Koc. J. Sci. Eng., 6(2): (2023) 114-128 https://doi.org/10.34088/kojose.1098804

Kocaeli University

Kocaeli Journal of Science and Engineering

http://dergipark.org.tr/kojose

Privacy-Preserving Wireless Indoor Localization Systems

Beyhan ADANUR DEDETURK [1, *], Burak KOLUKISA [2], Samet TONYALI [3]

[1] *Department of Computer Engineering, Abdullah Gul University, Kayseri, 38080, Turkey,* ***ORCID:*** *0000-0003-4983-2417*
[2] *Department of Computer Engineering, Abdullah Gul University, Kayseri, 38080, Turkey,* ***ORCID:*** *0000-0003-0423-4595*
[3] *Department of Software Engineering, Gumushane University, Gümüşhane, 29100, Turkey,* ***ORCID:*** *0000-0001-7799-2771*

Article Info

Review paper

Received : *April 5, 2022*
Accepted : *November 16, 2022*

Keywords

Location Privacy
Wireless Indoor Localization
Anonymity
Encryption Methods

Abstract

Recently the number of buildings and interior spaces has increased, and many systems have been proposed to locate people or objects in these environments. At present, several technologies, such as GPS, Bluetooth, Wi-Fi, Ultrasound, and RFID, are used for positioning problems. Some of these technologies provide good results for positioning outdoors whereas some others are effective for indoor environments. While GPS is used for outdoor localization systems, Wi-Fi, Bluetooth, Ultra WideBand, and RFID are used for indoor localization systems (ILSs). Today, due to the proliferation and extensive usage of Wi-Fi access points, wireless-based technologies in indoor localization are preferred more than others. However, even though the abovementioned technologies make life easier for their users, ILSs can pose some privacy risks in case the confidentiality of the location data cannot be ensured. Such an incident is highly likely to result in the disclosure of users' identities and behavior patterns. In this paper, we aim to investigate existing privacy-preserving wireless ILSs and discuss them.

1. Introduction

The number of studies on location-based systems has increased with the evolution of technology in recent years. Positioning techniques are, in general terms, a set of methods used to assess the position of an object or an animal. Many methods have been developed to establish an entity or creature's location, but there are some important points to be considered to determine the correct location [1]. The first of these is to determine the system requirements in detail and to choose the most appropriate method for them. The second is to minimize the external factors that cause errors and make measurements with the least error rate.

Separating the areas where localization is used as indoor and outdoor spaces provides an advantage to classify both the space-specific applications and the preferred technologies according to the space features. There are many different technologies used for localization problems. Some of these are GPS, Bluetooth, Wi-Fi, ultrasound and RFID [2]. While GPS is used for outdoor positioning systems, it is ineffective due to the signal-weakening effect of interior walls [1]. In an indoor positioning system, the type of signal used, and the type of measurement significantly affect performance. For this reason, global positioning systems do not perform adequately in confined spaces. The necessity of indoor positioning systems has emerged to overcome this problem. Today, with the increase in the number of interior spaces such as airports, shopping centers, business centers, hospitals, universities, courthouses and parking lots, it has become much more important to find the location of people or an object in these places. The general working principle of indoor positioning technologies can be summarized as finding a user's relative position to a transmitter using radio signal characteristics [3]. The main technologies used for indoor localization systems (ILSs) are Wi-Fi, Bluetooth, ultra-broadband, and RFID.

While the increase in the use of the mentioned technologies provides very convenience in people's lives, conversely, if the data obtained as a result of the methods cannot be secured, it can harm individuals by allowing identification and behavior determination of individuals [4]. This study mainly aims that present a review of the

* Corresponding Author: beyhan.adanur@agu.edu.tr

latest technology and privacy-preserving ILSs. The remainder of this paper is organized as follows. Similar survey works are summarized in Section 2. In Section 3, we describe indoor localization technologies and techniques. Section 4 illustrates the challenges of indoor localization systems. In Section 5, we examine and evaluate existing privacy-preserving wireless indoor localization systems. The study is concluded in Section 6.

