Journal of Computers Vol. 37 No. 5, October 2026, pp. 89-105
https://doi.org/10.63367/19911599202610370500 7

A Differentially Private Stacked Denoising Autoencoder-Based Fingerprint Localization Model in a Cloud Environment

Xuejun Zhang*, Hui Chen, and Chengze Li

School of Electronic and Information Engineering, Lanzhou Jiaotong University,
Lanzhou 730070, China

xuejunzhang@lzjtu.edu.cn

Received 29 June 2025; Revised 5 February 2026; Accepted 13 February 2026

Abstract. Indoor localization services in cloud environments face two key challenges: protecting user location privacy during crowdsourced Wi-Fi fingerprint sharing and maintaining localization accuracy when learning from high-dimensional and noise-perturbed received signal strength (RSS) data. To address these challenges, this paper proposes DP-SLocCE, a differentially private fingerprint-based indoor localization framework built on stacked denoising autoencoders. The proposed framework adopts shuffled differential privacy to provide user-level privacy protection during data transmission, while leveraging stacked denoising autoencoders to perform robust feature extraction and progressive dimensionality reduction from noisy RSS fingerprints. Extensive experiments on three real-world indoor localization datasets demonstrate that, under differential privacy constraints, DP-SLocCE consistently outperforms mainstream deep learning models in localization accuracy. Moreover, in high-dimensional scenarios, it achieves accuracy comparable to CNN-based approaches while significantly reducing training and testing time, highlighting its practicality for cloud-based indoor localization services.

Keywords: indoor localization, stacked denoising autoencoder, differential privacy, dimensionality reduction, deep learning, cloud environment, privacy protection, RSS fingerprinting

1 Introduction

The rapid development and widespread adoption of positioning technologies such as BeiDou and GPS have significantly enriched location-based services (LBS), greatly enhancing the convenience of daily life. However, GPS signals are highly susceptible to attenuation and blockage in complex indoor environments, which makes such technologies unsuitable for a wide range of indoor positioning applications [1]. In recent years, diverse wireless signal–based indoor localization techniques have been developed to satisfy the growing demand for accurate and robust indoor localization [3]. Among these approaches, Wi-Fi fingerprint-based localization using received signal strength (RSS) has attracted significant academic and industrial interest due to its cost-effectiveness, ease of deployment, and broad coverage, supported by the near-ubiquitous presence of Wi-Fi and Bluetooth access points in indoor environments [4].

Most existing fingerprint localization systems adopt a cloud-centric architecture, where user-collected RSS fingerprints are uploaded to cloud servers, which compute location estimates based on pre-established mappings between RSS patterns and physical coordinates [3]. To improve localization accuracy and reduce the cost and complexity of building fingerprint databases, researchers have proposed deep learning-based localization models [6, 9], which leverage large-scale labeled RSS datasets to train highly expressive and robust predictors.

However, collecting large-scale, high-quality RSS fingerprint data is labor-intensive and costly, which often exceeds the capabilities of a single service provider. To mitigate this challenge, crowdsourcing has emerged as a promising solution, allowing public users to contribute fingerprint data using standard mobile devices at minimal cost. Despite its advantages, crowdsourced RSS data often contains sensitive information, such as user identity and precise location. Uploading such data directly to untrusted cloud servers for model training or inference poses significant privacy risks [10-11, 26]. Consequently, privacy protection has become a critical barrier to the large-scale deployment of fingerprint-based indoor localization systems.

Current privacy-preserving techniques for user data primarily fall into two categories: homomorphic

* Corresponding Author

encryption [12-13] and differential privacy [14-15]. Homomorphic encryption enables computation directly on encrypted data; however, it incurs substantial computational overhead, particularly as the dataset size increases. Differential privacy protects user data by injecting randomized noise, but it comes in two main variants: centralized differential privacy (CDP), which assumes a trusted server, and local differential privacy (LDP), which eliminates trust assumptions but typically leads to significant degradation in data utility. To address this trade-off, Shuffled Differential Privacy (SDP) [16-17] has been proposed as an intermediate solution. This shuffling process effectively decouples individual users from their data, thereby enhancing privacy guarantees and mitigating identity linkage risks posed by adversaries.

Moreover, Wi-Fi RSS fingerprints are inherently susceptible to multipath propagation, environmental dynamics, and differential privacy-induced noise, all of which can degrade localization accuracy [8, 18]. In large-scale indoor environments such as airports, the number of deployed access points (APs) can reach into the hundreds or even thousands, resulting in extremely high-dimensional RSS vectors [19]. This high dimensionality poses significant challenges to model training, efficiency and system scalability.

The above observations give rise to a fundamental research problem: how to achieve accurate and efficient RSS fingerprint-based indoor localization in cloud environments while providing strong user-level privacy protection under crowdsourced data collection. On the one hand, privacy-preserving mechanisms such as differential privacy inevitably introduce noise that distorts RSS fingerprints and degrades localization performance. On the other hand, the high dimensionality of RSS data caused by dense access point deployment significantly increases training complexity and sensitivity to noise. Existing solutions often address these challenges in isolation, which limits their effectiveness in practical cloud-based localization systems.

While conventional filtering (e.g., Kalman or particle filters) and machine learning techniques (e.g., SVM and KNN) can partially address signal noise and device heterogeneity, they fall short in handling high-dimensional data and achieving scalable accuracy in complex indoor environments. By contrast, deep learning offers superior capabilities for extracting meaningful features from noisy, high-dimensional RSS fingerprints and learning complex signal patterns, even under privacy perturbation.

To address the aforementioned challenges, we propose DP-SLocCE, a cloud-oriented fingerprint localization model that jointly integrates shuffled differential privacy and stacked denoising autoencoders to achieve a practical balance between privacy protection, localization accuracy, and computational efficiency. This model integrates SDP and SDAE to simultaneously preserve user privacy and reduce the dimensionality of RSS fingerprint data. In particular, the SDP mechanism perturbs RSS fingerprints prior to cloud transmission, thereby mitigating the risk of privacy leakage during data sharing. Simultaneously, a multi-layer SDAE is employed to perform progressive dimensionality reduction and deep feature extraction, improving model robustness against high-dimensionality, environmental dynamics, and privacy-induced noise. The main contributions of this paper are summarized as follows:

(1) This study addresses privacy risks arising from crowdsourced RSS fingerprint sharing in cloud environments by incorporating shuffled differential privacy, in which a shuffler is used to decouple users from their perturbed fingerprints. This design provides stronger user-level privacy protection than conventional local randomization while maintaining data utility for downstream localization tasks.

(2) A SDAE-based deep localization model is proposed to enhance feature extraction from noisy RSS data. This model addresses the challenge of high-dimensional RSS fingerprints by performing hierarchical dimensionality reduction and robust representation learning, thereby enabling efficient training and scalable system deployment.

(3) Extensive experiments conducted on three real-world indoor RSS fingerprint datasets demonstrate that, compared with mainstream localization models such as MLP, DNN, and AE+DNN, the proposed DP-SLocCE achieves superior localization accuracy while effectively preserving data privacy. Furthermore, in high-dimensional scenarios, DP-SLocCE significantly reduces training and testing time compared to CNN-based models, confirming its computational efficiency, real-time responsiveness, and scalability in practical applications.

The remainder of this paper is organized as follows. Section 2 reviews related work on fingerprint-based localization, deep learning-based localization, and privacy-preserving indoor localization. Section 3 introduces the preliminary knowledge related to differential privacy, denoising autoencoders, and the shuffling mechanism. Section 4 presents the proposed DP-SLocCE framework and algorithmic details. Section 5 provides the security analysis. Section 6 reports experimental results and performance evaluations on real-world datasets. Finally, Section 7 concludes the paper and discusses future research directions.

