buildings

MDPI

Article

Confidentiality Preserved Federated Learning for Indoor Localization Using Wi-Fi Fingerprinting

Rajeev Kumar [1], Renu Popli [1,*], Vikas Khullar [1], Isha Kansal [1,*] and Ashutosh Sharma [1,2]

[1] Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura 140401, Punjab, India; rajeev_chauhan364@yahoo.co.in or rajeev.kumar@chitkara.edu.in (R.K.); vikas.khullar@chitkara.edu.in (V.K.)

[2] Department of Informatics, School of Computer Science, University of Petroleum and Energy Studies, Dehradun 248007, Uttarakhand, India

* Correspondence: renu.popli@chitkara.edu.in (R.P.); isha.kansal@chitkara.edu.in (I.K.)

Abstract: For the establishment of future ubiquitous location-aware applications, a scalable indoor localization technique is essential technology. Numerous classification techniques for indoor localization exist, but none have proven to be as quick, secure, and dependable as what is now needed. This research proposes an effective and privacy-protective federated architecture-based framework for location classification via Wi-Fi fingerprinting. The federated indoor localization classification (f-ILC) system that was suggested had distributed client–server architecture with data privacy for any and all related edge devices or clients. To try and evaluate the proposed f-ILC framework, different data from different sources on the Internet were collected and given in a format that had already been processed. Experiments were conducted with standard learning, federated learning with a single client, and federated learning with several clients to make sure that federated deep learning models worked correctly. The success of the f-ILC framework was computed using a number of factors, such as validation of accuracy and loss. The results showed that the suggested f-ILC framework performed better than traditional distributed deep learning-based classifiers in terms of accuracy and loss while keeping data secure. Due to its innovative design and superior performance over existing classifier tools, edge devices' data privacy makes this proposed architecture the ideal solution.

Keywords: deep learning; federated learning; indoor localization; multi-labeled classification; multi-class classification; Wi-Fi fingerprinting

Citation: Kumar, R.; Popli, R.; Khullar, V.; Kansal, I.; Sharma, A. Confidentiality Preserved Federated Learning for Indoor Localization Using Wi-Fi Fingerprinting. *Buildings* **2023**, *13*, 2048. https://doi.org/10.3390/buildings13082048

Academic Editors: Marco Domaneschi and Valentina Villa

Received: 28 June 2023
Revised: 27 July 2023
Accepted: 8 August 2023
Published: 10 August 2023

1. Introduction

The process of locating an object or a person inside an indoor setting, such as a building or facility, utilizing different technologies and procedures is known as indoor localization [1]. While GPS (Global Positioning System) is frequently used for outside localization, its limited precision and signal blocking make it less useful indoors. To effectively estimate position, indoor localization techniques often combine a number of distinct technologies. Indoor localization relies heavily on wireless technologies to transmit and receive signals [2]. Some prominent wireless technologies used in this context are given below:

(a) **Wi-Fi positioning**: By evaluating the signal intensity from surrounding access points, Wi-Fi signals can be utilized to determine a device's position. This technique is based on a database of well-known Wi-Fi access points and the patterns of their signal intensity inside a structure.

(b) **Bluetooth**: Indoor localization is possible with Bluetooth technology, especially Bluetooth Low Energy (BLE). It is feasible to determine a device's location inside a constrained area by deploying Bluetooth beacons or using the signal strength from already-existing Bluetooth devices.

(c) **Ultra-wideband (UWB)**: UWB is gaining popularity for high-precision indoor localization applications due to its ability to provide accurate distance measurements.

(d) **RFID (radio-frequency identification)**: RFID is often used for asset tracking and indoor localization in specific scenarios where tagged objects or assets need to be monitored.
(e) **Zigbee**: Zigbee is a low-power wireless communication technology commonly used in building automation and smart home systems, but it can also be utilized for indoor positioning.
(f) **Cellular network-based positioning**: In some cases, cellular networks can provide rough estimates of indoor positions by leveraging signal strengths from nearby cell towers.
(g) **IR (Infrared) and ultrasonic signals**: Infrared and ultrasonic signals are used in specialized applications, such as indoor localization for visually impaired individuals.

It is imperative to consider that the effectiveness of these indoor localization techniques and wireless technologies may vary depending on factors like the environment, infrastructure setup, hardware limitations, and the specific use case. Applications for indoor localization include asset tracking, location-based services, indoor mapping, assistance with navigation, and boosting safety and security in buildings [3]. However, the deployment strategy, the environment, and the particular technology being utilized can all affect how accurate and reliable indoor localization systems work.

One promising solution for indoor localization is Wi-Fi fingerprinting, which involves mapping the unique signal strengths of Wi-Fi access points within a building to create a "fingerprint" of that space. This fingerprint can then be used to locate devices and assets within the building with a high degree of accuracy. Wi-Fi fingerprinting has several advantages over other indoor localization technologies, such as Bluetooth and RFID, including its low cost and ease of implementation. In addition, Wi-Fi fingerprinting does not require any additional hardware or infrastructure, as it leverages the existing Wi-Fi network already present in most buildings. This makes it a convenient and cost-effective solution for businesses and organizations looking to implement indoor localization without significant investments. Furthermore, Wi-Fi fingerprinting can provide real-time tracking and updates, allowing for efficient asset management and improved security measures within the building. However, there are still challenges to overcome in terms of scalability and accuracy. For instance, Wi-Fi signals may be disrupted when they encounter interference from other devices or when they encounter physical impediments within the building. Despite these challenges, Wi-Fi fingerprinting holds great potential for improving safety and security measures in indoor spaces and optimizing operations for businesses.

Deep neural networks (DNNs) are frequently used in indoor localization using Wi-Fi fingerprints [4] to predict a device's or person's location within an indoor setting using received signal strength (RSS) readings from adjacent Wi-Fi access points. DNNs have proven to be highly effective in accurately estimating indoor locations based on Wi-Fi fingerprints. By analyzing the RSS readings from nearby Wi-Fi access points, DNNs can learn complex patterns and relationships to provide precise localization predictions. This technology has found applications in various domains, including asset tracking, navigation systems, and location-based services. This technique entails using a dataset of Wi-Fi fingerprints gathered at known locations inside the indoor environment to train a DNN model [5]. By examining a device's RSS values, the trained model may then be used to forecast its location.

The importance of Wi-Fi fingerprinting lies in its potential to revolutionize the way we approach safety and security measures in indoor spaces. By accurately identifying and tracking individuals within a building, Wi-Fi fingerprinting can help prevent unauthorized access and improve emergency response times. Additionally, businesses can benefit from the data collected through Wi-Fi fingerprinting by optimizing their operations and improving customer experiences. However, scalability and accuracy remain key challenges that must be addressed in order for Wi-Fi fingerprinting to reach its full potential. Despite these obstacles, the promise of improved safety and security measures makes continued research and development of Wi-Fi fingerprinting technology crucial for the future [6].

Despite its potential, Wi-Fi fingerprinting technology is not without limitations and challenges. One of the biggest challenges is the need for accurate and up-to-date maps of Wi-Fi signals, which can be difficult to maintain in dynamic environments. Additionally, privacy concerns have been raised as Wi-Fi fingerprinting can potentially track individuals' movements and behaviors. There are also technical limitations such as interference from other devices and the inability to accurately differentiate between multiple devices using the same Wi-Fi signal. These challenges must be addressed in order for Wi-Fi fingerprinting to reach its full potential and become a reliable tool for various industries.

The aim of this study is to develop multi-building data-based privacy-preserved classification for Wi-Fi-based indoor localization. For this, a federated learning ecosystem has been developed and deployed in multi-node architecture.

The article structure is as follows: In Section 2, a literature survey on indoor localization technologies is presented; the proposed technique, data collection and overall methodology are described in Section 3, while Section 4 shows experimental results and the discussion. And finally, conclusions are drawn in Section 5.

2. Literature Survey

Indoor localization technology has become increasingly important in recent years as more and more people spend time indoors, whether it is in offices, malls, or airports. The ability to track individuals and assets within these spaces can improve safety and security measures, as well as provide valuable data for businesses to optimize their operations [7]. However, there are still challenges to overcome in terms of accuracy and scalability of indoor localization systems [8–10]. This section describes the literature survey related to the study.

The idea of Wi-Fi fingerprint-based indoor positioning is introduced by He, S. et al. in 2019 [11], and it entails leveraging the distinctive qualities of Wi-Fi signals received at various locations to pinpoint a user's position within an indoor environment. They explore a variety of Wi-Fi fingerprinting approaches, including those that are based on signal strength, angle of arrival (AoA), time of arrival (ToA), and time difference of arrival (TDoA), among others. Each technique's benefits and drawbacks are discussed. A unique method for indoor localization using Wi-Fi fingerprints is proposed by [12] BelMannoubi, S. et al. in 2019 [12]. It entails training deep neural networks to discover the relationship between received signal strength (RSS) measurements and the associated locations inside a building. They test several network topologies, such as convolutional neural networks (CNNs) and feedforward neural networks (FNNs) and assess how well they perform in terms of localization accuracy.