2. Related Survey Works

In Table 1 we have determined 36 major survey papers that have been published between 2015 and 2022 on indoor localization [1-28, 54-61]. The 9 papers have shown a general examination of indoor localization systems [1-4, 17, 21, 22, 25, 55]. They examine technologies and techniques used in indoor localization, comparison of systems according to some metrics, related challenges and proposed solutions. The other 7 of them have focused on Wi-Fi-based indoor localization systems [13, 14, 19, 20, 26, 27, 61]. They classify and compare Wi-Fi based indoor localization systems, and some of them propose a solution for a specific challenge on related topic. The other 2 of the papers show wireless and general indoor localization systems which are based on crowdsourcing [15, 24]. Although these two papers contain general information about the wireless indoor localization, they mainly focus on crowdsourcing technique [29] and their applications in the literature. For this reason, they can help researchers who want to work on crowdsourcing. In the remaining 18 papers, the following topics are covered, respectively:

i. WSN-based indoor localization [12]
ii. Localization privacy and indoor localization systems for mobile networks [16, 23]
iii. Indoor localization systems based on visible light [5], computer vision [6], acoustic [7], spatial models [10], industry 4.0 [11], Bluetooth & Fingerprinting [18] and pedestrian dead reckoning [28]
iv. Simultaneous localization and mapping (SLAM) systems [8]
v. Image-based indoor localization [9]
vi. Indoor vehicle localization based on RFID [54]
vii. Machine-learning based indoor localization [56-58]
viii. Magnetic-field based indoor localization [59]
ix. Indoor localization for IoT-based applications [60]

As can be understood from the topics covered by these 18 studies, while the other 18 studies give a general review of indoor localization, they focus on more specific topics. Studies with such a special focus will help those who want to work on the same sub-topic. But even though each of them is focused on a particular subject, the overall subject is the difference in technologies used for indoor localization. As a result of the examination of the relevant survey studies, we assume, as far as we know, that no survey paper classifies and compares systems that only contain the challenges of wireless indoor positioning solutions.

The purpose of this work is to give a comprehensive examination of wireless indoor positioning systems that maintain privacy. This study provides the reader with some of the latest privacy-preserving wireless indoor localization systems and gives hints about solutions for privacy problems. Because the security and privacy of indoor localization systems that include the position of users and objects is one of the most important requirements of relevant systems and is still waiting to be solved. With this paper, we aim to attract other researchers' attention to further privacy-preserving wireless indoor localization research.

3. Indoor Localization Technologies and Techniques

In this section, we present the technologies and techniques used in indoor localization.

3.1. Indoor Localization Technologies

The technologies used for indoor localization systems are shown in Figure 1. Bluetooth technology is designed as a wireless alternative technology that requires low energy and low cost to be used in short-range data exchange. Bluetooth modules, Bluetooth tags or sensors, a server, and a WLAN compose the Bluetooth positioning system. Bluetooth devices in the range of Bluetooth sensors in the environment can be connected to the sensors. This leads to the sensor communicating the ID of the device to the server through WLAN. The server determines the computer's location and provides the information to the device's application [21].

ZigBee is a common protocol for communication using IEEE 802.15.4 and is also a radio device deployed in a WSN as a sensor node that communicates via WLAN to the network [30]. Lastly, in a positioning system using ZigBee technology, the location of a person or object is calculated utilizing sensor data from measurements made by fixed sensor nodes and connected to the network at known locations. It should be remembered here that sensor nodes' costs vary according to energy consumption, calculation speed, bandwidth and memory.

Table 1. General information of current indoor localization studies

2022	2021
• [59] Magnetic Field Based Indoor Localization • [60] Indoor Positioning Systems for IoT-Based Applications • [61] WiFi-based Indoor Localization Systems • for Smartphone	• [54] Indoor Vehicle Localization Based on RFID • [55] General Examination of Indoor Localization Techniques and Wireless Technologies • [56-58] Machine Learning Based Indoor Localization

2020	2019	2018
• [5] Indoor Localization Systems Based on Visible Light • [6] Indoor Localization Methods Based on Computer Vision • [7] Indoor Localization Systems Based on Acoustic • [8] Indoor Location and Mapping (SLAM) Systems	• [1] General Examination of Indoor and Outdoor Location Systems • [3] General Examination of Indoor Location Systems • [9] Image Based Indoor Localization • [10] Indoor Localization Methods Based on Spatial Models • [11] Indoor Localization Systems Based on Industry 4.0	• [12] Indoor Localization Algorithms Based on Wireless Sensor Networks (WSN) • [13,14] Indoor Localization Systems Based on Wi-Fi • [15] Wireless Indoor Localization System Based on Crowdsourcing • [16] Localization Privacy For Mobile Networks