2 Related Work

Indoor localization has been extensively studied over the past decades, particularly in the context of wireless fingerprinting and learning-based positioning systems. We further highlight the limitations of existing approaches and clarify the research gap addressed in this paper.

2.1 Fingerprint-Based Indoor Localization

Fingerprint-based indoor localization is one of the most widely adopted approaches due to its robustness against complex indoor environments and its compatibility with existing wireless infrastructures. A large body of research has investigated improvements in fingerprint construction, signal preprocessing, and matching strategies to enhance localization accuracy and robustness [2-3, 5-6]. However, the performance of fingerprint-based localization is highly dependent on the quantity and quality of collected RSS data. Moreover, traditional fingerprint-based systems typically assume centralized data collection and processing, which raises scalability and privacy concerns when deployed in cloud environments with crowdsourced data sources.

2.2 Deep Learning-Based Localization Models

Deep learning techniques have been widely introduced into fingerprint-based indoor localization to overcome the limitations of traditional machine learning methods. Models based on multilayer perceptrons (MLP), deep neural networks (DNN), convolutional neural networks (CNN), and autoencoder-based architectures have demonstrated strong capability in learning complex mappings between RSS fingerprints and physical locations [6-7, 9, 19]. Among these approaches, CNN-based models exploit spatial correlations in RSS data and often achieve high localization accuracy, particularly in dense deployment scenarios. Autoencoder-based models, including AE+DNN architectures, have been employed to perform dimensionality reduction and feature compression prior to localization, thereby improving training efficiency.

Nevertheless, most existing deep learning-based localization models are designed under the assumption that training and inference data are clean and centrally available. Their performance may degrade significantly when RSS data are perturbed by noise, especially noise introduced by privacy-preserving mechanisms. In addition, CNN-based models often incur substantial computational overhead, which limits their suitability for real-time cloud-based localization services.

2.3 Privacy-Preserving Indoor Localization

With the increasing adoption of crowdsourced fingerprint collection and cloud-based localization services, protecting user location privacy has become a critical research issue. Existing privacy-preserving indoor localization studies can be broadly categorized into cryptography-based approaches and differential privacy-based approaches. In cloud-based fingerprint localization, existing studies face significant challenges in providing strong user-level privacy protection while maintaining accurate and robust learning from high-dimensional, noise-sensitive RSS fingerprints, especially when privacy randomization distorts feature distributions.

Cryptography-based methods, such as homomorphic encryption and secure multi-party computation, enable computation on encrypted RSS data without revealing raw fingerprints [12-13]. Although these techniques provide strong privacy guarantees, they often introduce significant computational and communication overhead, which hinders their practical deployment in large-scale indoor localization systems.

Differential privacy (DP) has emerged as a lightweight and theoretically grounded alternative by injecting randomized noise [14-15, 26]. Most existing DP-based localization methods adopt either centralized differential privacy (CDP), which relies on a trusted server, or local differential privacy (LDP), which removes trust assumptions at the cost of substantial utility degradation. Recent studies have also explored DP in federated learning and crowdsourced localization scenarios [8-9], but they often suffer from accuracy loss when dealing with high-dimensional RSS data.

SDP has been proposed as an intermediate privacy model that achieves privacy amplification by randomly permuting locally perturbed data before server-side processing [16-17, 28]. SDP provides stronger user-level privacy guarantees than standard LDP while maintaining higher data utility. However, SDP-related studies

mainly focus on theoretical analysis or generic machine learning tasks, with limited attention to fingerprint-based indoor localization. More importantly, existing localization-oriented works rarely co-design privacy protection and robustness-oriented representation learning under the SDP model for high-dimensional RSS fingerprints in cloud settings. These aspects are summarized in Table 1 to illustrate how representative methods address privacy protection, high-dimensional RSS handling, and cloud-oriented deployment.

Table 1. Comparison of representative indoor localization methods

Method	Learning model	Privacy mechanism	High-dimensional RSS handling	Cloud-oriented deployment
Traditional Fingerprinting	KNN / SVM	None	Not considered	Not considered
AE+DNN-based Localization	AE + DNN	None	Partially addressed	Partially addressed
CNN-based Localization	CNN	None/LDP	Partially addressed	Not considered
DP-based Localization	DNN	CDP/LDP	Not considered	Partially addressed
DP-SLocCE (This Work)	SDAE	SDP	Explicitly considered	Explicitly considered

The key research problem addressed in this paper is to jointly achieve strong user-level privacy protection under the shuffled model and robust feature learning for high-dimensional RSS fingerprints in cloud-based indoor localization. Existing methods typically emphasize either privacy preservation or representation learning in isolation, which motivates the co-design of SDP and SDAE in DP-SLocCE.

3 Preliminary Knowledge

3.1 Differential Privacy

Definition 1 - Differential Privacy [20]:

Given two adjacent datasets D and D', which differ by at most one element $|D \oplus D'| = |D \cup D'| - |D \cap D'| = 1$, and a randomized algorithm M, let $\mathfrak{R}$ denote the set of all possible outputs of M. Here, $\oplus$ denotes the symmetric difference between two datasets, and $|D \oplus D'|$ indicates that D and D' differ in all records contributed by exactly one user. The algorithm M is said to provide ε-differential privacy if for all $S \subset \mathfrak{R}$, the following inequality holds:

$$\Pr[M(D) \in S] \leq e^{\varepsilon \times |D' \oplus D|} \times \Pr[M(D') \in S] \quad (1)$$

Here, ε is the privacy budget, which controls the degree of privacy: the smaller the ε, the stronger the privacy guarantee. The probability is taken over the internal randomness of the mechanism M.

Definition 2 — Laplace Mechanism [8]:

The Laplace mechanism achieves differential privacy by generating and adding Laplace noise to the original data, thereby ensuring that the perturbed results satisfy differential privacy and protect individual information. Given a query function g: $D \to \mathbb{R}^d$, let $\mathbb{R}$ denote the mapped real-valued space, and d be the query dimension of function g. Then, the algorithm g' is defined as:

$$g'(D) = g(D) + Lap(\Delta g / \varepsilon) \quad (2)$$

The $l1$-sensitivity of g is defined as $\Delta g = \max_{D,D' adjacent} \|g(D) - g(D')\|_1$, where $\|\cdot\|_1$ denotes the $l1$ norm. and $Lap(\Delta g/\varepsilon)$ denotes the random noise drawn from a Laplace distribution. For d-dimensional queries, $Lap(\Delta g/\varepsilon)$ denotes a vector whose elements are independently sampled from a Laplace distribution with scale $\Delta g/\varepsilon$.

Definition 3 — ε-Shuffled Differential Privacy [16]:

Let $M = (R, H)$ be a shuffled mechanism, where each user perturbs their data using mechanism $R : D \to \mathfrak{R}$. Let $H(M)$ denote the shuffled output, and let its range be $\mathfrak{R}'$. If $H(M)$: $\mathfrak{R} \to \mathfrak{R}'$ satisfies ε-differential privacy, then M satisfies ε-shuffled differential privacy:

$$Pr[H(M) \in \mathfrak{R}'] \leq e^{\varepsilon} \times Pr[H(M') \in \mathfrak{R}'] \quad (3)$$

where H denotes the shuffler, R represents the local randomization mechanism, and ε is the privacy budget. Equation (3) holds for any pair of adjacent datasets D and D' and for any measurable subset of the shuffled output space.