HiLoc, a unique indoor localization method that makes use of distributed antennas to improve positioning accuracy, is introduced by Liu, K. et al. in 2021 [13]. As it only requires one access point to function, the system is both affordable and simple to set up. They discuss the creation of the localization algorithm, calibration, and the design and implementation of the HiLoc system, which includes a number of processes. The method uses measurements of received signal strength (RSS) from numerous antennas to infer the user's position. A deep learning-based solution for indoor localization that makes use of RSS and CSI, which are derived from wireless signals sent by access points, is proposed by Hsieh, C. H. et al. in 2019 [14]. They outline the procedure for gathering data, which entails measuring CSI and RSS values at various points across an interior setting. A database is built using these measurements to train the deep learning model.

A sustainable indoor localization method is presented by Liu, T. et al. in 2021 [15] and uses structure cues like doors, walls, and corners as reference points for mapping radio signals inside an indoor environment. They suggest a three-step radio signal mapping process that includes data gathering, identifying structures as landmarks, and radio signal mapping. The approach relies on structure landmarks and is appropriate for long-term and sustainable interior localization applications because it does not call for large infrastructure deployment or frequent recalibration. A federated spectrum learning architecture for wireless edge networks that includes reconfigurable intelligent surfaces is proposed by Yang, B et al. in 2022 [16]. The objective is to distribute and cooperatively optimize spectrum allotment and resource use. The notion of reconfigurable intelligent surfaces—programmable surfaces capable of modifying wireless signals to improve communication performance in wireless networks—is introduced in this study. The advantages of including reconfigurable intelligent surfaces in wireless edge networks are covered in the article. The wireless propagation environment may be dynamically controlled thanks to RIS technology, which enhances spectrum efficiency, coverage, and energy efficiency.

An adversarial deep learning method for indoor localization is proposed by Wang, X et al. in 2022 [17], specifically using channel state information (CSI) tensors. The multipath effects are captured by CSI tensors, which also offer more details about the wireless channel properties. The study introduces the generator network and discriminator network architecture of the suggested deep learning model. Based on the input CSI tensors, the generator network provides indoor localization results, while the discriminator network assesses the reliability of the results. The adversarial deep learning model outperforms other deep learning models that do not make use of CSI tensors as well as conventional machine learning algorithms.

Channel state information (CSI) is a major component of the multi-level fingerprinting strategy for indoor localization proposed by Li, T. et al. in 2018 [18]. For precise localization, CSI gives comprehensive information about the wireless channel, including phase shifts, amplitude changes, and multipath effects. The notion of multi-level fingerprinting, which divides the indoor environment into various levels or zones based on their unique CSI properties, is introduced in the study.

A DNN-based method for indoor location is proposed by Wu, G. S. et al. in 2018 [19], and it makes use of the channel state information (CSI) gleaned from wireless signals sent by access points. The DNN model's architecture, which is employed for indoor positioning, is introduced in this study. Convolutional, pooling, and fully connected layers are among the many layers that make up the model. These layers are trained to learn how to transfer the input CSI data to the appropriate indoor positions. The authors outline the method for gathering data, which include measuring CSI at several points across an interior setting.

An innovative method for attaining accurate indoor localization utilizing Wi-Fi signals is presented by Yang, R. et al. in 2021 [20]. The authors provide a method that calculates the separation between a user and access points (APs) using channel state information (CSI) collected from Wi-Fi signals. They derive a collection of attributes that are employed for localization by examining the CSI's phase and amplitude properties. The authors use a machine learning approach known as random forest regression to increase the system's accuracy.

Using Wi-Fi signals, Chang, R. Y. et al. (2018) [21] suggest a device-free method for indoor localization. The elements that define the environment and human behaviors are extracted by the authors using the Channel state information (CSI) of Wi-Fi signals. The feature extraction module and the localization module are the two key components of the framework they introduce.

An examination of the literature revealed that Wi-Fi fingerprinting, which includes mapping the distinct signal intensities of Wi-Fi access points inside a structure to establish a "fingerprint" of that space, is a viable method for indoor localization. Then, with a high degree of precision, this fingerprint may be used to locate equipment and assets inside the facility. Compared to indoor localization technologies like Bluetooth and RFID, Wi-Fi fingerprinting has a number of benefits, including affordability and simplicity of use. But, there are still difficulties to be solved in terms of accuracy and scalability [22]. For instance, interference from other devices or actual obstructions inside the building can impact Wi-Fi signals. Despite these difficulties, Wi-Fi fingerprinting has a lot of potential for enhancing indoor safety and security measures and streamlining business processes.

Researchers are examining the potential of using Wi-Fi fingerprints for security purposes, such as detecting unauthorized access to a network or tracking the movement of people within a building, in comparison to other indoor localization techniques like Bluetooth and RFID, which could result in more accurate and dependable indoor positioning systems. In order to create immersive experiences that are personalized to the user's location, Wi-Fi fingerprinting may also be used with other technologies, such as augmented reality and virtual reality. Wi-Fi fingerprinting technology has the potential to revolutionize a variety of industries, from retail and hospitality to healthcare and transportation, as it continues to develop and get better. In the end, there are countless potential applications for Wi-Fi fingerprinting technologies.

The algorithms used to analyze Wi-Fi signals and extract location data have been the subject of numerous studies aimed at improving them. Researchers have also looked into the application of machine learning strategies to improve the precision of Wi-Fi fingerprinting. Dealing with signal interference and evolving Wi-Fi environments, however, continues to provide difficulties.

3. Proposed Work

In this section, the overall methodology used for the proposed framework is discussed. The description of collection of the dataset and preprocessing mechanism is also provided.

3.1. Federated Learning

The mathematical modelling of federated learning is the maintopicof this section. A distributed machine learning paradigm known as federated learning (FL) makes it possible to train neural networks (NNs) and conduct data analysis directly on the data storage [23,24]. In FL, the neural network is updated using result factors like NN weights to construct a mixed analytical model. FL devices do not store data centrally [25]. The three main parts of every FL system are the server, the communication framework, and the consumers. While the whole dataset (DSN = DS1 + DS2 +… + DSp) is referred to as DSN, FL needs the usage of individual client data sets (DS1, DS2,…, DSp) to train a single machine learning model. To train a deep learning model using a conventional distributed learning method, all distributed datasets (DNs) are combined into a single dataset. In FL, however, each client's data (DSi) is separately trained, and the resulting models work together without transferring any DSi to the server (SV) or the other clients (Mi). In this case, categorical cross entropy loss (L) from Equation (1) is used as the basis for classification.

$$L = -log\left(\frac{e^{SV_p}}{\sum_j^M e^{SV_j}}\right) \tag{1}$$

Equation (2), which minimizes the average loss across p training clients, is the standard expression for federated learning. It also reduces the number of training clients.

$$minF(w) = \frac{1}{p}\sum_{i=1}^{p} f_i(w) \tag{2}$$

During supervised learning with p unique clients, the loss function for weight values is denoted by the symbol $F(w)$. Regarding our clients' training, this can be viewed as locating a set of weights, which results in the smallest potential average loss. FL distributes data to p clients from a single system, which increases communication overhead. DJ, every user has a portion of the shared database. The function is represented by Equation (3).

$$F(w) = \sum_{j=1}^{J} \frac{p_j}{p}\left(\frac{1}{N_j}\sum_{i\in D_j} f_i(w)\right) \tag{3}$$

3.2. Dataset Collection and Pre-Processing

One can follow the link [26] to access the central data repository for studies on wireless fingerprinting-based indoor localization. To simulate the dataset in a federated setting, we randomly split all of the collected datasets into as many pieces as there were clients connected to our server. Additionally, pclients were randomly assigned one of p equal segments of communal data. This distribution represented a scenario in which each client came equipped with their own locally collected, heterogeneous dataset. The data from each pclient was then pre-processed in preparation for FL processing by being cleaned, tokenized, de-stopped, stemmed, and converted to a standard encoding.

3.3. Overall Methodology

The scalability of fingerprinting techniques becomes essential when indoor localization is to be used in a large campus or shopping mall with several buildings and multiple floors. Modern Wi-Fi fingerprinting techniques for indoor localization require a hierarchical approach in which the location's building, floor, and position (such as a label or set of coordinates) are all determined separately. In this technique, the IEEE 802.11b [27] standard is followed and the specifications of the IEEE 802.11b is tabulated in Table 1.

Table 1. Summary of 802.11b Wi-Fi standard specification for indoor localization.

