Privacy-Enhanced Federated WiFi Sensing for Health Monitoring in the Internet of Things

Zhuotao Lian, Qingkui Zeng, Zhusen Liu, Haoda Wang, Chuan Ma,
Weizhi Meng, Chunhua Su, and Kouichi Sakurai

***Abstract*—The development of the Internet of Things (IoT) has led to the widespread use of WiFi-enabled consumer electronic devices, which are now common in everyday life. These advancements in IoT have greatly improved data collection and analysis capabilities, especially for health monitoring applications. However, traditional centralized machine learning methods often fall short, raising significant privacy concerns and requiring extensive data collection, which is inefficient. To address these limitations within the distributed IoT environment, this paper presents a federated learning-based WiFi sensing system specifically designed for health monitoring. By enabling local model training, our system prevents the sharing of sensitive data, thus reducing the risk of privacy breaches. We further enhance our system with a secret sharing mechanism coupled with model sparsification to significantly improve privacy. Additionally, our improved Top-k model sparsification algorithm, equipped with adaptive residuals, reduces communication overhead while ensuring high accuracy. Extensive testing across various datasets and models confirms that our system outperforms existing benchmarks in terms of privacy protection and communication efficiency, marking a substantial advancement in health monitoring within the IoT.**

***Index Terms*—WiFi sensing, consumer internet of things, health monitoring, federated learning, secret sharing, model sparsification**

I. INTRODUCTION

The Internet of Things (IoT) has revolutionized the way we interact with the world around us. The Consumer Internet of Things (CIoT) represents a significant evolution of IoT, specifically focusing on the integration of smart consumer devices into everyday life. With the rapid growth of CIoT devices and increased demand for Internet access, WiFi technology has become ubiquitous [1]. It has enabled the connection of consumer electronic devices, to the internet, leading to the development of many intelligent systems, including device-free sensing.

WiFi sensing refers to the process of capturing and analyzing the signals emitted by WiFi networks in the vicinity, with the objective of comprehending the underlying physical attributes of a specific setting. The utilization of WiFi sensing has witnessed a surge in novel applications due to its ability to enable cost-effective monitoring (by leveraging existing WiFi infrastructure), as well as device-free and nonintrusive detection of human presence and physical movements [2]–[4]. This starkly contrasts with traditional sensor-based systems that necessitate dedicated devices to be physically attached to the human body. These systems utilize WiFi channel state information (CSI) to detect and analyze human presence and activities, thus enabling real-time health assessments without direct physical contact. The precise sensing of environmental dynamics through CSI is crucial for monitoring patient movements and vital signs across various healthcare settings.

Despite their advantages, the deployment of WiFi sensing for health monitoring introduces significant privacy concerns. The sensitivity of WiFi-sensed data, inherently containing personal and behavioral patterns, could potentially be exploited by malicious actors to track users' activities and habits [5]. This vulnerability poses significant challenges to traditional AI methods, which typically involve the central collection of data on servers for model training [6], [7]. In response to these privacy risks, we propose a federated learning approach where data is locally gathered and used for machine learning training within environments such as individual patient rooms, hospital treatment areas, or broader medical center facilities. This approach aligns with federated learning principles, allowing local training of models without requiring data transmission to a centralized server. By implementing local training, we enhance both individual and communal healthcare data privacy, ensuring robust protection against unauthorized access while effectively supporting health monitoring systems.

While applying federated learning to health monitoring enhances local data privacy, it still faces common privacy threats inherent in federated learning, such as model inference attacks and model inversion attacks [8]–[10]. These attacks, by analyzing model outputs or intermediate states, can potentially expose sensitive data. To counter these threats and enhance the robustness of our system, we have integrated advanced privacy-preserving technologies. By combining secret sharing and an optimized model sparsification strategy, our approach not only protects model privacy during the federated learning process but also significantly reduces communication costs associated with model transmission. These enhancements ensure that our federated WiFi sensing-based health monitoring sys-

Zhuotao Lian and Kouichi Sakurai are with the Graduate School of Information Science and Electrical Engineering, Kyushu University, Fukuoka, Japan.

Qingkui Zeng is with the School of Electronics and Information Engineering, Nanjing University of Information Science & Technology, Nanjing, China.

Zhusen Liu is with Research Center for Data Hub and Security, Zhejiang Lab, Hangzhou, China

Chuan Ma is with the School of Computer Science, Chongqing University, China. He is also with Key Laboratory of Computer Network and Information Integration (Southeast University), Ministry of Education.

Haoda Wang and Chunhua Su are with the Department of Computer Science and Engineering, the University of Aizu, Aizuwakamatsu, Japan.

Weizhi Meng is with the Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Denmark. (e-mail: weme@dtu.dk)

tem delivers strong performance while meeting high standards of privacy and efficiency.