Theorem 1 — Post-processing Property:

Suppose that a randomized algorithm $M(D)$ satisfies ε-differential privacy. Then any algorithm $F(M(D))$ that post-processes the output of $M(D)$ also satisfies ε-differential privacy. Here, $F(\cdot)$ denotes any (possibly randomized) function mapping from the output space of M to an arbitrary output space.

3.2 Denoising Autoencoder Deep Neural Network

An Autoencoder (AE) [21] is a type of neural network designed to extract hidden features from input data and reconstruct the original information, thereby obtaining efficient feature representations. The encoder compresses the input into a latent representation whose dimensionality is smaller than that of the original input, making the autoencoder inherently capable of dimensionality reduction.

A Denoising Autoencoder (DAE) [22] is a variant of AE that takes corrupted data as input and is trained to predict the original, uncorrupted data as output. By encoding and decoding perturbed inputs, the DAE preserves underlying semantic features, thereby enhancing robustness against noise and environmental variation.

3.3 Shuffling Mechanism

The core of the shuffling mechanism lies in aggregating and randomizing user-uploaded data to break the direct association between users and their data records. Assume there are n users, each submitting one data item. The collected data set on the server side is denoted as:

$$D = \{x_1, x_2, ..., x_n\} \tag{4}$$

For simplicity, although curly braces are used, datasets are treated as ordered sequences when applying the shuffling operation.

The shuffling process applies a uniformly random permutation function π to reorder the data, producing a new sequence:

$$D^{'} = \{x_{\pi(1)}, x_{\pi(2)}, ..., x_{\pi(n)}\} \tag{5}$$

Here, π is a random bijection selected uniformly from all permutations of the index set $\{1,2,\ldots,n\}$, i.e., π: $\{1, 2, ..., n\} \rightarrow \{1, 2, ..., n\}$. Under the differential privacy setting, each user locally perturbs their data using a randomized mechanism before uploading. The resulting data received by the server becomes:

$$Z = \{z_1, z_2, ..., z_n\}, z_i = Noise(x_i) \tag{6}$$

The $Noise(\cdot)$ function corresponds to the local randomization mechanism R defined in Definition 3, which is instantiated as Laplace perturbation in our implementation.

The shuffler finally reorders the perturbed dataset:

$$Z^{'} = \{z_{\pi(1)}, z_{\pi(2)}, ..., z_{\pi(n)}\} \tag{7}$$

Since the server cannot identify which perturbed record originates from which user, this mechanism further amplifies privacy at the user level. This phenomenon is formally known as shuffle amplification.

The shuffling mechanism adopted in this work is based on the SDP framework, which aims to balance privacy protection and data utility. Prior studies have demonstrated that SDP provides favorable trade-offs in both theoretical guarantees and empirical performance. Cheu et al. [27] and Balle et al. [28]. show that shuffling has only a limited impact on data structure and does not significantly degrade the learning performance of downstream models. Moreover, the computational overhead introduced by shuffling is confined to lightweight preprocessing on the client side, making SDP practical for privacy-sensitive machine learning applications.

4 The DP-SLocCE Method

4.1 System Architecture

To effectively balance RSS fingerprint privacy, model accuracy, training efficiency, and real-time localization responsiveness, we propose a Differentially Private Stacked Denoising Autoencoder-based Fingerprint Localization Model for Cloud Environments (DP-SLocCE). The design comprehensively considers multiple factors, including RSS fingerprint privacy protection, the high dimensionality of RSS features, model performance, and computational overhead.The overall system architecture of DP-SLocCE is depicted in Fig. 1.

The proposed architecture comprises three key entities: multiple terminal users, a shuffler, and a cloud server. To access cloud-based localization services, users measure RSS fingerprint data corresponding to their current physical locations and voluntarily contribute these data to the cloud server. Since RSS fingerprints are closely linked to personal identity and location privacy, directly sharing such data poses significant privacy risks. To mitigate these risks, each user first applies a local differential privacy mechanism to locally perturb their RSS data. Subsequently, a shuffler is employed to break the linkage between users and their perturbed fingerprints. This two-stage privacy mechanism effectively prevents semi-trusted cloud servers or external attackers from associating RSS data with specific individuals. After the shuffled and privatized data are uploaded, the cloud server leverages an SDAE-based localization model to perform hierarchical dimensionality reduction and extract robust features. This enables efficient model training while supporting real-time localization services under strict privacy-preserving constraints.

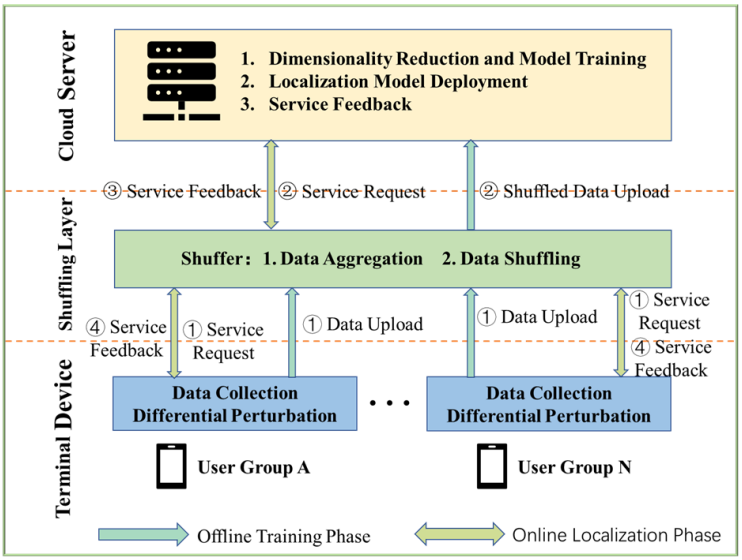


Fig. 1. System architecture

4.2 DP-SLocCE Algorithm

Offline Training.

a. Data Collection and Perturbation.

Each user collects RSS fingerprint data within their respective physical region to construct a dataset denoted as X. After data preprocessing, the fingerprint data are transformed into a set of feature vectors $X_i^c = \{(x_i^c, y_i^c) | i = 1, 2, 3, ..., N\}$. Let N represent the set of participating users, x_i^c denote the fingerprint feature vector of the i-th user, and y_i^c denote the corresponding location label of the feature vector. To utilize the localization service, each user submits X_i^c to the cloud server for localization model training. Considering that the cloud server is semi-trusted, directly sharing raw data may lead to privacy leakage. Therefore, before uploading RSS fingerprint features to

the cloud, users employ Shuffled Differential Privacy to perturb their respective RSS fingerprint feature sets by adding appropriate random noise X_i^c to $Lap(\Delta g/\varepsilon)$, in order to achieve differential privacy protection.

This mechanism breaks the correspondence between users and their submitted records, while preserving the correspondence between each RSS fingerprint feature vector x_i^c and its location label y_i^c. The perturbed data are then uploaded to a shuffler for aggregation and permutation. The obfuscated RSS fingerprint features are denoted as $(x_i^{c'}, y_i^c)$, and $x_i^{c'}$ can be expressed as:

$$x_i^{c'} = x_i^c + Lap(\Delta g / \varepsilon) \tag{8}$$

where $Lap(\cdot)$ is a controllable random noise drawn from a Laplace distribution, and ε is the privacy budget, which balances the trade-off between privacy strength and data utility. The sensitivity Δg defines the upper bound of the noise scale required for differential privacy, and in this paper, it is computed using the Manhattan distance, given by: $\Delta g = \max \mid g(x_i^c) - g(x_j^c) \mid_1$. In this work, the query function g is instantiated as the identity function on the RSS fingerprint vector. Each RSS dimension is clipped to a bounded range before perturbation, ensuring a finite $l1$-sensitivity.

b. Shuffling of Noisy Data by the Shuffler.