Parameter/Model	**Value**
Date of standard approval	July 1999
Maximum data rate (Mbps)	11
Typical data rate (Mbps)	5
Typical range indoors (Metres)	~30
Modulation	CCK (DSSS)
RF band (GHz)	2.4
Channel width (MHz)	20

This standard provides guidelines for the use of Wi-Fi technology in indoor environments, ensuring compatibility and accuracy in the fingerprinting process. Additionally, the tabulated specifications include details on signal strength, signal-to-noise ratio, and other parameters that are crucial for accurately determining a device's location within the indoor space. The proposed architecture for f-ILC (federated indoor localization classification), which is shown in Figure 1, comprises the layers. A client–server architecture was necessary for the suggested framework for federated machine learning or deep learning, with each end utilizing its own code to carry out prescribed tasks. One server and N clients, each running their own code, made up a federated cluster. The suggested federated learning architecture for indoor localization categorization was implemented using two Python programming libraries, Keras and Tensorflow. Since each N-client network node has its own processing and storage unit, each might use its own structured data to generate the training model and weights. The remote server processed federated global weights from N-client trained models. In contrast to traditional distributed ML and DL frameworks, the suggested federated architecture guaranteed client data privacy by just transmitting training weights between client and server. This also reduced processing latency.

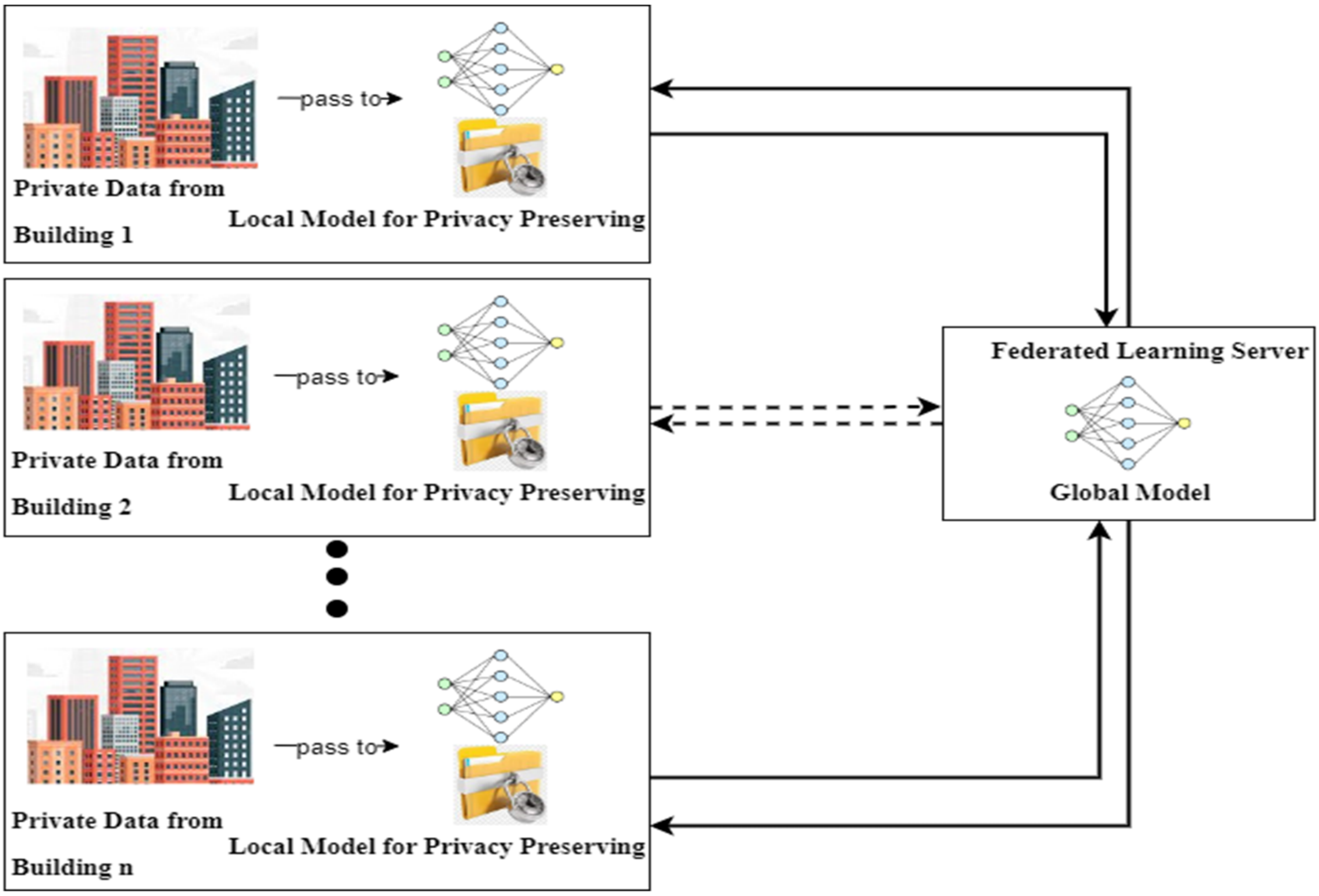


Figure 1. Proposed framework for Wi-Fi fingerprinting based indoor localization using federated learning.

Figure 2 depicts the comprehensive deployment procedure for the proposed f-ILC. The implementation stages appeared as follows:

1. Each individual client in the N-client system was responsible for gathering the Wi-Fi fingerprinting data using its own resources. This information was then saved in each client's individual storage system.
2. On the sets of data that were provided, individual data cleansing and preprocessing operations were carried out by the Nclients.
3. In the suggested client–server architecture, N-client edge nodes could access the already processed dataset for federated learning with predefined codes to classify.
4. The federated learning process's initial weights are likewise determined by the server.
5. In a client–server architecture, the server distributed the initial weights among N consumers.
6. Nclients, after obtaining the weights, began or simulated their own training and validation with their own readily available datasets.
7. After the training phase was over, the weights of each client's trained model were uploaded to the server.
8. In this phase, the server calculated the federated average weights using the weights it had collected from all connected clients.
9. The federated server determined the federated weights and sent them back to all of the connected clients after the computation.

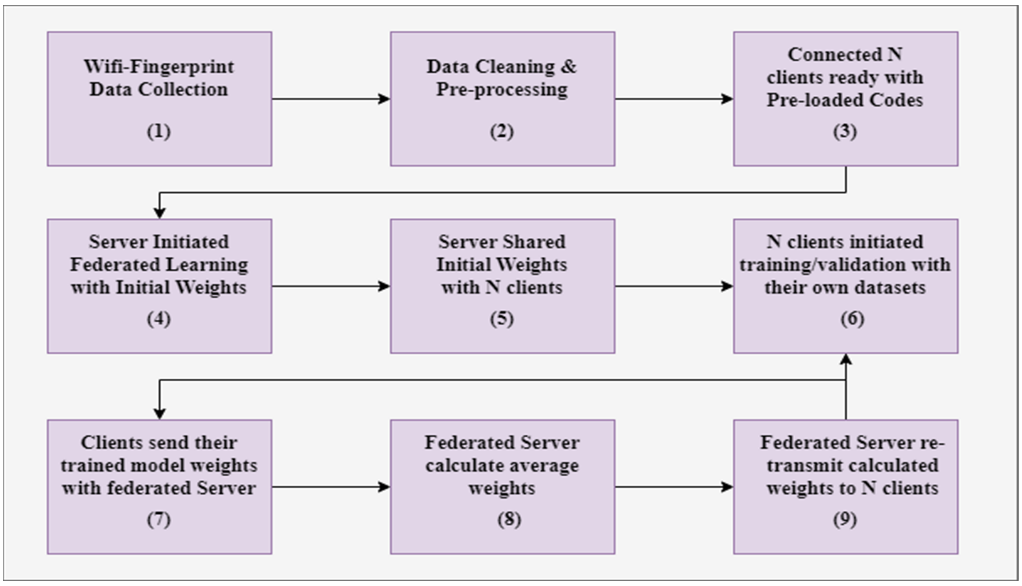


Figure 2. Steps involved in f-ILC.

The major outcomes of the proposed work are described as follows:

1. This study uses DNNs to classify buildings, floors, and locations, demonstrating advantages such as resistance to signal fluctuations, noise effects, and device dependence.
2. It suggests a federated learning-based paradigm for classification.
3. The proposed that f-ILC framework outperforms conventional distributed deep learning in multi-client settings and single-client situations.
4. LSTM, CNN-LSTM, BiLSTM, and DenseNet are used to test the architecture on IID and non-IID datasets.

4. Experimental Results and Discussions

The effectiveness of the suggested secure and efficient f-ILC framework was tested through a number of experiments. On IID datasets as well as non-IID datasets, performance was evaluated based on accuracy, validation loss, and resource utilization. We also showed how well our models fared in comparison to models that were taught the traditional way.

4.1. Simulation Set-Up

On a computer with an Intel i5 processor and 8 GB of RAM, experiments with the suggested f-ILC were carried out. A multi-client scenario was formed by giving various commands in response to the existence of many clients. Several computer models were put into practice to assess how well the proposed f-ILC performed. A total of 50 training epochs, 64 segments, and a learning rate of 0.001 were the system's standard training parameters. The local minimum batch size in the federated system was set to 64 on each client, the number of epochs before the global model update (E) was set to 5, and r was set to 0.001 on each client. The simulation process is given in Table 2 as follows:

4.2. Indoor Localization Using Basic Deep Learning

To categorize the indoor localization in this case, conventional deep learning algorithms such as CNN-LSTM, Bi LSTM, and DenseNet were used [28,29]. LSTM, CNN-LSTM, Bi LSTM, and DenseNet models were trained and verified over the course of 50 epochs. We specified, 64 for the batch size, 50 for the epochs, and 0.001 for the learning rate in the hyper parameters.