2017	2016	2015
• [2, 17] General Examination of Indoor Location Systems • [18] Indoor Localization Systems Based on Bluetooth and Fingerprinting	• [19, 20] Wireless Indoor Localization System • [23] Indoor Localization System for Mobile Networks • [24] Indoor Localization System Based on Crowdsourcing • [4, 21, 22, 25] General Examination of Indoor Location Systems	• [26, 27] Indoor Localization Systems Based on Wi-Fi • [28] Indoor Localization Systems Based on Pedestrian Dead Reckoning

The Radio Frequency Identification System (RFID) is an automated identification mechanism that uses electromagnetic transmission-based RF wireless technologies between RFID readers and RFID tags for monitoring purposes. In a positioning system using RFID technology, a tag is attached to the living or object whose position needs to be known. Radio frequency signals are then sent by the reader for identification. The label, which has entered the radio frequency field of the reader, takes the energy needed for data transfer from this field. It then modulates the carrier signal based on the data preloaded on it. The modulated carrier is sent to the reader from the label. The reader detects and demodulates the modulated signal, then read the data [31].

With its susceptibility to non-line-of-sight propagation (NLOS) and multipath effects, Ultra WideBand (UWB) is a wireless communication technology that uses a short-range, high-speed radio. Owing to its high bandwidth, it is preferred by various applications and positioning systems. In a positioning system, three or more ultra-broadband readers transmit a very broad pulse over the GHz spectrum using UWB technology. Then readers listen to chirps from tags that are ultra-broadband. Such labels have a trigger of the spark-gap type that produces a tiny blast inside them, producing a short, coded, very large, almost instantaneous explosion. Then readers report the measurements back to the central server or cloud from the tags [32].

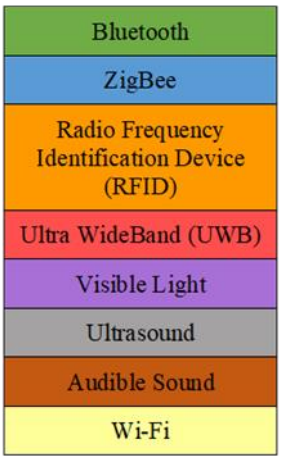

Figure 1. The technologies used in indoor localization

The Visible Light (VL) positioning systems use visible lights to locate an object for tracking and navigation. The positioning system for the VL consists of a transmitter or light source, a handheld terminal or receiver, and a contact path for the LOS. Light sources are positioned on the ceiling of a room or the side wall as base stations in this system to broadcast their known location information. The information is received from a location unknown by a mobile terminal or an image sensor and demodulated. The unbeknown location is then calculated using this information [33].

Positioning mechanisms for ultrasound require the ultrasonic markers' utilization or nodes which are on users and objects. The above-mentioned labels or nodes work qua receivers or transmitters; the other will be in motion while one is fixed. Active Bat, Cricket Device and Dolphin [2] are widely recognized ultrasound positioning systems. Audible Sound based localization is a system where standard device sound cards determine a person's or an object's position in a building by using audible sound waves. Audible sound-based localization systems generally use both software and hardware infrastructures [34].

The Internet can be accessed wirelessly via tablets, phones, smart watches and similar devices in the Wi-Fi signal area. In a positioning system using Wi-Fi technology, which is the main focus of our work, easy packets are transmitted by Wi-Fi transmitters to a range of Wi-Fi connection points in a facility [27]. These access points provide the time and intensity of their readings to a server, which calculates position using algorithms. The location information is then transferred to a cloud or server. The difficulty with privacy begins at the moment that location data is exchanged with the cloud or server.

The advantages and disadvantages of indoor localization technologies are given in Table 2. When deciding which technology should be used in an indoor localization system, the most important thing is to determine the system requirements thoroughly and select the most suitable one considering these advantages and disadvantage of technologies. For this reason, it would be wrong to say for any technology has the best performance and features. However, it can be said that wireless-based technologies are preferred more than other technologies in indoor location systems due to the increase in Wi-Fi usage all over the world.

