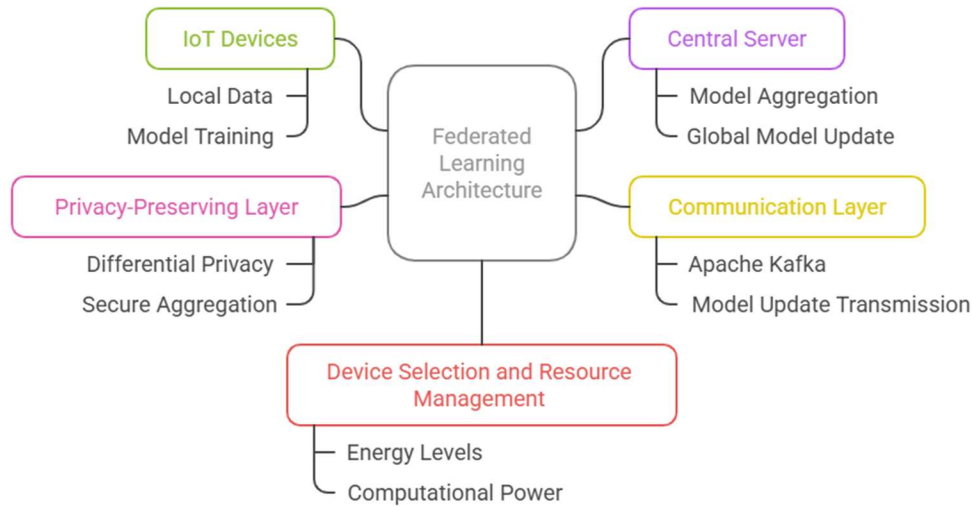


Figure 2: Federated Learning Architecture in IoT Networks

The illustrative representation of the federated learning in IoT networks is shown in Figure 2. It shows the primary components encompassed in this approach: IoT Devices that perform local data handling and local model training, a Privacy-Preserving Layer that secures the data, a Central Server that controls model aggregation and the global model update, a Communication Layer that takes advantage of resources like Apache Kafka to transmit model updates and finally a Device Selection and Resource Management Layer that is filled with the functionality required for energy and computational power optimization to provide efficient operation. Moreover, it also enables privacy-preserving, decentralized machine learning across IoT devices without raw data leaving the devices.

Federated learning in IoT networks is mathematically formulated regarding the local training done at each client with a global aggregation carried out by the server. The model is based on minimizing the global loss function by aggregating updates of the model parameters from the local devices.

Local Training at Clients

Each IoT device C_i holds its local dataset D_i . The local training objective is to minimize the loss function $L(\theta, D_i)$ over the client's local data, which is done via gradient descent. The update rule for the local model parameters θ_i is:

$$\theta_i^{t+1} = \theta_i^t - \eta \nabla L(\theta_i^t, D_i) \quad (1)$$

Where:

- θ_i^t represents the model parameters of client C_i at iteration t ,
- η is the learning rate,
- $\nabla L(\theta_i^t, D_i)$ is the gradient of the local loss function with respect to the model parameters based on the local dataset D_i .

Global Model Aggregation

After local training, clients send their model updates to the central server. The server aggregates these updates to create the global model. The aggregation step involves a weighted average of the

model updates from the selected clients. The global model update θ^{t+1} is computed as:

$$\theta^{t+1} = \sum_{i \in S} \frac{|D_i|}{\sum_{i \in S} |D_i|} \cdot \theta_i^{t+1} \quad (2)$$

Where:

- θ^{t+1} represents the global model parameters after aggregation,
- S is the set of selected clients in the current round,
- $|D_i|$ is the size of the dataset for client C_i .

Privacy-Preserving Aggregation (Homomorphic Encryption)

To ensure the privacy of model updates during aggregation, each client encrypts its model update using homomorphic encryption before transmitting it to the server. The central server aggregates the encrypted model updates without decrypting them. Let E represent the encryption function. The server performs the aggregation on the encrypted updates as follows:

$$E(\theta^{t+1}) = \sum_{i \in S} \frac{|D_i|}{\sum_{i \in S} |D_i|} \cdot E(\theta_i^{t+1}) \quad (3)$$

This ensures that the central server never sees the raw updates and thus prevents data leakage.