Table 2. Simulation setup.

Simulation Configurations/Steps	Related Data/Source
Software configurations	Python version 3.11.4 Tensorflowfederated Keras 2.11.0 Tensorflow version 2.13.0
System configuration (server side)	1 server I7 processor 16GB RAM NVIDIA 1650 4 GB Dedicated Graphics Memory
System configuration (Client side)	No of clients:5 I5 processor 8GB RAM NVIDIA 1650 4 GB Dedicated Graphics Memory
Data collection and preprocessing	Refer to Section 3.2
Benchmark single system analysis	Refer to Section 4.2
Data distributed according to clients as per IID and Non IID.	Refer to Sections 4.3.1 and 4.3.2
Analysis on federated ecosystem	Refer to Section 4.3

According to the findings, on applying direct deep learning based models for indoor localization, various parameters have been shown in Table 3, where theaccuracy attained by BiLSTM_Dense, CNNLSTM, DenseNet, LSTM_Dense is 99.78% (highest), 98.97%, 99.64% and 99.78% (highest), respectively, where the validation accuracy measured is 99.65%, 99.65%, 86.75% (least) and 99.65%, respectively. Talking about loss, which is the same for all the models, i.e., 0.01, whereas validation loss is slightly different, i.e., 0.02, 0.00 (least), 0.40 and 0.02, respectively. According to Figure 3d, the validation losses over 50 epochs were found to be 0.00 for CNNLSTM. According to the research shown in Figure 3, CNNLSTM outperformed the other deployed learning models including LSTM, DenseNet and Bi-LSTM and was more consistent with regard to both its accuracy and its losses.

Table 3. Comparative analysis of traditional deep learning algorithms for indoor localization using Wi-Fi fingerprinting.

Parameter/Model	BiLSTM_Dense	CNNLSTM	Dense	LSTM_Dense
Accuracy	99.78	98.97	99.64	99.78
Validation Accuracy	99.65	99.65	86.75	99.65
Loss	0.01	0.01	0.01	0.01
Validation Loss	0.02	0.00	0.40	0.02

4.3. Indoor Localization Using Federated Learning

In the current scenario, the proposed f-FNC framework's performance was evaluated. For the indoor localization classification using current datasets, deep learning algorithm CNNLSTM was implemented in a federated environment because of its better performance. The system consists of five clients C_0, C_1, C_2, C_3, C_4. The model CNNLSTM outperformed the other deep learning models, and therefore, this model was selected and all the clients trained their data using CNNLSTM. After training their models, all the clients send their trained model to the federated server. Multiple rounds of this process occur until the desired accuracy and loss is achieved by the server. Both independent and identically distributed data (IID) and non-IID scenarios are taken into consideration for evaluation [30].

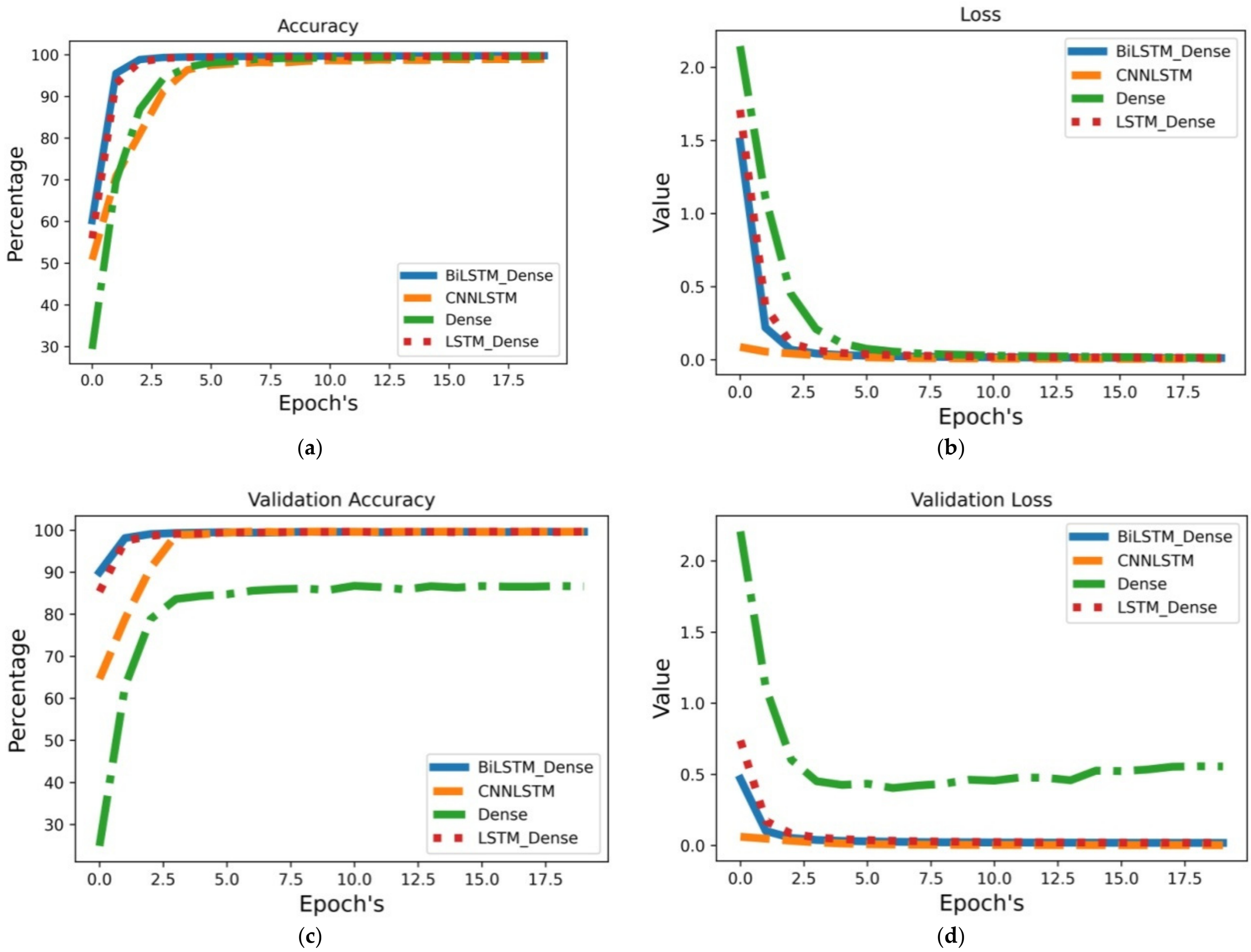


Figure 3. (**a**) Accuracy; (**b**) loss; (**c**) validation accuracy; (**d**) validation loss.

4.3.1. IID Database

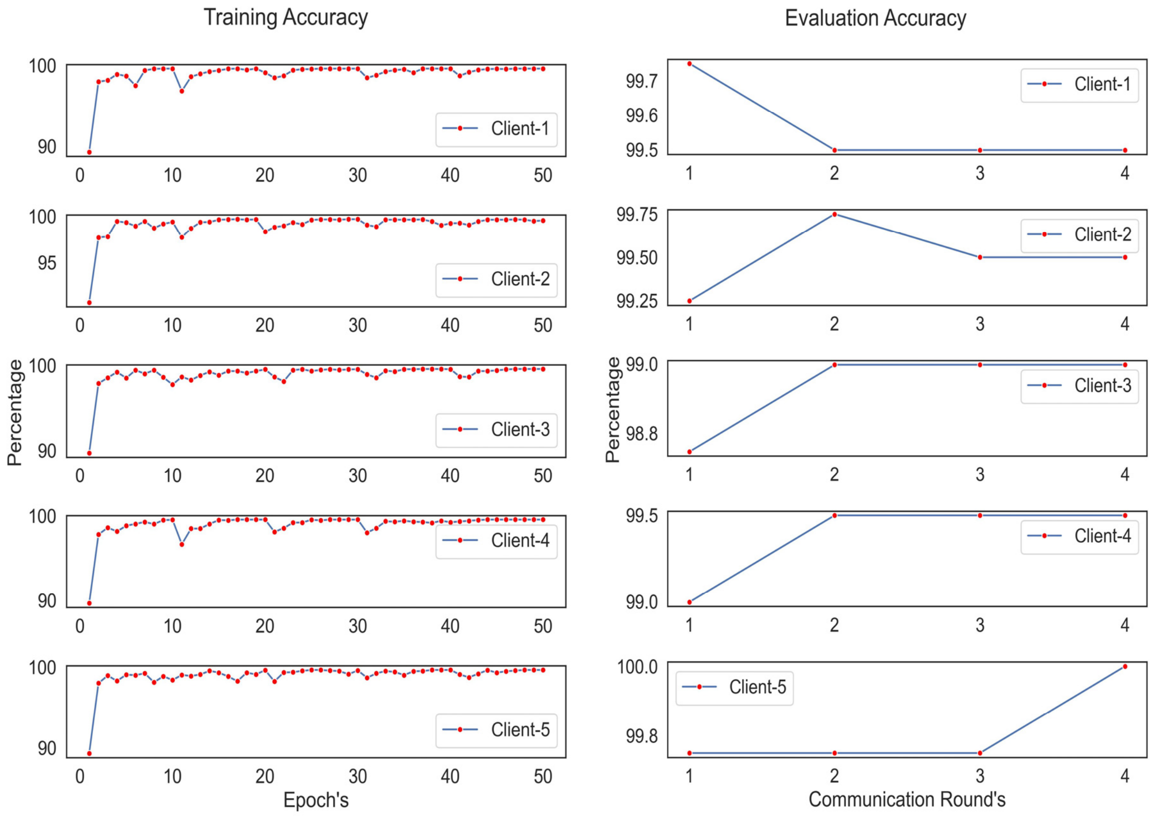
This section analyses the suggested FL architecture using independently and identically distributed data. The following guidelines must be followed in order for a client relationship to be referred to as IID:

- Independent, which loosely translates to "data generation is consistent"; as a result, for any class l and feature set S, P(S, l) = P(S).P(l), here . represents dot product.
- Identically distributed means that the client's dataset (Di) follows the same probability distribution; as a result, P(l | D1) = P(l | D2)... = P(l | Dn) for any class y.

For balanced training and testing, data were split evenly across the five nodes in this work. To analyze the balance in the initial model training, the equally distributed dataset was taken into consideration. Results in Figures 4–7 show that every client had an even distribution of training and validation accuracy with the fewest losses.

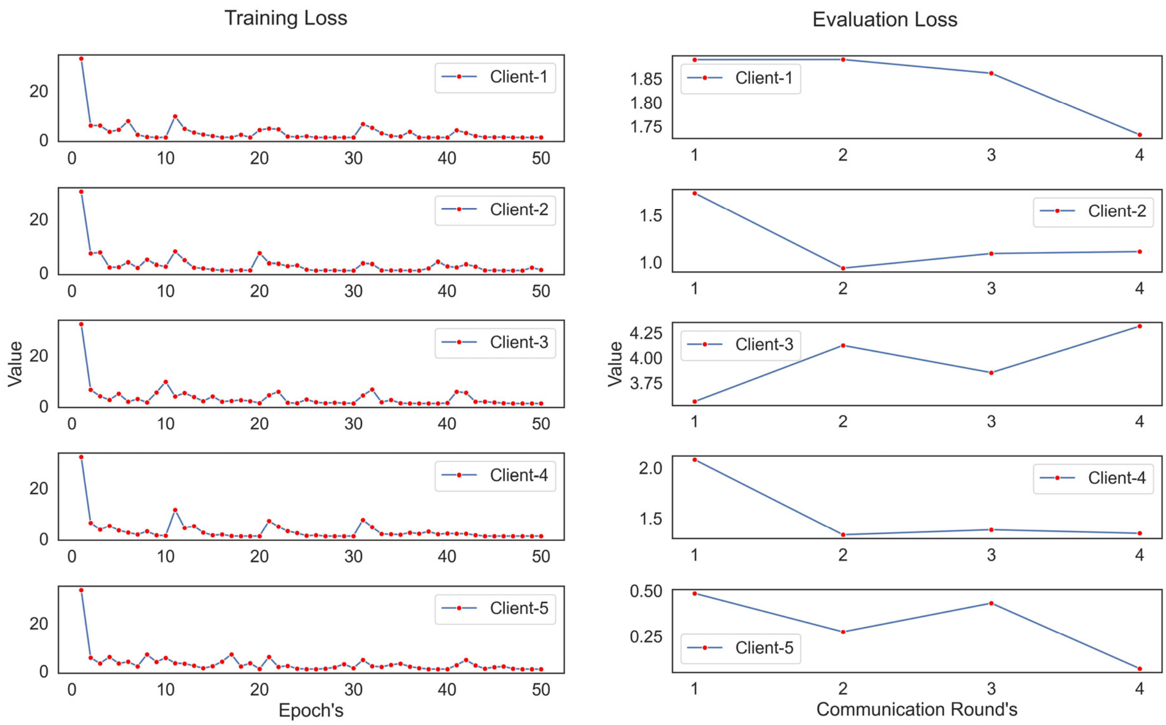
4.3.2. Non-IID Database

In this section, the proposed FL architecture were analyzed on the basis of non-IID data [31,32]. Violating any of the rules mentioned in Section 4.3.1 implies a non-IID context. Here, in this work, data was unequally distributed among all five nodes for unbalanced training and testing. The unequally distributed dataset was considered to analyze the resultant training of models. Even with unbalanced non-IID data, all individual clients resulted in balanced and nearly equal outcomes in terms of training and validation accuracy with minimum losses as shown in Figures 8–11.



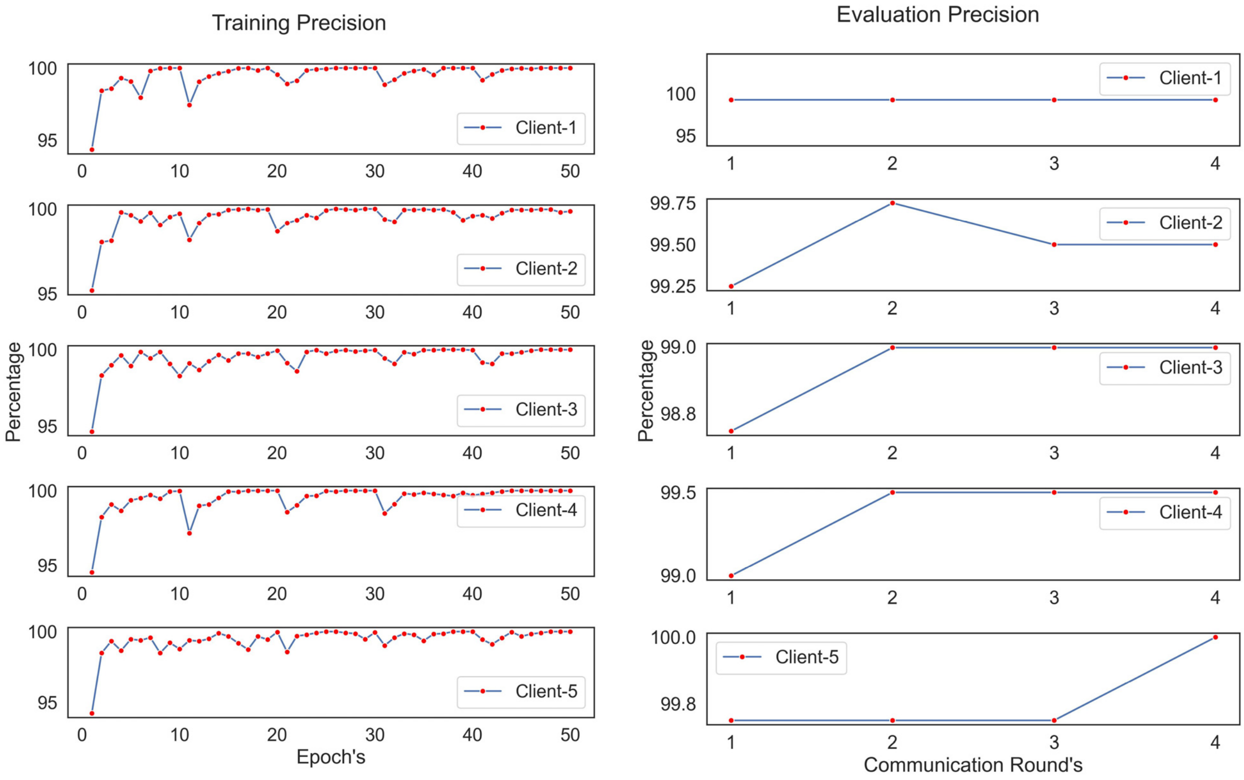
(**a**) (**b**)

Figure 4. For IID data (**a**) Training accuracy; (**b**) evaluated accuracy.