3.2. Indoor Localization Techniques

The techniques used in indoor localization systems can be categorized as signal properties and algorithms. Although signal properties are utilized to determine and approximate the position of sensor nodes to increase the precision of localization, algorithms are used to transform the properties of the registered signal in distances and angles and after to measure the target object's real position.

Signal properties used for indoor localization systems are shown in Figure 2. The angle of arrival (AOA) is the measured angle and distance dependent on the intersection of path lines between reference points in relation to two or more reference points. The angle and distance calculation is used for estimating and determining a transmitter's position, and the information is used for purposes of tracking or navigation [3]. With AOA few sensors can be used to determine a position.

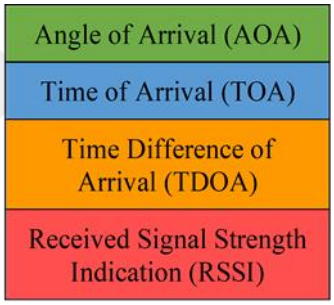

Figure 2. Signal properties for indoor localization

Time of Arrival (TOA) is the time taken from a fixed transmitter to arrive at a receiver through a signal, with the transmitter qua a reference point. In addition, instead of using the time difference determined between departure from a transmitter and arrival at the receiver, TOA uses the absolute time of arrival at the receiver. Therefore, it is possible to precisely calculate the distance between the transmitter and the receiver from the TOA, and the position can be calculated using this information [2]. Time Difference of Arrival (TDOA) determines a mobile transmitter's relative location based on the difference between the time of transmission of the transmitter and the different reference points or sensors. With this information, when the location of the mobile transmitter is identified,

monitoring may be impaired.

Received Signal Strength Indication (RSSI) is a calculation of the received signal strength (RSS) power level present in a radio infrastructure compared to angular and distance-dependent metrics. RSSI may be utilized to determine how far apart handheld computers are. Also known, to measure signal intensity reduction or loss due to transmission, the RSSI mechanism determines how much broadcast signals are attenuated. As a result, the distance among handheld computers can be calculated. Location information can be acquired through estimation [35].

Briefly, in position determination, the signal property is an integral element as it will be important in position calculation and estimation. In determining the positioning technique's potency, the signal property used with a positioning algorithm goes a long way. Thus, to use the most acceptable property, it is necessary to understand the positioning algorithms.

Table 2. Advantages and disadvantages of indoor localization technologies

Technology	Advantages	Disadvantages
Bluetooth	• High security, throughput and reception rate • Low cost and power • Small size	• Low localization accuracy • Has not resistance to noise • High cost to ensure privacy
ZigBee	• Uses for WSN • Cost-effective	• Not readily available on majority of the user devices • Difficult to find suitable position for non-anchor nodes • Low localization accuracy
RFID	• Needs low power • Has wide range	• Low localization accuracy
UWB	• Has resistance to interference • Provides high accuracy	• Shorter range • Needs extra hardware • High cost
Visible Light	• Widely available • High accuracy • Multipath-free	• Needs high power and LoS • Obstacles affect range
Ultrasound	• Less absorption	• High dependence on sensor placement
Audible Sound	• Uses in proprietary applications • Provides high accuracy	• Has not resistance to sound pollution • Needs extra hardware
Wi-Fi	• Eliminates LoS issues • Widely available • Provides high accuracy • No need complex extra hardware	• Inclined to noise • Uses complex processing algorithms • Low speed

The algorithms used for indoor localization systems are shown in Figure 3, and their advantages and disadvantages are shown in Table 3.

To approximate the location of a target object, triangulation uses triangular geometric properties by calculating angular measurements based on two supplied

reference points. Another saying, the intersection of two sets of angle directions is used to determine the target object's position, a technique acknowledged qua direction finding. To locate an item, AOA calculates the distance between direction lines or fixed points. The position of the transmitter is calculated based on the angle and distance between the reference points to estimate the object's location [36].

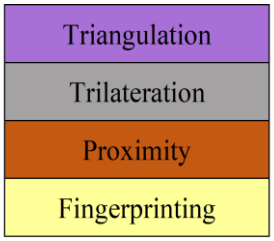

Figure 3. Algorithms used in indoor localization

The target object's location is calculated using TOA to calculate the time a signal takes to get from a transmitter to a receiver. In certain cases, TDOA, which is an upgrade on TOA, is also used. Trilateration also uses triangular geometry to estimate a target object's location. Nonetheless, in this situation, distance measurements are used to assess the location by calculating the attenuation relative to the three given reference points of the transmitted signal [36].