Aiming to address these concerns, we have developed a novel federated WiFi sensing system for health monitoring that enhances both privacy and communication efficiency. We have integrated a secret sharing mechanism to safeguard the privacy and security of models within the federated learning process. This mechanism securely aggregates model parameters, allowing updates from multiple devices to be combined while preserving the confidentiality of each individual update. This effectively shields sensitive information and guards against threats such as model inference attacks. Furthermore, we have developed a model sparsification method with adaptive residuals to minimize the system's communication overhead. This method selectively transmits only essential data during the federated learning cycles, significantly reducing the volume of data exchanged while maintaining high model accuracy and system efficiency. The contributions of our work can be summarized as follows:

- We have designed a federated WiFi sensing system specifically tailored for health monitoring. This system utilizes federated learning to collaboratively train a global model, keeping sensitive health data localized and enhancing patient privacy.
- To further enhance model privacy, our system integrates a secret sharing mechanism that securely aggregates model parameters during the federated learning process. This approach safeguards against the potential exposure of sensitive health data that could result from attacks on the model updates.
- We have refined a residual-based model sparsification algorithm to lessen the communication overhead during the secret-sharing stages of federated learning. This enhancement not only sustains high model performance but also makes the federated learning process more efficient.
- Comprehensive experiments conducted across multiple sensing datasets and models validate the effectiveness of our system. The results confirm superior performance in terms of privacy protection, communication efficiency, and model utility in AI-based health monitoring contexts.

The paper structure is as follows: Section II introduces AI-based health monitoring and federated learning. Section III presents the system design, including the workflow and implementation strategies for model sparsification and secret sharing. Section IV conducts simulation experiments to evaluate the system's effectiveness, sparsification methods' performance, and communication overhead variations. Section V provides a comparison with related studies. Finally, section VI summarizes the paper.

II. Preliminaries

A. WiFi Sensing in the Consumer Internet of Things

With continued improvements in accuracy, range, and application diversity, WiFi sensing has become more prevalent in Internet of Things [11]. In the Consumer Internet of Things (CIoT), WiFi sensing leverages WiFi signals to detect and interpret environmental changes, enabling applications that enhance convenience and efficiency in smart homes and other consumer settings. Emerging applications include detailed health monitoring, advanced home automation, and enhanced user interaction experiences. Commercial interest in WiFi sensing has grown, with companies integrating these capabilities into consumer products, particularly for health monitoring [12]. Devices equipped with WiFi sensing capabilities transmit and receive signals that are reflected, absorbed, or scattered by objects and people in the environment. These signals are then analyzed to detect falls [13], monitor respiratory rates, and track daily activities for elderly care [14]. The COVID-19 pandemic further accelerated interest in non-contact sensing technologies [15], with WiFi sensing gaining attention for remote health monitoring applications .

B. Efficient and Secure Federated Learning

Unlike cameras or microphones, WiFi sensing does not capture visual or audio raw data, thereby reducing potential privacy compromises. However, it inherently involves collecting personal and behavioral pattern data, which can be highly sensitive. Federated Learning (FL) is a distributed machine learning technique that allows multiple parties to collaboratively train a model while maintaining data privacy [16]. In FL, the model is trained on decentralized data sources, and updates are sent to a central server for aggregation to update the global model [17]. FL is especially beneficial when data is stored on personal devices like smartphones, IoT devices, or edge computing nodes. The global objective function of FL can be expressed as follows:

$$arg\min_{\omega}\sum_{i=1}^{C}p_i F_i(\omega_i), \tag{1}$$

In Equation (1), ω represents the global model, C denotes the number of participated clients, $F_i(\omega_t^i)$ corresponds to the local objective function for the i-th client, and p_i specifies the proportion of the i-th client. At the beginning of each communication round, the server transmits the current global model state to these clients. Upon receiving the global model or initial parameters, the clients proceed to iterate their models and compute gradients using their local datasets. When the clients complete the t-th round of training, the local model updates are then uploaded to the server. Afterward, the server aggregated a new global average model from local updates. The update for the $e+1$-th communication round of global model parameters is then computed as:

$$\omega_{e+1} \leftarrow \omega_e - \eta\sum_{i=1}^{m}p_i \nabla F_i(\omega_e^i), \tag{2}$$

In Equation (2), $\nabla F_i(\omega_e^i)$ represents the gradient of the local objective function for the i-th client in the e-th round, and η denotes the learning rate. This communication process is repeated iteratively until the global model reaches the desired state.

In federated learning-based health monitoring, a major challenge is the communication overhead when transmitting model parameters between health devices and medical institutions, especially for large models with many parameters. Sparsification, a technique from deep learning, addresses this by compressing model transmissions [18]. It involves sending selected indexes and values instead of the entire model, reducing the amount of data transmitted [19]. Two main sparsification schemes are Random-k and Top-k, which randomly choose parameters or select the highest-ranked values, respectively [20]–[23].

Privacy and security are also critical challenges in federated learning. Secret sharing techniques, like Shamir secret sharing [24], enhance privacy and security by dividing local model updates into shares, aggregated by a central server. This method prevents the direct exposure of individual contributions during transmission, ensuring robust client aggregation, even with a few dropouts [25].

III. System Design

A. Threat Model

In the health monitoring data collection and analysis task, the user's monitoring device transmits sensitive medical information to the server. In this process, the monitoring device monitors the user's health information in a trustworthy manner, but there are still threats. For example, malicious adversaries trying to access individual medical data for their profit, unreliable servers trying to infer users' real data, and degradation of service due to corruption in the network or hardware. Therefore, there are three main threats in federated WiFi sensing for health monitoring as follows:

1) **Adversaries:** Stealing local updates from health monitoring devices to capture user private information.
2) **Offline/asynchronous monitoring Devices:** Some health monitoring devices fail to send or receive data due to hardware or network problems, compromising service quality.
3) **Honest but curious parameter server:** Parameter server may infer raw data based on updates from health monitoring devices when performing aggregation operations.