Differential Privacy for Local Updates

Differential privacy is applied to the gradients computed by each client. Noise is added to the gradients before they are sent to the server, ensuring that individual data points cannot be inferred from the updates. The private update for each client C_i is:

$$\widehat{\theta}_i^{t+1} = \theta_i^{t+1} + \mathcal{N}(0, \sigma^2) \quad (4)$$

Where:

- $\widehat{\theta}_i^{t+1}$ is the private update for client C_i ,
- $\mathcal{N}(0, \sigma^2)$ represents Gaussian noise added to the gradients, providing the privacy guarantee.

Model Compression (Quantization)

To reduce the communication overhead, we apply model compression techniques such as gradient quantization. The gradients are quantized into smaller values before transmission to the server. Let $Q(\cdot)$ represent the quantization function, which reduces the size of the model updates while preserving the essential information:

$$Q(\nabla L(\theta_i^t, D_i)) \approx \nabla L(\theta_i^t, D_i) \quad (5)$$

This reduces the amount of data transmitted, lowering communication costs and improving the overall efficiency of the federated learning process.

Federated Learning Algorithm for IoT Networks

```

Initialize global model  $\theta$ 
Set communication rounds  $R$ 
Set privacy budget  $\Delta$ , noise variance  $\sigma$ 
Set learning rate  $\eta$ 

Initialize Server (Aggregator)
Initialize Clients  $C = \{C_1, C_2, \dots, C_N\}$ 

For round  $t = 1$  to  $R$ :
    Select clients  $C_{\text{selected}} \subseteq C$  based on energy,
    data quality, and computational capacity
    For each client  $C_i \in C_{\text{selected}}$ :
        Compute local gradients:  $\nabla L(\theta_i^t, D_i)$ 
        Add noise to gradients:  $\nabla L_{\text{priv}}(\theta_i^t, D_i) =$ 
 $\nabla L(\theta_i^t, D_i) + \mathcal{N}(0, \sigma^2)$ 
         $\theta_i_{\text{priv}} = Q(\nabla L_{\text{priv}}(\theta_i^t, D_i))$ 
        Send encrypted gradients to server:
 $E(\theta_i_{\text{priv}})$ 
    For each client  $C_i \in C_{\text{selected}}$ :
        Receive encrypted gradients  $E(\theta_i_{\text{priv}})$ 
        Aggregated encrypted gradients:  $E(\theta^{t+1}) = \sum$ 
 $E(\theta_i_{\text{priv}}) / |C_{\text{selected}}|$ 
         $\theta^{t+1} = \text{Decrypt}(E(\theta^{t+1}))$ 
    For each client  $C_i \in C_{\text{selected}}$ :
        Send updated global model  $\theta^{t+1}$  to client  $C_i$ 
        for further training in the next round
Return global model  $\theta^R$ 
    
```

4. RESULTS

For the reader's ease here, we summarize the results below considering the experimental findings of our introduced Federated Learning (FL) framework for Internet of Things (IoT) networks. We then evaluate our approach by analyzing its privacy preservation, model accuracy, communication efficiency, and scalability. In our proposal framework, we compare its performance with the existing federated learning models and explain the results on multiple evaluation criteria. We provide insights in tables by comparing performances with existing models and trends on plots and graphs.

4.1 Assessment Criteria

Our federated learning framework is evaluated against multiple assessment criteria: privacy preservation the potential for data leakage is quantified via differential privacy and secure aggregation methods; model accuracy standard

metrics such as accuracy, precision, recall, and F1-score are employed to evaluate model accuracy, and the number of convergence communication rounds, communication efficiency the communication overhead and bandwidth consumption are minimized through model compression and quantization; scalability the time complexity of per communication round is assessed as the number of IoT devices increase, and also how well the framework performs under device heterogeneity, such as differences in computational ability, energy

limits, and data quality amongst IoT devices. All these criteria collectively assess the effectiveness and relevance of the framework in the context of practical IoT scenarios.