As in triangulation and trilateration, proximity does not provide an absolute or relative position estimate, because it merely offers location knowledge. To decide the position to supply the data, a grid of antennas with specified locations is used. If a mobile device is detected in motion, it uses the nearest antenna to determine its position. Yet, if a mobile device is detected by more than one antenna, the strongest signal antenna is used to measure its location [37]. The location of the mobile device is calculated using RSSI, which is typically used close to measure the distance between mobile devices to gain knowledge about the location of the device.

In fingerprinting, which is also called Scene Analysis, the location calculation is performed independently of the angle or the distance. Fingerprinting collects data or features from a scene or observation and then calculates the location of an object by matching or comparing the information collected in an existing database with that. It is an algorithm based on the RSS in wireless or RF networks. The fingerprinting system uses an RSS-value database to assess a Wi-Fi device's location within a Wi-Fi coverage area. Location fingerprinting refers to the fingerprint of any feature of a position-based signal. It can be performed in two stages, in other words offline and online. The area inside a building is surveyed in the offline process, and grid points are measured at different locations in the building [38].

For the locations with visible access points, each grid point has a list of RSSI values. Furthermore, for position estimation purposes, the respective position information and signal strengths are collected from the different locations. The precision accuracy obtained by this method is greater than the RF-based indoor positioning technique. In the online process, the object's most feasible location is computed by gathered grid points and localization information.

Fingerprinting is an RSS-based technology and is also widely utilized as an interior localization method. Fingerprinting is an RSS-based technology and is also widely utilized as an interior localization method.

The main idea of this approach is to estimate the user location using the pre-built database. One of the first studies is Radar, which is an RF-based system and obtained accuracies of 2 to 3 meters (The median error distance is 2 to 3 meters). Furthermore, today, many studies and applications are available in the fingerprinting approach. Fingerprinting consists of 2 stages. The offline part is known as the first stage. Designated interior spaces are divided into grids, and in each grid, the RSS values emitted by the Wi-Fi and Access Point devices are collected, and Radiomap is generated. As can be seen in Equation (1), while creating the database, "i" indicates the index, x and y hold the coordinate point of the index "i," and "V_i" is an array of the signal strength of all Wi-Fi and Access Points at that point, and "n" represents the number of devices overall. It should be noted here that when a grid is smaller the performance is lower. The second phase is called the online part. According to the RSS values received by the user, $V' = <V_1, V_2, V_3, ..., V_n>$, the (x_i, y_i) point is determined by using the k-Nearest Neighbor (KNN) algorithm.

$$<i, (x_i, y_i), V_i>$$
$$V_i = < V_1, V_2, V_3, ..., V_n > \quad (1)$$

Machine learning (ML) is characterized by an algorithm that can automatically recognize and understand data patterns. Based on this learning, an algorithm can recognize patterns or conduct various decision-making tasks for unknown incoming data. ML is often divided into three basic categories: supervised learning, unsupervised learning, and reinforcement learning. In supervised learning, all training samples have labels available.

Table 3. Advantages and disadvantages of indoor localization algorithms

Localization Algorithm	Signal Property	Advantages	Disadvantages
Triangulation	Angle of Arrival	Easy of its application Low cost and high accuracy at room level	Complex, expensive and low accuracy at wide coverage
Trilateration	Time of Arrival / Time Difference of Arrival	High accuracy	Complex and expensive due to hardware complexity
Proximity	Received Signal Strength Indication	High accuracy	Complex and expensive
Fingerprinting	Received Signal Strength Indication	High performance and easy to use	Complex, expensive, low medium accuracy and time consuming

In unsupervised learning, none of the training samples have labels. In reinforcement learning, an agent learns how to function or conduct actions in a potentially unpredictable and complicated environment in exchange for incentives. Another subtype of ML is semisupervised learning, in which some training samples are labeled but the remainder is not. On a variety of tasks, ML approaches can achieve human-level performance. Therefore, researchers have utilized ML in indoor localization to achieve high performance and compensate for or alleviate different difficulties encountered during data collecting, such as missing RSSIs, redundant RSSIs, and abnormalities (or mistakes) in RSSI fingerprints [56-58].