Within our federated WiFi sensing system, the parameter server is presumed to be honest but curious [26], as it follows the federated learning framework for aggregating parameters. However, it exhibits curiosity toward participants' private data and attempts to infer the training data from the received local updates in each round, thereby posing a significant threat to data privacy.

To effectively counter these threats, it is crucial to enforce stringent security measures. We employ the secret sharing method to guarantee encryption support for clients. This cryptographic measure serves the paramount purpose of precluding the server from accessing specific user updates, thereby fortifying the confidentiality of individual user data. Consequently, the server is restricted to accessing only aggregated results, safeguarding the privacy of user-specific information. In tandem with this encryption strategy, we have devised an adaptive sparsification update algorithm tailored to optimize communication efficiency within our system.

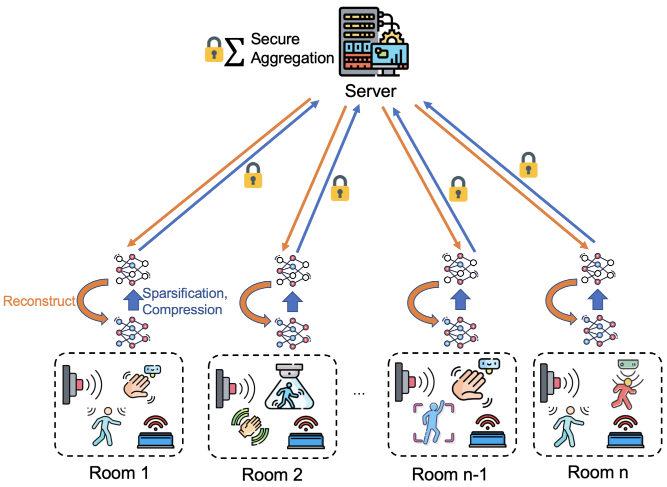


Fig. 1: System Design

B. System Workflow

Our WiFi sensing system consists of a centralized server and multiple health monitoring devices communicating wirelessly. Following the federated learning framework, the server orchestrates global aggregation while the devices conduct local training and send model updates. To improve performance and security, we proposed the Communication-efficient and Privacy-enhanced Federated Learning system. The system's architecture is illustrated in Figure 1. Below, we summarize the key steps in our system's workflow.

1) **Server sending:** The centralized server gets a global model w_e and the mask matrix M, and distributes it to all monitoring devices. Adaptive model sparsification will be performed at every interval of a fixed number of t rounds to obtain a new mask matrix.
2) **Local Training:** Each device performs local training on its dataset using the current global model w_e and generates a local model update w_e^i.
3) **Adaptive Model sparsification:** To reduce the communication overhead, we introduce model sparsification by pruning the local model updates. Specifically, we retain only the Top-k percentage of the absolute values of the model parameters, incorporating adaptive residuals. The hyperparameter k can be fine-tuned to optimize the utilization of the available communication bandwidth.
4) **Secret sharing and aggregation:** To enhance the privacy of the local models, we use secret sharing to split each local model update w_e^i into multiple shares. The shares are then sent to the centralized server for aggregation. The server performs sparse model aggregation on the shares to obtain the global model update w_{e+1}, which is sent back to the devices for the next round of training.
5) **Repeat:** Processes 2-4 are repeated for a fixed number of rounds or until convergence is achieved.

Algorithm 1 Server-side Adaptive Model Sparsification

```
1: Input: Global model $w(e)$ and $w(e-1)$, sparsification number $k$, current epoch $e$, total epochs $T$
2: Output: Mask matrix $M(e)$
3: Global update $\Delta w = w_e - w_{e-1}$
4: Flatten $\Delta w$ into one dimension.
5: Initial residual storage $Res = 0$
6: $Diff$ = $\Delta w$ + $Res$
7: Select matrix inside: index = Top-$k(Diff, k)$
8: Determine mask matrix $M(e)$ by changing the corresponding element value to 1
9: $\Delta w[index] = 0$
10: Set the residuals to the parameter values that are not selected at each layer: $Res$ = $\Delta w$
11: Flatten $Res$ into one dimension
12: return $M(e)$
```

C. Adaptive Model Sparsification

Top-k sparsification is a technique in machine learning and data compression that reduces model size and complexity. Discarding less important parameter values helps reduce communication overhead and computational burden during model aggregation. The retained top-k parameters are sent to the central server for aggregation, improving federated learning efficiency and easing the load on resource-constrained devices. In Top-k sparsification, parameter selection is guided by sorting values based on magnitudes, ensuring the preservation of critical model characteristics. A key advantage is the ability to balance communication overhead reduction with maintaining acceptable accuracy. The value of k can be adjusted to fine-tune the sparsification process for federated learning requirements. Hence, we propose using Top-k sparsification to selectively compress the model by eliminating parameters with minimal impact on convergence.

Utilizing historical residual methods in Top-k sparsification has shown promise in addressing convergence issues [22]. However, in federated learning, storing and accumulating residuals for each round consumes significant storage space, a concern for WiFi sensing systems. Therefore, we developed an innovative sparsification technique incorporating adaptive residual storage. Our approach dynamically adjusts residuals based on factors like model layers and training progression, enhancing flexibility and performance. To further reduce storage space, we avoid storing residuals for each round, considering their relatively large overhead. Our method overcomes the limitations of cumulative historical residuals, providing a rational approach to leveraging update differences without introducing additional parameters. In subsequent sections, we detail our improved sparsification method.

To ensure consistent mask vectors for model sparsification in secure sparse model aggregation, the server generates the mask vector for each round and transmits it, along with aggregated results, to participants. The algorithm comprises server-side and user-side components.