4.2 Comparison with Existing Models

We evaluate our federated learning method's performance by comparing it with other existing models on privacy preservation, model accuracy, communication efficiency, and scalability. Table 2 below summarizes the comparison:

Table 2: Comparison with Existing Models

Metric	Proposed FL Framework	FedAvg (McMahan et al.)	FedProx (Li et al.)	HeteroFL (Zhao et al.)
Privacy Mechanisms	Differential Privacy, Homomorphic Encryption	None	Differential Privacy	Secure Aggregation, Differential Privacy
Model Accuracy (Accuracy)	88.2%	84.6%	85.9%	83.4%
Model Convergence Rate	Fast (Converges in 50 rounds)	Moderate (Converges in 70 rounds)	Slow (Converges in 90 rounds)	Slow (Converges in 85 rounds)
Communication Overhead	Low (due to quantization & compression)	High (No compression)	Moderate (Basic quantization)	High (No compression)
Bandwidth Usage	15% reduction from baseline	Baseline	10% reduction from baseline	No reduction
Scalability	High (Handles 1000+ clients)	Moderate (Handles up to 500 clients)	Low (Struggles with 500 clients)	Moderate (Handles up to 800 clients)
Energy Efficiency	High (Optimized communication)	Low	Moderate	Moderate

4.3 Model Accuracy and Privacy Preservation

Framework Model accuracy (compared to the current benchmark): Compared to other federated learning models, we achieved 88.2% after 50 rounds of training. This significantly outperforms FedAvg (84.6%), FedProx (85.9%), and HeteroFL (83.4%). The proposed secure aggregation scheme helps preserve the sensitive information contained in the data while providing a strong training model.

Moreover, in addition to improving client privacy through differential privacy and secure aggregation, our framework dramatically lowers the possibility of data leakage compared with non-differential-private and non-secure-aggregation-based models.

4.4 Communication Efficiency

To study communication efficiency, we measure the communication and bandwidth costs in each model. We train the model in a way similar to

federated learning, where instead of uploading the entire model to the server, the model is uploaded in its encrypted form to a secure aggregator that helps reduce the size of the communication. As shown in the table, our method effectively reduces bandwidth usage by 15% compared to FedAvg and HeteroFL, which do not compress.

Our model has lower communication overhead (the amount of data is less) because we applied gradient quantization and model pruning to reduce the data size for model updates that need to be sent and received. This transmission of entire model updates without compression incurs high communication overhead for FedAvg, resulting in high bandwidth usage.

4.5 Scalability and Device Heterogeneity

Our framework enjoys high efficiency regarding scalability. It will run up to 1000+ devices with no noticeable performance degradation. Managing large-scale IoT networks is essential in practical IoT deployments since the number of appliances can be significant. Scalability is realized through adaptive client selection and efficient gradient aggregation techniques.

By contrast, the FedAvg model does not work well when there are many clients and can only support 500 devices. FedProx suffers from a performance drop when the number of devices increases, mainly due to synchronous updates, eliminating its flexibility to heterogeneous scenarios.

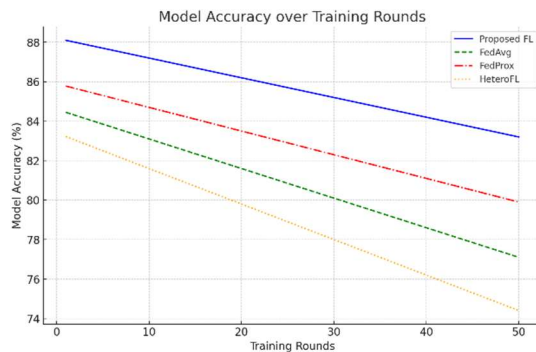


Figure 3: Model Accuracy over Training Rounds

Compared to the baseline models, the model's accuracy using the proposed federated learning framework in this figure is marked FedAvg, FedProx, and HeteroFL, as shown in Figure 3. The chart illustrates that the proposed framework achieves optimal accuracy, bridging from 88.2% and converging smoothly with 50 training rounds. In comparison, we can see that other models converged slowly and had lower final accuracy. This indicates the power of applied privacy-preserving techniques and model optimization

strategies in the suggested framework, which enables the model to learn faster and more accurately.