After receiving the perturbed data $(x_i^{c'}, y_i^c)$ uploaded by the crowdsourced users, the shuffler aggregates these data into a unified dataset (X_i, Y_i). The shuffler then applies a random permutation to (X_i, Y_i), producing the shuffled dataset (X'_i, Y'_i). This shuffling process severs the association between users and their data, thereby obfuscating user identities from both semi-trusted cloud servers and malicious adversaries. The shuffled data (X'_i, Y'_i) are subsequently forwarded to the cloud server for localization model training. The shuffling operation is expressed as:

$$(X_i', Y_i') = Shuffler(X_i, Y_i) \tag{9}$$

where Shuffler [16-17] is a module capable of performing random permutation to disrupt the correspondence between users and their RSS fingerprint data.

c. Data Denoising, Dimensionality Reduction, and Model Training on the Cloud Server

Upon receiving the shuffled and noised RSS fingerprint data (X'_i, Y'_i) from the shuffler, the cloud server utilizes the proposed SDAE-based deep localization model to perform denoising, dimensionality reduction, and feature extraction on the dataset (X'_i, Y'_i), thereby enabling effective training of the localization model. The overall structure of the SDAE network is illustrated in Fig. 2.

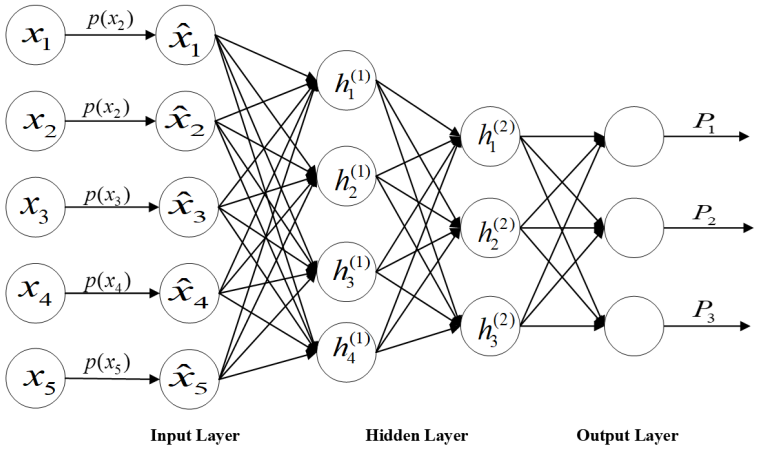


Fig. 2. Stacked-Denoising-Autoencoder deep network

To implement the denoising and progressive dimensionality reduction strategy described above, we design a SDAE-based deep localization model consisting of two denoising autoencoders followed by a classifier. The

first denoising autoencoder is composed of three fully connected layers and is responsible for initial feature transformation of the shuffled and noise-perturbed RSS fingerprints. Its primary role is to suppress unstable signal components and reduce the original feature dimensionality to a compact intermediate representation. Building upon this representation, the second denoising autoencoder, which consists of five fully connected layers, performs deeper feature abstraction and further dimensionality compression. This hierarchical encoding structure enables the model to progressively extract discriminative features while mitigating the negative impact of privacy-induced noise. The two-stage encoder depth (a 3-layer encoder followed by a 5-layer encoder) is adopted to balance representation capacity and training stability under noisy inputs, avoiding unnecessary network depth that would increase computational overhead without yielding significant accuracy gains. Finally, a classifier with a Softmax activation function is employed to map the learned low-dimensional features to location labels and complete the localization task. All layers in the denoising autoencoders use the ReLU activation function. The detailed layer configurations and parameter settings are summarized in Tables 2, Table 3, and Table 4.

The proposed SDAE offers two key advantages: (1) It can eliminate dependencies among input data, thereby enabling more effective extraction of localization-related features. (2) It maintains robust and stable outputs even when the input data are subjected to noise perturbations. Experimental results demonstrate that the proposed SDAE exhibits strong feature extraction capabilities and shows significant advantages in handling high-dimensional data.

Table 2. Denoising-Autoencoders 1 parameters

Layer (type)	Output shape	Param
Dense_1 (Dense)	(None, 256)	9216
dense_2 (Dense)	(None, 256)	65792
dense_3 (Dense)	(None, 12)	3084
Total parameters: 78,092		

Table 3. Denoising-Autoencoders 2 parameters

Layer (type)	Output shape	Param
dense_4 (Dense)	(None, 128)	1664
dense_5 (Dense)	(None, 128)	16512
dense_6 (Dense)	(None, 128)	16512
Dropout_1 (Dropout)	(None, 128)	0
dense_7 (Dense)	(None, 10)	1290
Total parameters: 35,978		

Table 4. Stacked-Denoising-Autoencoder positioning model

Layer (type)	Output shape	Param
flatten_1 (Flatten)	(None, 35)	0
sequential_2 (Sequential)	(None, 12)	78092
sequential_3 (Sequential)	(None, 10)	35978
dense_8 (Dense)	(None, 10)	110
Total parameters: 114,180		

Online Localization.

a. Users first utilize their terminal devices to obtain the RSS fingerprint data of their current location. Before transmission, each user adds appropriate random noise to the data to achieve differential privacy protection, and then uploads the privacy-preserved RSS data to the shuffler.

b. The shuffler performs random permutation using the Shuffler tool, thereby severing the association between users and their data. The shuffled RSS fingerprint data are then uploaded to the cloud server.

c. The cloud server uses the pre-trained SDAE-based deep localization model and the received shuffled, noisy RSS data to predict the actual location of users. The predicted locations are then sent back to the shuffler.

d. The shuffler maps the predicted locations to the corresponding users based on the pre-shuffling relationship and returns the final localization results to each user.

5 Security Analysis

Proof: Let the privacy budget be denoted by ε, and let D be the fingerprint dataset collected by the user. The randomized algorithm $M : D \rightarrow \Re$ operates on D. According to the definition of differential privacy, we have:

$$\forall r \in \Re, Pr[M(D) = r] \leq e^{\varepsilon \times |D \oplus D'|} \times Pr[M(D') = r],$$

This means that the process of uploading RSS fingerprint data to the cloud server satisfies the definition of ε-differential privacy.

To analyze the process of uploading RSS fingerprint data to the server, let us consider a scenario where $\forall i \in \{1, 2, ..., N\}$, each participating user P_i owns a dataset D_i. Let each user's randomized algorithm $M_i : D_i \rightarrow \Re$ satisfy ε-differential privacy.