On the server side (Algorithm 1), the global model change, Δw, is flattened into a one-dimensional matrix. This matrix is then accumulated with the previous round's residual to compute *Diff*. Top-k parameters are selected based on *Diff*, generating the mask matrix $M(e)$. Model parameter values corresponding to Top-k indices are set to zero, forming the residual Res. The server retains Res and transmits $M(e)$ to clients. Clients receive aggregated results and the mask vector, performing local training and multiplying results with the mask vector (Algorithm 2). Each participant undergoes the same sparsification process, enabling additional compression by transmitting only selected element values. This reduces communication costs. Updating residual storage in each round enhances mask vector generation efficiency, eliminating the need for accumulated residuals. Adaptive residual updates on a round-by-round basis optimize overall efficiency.

Algorithm 2 Client-side Adaptive Model Sparsification

```
1: Input: Mask matrix $M(e)$, local model $w_i$
2: Output: Sparsified model $\hat{w}_i$
3: $M_i = M(e)$
4: $\hat{w}_i = M_i \circ w_i$
5: return $\hat{w}_i$
```

D. Secret Sharing and Aggregation

In AI-based health monitoring scenarios, bandwidth limitations pose challenges for federated learning, exacerbating communication consumption. Our proposed approach involves determining a sparsified mask matrix on the server side before secret sharing gradient updates corresponding to specific locations on the client side. This method diverges from conventional practices by sharing gradient updates individually, enhancing security and efficiency in WiFi-aware environments. The steps for secret sharing in our method are as follows.

Step 1: The server obtains the mask matrix of the pre-trained model by adaptive model sparsification and sends the pre-trained model and the mask matrix to all clients. Meanwhile, the server sends secret sharing parameters to the client such as the Shamir threshold t and the large modulus p.

Step 2: Each client generates Shamir polynomials to send to the server.

Step 3: The server collects at least t shares from each client and uses these shares to perform polynomial interpolation to reconstruct the model updates.

Step 4: The server aggregates these updates to obtain a new global model and sends it to the clients. After interval of a fixed number of rounds, a new mask matrix is generated using Top-k based adaptive model sparsification, and then the global model and the new mask matrix are sent to the clients.

Step 5: Repeat the above steps until the federated learning training reaches the specified number of rounds.

To mitigate client dropouts in federated learning, the server employs a protocol where all clients contribute parts of their local model updates as secret shares. This utilizes a modified Shamir's Secret Sharing scheme, tailored for federated learning, where the 'secret' corresponds to each client's sparse model update $\hat{w}_i(e)$. The scheme ensures the server can reconstruct the global model update with at least t out of

Algorithm 3 secret sharing and aggregation

```
Input: Communication rounds $E$
Output: $e+1$ round encrypted global model $w_{e+1}$
Server obtains mask matrix $M$ using adaptive model sparsification.
for each clients $i$ in $N$ do
    Compute current round model sparsification $\hat{w}_i(e)$.
    Generate a random polynomial $f_i(x_i)$.
    Each share $(x_i, f_i(x_i))$ is distributed to a different client, and clients receive their respective shares.
end for
Wait to receive all clients' shares.
The server uses polynomial interpolation with the collected shares from at least $t$ clients to reconstruct the aggregated model update $w(e+1)$.
return $w(e+1)$.
```

n shares without accessing individual updates. Algorithm 3 adapts Shamir's algorithm to distribute model masks as secret shares, where the secret s corresponds to $\hat{w}_i(e)$ for each client i, and the shares are defined accordingly.

1) The server generates a random polynomial of degree $t-1$ for each client i, where t is the threshold number of clients needed to reconstruct the global model update. The polynomial for client i's update is defined as:

$$f_i(x) = \hat{w}_i(e) + a_{i1}x + a_{i2}x^2 + \ldots + a_{i(t-1)}x^{t-1}, \quad (3)$$

where $a_{i1}, a_{i2}, \ldots, a_{i(t-1)}$ are coefficients randomly chosen from a finite field $\mathbb{Z}_p$, ensuring the sparsity of the polynomial in alignment with the sparsification of the model update.

2) Each client i computes its share of the sparsified update by evaluating the polynomial at a distinct point x_i, which is unique to each client and securely communicated to them. The share for client i is given by:

$$s_i = f_i(x_i), \quad (4)$$

where s_i represents the portion of the model mask that client i will contribute to the server.

3) To reconstruct the sparsified global model update, the server requires at least t clients to submit their shares. If clients $i_1, i_2, \ldots, i_t$ represent the subset of clients that remain, their shares are used in the reconstruction.

4) The server collects the shares $s_{i_1}, s_{i_2}, \ldots, s_{i_t}$, which are the sparsified updates from the clients that have not dropped out.

5) The sparsified global model update is reconstructed using Lagrange interpolation, with the reconstruction formula given by:

$$w(e+1) = \sum_{j=1}^{t} s_{i_j} \cdot \left(\prod_{\substack{k=1 \\ k \neq j}}^{t} \frac{x_{i_k}}{x_{i_k} - x_{i_j}} \right) (mod\, p)\,, \quad (5)$$

where $w(e+1)$ is the sparsified update for the next round, reconstructed from the shares of the clients who have contributed.