In indoor localization applications, the ML algorithms used for data preprocessing and dimensionality reduction are as follows [62-69]:

i. Singular value decomposition (SVD)
ii. Principal component analysis (PCA)
iii. Kernel PCA (KPCA)
iv. Locally linear embedding (LLE)
v. Linear discriminant analysis (LDA)
vi. t-distributed stochastic neighbor embedding (t-SNE)
vii. Autoencoders

Data that has been preprocessed is utilized to train machine learning prediction models for indoor localisation. The hyperparameters of the models are optimized for high accuracy and to minimize under- and/or overfitting. The authors of [70] provide a guideline for selecting the optimal hyperparameters of many ML models, including k-nearest neighbors (kNN), support vector machine (SVM), decision tree (DT), artificial neural networks (ANN), evolutionary algorithms, and federated computing. Each of these ML models has distinct underlying results based on their respective prediction methods. Typically, the performance of prediction models is assessed using a validation/test subset of database/radio maps. Additionally, the aforementioned prediction models may be used in a supervised, unsupervised, or semisupervised (partial labels for data) manner for the indoor localization problem.

Postprocessing [71] is an extra operation that enhances the performance of the ML model output. Post-processing methods include various pruning systems, quality processing standards, sorting rules, etc. These approaches apply different example filters on information generated by an algorithm that is noisy, imprecise, or unwanted. Similarly, post-processing is required for an indoor localization output, since it may wrongly forecast the location of the user owing to insufficient signal strength of the APs, hardware problems, etc., resulting in faulty positioning models. When constructing ML models, frequent retraining is required to account for data changes and the dynamic nature of the environment. This retraining of the model may increase the system's downtime, expense, and complexity. To prevent these challenges, researchers have begun employing a transfer learning (TL) approach. TL is an ML approach for storing the

information obtained during problem-solving and applying it to the solution of other related issues [72].

4. Challenges of Indoor Localization Sytems

In this section, some of the major challenges of indoor localization and its adoption are presented. Using a technology that is readily accessible to the user and does not require special hardware at the user end, availability is supported in indoor localization. The accuracy of UWB-based systems, for example, is high, but there are no UWB chips for most current user devices. So, it is necessary to obtain localization systems that will operate seamlessly with commonly available devices such as smartphones [3]. Wi-Fi, which is ready for use on almost all user computers, is the most widely used technology nowadays.

Cost is the key element in a market's acceptance of localization systems. It is a complex factor that is not confined to hardware alone. In the development and installation of a product, time and human resources are essential aspects that must be addressed. So the cost of the indoor localization systems should be low. Generally, as the hardware number used increases, system accuracy and cost increase. In this regard, the aim of today's indoor localization studies is to develop systems with high accuracy despite the minimum number of equipment and low cost [20].

It is optimal for an industrial localization system to cover vast areas with the fewest number of nodes, resulting in a cost-effective solution. However, if the ranges are expanded, the performance may suffer. Tx-power is the primary element for altering the system's coverage according to the use case. The capacity of a system to withstand interruptions and signal losses that might impair its functionality. A strong positioning system must account for environmental cues that are inaccurate. This measure is essential for the constant operation of all systems, especially on industrial sites and in emergency situations [60].

Another fundamental requirement of indoor localization is energy efficiency due to systems that consume a great deal of energy, drains battery from consumer devices cannot be commonly used [4]. Periodicity, transmission capacity and computational complexity are possible variables that could have an impact on any localization system's energy consumption. They can be done by using less energy-using technologies or by discharging the localization algorithm's computational portion to a server or any organization that has access to the uninterrupted power supply and high processing ability.

One of the most critical aspects of the localization method [21] is the accuracy. Accuracy is the proximity between the measured or predicted position and the actual position [39]. It depends on many factors, such as noise, LoS, signal propagation, and so on. The presence of obstacles and multi-path impacts make indoor localization more difficult to work on. Hence, to achieve highly accurate systems, it is necessary for the device to minimize the impact of multipath effects and other noises from the environment. This could include comprehensive signal processing and noise reduction, which is a very difficult job. A positioning approach should have the ability to locate the occupant or object within 10 cm of accuracy, preferably.