Assume that the outputs of any two algorithms M_i and M_j are independent. Based on the definition, we have:

$$Pr[M_i(D_i) = r_i] \leq e^{\varepsilon_i} \times Pr[M_i(D'_i) = r_i], \forall r_i \in \Re$$

Define a composed mechanism: $M = \prod_{i=1}^{N} M_i$, if each M_i satisfies ε-differential privacy, then:

$$M = \{M_1, M_2, ..., M_N\}$$

Let the joint output of the mechanism be $O = \{r_1, r_2, \ldots, r_N\}$. Since the randomized algorithms M_i are mutually independent, we have:

$$\forall O \subset \Re, Pr[M(D) = O] = \prod_{i=1}^{N} Pr[M_i(D_i) = r_i]$$

From the condition $|R \oplus S| \in \mathbb{N}$, we know that in the entire neighboring dataset collection $| D_i \oplus D'_i |$, $i \in \{1, 2, ..., N\}$, only one dataset satisfies $| D_i \oplus D'_i | = 1$, while all other neighboring datasets satisfy $| D_i \oplus D'_i | = 0$, where $j \neq i$. Therefore, for any output $\forall O \subset \Re$, we have:

$$\begin{aligned} &Pr[M(D) = O] = \prod_{i=1}^{N} Pr[M_i(D_i) = r_i] \leq \prod_{i=1}^{N} e^{\varepsilon_i \times |D_i \oplus D'_i|} \times Pr[M_i(D'_i) = r_i] \\ &\leq e^{\varepsilon_i \times |D_i \oplus D'_i|} \times \sum_{i=1}^{N} Pr[M_i(D'_i) = r_i] \leq e^{\varepsilon_i} \times Pr[M(D') = O]. \end{aligned}$$

Equality holds only if $\varepsilon \geq \varepsilon_i$, hence: $Pr[M(D) = O] = e^{\varepsilon} \times Pr[M(D') = O]$. Thus, we obtain:

$$\varepsilon = \min\{\varepsilon \mid \varepsilon \geq \varepsilon_i, 1 \leq i \leq N\} = \min\{\varepsilon \mid \varepsilon \geq \max_{1 \leq i \leq N} \varepsilon_i\} = \max_{1 \leq i \leq N} \varepsilon_i,$$

Therefore, the randomized mechanism M satisfies $(\max_{1 \leq i \leq N} \varepsilon_i)$-differential privacy, which completes the proof. According to Theorem 1 (Post-Processing Invariance), the fingerprint data perturbed by differential privacy (DP) noise will continue to satisfy the differential privacy guarantee throughout subsequent computations. Hence, the transmission, sharing, and application of RSS fingerprint data in the proposed DP-SLocCE model comply with the formal definition of differential privacy. As a result, the Stacked Denoising Autoencoder-based deep localization model trained using such data is differentially private.

6 Experimental Results and Analysis

6.1 Datasets and Parameter Settings

The experiments were conducted using two collected datasets, Mall-WiFi [23] and Mall [24], as well as the public dataset UJIIndoorLoc [25]. Each sample in the Mall-WiFi dataset consists of one region ID and 35-dimensional Wi-Fi signal features. Each sample in the Mall dataset contains one region ID, 35-dimensional Wi-Fi features, and 22-dimensional Bluetooth RSS features. In the UJIIndoorLoc dataset, each sample includes a floor ID and 520-dimensional Wi-Fi signal features. The datasets were split into 90% for training and 10% for testing.

Software and hardware environment: The model was implemented using TensorFlow with the Adam optimizer, a learning rate of 0.001, 600 training epochs, and a batch size of 32. The experiments were conducted on a machine equipped with an Intel(R) Core(TM) i5-8250U CPU @ 1.60 – 1.80GHz and 16.0 GB RAM.

6.2 Performance and Efficiency Analysis of DP-SLocCE

To evaluate the performance and efficiency of the proposed DP-SLocCE method, extensive experiments were conducted on the Mall-WiFi, Mall, and UJIIndoorLoc datasets. Comparisons were made with the following baseline deep learning models: DNN [6], MLP [7], CNN [8], and AE+DNN(without privacy protection) [9]; their corresponding differential privacy-enhanced versions, including DP+DNN, DP+MLP, DP+CNN, and DP+AE+DNN; and SLocCE, a version of our model architecture without privacy protection. Component-wise insights regarding the roles of the privacy mechanism (SDP) and the representation learning module (SDAE) are discussed together with the experimental comparisons in the following subsections.

Impact of Different Privacy Budgets on DP-SLocCE. To protect user privacy, the proposed model adopts the differential privacy mechanism introduced in Section 3.1, where a Laplace mechanism is applied to perturb the RSS fingerprint data. The privacy budget ε determines the magnitude of the added noise: smaller values of ε result in stronger privacy protection but introduce more noise, leading to higher data distortion; conversely, larger values provide better data utility but weaker privacy guarantees.

As such, the setting of ε directly influences both feature extraction effectiveness and localization accuracy. Table 5 presents the performance of the proposed DP-SLocCE model on the Mall-WiFi dataset under different values of ε. According to prior research [8], data with richer features is less vulnerable to privacy leakage, while low-dimensional data is more sensitive and benefits more from differential privacy protection. Given that the Mall-WiFi dataset contains only 35-dimensional features, its limited expressiveness makes it particularly suitable for sensitivity analysis.

Table 5. Model performance under different privacy budgets

ε	Training accuracy (%)	Testing accuracy (%)
0.5	92.18	61.22
1.0	93.34	78.61
1.5	95.74	86.29
2.0	**96.33**	**92.88**
3.0	96.56	93.03
4.0	96.19	93.85
5.0	96.25	95.31

As shown in Table 5, when $\varepsilon \geq 2$, the model maintains high accuracy and effectively extracts stable features from perturbed RSS data. However, when $\varepsilon < 2$, the performance of the model degrades significantly, indicating that excessive noise severely distorts fingerprint structures and impairs localization precision. Notably, at $\varepsilon = 2$, the model achieves an optimal trade-off between privacy protection and localization performance. Therefore, a privacy budget of $\varepsilon = 2$ is adopted in all subsequent experiments to balance privacy guarantees and model practicality.

Model Accuracy and Time Overhead on the Mall-WiFi Dataset. The localization model training and testing accuracy on the low-dimensional Mall-WiFi dataset are illustrated in Fig. 3 and Fig. 4, respectively. As shown in the figures, the models begin to converge after approximately 400 training epochs, and both training and testing accuracy become relatively stable. The training accuracies of models without privacy protection, including CNN, AE+DNN, DNN, MLP, and SLocCE, were 92.25%, 88.59%, 70.66%, 69.30%, and 97.67%, respectively. The corresponding testing accuracies were 95.29%, 85.86%, 66.43%, 63.86%, and 94.43%. Compared with other models, SLocCE improved training accuracy by 5.42%, 9.08%, 27.01%, and 28.37%, respectively, while achieving comparable testing accuracy to CNN and higher testing accuracy gains of 8.57%, 28.00%, and 30.57% over AE+DNN, DNN, and MLP, respectively, demonstrating its strong capability in extracting RSS features and achieving high localization performance.