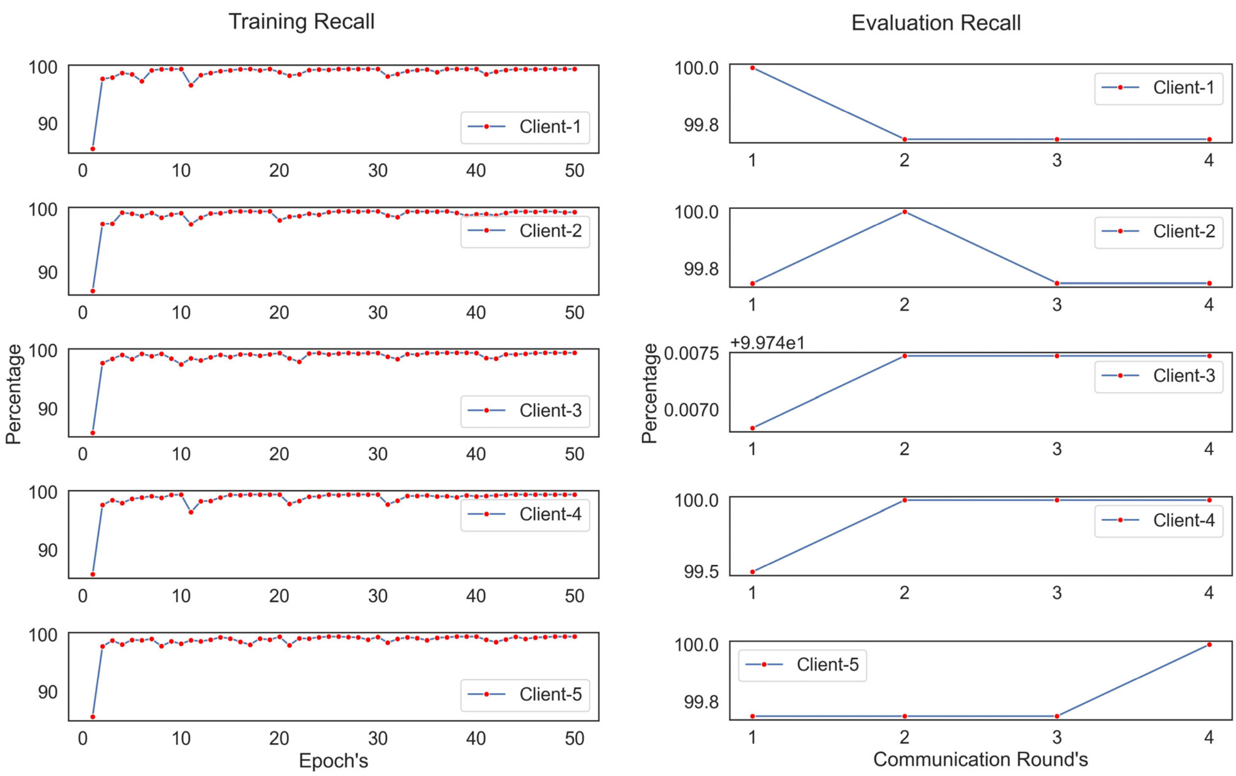
(**a**) (**b**)

Figure 5. For IID data (**a**) Training loss; (**b**) evaluated loss.



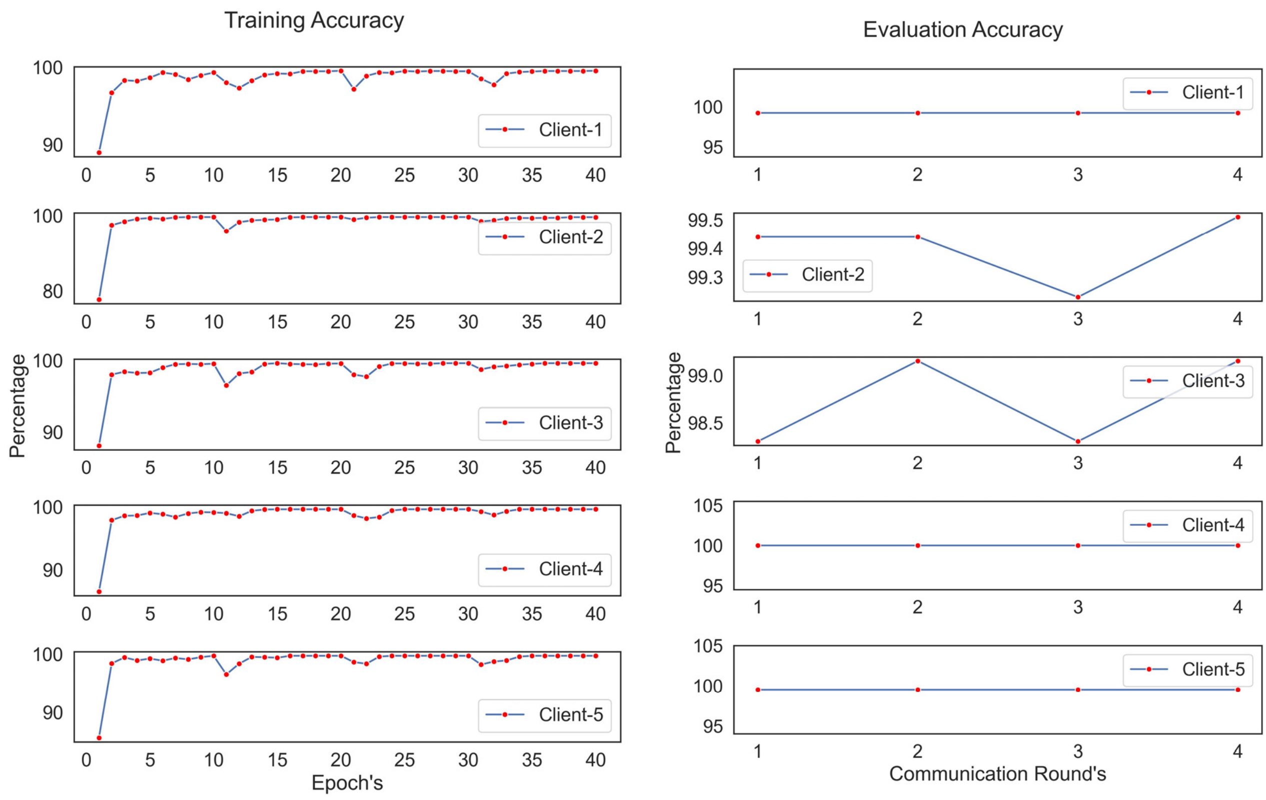
(a) (b)

Figure 6. For IID data (**a**) Training precision; (**b**) evaluated precision.



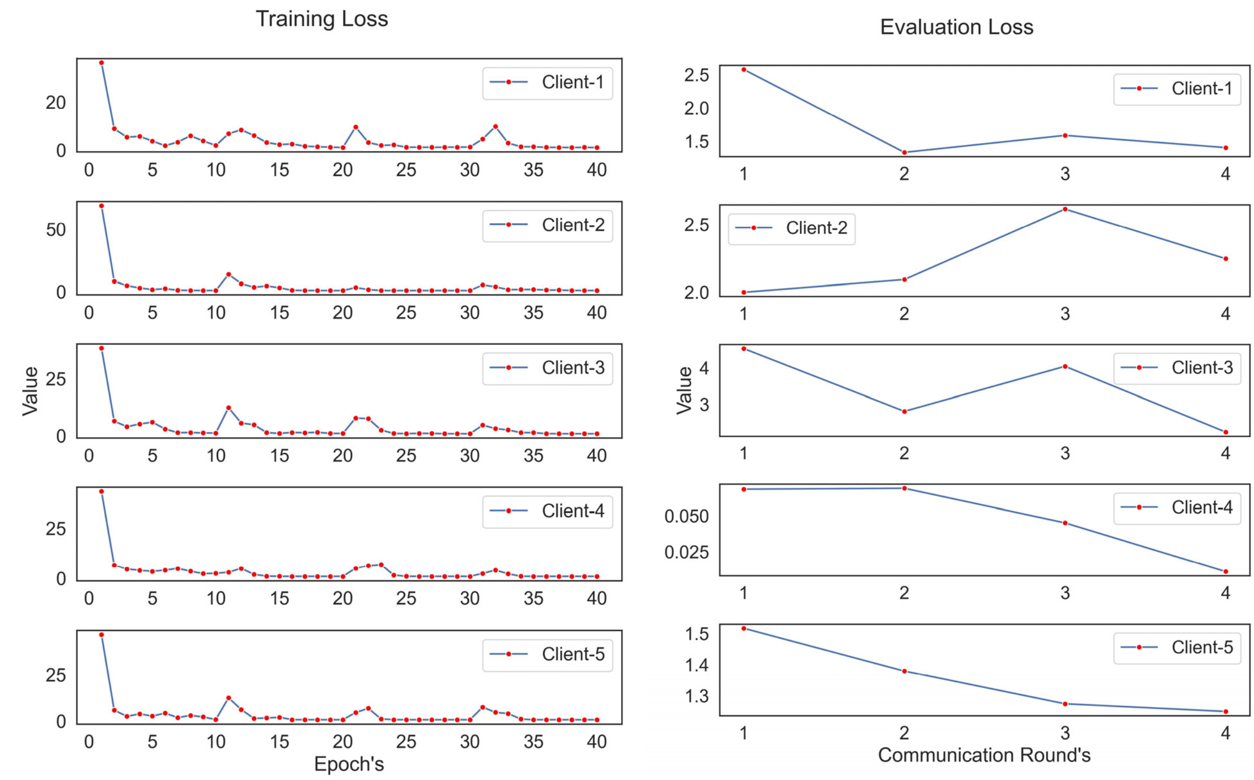
(a) (b)

Figure 7. For IID data (**a**) Training recall; (**b**) evaluated recall.