This adaptation of Shamir's Secret Sharing to federated learning ensures that the server can only reconstruct the sparsified global model update when a sufficient number of clients have participated, thus maintaining the privacy of individual client updates. It also aligns with the federated learning process by incorporating the sparsity directly into the secret sharing scheme, reducing communication overhead and preserving the efficiency of the learning process.

E. Security Analysis

Theorem 1. *Our scheme is robust and tolerates at most $N-t$ clients' dropout or failness.*

Proof. In our FL system, each client updates its local gradients and uses secret sharing technique to distribute these updates to other clients. Then, each client aggregates the shares locally, and sends the aggregated result to the parameter server for reconstruction of the global gradients. In the process of gradient submission and global gradient update, a subset of n clients may fail or drop out and influence the learning process. However, the impact is limited by the inherent properties of Shamir's (t, n) secret sharing scheme. The semi-honest server can reconstruct the global gradient with the aggregate shares from t clients. Therefore, the scheme can tolerate at most $N-t$ clients' dropout or failness and continue to update the correct global gradients. □

Theorem 2. *Our scheme maintains confidentiality and collusion resistance of at most $t-1$ clients and the server.*

Proof. In our FL scheme, every clients use Shamir's (t, n) secret sharing scheme to share their local gradients with other clients. Hence, each client receives a secret share of other clients' local gradients. The secret sharing scheme is information theoretically secure without at least t clients' collusion, so every client can not reveal the true local gradient of other client. Besides, every client aggregates all received shares locally, and then, sends the aggregated result to the server, so the server can not deduce the local share of every client rather than the final global gradients. Employing the (t, n) secret sharing scheme, our scheme maintains the confidentiality of the client's local gradient with resistance aggainst at most $t-1$ collusion of clients and the server. □

TABLE I: Simulation Parameters

Parameter	**Value**
Number of Clients	20
Dataset	UT-HAR, Widar
Model	MLP, LeNet, and RNN
Global Epochs (UT-HAR)	200
Global Epochs (Widar)	100
Local Epochs	3
Number of Selected Clients	10
Batch Size	64
Learning Rate	0.001
Momentum	0.0001

IV. Experiment

A. Experimental Setup

In our experimental setup, we utilized a 13th Gen Intel Core i9-13900K processor coupled with an NVIDIA GeForce RTX 4090 graphics card, which boasts 24 GB of dedicated memory, to handle computational demands efficiently. The experiments were conducted using PyTorch version 1.5.1, supported by CUDA version 10.1 (cu101), and torchvision version 0.4.2 for vision-related tasks, all implemented in Python version 3.6.13. Table I presents the key parameters used in the simulation of our system. "Number of Clients" denotes the total number of participants involved in the training, while "Number of Selected Clients" indicates the subset of clients randomly chosen for each training round.

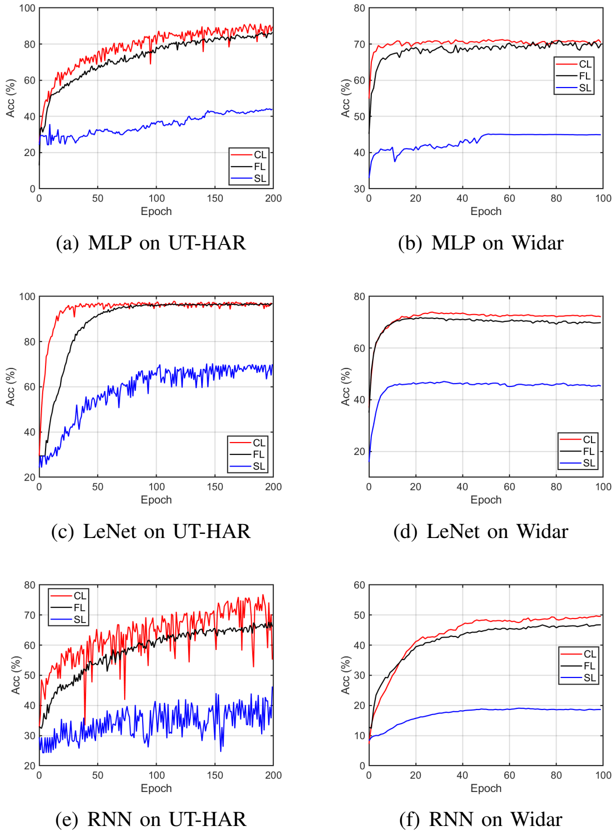
B. Datasets and Models

To validate our sensing-based health monitoring approach, we selected two public CSI datasets, UT-HAR [27] and Widar [28], which are specifically related to human activity and gesture recognition—key components of health monitoring. The UT-HAR dataset, collected using Intel 5300 NIC, captures detailed movements across seven activity categories in a controlled setting, ideal for assessing basic human motions relevant to health applications. The Widar dataset, with its extensive collection of 43,000 samples across 22 gesture categories in diverse environments, provides a broad basis for understanding complex patient behaviors. We employed standardized preprocessing methods to both datasets to ensure consistency and relevance to our study's objectives.

To evaluate the reliability of our system, we selected three representative models from the latest WiFi sensing benchmark: MLP, LeNet, and RNN, as detailed in the work by [29]. The MLP model features three fully connected layers with activation functions designed to capture complex nonlinear relationships within the data. The LeNet model consists of three convolutional layers followed by activation functions and max-pooling layers, which enable it to learn hierarchical features and extract meaningful representations from the input. Meanwhile, the RNN model employs a one-layer structure with a hidden dimension of 64, ideal for capturing temporal dependencies and sequential patterns in the data, concluding with a fully-connected layer for classification. For further details on the datasets and model architectures used in our study, please refer to the open-source code repository available at *https://github.com/xyanchen/WiFi-CSI-Sensing-Benchmark*.