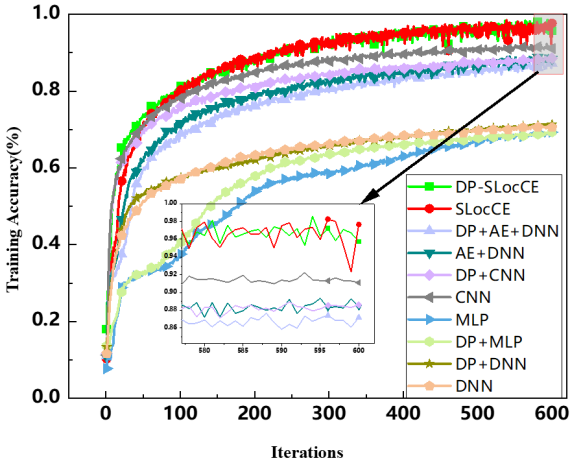


Fig. 3. Comparison of training accuracy on the Mall-WiFi

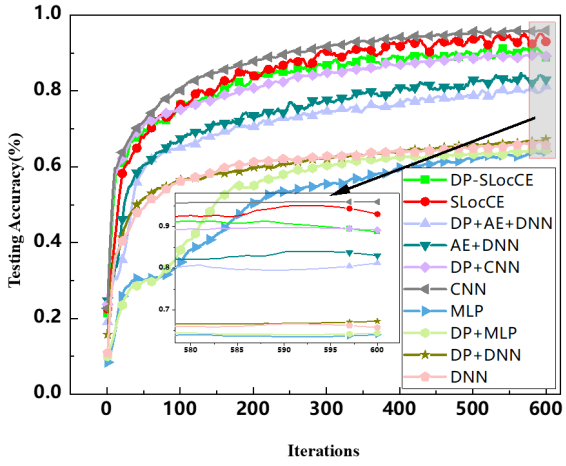


Fig. 4. Comparison of testing accuracy on the Mall-WiFi

For models with differential privacy protection, the training accuracies of DP+CNN, DP+AE+DNN, DP+DNN, DP+MLP, and DP-SLocCE were 88.60%, 87.14%, 71.35%, 69.33%, and 96.33%, respectively. Their testing accuracies were 89.52%, 81.57%, 67.03%, 64.24%, and 92.88%. Compared to other privacy-preserving models, DP-SLocCE improved training accuracy by 7.73%, 9.19%, 24.98%, and 27.00%, and testing accuracy by 3.36%, 11.31%, 25.85%, and 28.64%, respectively. This isolates the effect of representation learning under identical differential privacy constraints, indicating that DP-SLocCE achieves superior localization accuracy

compared with other privacy-preserving models owing to its optimized stacked denoising autoencoder, which enables progressive dimensionality reduction and robust feature extraction. Fig. 3 and Fig. 4 also show that, compared to SLocCE (w/o SDP), DP-SLocCE yields only minor reductions of 1.34% (training) and 1.55% (testing) while providing privacy protection. This indicates that SDAE-based denoising and progressive compression effectively mitigate DP-induced perturbations, thereby preserving localization accuracy.

To further validate the efficiency of DP-SLocCE, we compare its time overhead with that of other models. Time overhead includes data preprocessing time, training time, and testing time. The detailed results are presented in Table 6.

Table 6. Comparison of time performance on the Mall-WiFi

Method name	Data preprocessing (s)	Training time (s)	Testing time (s)
CNN	0.2434	511.3686	0.0269
DP+CNN	9.7317	508.4081	0.0239
AE+DNN	0.2256	208.5098	0.0128
DP+AE+DNN	9.5132	222.8390	0.0150
DNN	0.2185	200.2723	0.0110
DP+DNN	9.2427	202.3856	0.0120
MLP	0.2215	203.2930	0.0150
DP+MLP	9.2868	213.8033	0.0141
SLocCE	**0.2651**	**326.1676**	**0.0159**
DP-SLocCE	**9.4013**	**327.9594**	**0.0199**

As shown in Table 6, localization models incorporating differential privacy (DP) incur significantly higher preprocessing time than those without DP protection. This increase is primarily due to the computational cost associated with generating and adding noise to the RSS data. Among all evaluated models, CNN and DP+CNN exhibit the highest training and testing times, which is attributed to the computational complexity of convolutional operations. In contrast, DNN and DP+DNN demonstrate the lowest execution times, likely due to their relatively simple network architecture. Models such as AE+DNN, DP+AE+DNN, MLP, and DP+MLP exhibit similar levels of training and testing overhead, all slightly lower than SLocCE and DP-SLocCE. However, these baseline models deliver lower localization accuracy compared to SLocCE and DP-SLocCE. Specifically, compared to CNN, the SLocCE model reduces training and testing time by 36.22% and 40.89%, respectively. Likewise, DP-SLocCE reduces training and testing time by 35.49% and 16.74% compared to DP+CNN, while maintaining comparable accuracy. This efficiency can be largely attributed to the dimensionality reduction performed by the stacked denoising autoencoder architecture, which compresses high-dimensional RSS features and accelerates model convergence. In summary, the proposed DP-SLocCE model strikes a better balance among data privacy, localization accuracy, and computational efficiency, offering a reliable and low-latency solution for privacy-preserving indoor localization.

Model Accuracy and Time Overhead on the Mall Dataset. To better balance localization performance and model efficiency on the low-dimensional Mall dataset, the DP-SLocCE model first reduces the original 57-dimensional RSS data to one-third of its original dimensionality (i.e., 19 dimensions), and subsequently to 10-dimensional feature embeddings. The experimental results are summarized in Table 7.

As shown in Table 7, without applying DP protection, the proposed SLocCE model achieves training accuracy improvements of 3.71% to 27.93% and testing accuracy gains of –0.78% to 26.27% over traditional models such as CNN, AE+DNN, DNN, and MLP. Its testing performance is only 0.78% lower than that of CNN, which benefits from its convolutional structure. When applying DP protection to RSS data, the DP-SLocCE model still achieves the highest accuracy across all models. Specifically, it improves training accuracy by 4.1% to 29.18% and testing accuracy by 1.79% to 27.88% compared to DP+CNN, DP+AE+DNN, DP+DNN, and DP+MLP. Notably, the training and testing accuracy of DP-SLocCE are only 0.13% and 0.12% lower than its non-private counterpart, SLocCE. These results indicate that the model maintains strong localization performance despite the perturbation introduced by differential privacy, owing to the denoising capability of the stacked denoising autoencoder, which enables robust feature extraction from noisy RSS fingerprints.

Table 7. Performance comparison of various methods on the Mall

Method name	Training acc. (%)	Testing acc. (%)	Data prep. (s)	Training (s)	Testing (s)
CNN	93.41	96.76	0.3631	960.9607	0.0369
DP+CNN	92.89	94.07	16.6358	924.7386	0.0349
AE+DNN	89.69	87.2	0.3288	221.3325	0.0150
DP+AE+DNN	87.37	84.52	16.6451	225.9808	0.0150
DNN	74.03	73.14	0.3368	201.6613	0.0119
DP+DNN	67.81	67.98	16.1791	198.4175	0.0119
MLP	69.19	69.71	0.3341	218.3422	0.0189
DP+MLP	70.34	70.29	16.5028	205.3940	0.0149
SLocCE	**97.12**	**95.98**	**0.4266**	**330.5851**	**0.0189**
DP-SLocCE	**96.99**	**95.86**	**16.4282**	**319.1215**	**0.0170**

Moreover, Table 7 shows that the proposed stacked denoising autoencoder-based model significantly reduces computational cost compared to CNN-based approaches. When no privacy protection is applied, the SLocCE model reduces training and testing time by 65.6% and 48.78%, respectively. Under DP settings, the reductions are 65.49% and 51.29%, respectively. This efficiency stems from the model's ability to progressively reduce the dimensionality of high-dimensional RSS data, alleviating training difficulty and improving real-time responsiveness.

Model Accuracy and Time Overhead on the UJIIndoorLoc Dataset. In the UJIIndoorLoc dataset, each RSS sample consists of 520-dimensional Wi-Fi received signal strength features, resulting in high-dimensional, information-rich data. Due to the richness of features and rapid convergence of models on this dataset, the number of training iterations was set to 50 epochs in this experiment. Using the proposed SDAE, the original 520-dimensional RSS data were first reduced to 104 dimensions (i.e., 1/5 of the original dimensionality), and then further compressed into 10-dimensional feature encodings. The training and testing accuracy curves of the model are shown in Fig. 5 and Fig. 6, respectively.