An indoor localization model is expected to be capable of recording occupant locations and coordinates without apparent delay. For this to happen, user location should be reported with a small number of reference signals, and complex operations are performed in milliseconds granularity [3]. However, this process will have some delay. To reduce delay, optimized signal processing is required which should remove noise and provide a visible delay to the user position.

Numerous heterogeneous devices supporting diverse communication technologies and protocols are included in location-based systems. Consequently, the interaction between many components is one of the greatest obstacles in this field. Developing n interoperable middleware for interaction between diverse components and standardized equipment and protocols may be a viable solution for this issue. Consequently, the establishment of a complete central platform or hub outfitted with all communication technologies might be a viable solution.

The security and privacy of indoor localization systems including the position of users and objects is the focus of this study and among the most critical needs for relevant structures. An occupant position can now be correlated with several device locations and show much more personal details such as people's health, mood, and behavior [16]. Even if the consumer does not have a mobile device, several IoT sensors can deduce its location and actions by processing a sequence of data collected in an immediate indoor environment. In the WLAN-IPS environment, traditional indoor positioning services (IPS) are endangered. Because a mobile device collects measurements from all AP devices and personal information, the RSS-based positioning system poses a security risk. The IPS server, for example, receives the AP ID. Privacy in IPSs may also be improved by regulating access to information dissemination and location information. From a software and system architectural standpoint, IPS security and privacy may also be improved. When calculating the position of the target device, for example, position system design dealing with

self-location will ensure consumers a high level of privacy and safety. Therefore, no one in Personal Networks can access the location information if an entity does not obtain it from the target device [40, 41].

5. Evaluation of Existing Privacy-Preserving Wireless Indoor Localization Systems

We have found 15 studies [42-51, 73-77] in the literature on privacy-preserving Wi-Fi-based indoor localization published between 2018 and 2022. In Table 4, related papers are classified according to their publication year, used technologies, algorithms, signal properties and methods for providing localization privacy. Below, we summarized the relevant studies briefly.

The study [73] proposes a Bloom filter-based preserving anonymity localization approach that creates a partial radio map during the localization process. Anonymizers hide user identities from Location Service Providers. The suggested approach is simpler than encryption or clustering methods and offers a strategy that increases the radio map by verified users without sacrificing privacy to reduce complexity and boost accuracy. Using the Hilbert curve to preserve user location uncertainty improves this strategy, and Location Service Providers provide verified user certificates. This certificate boosts users' Location Based Services queries. Simulations and observations reveal that the suggested strategy increases localization accuracy compared to location privacy methods.

Wang et al. [74] design a privacy-preserving IPS using a time difference of arrival (TDOA) positioning algorithm applied in an environment backed by a resourceful cloud system. Inner product encryption is used to protect users' privacy against attackers. Moreover, k-anonymity is used to ensure the security of data stored on cloud systems that can be modeled as semi-honest. Thus, the proposed scheme does not disclose private anchor information and users' location. In the proposed scheme, the least-squares estimation method used in the TDOA algorithm is decomposed into the basic form of inner products. This computation is performed on the ciphertext that holds distance difference and anchor information. Hence, the attackers cannot extract any useful information but the inner product from which they cannot determine users' location. Additionally, the client device adds some fake distance difference information in the location request sent to the cloud server, so it cannot distinguish users' real location from the fake data. Experimental results show that the proposed scheme both provides user privacy and meets efficiency and computational expectations for real-time indoor localization.

Beets et al. [75] design and implement a fingerprint-based privacy-preserving indoor localization scheme using a secure two-party computation protocol on RSS data obtained from a Wi-Fi access point. The proposed scheme provides privacy not only to users but also to service providers. The localization protocol is divided into vector-matrix multiplication with secret arithmetic shares and the k-nearest neighbor algorithm. With the proposed techniques, it is possible to make the online localization phase work 16 times faster. Finally, the paper presents an implementation of an indoor localization scheme based fully on Yao's Garbled Circuits. Although it cannot achieve the same level of localization accuracy when compared to the proposed scheme it can be employed in some scenarios where accuracy objectives are relaxed.

Zhang et al. [76] combine Wi-Fi and BLE fingerprints to develop a semi-supervised machine-learning model for indoor positioning. They take advantage of the computational capabilities of edge and cloud servers in the localization process. To prevent attackers and third-party cloud positioning servers from accessing users' real-time location data, they utilize the ε-differential privacy technique. According to the results obtained from experiments conducted in real indoor environments, the proposed model both reduces human intervention for calibration and outperforms five semi-supervised learning methods and six localization methods in terms of location accuracy and time consumption, respectively.