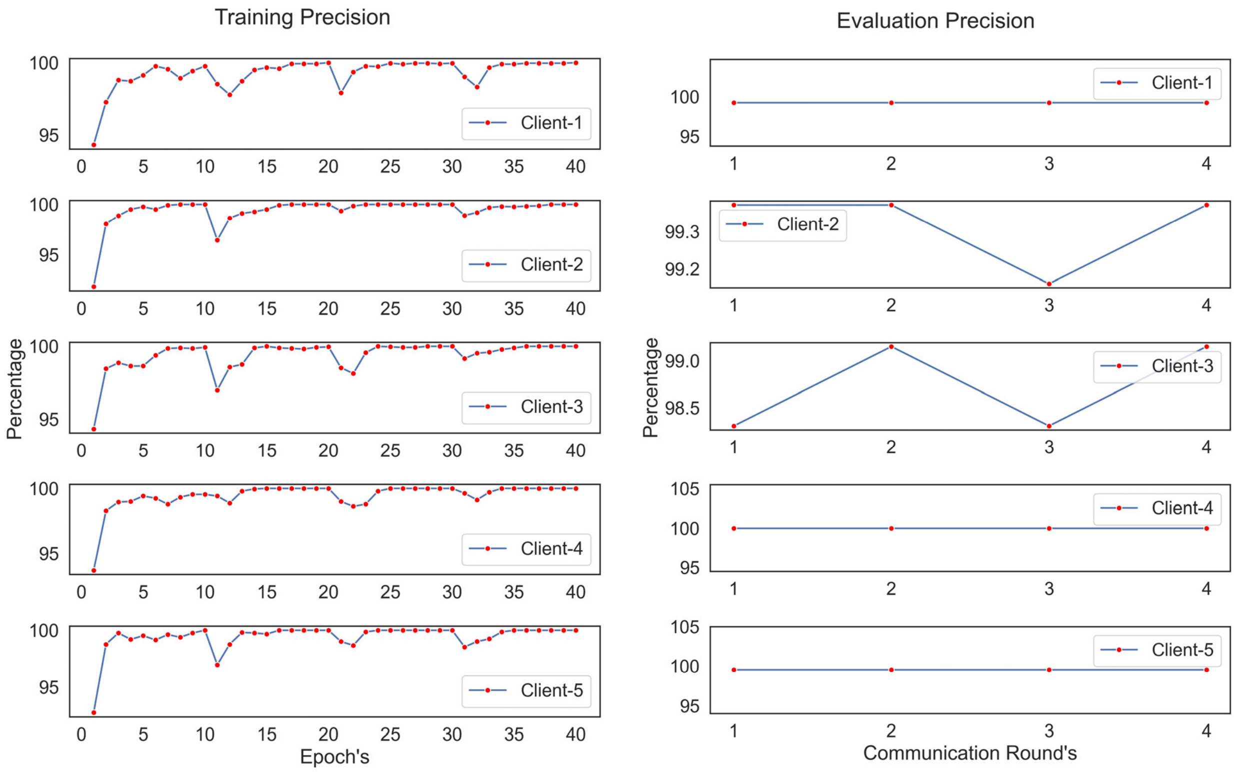
(**a**) (**b**)

Figure 8. For Non IID data (**a**) Training accuracy; (**b**) evaluated accuracy.



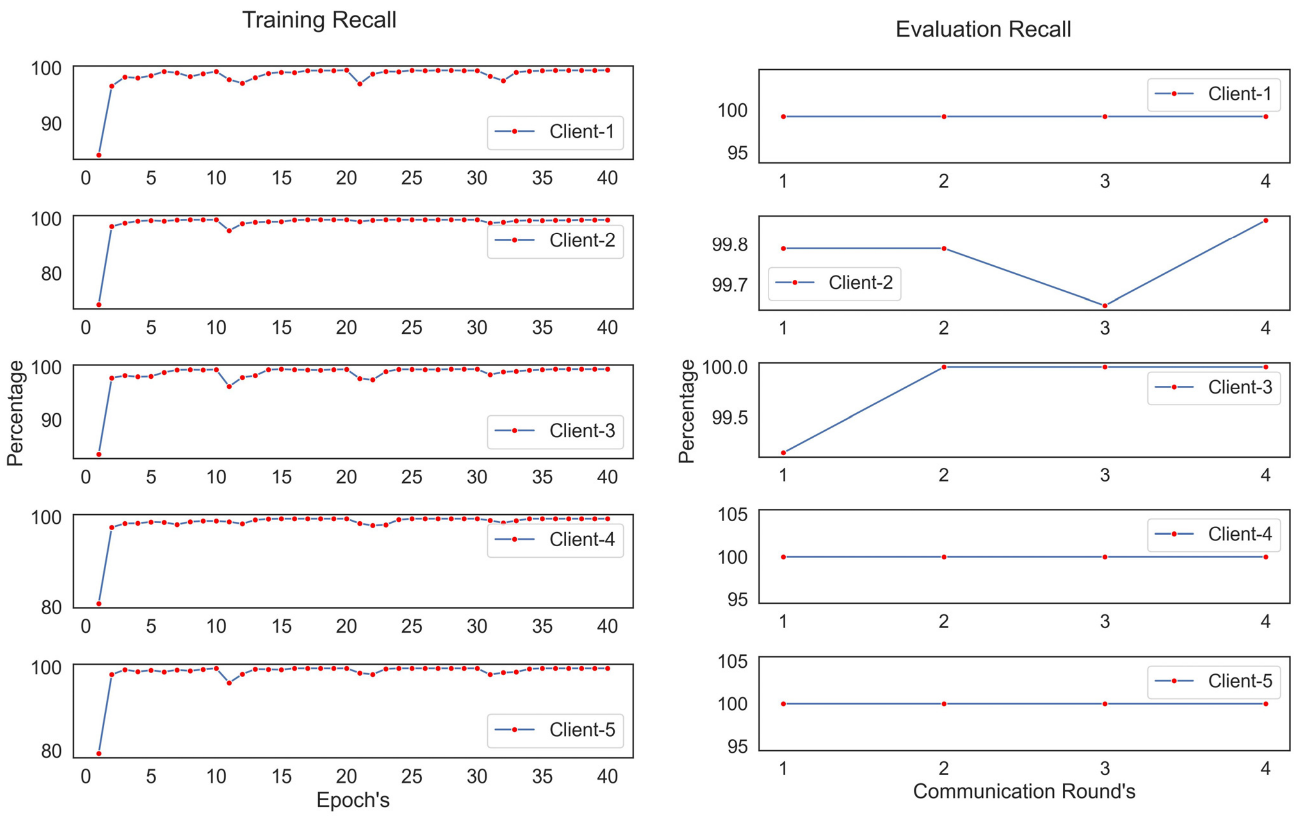
(**a**) (**b**)

Figure 9. For Non IID data (**a**) Training loss; (**b**) evaluated loss.



(**a**) (**b**)

Figure 10. For Non IID data (**a**) Training precision; (**b**) evaluated precision.



(**a**) (**b**)

Figure 11. For Non IID data (**a**) Training recall; (**b**) evaluated recall.

Table 4 shows that in terms of accuracy and loss, for both IID and non-IID data, the federated learning environment produces almost comparable results. Both the validation parameters suggested that the federated-ILC architecture performed better than the competition. Data privacy, together with equal accuracy and fewer errors were the most prominent features of the suggested f-ILC framework, which were overlooked by the traditional deep learning architecture. With accuracy scores between 99.085% and 99.85%, the suggested research exceeded the previously reviewed deep learning-related literature for indoor localization. Ultimately, it was shown that the suggested method is substantially more effective and secure than traditional frameworks. The mapping of current federated learning programming frameworks might take more time and effort. The suggested effort could be hampered by this. It is feasible to use the suggested technique as a classification system for distributed real-time indoor localization systems in the future.

Table 4. Comparative analysis of federated learning algorithm using IID/non-IID for indoor localization using Wi-Fi fingerprinting.

Train/Validation	Data	Accuracy	Loss	Precision	Recall
Training	IID	99.5	0.02	99.45	99.085
Training	Non-IID	99.57	0.01	99.55	99.85
Validation	IID	99.61	0.01	99.99	99.61
Validation	Non-IID	99.62	0.01	100	99.62

5. Conclusions

DNNs are employed in this work to classify buildings, floors, and locations within those levels. The advantages of DNN-based approaches, including resistance to signal fluctuations, noise effects, and device dependence, as well as the removal of the time-consuming manual process of finding the best match against each fingerprint in a database, are demonstrated by preliminary results for classifying buildings and floors and floor-level location estimation. Additional studies on hierarchical building/floor categorization and scalable, higher-resolution floor-level localization are required. In light of this, this study suggests a federated learning-based paradigm for classification. LSTM, CNN-LSTM, BiLSTM, and DenseNet were among the deep learning algorithms used to test the proposed architecture utilizing IID and non-IID datasets. Initially, the results for indoor localization are shown at individual clients using a basic deep learning model, in which CNNLSTM outperforms the other models with a validation accuracy and loss of 99.65 and 0.00 (rounded off to the second decimal place). After that, in the federated learning multi-client environment, each client was trained using the CNNLSTM model and all clients shared their data with the centralized server. Finally, on the centralized server, results comparable to CNNLSTM were achieved along with maintaining the concept of data privacy.