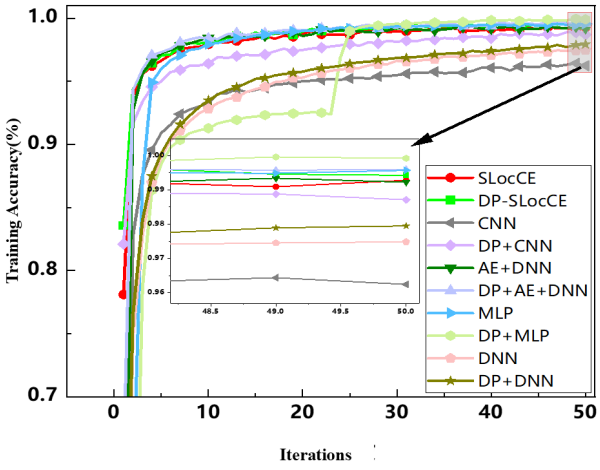


Fig. 5. Comparison of training accuracy on the UJIIndoorLoc

As shown in Fig. 5 and Fig. 6, the training accuracies of CNN, AE+DNN, DNN, MLP, and SLocCE are 96.44%, 99.26%, 97.40%, 99.45%, and 99.28%, respectively. The corresponding testing accuracies are 96.85%, 96.30%, 95.29%, 96.96%, and 97.04%. For the models with differential privacy protection, including DP+CNN, DP+AE+DNN, DP+DNN, DP+MLP, and DP-SLocCE, the training accuracies are 98.71%, 99.60%, 97.81%, 99.74%, and 99.43%, while the testing accuracies are 97.69%, 96.13%, 95.04%, 96.67%, and 96.54%, respectively. Due to the high dimensionality (520 features) and richness of signal information in each RSS fingerprint sample, all localization models achieve excellent accuracy. Furthermore, by comparing models with

and without differential privacy, the experimental results show that the impact of privacy noise on localization performance is minimal in this high-dimensional setting. This suggests that, in this dataset, higher-dimensional RSS fingerprint data provide stronger robustness to privacy noise perturbations.

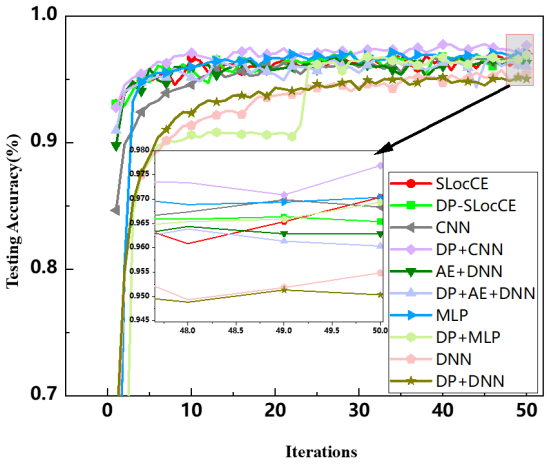


Fig. 6. Comparison of testing accuracy on the UJIIndoorLoc

Table 8 presents the comparison of time overhead between DP-SLocCE and other baseline models on the UJIIndoorLoc dataset.

Table 8. Comparison of time performance on the UJIIndoorLoc

Method name	Data preprocessing (s)	Training (s)	Testing (s)
CNN	8.8684	1560.9905	0.4080
DP+CNN	428.6454	1531.9828	0.4463
AE+DNN	7.6056	76.0009	0.0524
DP +AE+DNN	429.6412	73.8952	0.0516
DNN	8.8106	44.4309	0.0309
DP+DNN	429.0583	42.8823	0.0348
MLP	7.5041	140.0846	0.0559
DP +MLP	433.4904	145.3385	0.0609
SLocCE	**7.5141**	**95.5211**	**0.0718**
DP-SLocCE	**426.2854**	**98.6631**	**0.0678**

From Table 8, it is evident that the CNN and DP+CNN models incur the highest training and testing time overhead. In contrast, SLocCE and DP-SLocCE exhibit lower training and testing time costs than MLP and DP+MLP models. Specifically, SLocCE reduces training time and testing time by 93.88% and 82.4%, respectively, compared to CNN, while DP-SLocCE reduces these times by 93.56% and 84.81%, respectively, compared to DP+CNN. This can be attributed to the computational complexity of convolutional operations in CNN-based models, especially on high-dimensional RSS data, leading to longer processing times. In contrast, the proposed stacked denoising autoencoder-based deep localization model performs progressive dimensionality reduction, effectively mitigating the negative impact of high-dimensional RSS data on model training.

In summary, the proposed DP-SLocCE model achieved training accuracies of 96.33%, 96.99%, and 99.43%, and testing accuracies of 92.88%, 95.86%, and 96.54% on the Mall-WiFi, Mall, and UJIIndoorLoc datasets, respectively. These results demonstrate the model's strong adaptability and stability across different scenarios. As the dimensionality of RSS fingerprint data increases from 35 to 520 in our experiments, the model is able to extract increasingly rich and discriminative features, resulting in improved localization performance. This indicates that high-dimensional RSS signals contain more distinctive patterns that can enhance model accuracy. In terms of computational efficiency, DP-SLocCE significantly reduces both training and testing time compared

to CNN-based models, as detailed in Table 6, Table 7, and Table 8. The performance gap is especially evident on the high-dimensional UJIIndoorLoc dataset, where the model's dimensionality reduction and feature extraction capabilities are most prominent. These improvements can be largely attributed to the stacked denoising autoencoder architecture, which effectively mitigates the impact of differential privacy noise while accelerating training and inference processes. Overall, DP-SLocCE demonstrates strong noise resilience, computational robustness, and practical deployment potential, making it well-suited for constructing high-performance cloud-based indoor localization systems under differential privacy constraints.

7 Conclusion

To achieve a better trade-off among data privacy, localization accuracy, training efficiency, and real-time responsiveness in indoor fingerprint-based positioning systems, this paper presents a cloud-based localization model named DP-SLocCE, which integrates a shuffled differential privacy mechanism and a stacked denoising autoencoder architecture, tailored to the characteristics of indoor Wi-Fi signals. By perturbing RSS fingerprint data on the client side and introducing a Shuffler to disrupt user-data associations, the model effectively reduces the risk of privacy leakage. In parallel, its multi-layered feature extraction and progressive dimensionality reduction design alleviate the challenges imposed by high-dimensional RSS fingerprints during model training. Experiments on three real-world Wi-Fi fingerprint datasets with varying dimensionalities demonstrate that DP-SLocCE achieves superior performance compared with mainstream localization models in terms of both accuracy and efficiency. The model is particularly effective in high-dimensional scenarios, where its training and testing times are significantly reduced, demonstrating its practicality and robustness under differential privacy constraints.

Nevertheless, the current approach is still based on a centralized cloud architecture, which limits its adaptability in highly dynamic or edge computing scenarios. Future research will focus on exploring decentralized privacy-preserving mechanisms without trusted central servers, aiming to enable efficient, trustworthy, and real-time localization services on edge devices.

8 Acknowledgments

This work is supported by the Key Research and Development Program of Gansu Province (No. 25YFFA089); the Industry Support Fund of Education Department of Gansu Province (No. 2022CYZC-38); and the National Natural Science Foundation of China (No. 61762058).