C. Comparison with centralized learning and single-device learning

In this subsection, we evaluate our federated sensing system for health monitoring, incorporating sparse updates and secret sharing. The sparsification parameter k is set at 0.1 to select only 10% of the parameters for global aggregation. Our setup involved 20 participants, with 10 chosen randomly for each training round. "Epoch" refers to global model updates, and "Acc" measures model precision. For centralized training (CL), we used a centralized dataset; for single-device training (SL), each participant had 5% of the global dataset, aligning with our federated scenario. Results depicted in Figure 2 demonstrates the contrasts in performance.



(a) MLP on UT-HAR (b) MLP on Widar
(c) LeNet on UT-HAR (d) LeNet on Widar
(e) RNN on UT-HAR (f) RNN on Widar

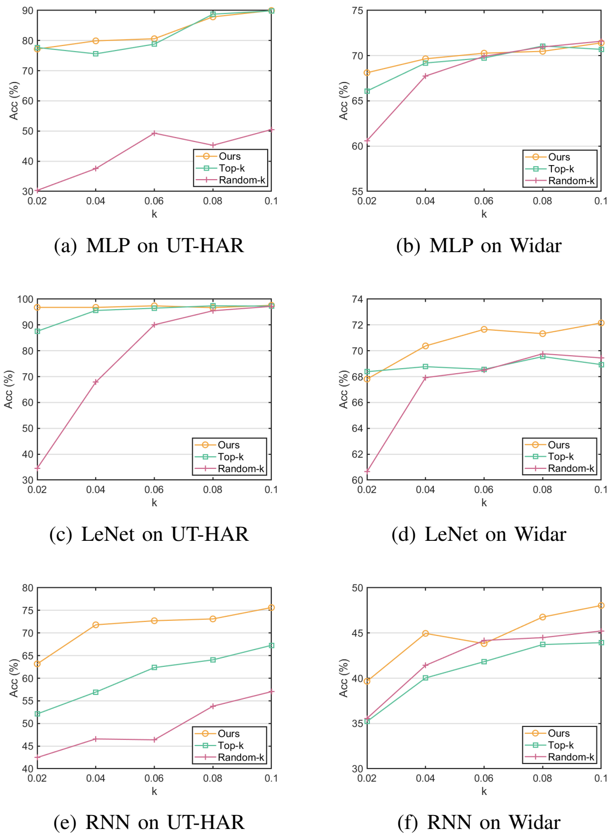
Fig. 2: Accuracy vs. Epoch across CL, FL, and SL.

Our federated sensing system not only safeguarded data privacy but also demonstrated competitive accuracy and efficiency compared to CL. As shown in Subfigures 2(b) and 2(c), while the convergence speed of FL was slightly slower than CL, it ultimately achieved comparable accuracy levels. In other subfigures, the performance gap was also minimal. SL consistently showed the lowest effectiveness. For example, FL achieved approximately 1.9 times and 1.4 times higher accuracy than SL on the MLP and LeNet models, respectively, as observed in Subfigures 2(a) and 2(c).

D. Comparison of Sparsification Methods

In this analysis, we evaluated three sparsification methods: Random-k, Top-k, and our method with residual optimization, referred to as "Ours" in Figure 3. These methods transmit a selected fraction k of a model's parameters, setting the rest to zero. Our approach modifies Top-k by incorporating adaptive residuals to improve the performance further.

At lower values of k (0.02 to 0.1), "Ours" significantly outperforms the others, especially evident at "k=0.02" where it leads Random-k and Top-k by 48% and 21%, respectively, as shown in Subfigure 3(e). When k increases to 0.08 and 0.1, as seen in Subfigures 3(b) and 3(c), the performance of all three methods becomes comparable. Even in such cases,



(a) MLP on UT-HAR

(b) MLP on Widar

(c) LeNet on UT-HAR

(d) LeNet on Widar

(e) RNN on UT-HAR

(f) RNN on Widar

Fig. 3: Accuracy vs. k across different sparsification methods.

our method remains competitive. Through experiments on the UT-HAR and Widar datasets, we demonstrate the stability and reliability of our sparsification method. Moreover, as k decreases, the performance gains become more prominent.

E. Variations of Communication Overhead with k and n through Secret Sharing

In this subsection, we visualized the communication overhead as a function of the sparsification parameter k and the number of training epochs. Figure 4 illustrates a three-dimensional surface plot where the communication overhead is represented on the z-axis. We focused on examining the theoretical impact of sparsification on communication overhead, disregarding factors such as storage file formats. This assumption is reasonable because in our system, the mask vector is generated by the server and broadcast to users. Therefore, the server can reconstruct the global update without requiring participants to upload element position information (typically a matrix recording the indices of non-zero elements). Moreover, in the secret sharing period, the secret is divided into n shares based on the number of clients, thereby influencing the communication overhead. Consequently, the communication overhead on the client's side exhibits approximate linear changes concerning both the sparsification parameter k and the number of clients n. The depicted plot reveals a discernible trend in which communication overhead increases with higher values of k and an increased number of clients n.

Additionally, in our system, the server transmit the sparsified results of secure aggregation, as illustrated in Figure 1, allowing the client to perform the reconstruction. The specific choice depends on various factors such as client's computational and communication capabilities, among others, which need to be considered holistically. Regardless, our system design provides the feasibility to address these considerations.