Author Contributions: Conceptualization, R.K.; Methodology, I.K.; Software, V.K.; Validation, V.K.; Formal analysis, I.K.; Resources, A.S.; Writing—original draft, R.P.; Writing—review & editing, R.K.; Visualization, A.S. All authors have read and agreed to the published version of the manuscript.

Funding: The research received no external funding.

Data Availability Statement: All data used in the manuscript has been mentioned and cited with proper care.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Dang, X.; Tang, X.; Hao, Z.; Liu, Y. A Device-Free Indoor Localization Method Using CSI. *Sensors* **2019**, *19*, 3233. [CrossRef]
2. Huthaifa, O.; Shuaieb, W.; Obeidat, O.; Abd-Alhameed, R. A review of indoor localization techniques and wireless technologies. *Wirel. Pers. Commun.* **2021**, *119*, 289–327.
3. Yassin, A.; Nasser, Y.; Awad, M.; Al-Dubai, A.; Liu, R.; Yuen, C.; Raulefs, R.; Aboutanios, E. Recent advances in indoor localization: A survey on theoretical approaches and applications. *IEEE Commun. Surv. Tutor.* **2016**, *19*, 1327–1346. [CrossRef]

4. Wu, Z.; Wu, X.; Long, Y. Multi-Level Federated Graph Learning and Self-Attention Based Personalized Wi-Fi Indoor Fingerprint Localization. *IEEE Commun. Lett.* **2022**, *26*, 1794–1798. [CrossRef]
5. Kumar, A.; Sharma, S.; Goyal, N.; Singh, A.; Cheng, X.; Singh, P. Secure and energy-efficient smart building architecture with emerging technology IoT. *Comput. Commun.* **2021**, *176*, 207–217. [CrossRef]
6. Jang, J.; Hong, S. Indoor Localization with Wi-Fi Fingerprinting Using Convolutional Neural Network. In Proceedings of the 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, Czech Republic, 3–6 July 2018; pp. 753–758.
7. Alhomayani, F.; Mahoor, M.H. Deep learning methods for fingerprint-based indoor positioning: A review. *J. Locat. Based Serv.* **2020**, *14*, 129–200. [CrossRef]
8. Bregar, K.; Mohorcic, M. Improving Indoor Localization Using Convolutional Neural Networks on Computationally Restricted Devices. *IEEE Access* **2018**, *6*, 17429–17441. [CrossRef]
9. Dhiman, P.; Kukreja, V.; Manoharan, P.; Kaur, A.; Kamruzzaman, M.; Dhaou, I.B.; Iwendi, C. A novel deep learning model for detection of severity level of the disease in citrus fruits. *Electronics* **2022**, *11*, 495. [CrossRef]
10. Zhou, M.; Member, S.; Long, Y.; Zhang, W.; Pu, Q. Adaptive Genetic Algorithm-Aided Neural Network with Channel State Information Tensor Decomposition for Indoor Localization. *IEEE Trans. Evol. Comput.* **2021**, *25*, 913–927. [CrossRef]
11. He, S.; Member, S.; Chan, S.G.; Member, S. Wi-Fi Fingerprint-Based Indoor Positioning: Recent Advances and Comparisons. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 466–490. [CrossRef]
12. BelMannoubi, S.; Touati, H. Deep neural networks for indoor localization using WiFi fingerprints. In Proceedings of the Mobile, Secure, and Programmable Networking: 5th International Conference (MSPN 2019), Mohammedia, Morocco, 23–24 April 2019; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; pp. 247–258.
13. Liu, K.; Tian, Z.; Li, Z.; Wang, J.; Zhou, M. HiLoc: Sub-Meter Level Indoor Localization Using a Single Access Point with Distributed Antennas in Wireless Sensor Networks. *IEEE Sens. J.* **2022**, *22*, 4869–4881. [CrossRef]
14. Hsieh, C.; Chen, J.; Nien, B. Deep Learning-Based Indoor Localization Using Received Signal Strength and Channel State Information. *IEEE Access* **2019**, *7*, 33256–33267. [CrossRef]
15. Liu, T.; Zhang, X.; Zhang, H.; Tahir, N.; Fang, Z. A Structure Landmark-Based Radio Signal Mapping Approach for Sustainable Indoor Localization. *Sustainability* **2021**, *13*, 1183. [CrossRef]
16. Yang, B.; Cao, X.; Huang, C.; Yuen, C.; Di Renzo, M. Federated Spectrum Learning for Reconfigurable Intelligent Surfaces-Aided Wireless Edge Networks. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 9610–9626. [CrossRef]
17. Wang, X.; Wang, X.; Mao, S.; Zhang, J.; Periaswamy, S.C.G.; Patton, J. Adversarial Deep Learning for Indoor Localization with Channel State Information Tensors. *IEEE Internet Things J.* **2022**, *9*, 18182–18194. [CrossRef]
18. Li, T.; Wang, H.; Shao, Y.; Niu, Q. Channel state information-based multi-level fingerprinting for indoor localization with deep learning. *Int. J. Distrib. Sens. Netw.* **2018**, *14*, 1550147718806719. [CrossRef]
19. Wu, G.-S.; Tseng, P.-H. A Deep Neural Network-Based Indoor Positioning Method using Channel State Information. In Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 5–8 March 2018; pp. 290–294. [CrossRef]
20. Yang, R.; Yang, X.; Wang, J.; Zhou, M.; Tian, Z.; Li, L. Decimeter Level Indoor Localization Using Wi-Fi. *IEEE Sens. J.* **2022**, *22*, 4940–4950. [CrossRef]
21. Chang, R.Y.; Liu, S.; Cheng, Y. Device-Free Indoor Localization Using Wi-Fi Channel State Information for Internet of Things. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–7.
22. Etiabi, Y.; Chafii, M.; Amhoud, E.M. Federated Distillation based Indoor Localization for IoT Networks. *arXiv* **2022**, arXiv:2205.11440.
23. Khullar, V.; Pal, H. f-FNC: Privacy concerned efficient federated approach for fake news classification. *Inf. Sci.* **2023**, *639*, 119017. [CrossRef]
24. Nilsson, A.; Smith, S.; Ulm, G.; Gustavsson, E.; Jirstrand, M. A performance evaluation of federated learning algorithms. In Proceedings of the Second Workshop on Distributed Infrastructures for Deep Learning (DIDL), Rennes, France, 10–11 December 2018; pp. 1–8.
25. Ghimire, B.; Member, G.S.; Rawat, D.B.; Member, S. Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 8229–8249. [CrossRef]
26. Kim, K.; Lee, S.; Huang, K. A scalable deep neural network architecture for multi-building and multi-floor indoor localization based on Wi-Fi fingerprinting. *Big Data Anal.* **2018**, *3*, 4. [CrossRef]
27. Cesana, M.; Maniezzo, D.; Bergamo, P.; Gerla, M. Interference aware (IA) MAC: An enhancement to IEEE802. 11b DCF. In Proceedings of the 2003 IEEE 58th Vehicular Technology Conference, VTC 2003-Fall (IEEE Cat. No. 03CH37484), Orlando, FL, USA, 6–9 October 2003; Volume 5, pp. 2799–2803. [CrossRef]
28. Wang, X.; Gao, L.; Mao, S. PhaseFi: Phase Fingerprinting for Indoor Localization with a Deep Learning Approach. In Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–6. [CrossRef]

29. Wang, X.; Gao, L.; Mao, S.; Pandey, S. DeepFi: Deep learning for indoor fingerprinting using channel state information. In Proceedings of the 2015 IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, USA, 9–12 March 2015; pp. 1666–1671. [CrossRef]
30. Arafeh, M.; Hammoud, A.; Otrok, H.; Mourad, A.; Talhi, C.; Dziong, Z. Independent and Identically Distributed (IID) Data Assessment in Federated Learning. In Proceedings of the GLOBECOM 2022—2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 4–8 December 2022; pp. 293–298. [CrossRef]
31. Jeong, M.; Won, S.; Kim, S. A tutorial on Federated Learning methodology for indoor localization with non-IID fingerprint databases. *ICT Express*, 2023, *in press*. [CrossRef]
32. Zhu, H.; Xu, J.; Liu, S.; Jin, Y. Federated Learning on Non-IID Data: A Survey. *Neurocomputing* **2021**, *465*, 371–390. [CrossRef]