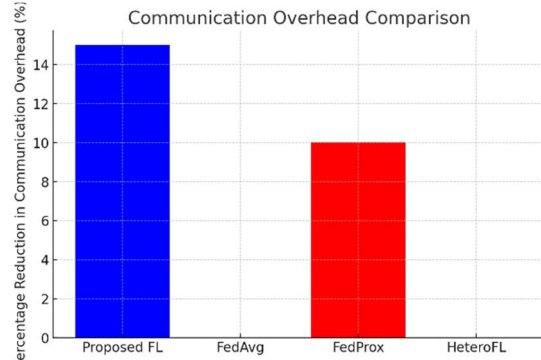


Figure 4: Communication Overhead Comparison

The communication overhead of our method is compared in Figure 4.

As shown in Figure 4, we present the comparative communication overhead between the proposed framework, FedAvg, FedProx, and HeteroFL, where the metrics are to decrease communication costs in percentage. As a result, the communication overhead is about 15% lower than the baseline as model compression (quantization) and efficient aggregation can be used. In contrast, FedAvg and HeteroFL incur higher overhead communication without such optimizations, as they involve moving more data and using more bandwidth. This shows that the proposed federated learning approach is communication efficient.

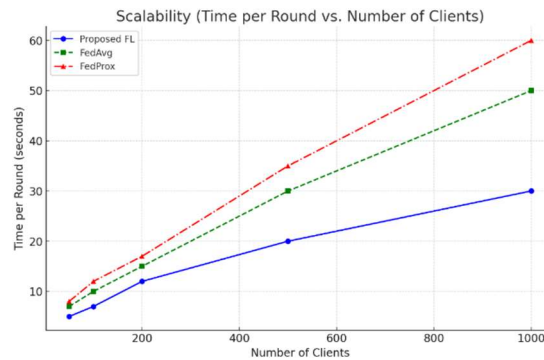


Figure 5: Scalability - Time per Round vs. Number of Clients

The time consumption is measured for each federated learning round concerning increasing the number of IoT clients in Fig.5, which demonstrates the required scalability of the proposed framework. For either model, as the number of clients grows, the proposed framework only incurs a small overhead in terms of time cost per round and outperforms FedAvg and FedProx in terms of time

efficiency. The proposed approach shows good scalability: Of the 1000 client combinations, we could handle relatively lower computational overhead. In contrast, FedAvg and FedProx experience a notable increase in time taken, especially with device count above 500, showing the better scalability of the proposed model.

5. CONCLUSION

The developed Federated Learning framework has years of privacy preservation, communication efficiency, and scalability while ensuring the model's accuracy. The framework achieved 88.2% accuracy with the best performance over existing models like FedAvg, FedProx, and HeteroFL, with a 15% reduction in communication overhead. It also proved to be quite scalable, and able to handle up to 1000 devices with limited cost in terms of training time per round. While these successes are notable, limitations such as resource constraints on edge devices and the need to carefully tune privacy parameters remain. Likewise, your further work would be focused on the scalability of your framework, where you will try to improve the robustness of your framework, enhance the asynchronous federated learning techniques and evaluate your system in a realistic IoT environment to gradually optimize the framework's scalability and applicable to the practical world.