V. Related Work

In prior works, [30] utilized CNN and AOA for Human Activity Recognition but faced privacy challenges due to centralized training. Although [31] applied federated learning to WiFi sensing and enhanced accuracy, they lacked comprehensive security measures and communication optimization. Similarly, [32] addressed limited labeled data in wireless human sensing, while [33] focused on privacy in indoor sensing but did not optimize communication. [34] introduced 2DFL with some security measures but neglected communication optimization. Unlike these, our improved model sparsification method can significantly reduce communication overhead by over 90% while maintaining model's high performance. Moreover, our approach enhances privacy by sparsification and secret sharing, highlighting its superiority.

VI. Conlusion

Our study introduces novel Federated WiFi Sensing tailored for health monitoring in the IoT. Leveraging Federated Learning, our system allows model training on client devices without compromising user privacy by sharing raw data with the server. We addressed key challenges, including communication overhead and privacy threats, by designing improved top-k sparsification with adaptive residuals and implementing secret-sharing techniques. Experimental evaluations on two public datasets underscored that our system achieved superior accuracy while notably reducing communication overhead and enhancing privacy compared to state-of-the-art methods. These findings highlight the practical relevance and efficacy of our Federated WiFi Sensing system in the IoT, particularly in safeguarding user privacy.

Acknowledgment

References

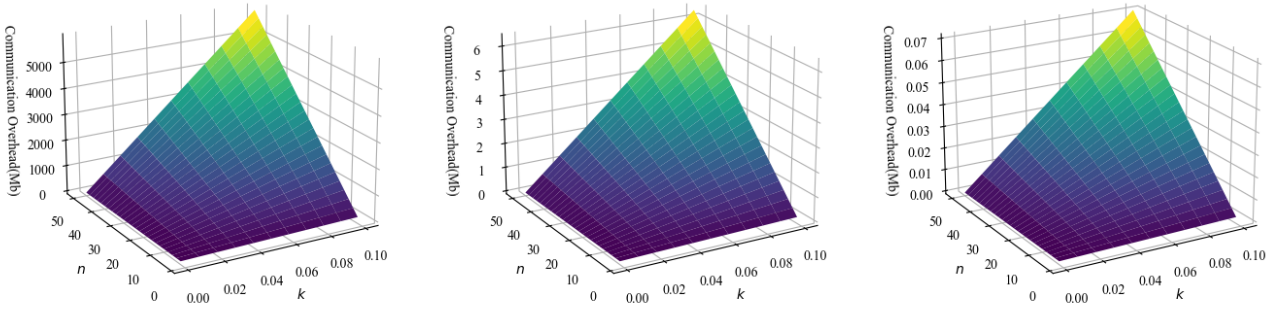
[1] J. Yang, X. Chen, H. Zou, D. Wang, Q. Xu, and L. Xie, "Efficientfi: Toward large-scale lightweight wifi sensing via csi compression," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13 086–13 095, 2022.

[2] B. Fu, N. Damer, F. Kirchbuchner, and A. Kuijper, "Sensing technology for human activity recognition: A comprehensive survey," *IEEE Access*, vol. 8, pp. 83 791–83 820, 2020.

[3] L. Zhao, Q. Yang, H. Huang, L. Guo, and S. Jiang, "Intelligent wireless sensing driven metaverse: A survey," *Computer Communications*, vol. 214, pp. 46–56, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366423004218

[4] L. Zhao, H. Huang, W. Wang, and Z. Zheng, "An accurate approach of device-free localization with attention empowered residual network," *Applied Soft Computing*, vol. 137, p. 110164, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1568494623001825

[5] V.-L. Nguyen, R.-H. Hwang, B.-C. Cheng, Y.-D. Lin, and T. Q. Duong, "Understanding privacy risks of high-accuracy radio positioning and sensing in wireless networks," *IEEE Communications Magazine*, pp. 1–7, 2023.



(a) MLP

(b) LeNet

(c) RNN

Fig. 4: Communication Overhead vs. n and k.

[6] H. Huang, T. Huang, W. Wang, L. Zhao, H. Wang, and H. Wu, "Federated learning and convex hull enhancement for privacy preserving wifi-based device-free localization," *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2023.

[7] N. Zhu, M. Xu, D. Zhuang, and Y. Han, "Wisa: Privacy-enhanced wifi-based activity intensity recognition in smart buildings using personalized federated learning," *Energy and Buildings*, p. 114176, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378778824002925

[8] "A robust analysis of adversarial attacks on federated learning environments," *Computer Standards & Interfaces*, vol. 86, p. 103723, 2023.

[9] A. Hatamizadeh, H. Yin, P. Molchanov, A. Myronenko, W. Li, P. Dogra, A. Feng, M. G. Flores, J. Kautz, D. Xu, and H. R. Roth, "Do gradient inversion attacks make federated learning unsafe?" *IEEE Transactions on Medical Imaging*, vol. 42, no. 7, pp. 2044–2056, 2023.

[10] W. Issa, N. Moustafa, B. Turnbull, and K.-K. R. Choo, "Rve-pfl: Robust variational encoder-based personalised federated learning against model inversion attacks," *IEEE Transactions on Information Forensics and Security*, pp. 1–1, 2024.