References

[1] K. Lin, M. Chen, J. Deng, M.M. Hassan, G. Fortino, Enhanced fingerprinting and trajectory prediction for IoT localization in smart buildings, IEEE Transactions on Automation Science and Engineering 13(3)(2016) 1294-1307. https://doi.org/10.1109/TASE.2016.2543242

[2] R. Li, J. Li, Research on a device-free passive indoor regional localization method, Journal of Computer Research and Development 57(7)(2020) 1381-1392. https://doi.org/10.7544/issn1000-1239.2020.20190585

[3] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, J.-P. Hubaux, Quantifying location privacy, in: Proc. IEEE Symposium on Security and Privacy (SP), 2011. https://doi.org/10.1109/SP.2011.18

[4] X. Zhu, W. Qu, T. Qiu, L. Zhao, M. Atiquzzaman, D.O. Wu, Indoor intelligent fingerprint-based localization: principles, approaches and challenges, IEEE Communications Surveys & Tutorials 22(4)(2020) 2634-2657. https://doi.org/10.1109/COMST.2020.3014304

[5] F. Zafari, A. Gkelias, K.K. Leung, A survey of indoor localization systems and technologies, IEEE Communications Surveys & Tutorials 21(3)(2019) 2568-2599. https://doi.org/10.1109/COMST.2019.2911558

[6] Y. Etiabi, E.M. Amhoud, Federated distillation based indoor localization for IoT networks, IEEE Sensors Journal 24(7) (2024) 11678-11692. https://doi.org/10.1109/JSEN.2024.3357798

[7] Z. Wu, X. Wu, X. Long, Y. Long, A privacy-preserved online personalized federated learning framework for indoor localization, in: Proc. IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2021. https://doi.org/10.1109/SMC52423.2021.9658722
[8] X. Zhang, F. He, J. Gai, J. Bao, H. Huang, X. Du, A differentially private federated learning model for fingerprinting indoor localization in edge computing, Computer Research and Development 59(12)(2022) 2667-2688. https://doi.org/10.7544/issn1000-1239.20210270
[9] B. Gao, F. Yang, N. Cui, K. Xiong, Y. Lu, Y. Wang, A federated learning framework for fingerprinting-based indoor localization in multibuilding and multifloor environments, IEEE Internet of Things Journal 10(3)(2023) 2615-2629. https://doi.org/10.1109/JIOT.2022.3214211
[10] A. Konstantinidis, G. Chatzimilioudis, D. Zeinalipour-Yazti, P. Mpeis, N. Pelekis, Y. Theodoridis, Privacy-preserving indoor localization on smartphones, IEEE Transactions on Knowledge and Data Engineering 27(11)(2015) 3042-3055. https://doi.org/10.1109/TKDE.2015.2441724
[11] J. Zhang, Y. Zhao, J. Wang, B. Chen, FedMEC: Improving efficiency of differentially private federated learning via mobile edge computing, Mobile Networks and Applications 25(6)(2020) 2421-2433. https://doi.org/10.1007/s11036-020-01586-4
[12] C. Jia, Y. Wang, Y. Chen, M. Sun, F. Ge, Machine learning algorithm for a homomorphic encrypted data set, Journal of Tsinghua University (Science and Technology) 60(6)(2020) 456-463. https://doi.org/10.16511/j.cnki.qhdxxb.2020.25.011
[13] J. Li, X. Kuang, S. Lin, X. Ma, Y. Tang, Privacy preservation for machine learning training and classification based on homomorphic encryption schemes, Information Sciences 526(2020) 166-179. https://doi.org/10.1016/j.ins.2020.03.041
[14] S. Li, H. Li, L. Sun, Privacy-preserving crowdsourced site survey in WiFi fingerprint-based localization, EURASIP Journal on Wireless Communications and Networking 2016(1)(2016) 123. https://doi.org/10.1186/s13638-016-0624-2
[15] Y. Wang, M. Gu, J. Ma, Q. Jin, DNN-DP: Differential privacy enabled deep neural network learning framework for sensitive crowdsourcing data, IEEE Transactions on Computational Social Systems 7(1)(2020) 215-224. https://doi.org/10.1109/TCSS.2019.2950017
[16] Y. Liu, N. Wang, Z. Wang, Y. Gu, Z. Wei, X. Zhang, G. Yu, Collecting and analyzing multidimensional categorical data under shuffled differential privacy, Journal of Software 33(3)(2022) 1093-1110. https://doi.org/10.13328/j.cnki.jos.006450
[17] K. Li, H. Zhang, Y. Xu, Z. Liu, A range query scheme for spatial data with shuffled differential privacy, Mathematics 12(13)(2024) 1934. https://doi.org/10.3390/math12131934
[18] J. Bai, Y. Sun, W. Meng, C. Li, Wi-Fi fingerprint-based indoor mobile user localization using deep learning, Wireless Communications and Mobile Computing 2021(1)(2021) 6660990. https://doi.org/10.1155/2021/6660990
[19] K. Chow, S. He, J. Tan, S. Chan, Efficient locality classification for indoor fingerprint-based systems, IEEE Transactions on Mobile Computing 18(2)(2019) 290-304. https://doi.org/10.1109/TMC.2018.2839112
[20] Y. Li, J. Chen, Q. Li, A. Liu, Random forest algorithm under differential privacy based on out-of-bag estimate, Journal of Harbin Institute of Technology 53(2)(2021) 146-154. https://doi.org/10.11918/201912140
[21] C. Hong, J. Yu, J. Wan, D. Tao, M. Wang, Multimodal deep autoencoder for human pose recovery, IEEE Transactions on Image Processing 24(12)(2015) 5659-5670. https://doi.org/10.1109/TIP.2015.2487860
[22] P. Vincent, H. Larochelle, Y. Bengio, P. Manzagol, Extracting and composing robust features with denoising autoencoders, in: Proc. 25th International Conference on Machine Learning (ICML), 2008. https://doi.org/10.1145/1390156.1390294
[23] X. Jiang, Y. Chen, J. Liu, Y. Gu, L. Hu, FSELM: Fusion semi-supervised extreme learning machine for indoor localization with Wi-Fi and Bluetooth fingerprints, Soft Computing 22(11)(2018) 3621-3635. https://doi.org/10.1007/s00500-018-3171-4
[24] J. Torres-Sospedra, R. Montoliu, A. Martínez-Usó, J.P. Avariento, T.J. Arnau, M. Benedito-Bordonau, J. Huerta, UJIIndoorLoc: A new multi-building and multi-floor database for WLAN fingerprint-based indoor localization problems, in: Proc. International Conference on Indoor Positioning and Indoor Navigation (IPIN), 2014. https://doi.org/10.1109/IPIN.2014.7275492
[25] W. Zhang, S. Zhou, D. Peng, L. Yang, F. Li, H. Yin, Understanding and modeling of WiFi signal-based indoor privacy protection, IEEE Internet of Things Journal 8(3)(2021) 2000-2010. https://doi.org/10.1109/JIOT.2020.3015994
[26] X. Zhang, F. He, Q. Chen, X. Jiang, J. Bao, T. Ren, X. Du, A differentially private indoor localization scheme with fusion of WiFi and Bluetooth fingerprints in edge computing, Neural Computing and Applications 34(6)(2022) 4111-4132. https://doi.org/10.1007/s00521-021-06815-9

[27] A. Cheu, A. Smith, J. Ullman, D. Zeber, M. Zhilyaev, Distributed differential privacy via shuffling, in: Proc. Advances in Neural Information Processing Systems (NeurIPS), 2019.
https://doi.org/10.1007/978-3-030-17653-2_13
[28] B. Balle, J. Bell, A. Gascón, K. Nissim, The privacy blanket of the shuffle model, in: Proc. CRYPTO 2019: 39th Annual International Cryptology Conference, 2019.
https://doi.org/10.1007/978-3-030-26951-7_22