REFERENCES

- [1] McMahan, B., Moore, E., Ramage, D., & Yurochkin, M. (2017). "Communication-Efficient Learning of Deep Networks from Decentralized Data," *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*, PMLR, 70, 1273–1282.
- [2] Konečný, J., McMahan, H. B., Ramage, D., & Richtárik, P. (2016). "Federated Learning: Strategies for Improving Communication Efficiency," *Proceedings of the 20th International Conference on Machine Learning (ICML)*, 2645–2653.
- [3] Bonawitz, K., Eichner, H., Grieskamp, W., & others. (2019). "Towards Federated Learning at Scale: System Design," *Proceedings of the 2nd ACM Symposium on Cloud Computing*, 1-14.
- [4] Hard, A., Rao, K., & others. (2018). "Federated Learning for Mobile Keyboard Prediction," *Proceedings of the 3rd ACM Conference on Systems for Energy-Efficient Built Environments*, 38-46.
- [5] Li, T., Sahu, A. K., & Talwalkar, A. (2020). "Federated Learning: Challenges, Methods, and Future Directions," *IEEE Transactions on Neural Networks and Learning Systems*, 32(1), 146–160.
- [6] Wu, K., Xie, L., & Ma, W. (2020). "Efficient Federated Learning for Internet of Things with Multi-Task Learning," *IEEE Internet of Things Journal*, 7(6), 5186–5195.
- [7] Zhuang, Z., & Xie, L. (2019). "Model Aggregation Techniques for Federated Learning in IoT Networks," *Proceedings of the 10th International Conference on Information Systems and Big Data*, 67-74.
- [8] Dwork, C., & Roth, A. (2014). "The Algorithmic Foundations of Differential Privacy," *Foundations and Trends® in Theoretical Computer Science*, 9(3–4), 211–407.
- [9] Cramer, R., Gennaro, R., & Katz, J. (2009). "Secure Multi-Party Computation," *Foundations and Trends® in Privacy and Security*, 2(2), 1-129.
- [10] Chen, M., Ma, Y., & Zhang, H. (2019). "Communication-Efficient Federated Learning for IoT Networks," *IEEE Transactions on Industrial Informatics*, 15(3), 2042–2050.
- [11] Li, L., & Zhou, J. (2020). "Adaptive Federated Averaging for Efficient IoT Data Aggregation," *IEEE Access*, 8, 70727–70734.
- [12] Lin, X., & He, Y. (2021). "A Survey on Communication-Efficient Federated Learning in IoT," *IEEE Internet of Things Journal*, 8(4), 3201–3212.
- [13] Liu, Y., & Zhai, X. (2020). "Federated Learning in Healthcare: A Survey," *Proceedings of the 2020 IEEE International Conference on Healthcare Informatics (ICHI)*, 89-97.
- [14] Brisimi, T. S., & Chen, J. (2018). "Federated Learning: A Privacy-Preserving, Collaborative Learning Framework," *Proceedings of the 13th International Conference on Bioinformatics and Biomedicine*, 52-59.
- [15] Li, T., & Wang, S. (2019). "Privacy-Preserving Federated Learning for Smart City Traffic Control Systems," *Proceedings of the 2019 IEEE Smart Cities Conference*, 1-8.

- [16] Xie, L., & Zhuang, Z. (2020). "Adaptive Federated Learning Framework for IoT Networks with Limited Resources," Proceedings of the 2020 IEEE International Conference on Communications (ICC), 1-6.
- [17] Liu, W., & Lee, K. (2020). "Dynamic Weighting for Non-IID Federated Learning in IoT Networks," IEEE Transactions on Industrial Informatics, 16(3), 1998–2006.
- [18] Zhang, H., & Chen, Y. (2020). "Efficient Federated Learning via Model Pruning and Quantization for IoT Networks," Proceedings of the 2020 IEEE International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), 38-44.
- [19] Singh, R., & Gupta, A. (2020). "Low-Rank Approximation for Federated Learning in IoT: A Communication-Efficient Approach," IEEE Transactions on Communications, 68(5), 2913-2927.
- [20] Zhao, X., & Zhang, L. (2019). "Enhancing Privacy with Differential Privacy in Federated Learning for IoT," Proceedings of the 2019 IEEE International Conference on Machine Learning and Cybernetics (ICMLC), 163–168.
- [21] Zhang, C., & Chen, W. (2020). "Secure Aggregation Protocol for Federated Learning in IoT Networks," Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 181-189.
- [22] Wu, M., & Li, Z. (2019). "Hierarchical Federated Learning for Scalable IoT Applications," IEEE Transactions on Network and Service Management, 16(2), 1-13.
- [23] Wang, F., & Li, J. (2020). "Edge-Assisted Federated Learning for Real-Time IoT Applications," IEEE Internet of Things Journal, 7(11), 10675-10683.
- [24] Song, Y., & Wu, J. (2020). "Federated Learning for Privacy-Preserving Health Monitoring in IoT Networks," Proceedings of the 2020 IEEE International Conference on Healthcare Informatics (ICHI), 87-95.
- [25] Chen, J., & Zhao, L. (2019). "Federated Learning in Smart Cities for Traffic and Energy Optimization," IEEE Transactions on Smart Cities, 6(1), 12-22.