[11] A. Taneja, S. Rani, J. Breñosa, A. Tolba, and S. Kadry, "An improved wifi sensing based indoor navigation with reconfigurable intelligent surfaces for 6g enabled iot network and ai explainable use case," *Future Generation Computer Systems*, vol. 149, pp. 294–303, 2023.

[12] H. R. Chi, M. de Fátima Domingues, H. Zhu, C. Li, K. Kojima, and A. Radwan, "Healthcare 5.0: In the perspective of consumer internet-of-things-based fog/cloud computing," *IEEE Transactions on Consumer Electronics*, 2023.

[13] J. Ding and Y. Wang, "A wifi-based smart home fall detection system using recurrent neural network," *IEEE Transactions on Consumer Electronics*, vol. 66, no. 4, pp. 308–317, 2020.

[14] P. Kulurkar, C. kumar Dixit, V. Bharathi, A. Monikavishnuvarthini, A. Dhakne, and P. Preethi, "Ai based elderly fall prediction system using wearable sensors: A smart home-care technology with iot," *Measurement: Sensors*, vol. 25, p. 100614, 2023.

[15] R. K. Nv and B. E, "Detection and monitoring of the asymptotic covid-19 patients using iot devices and sensors," *International Journal of Pervasive Computing and Communications*, vol. 18, no. 4, pp. 407–418, 2022.

[16] N. Kourtellis, K. Katevas, and D. Perino, "Flaas: Federated learning as a service," in *Proceedings of the 1st workshop on distributed machine learning*, 2020, pp. 7–13.

[17] J. Song, W. Wang, T. R. Gadekallu, J. Cao, and Y. Liu, "Eppda: An efficient privacy-preserving data aggregation federated learning scheme," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 5, pp. 3047–3057, 2023.

[18] A. F. Aji and K. Heafield, "Sparse communication for distributed gradient descent," in *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing*, 2017, pp. 440–445.

[19] X. Qiu, J. Fernandez-Marques, P. P. Gusmao, Y. Gao, T. Parcollet, and N. D. Lane, "Zerofl: Efficient on-device training for federated learning with local sparsity," in *International Conference on Learning Representations*, 2022.

[20] S. U. Stich, J.-B. Cordonnier, and M. Jaggi, "Sparsified sgd with memory," *Advances in Neural Information Processing Systems*, vol. 31, 2018.

[21] B. Guo, Y. Liu, and C. Zhang, "A partition based gradient compression algorithm for distributed training in aiot," *Sensors*, vol. 21, no. 6, p. 1943, 2021.

[22] F. Sattler, S. Wiedemann, K.-R. Müller, and W. Samek, "Robust and communication-efficient federated learning from non-iid data," *IEEE transactions on neural networks and learning systems*, vol. 31, no. 9, pp. 3400–3413, 2019.

[23] S. Shi, Q. Wang, K. Zhao, Z. Tang, Y. Wang, X. Huang, and X. Chu, "A distributed synchronous sgd algorithm with global top-k sparsification for low bandwidth networks," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2019, pp. 2238–2247.

[24] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[25] H. Xie, S. Chen, Y. Wang, and Q. Jin, "A privacy-preserving federated learning scheme using threshold multi-key homomorphic encryption," in *2023 3rd International Conference on Communication Technology and Information Technology (ICCTIT)*. IEEE, 2023, pp. 187–192.

[26] P. Kukreja and V. Mahendran, "Contention matters: Modeling and analyzing the performance of federated learning over wifi," in *2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2023, pp. 1–6.

[27] S. Yousefi, H. Narui, S. Dayal, S. Ermon, and S. Valaee, "A survey on behavior recognition using wifi channel state information," *IEEE Communications Magazine*, vol. 55, no. 10, pp. 98–104, 2017.

[28] Y. Zhang, Y. Zheng, K. Qian, G. Zhang, Y. Liu, C. Wu, and Z. Yang, "Widar3. 0: Zero-effort cross-domain gesture recognition with wi-fi," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 44, no. 11, pp. 8671–8688, 2021.

[29] J. Yang, X. Chen, D. Wang, H. Zou, C. X. Lu, S. Sun, and L. Xie, "Sensefi: A library and benchmark on deep-learning-empowered wifi human sensing," *Patterns*, vol. 4, no. 3, 2023.

[30] A. Dahou, M. A. Al-qaness, M. Abd Elaziz, and A. Helmi, "Human activity recognition in ioht applications using arithmetic optimization algorithm and deep learning," *Measurement*, vol. 199, p. 111445, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S026322412200673X

[31] S. M. Hernandez and E. Bulut, "Wifederated: Scalable wifi sensing using edge-based federated learning," *IEEE Internet of Things Journal*, vol. 9, no. 14, pp. 12 628–12 640, 2022.

[32] K. Zhang, X. Liu, X. Xie, J. Zhang, B. Niu, and K. Li, "A cross-domain federated learning framework for wireless human sensing," *IEEE Network*, vol. 36, no. 5, pp. 122–128, 2022.

[33] W. Qi, R. Zhang, J. Zhou, H. Zhang, Y. Xie, and X. Jing, "A resource-efficient cross-domain sensing method for device-free gesture recognition with federated transfer learning," *IEEE Transactions on Green Communications and Networking*, vol. 7, no. 1, pp. 393–400, 2023.

[34] X. Zhou, W. Liang, J. Ma, Z. Yan, and K. I.-K. Wang, "2d federated learning for personalized human activity recognition in cyber-physical-social systems," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 6, pp. 3934–3944, 2022.