Hu et al. [77] extend an IPS named Horus which is based on maximum likelihood estimation and introduces PriHorus which provides privacy both for users' location and the IPS operator. To this end, PriHorus employs Paillier's cryptosystem, and experimental results show that it can achieve the same level of accuracy as Horus with an acceptable level of the computational burden.

Nieminen R. et al. [42] propose an indoor localization method that protects privacy based on measurements of signal intensity obtained from WiFi access points. Using secure two-party computing with Paillier encryption and garbled circuits, this technique tries to preserve the privacy of both the client's location and the service provider's database. It describes several optimizations that reduce the scheme's overheads in computation and present those overheads' theoretical assessments. They further illustrate the scheme's practicality by constructing a proof-of-concept implementation for Android devices and commodity servers. Hereby, it has been shown that the scheme is not eligible for real-world indoor localization applications, or that some applications require at least some additional measures to suit it. The downside is that there is more processing and communication overhead, which leads to slower response times, greater power consumption, and higher per-query data use.

Zhang G. et al. [43] propose a low-cost, lightweight privacy-preserving scheme (LWP2) that preserves the privacy of both the location and data. The fundamental idea is to first describe the problem of privacy-preserving localization as reducing the least squared error for an overdetermined linear formulation, and then to build a lightweight method exploiting the overdetermined linear formulation's particular structure in ciphertext space. Cost analysis, privacy, average time cost, bandwidth cost, and localization error metrics are used to demonstrate the study's performance.

To maintain anonymity for localization, The Encrypted Indoor Positioning Service (EIPS) approach proposed by Wang W. et al. [44] protects user privacy from a centralized server while maintaining localization accuracy. Their EIPS approach allows customers to encrypt and decrypt their requests bi-directionally utilizing an EDS (Encryption and Decryption Server) in a commutative manner, ensuring that both EIPS and EDS remain anonymous. To prevent Known Plaintext Attacks, they frequently offer Query Split, Artificial Dimensions, and Columns. The performance of the study is shown with the accuracy and time efficiency of EIPS, and energy consumption metrics. This scheme works without loss of quality, for both snapshot and continuous queries.

Eshun S.N. Et al. [45] offer an indoor privacy-preserving protocol that allows a service provider (SP) to query the location of a user without compromising their users' privacy. The protocol preserves the privacy of both the user and the SP while also delivering the service based on the user's location. They claim that most of the user-side computational overhead is delegated to the server using Paillier's cryptosystem during keeping the server's precise location hidden.

Järvinen K. et al. [46] introduced Practical Privacy-Preserving Indoor Localization Using OuTsourcing (PILOT), which safeguards the privacy of user locations and protects the database of the server. To save electricity and network bandwidth for mobile end devices in privacy-preserving indoor localization, PILOT safely outsources the computations to two non-colluding semi-honest parties (PPIL). After evaluating system performance, they claim that PILOT is the first PPIL system with realistic run-times of less than 1 s online and is quicker than previous works by many orders of magnitude.

Zhang X. et al. [47] proposed a lightweight, indoor privacy-conserving mechanism called EC-DPELM (a lightweight differential privacy-based indoor localization privacy-preserving mechanism) for a complex and dynamic Edge Computing environment. The RSSI dataset, which is utilized to train the model for indoor localization, will be adequately insulated within EC-DPELM. EC-DPELM also uses an edge-computing architecture, which means that the training cycle is distributed throughout the network's edges, reducing the load on cloud servers. Their tests revealed that the model is capable of ensuring both privacy and indoor localization accuracy while consuming less time.

Yang Z. et al. [48] introduce the privacy model for PPIL-based Wi-Fi fingerprint systems, where both client and server privacy is built to cover current active attacks in a unilateral malicious environment. Client privacy is defined based on the classic notion of distinguishability, and server privacy is defined computationally.

Zhao P. et al. [49] presented a Privacy-Preserving Paradigm-driven framework for indoor Localization (P3-LOC), a system for indoor localization privacy. P3-LOC takes advantage of the fact that most indoor localization systems follow a growing two-stage localization paradigm: measuring information and estimating locations. On this basis, P3-LOC perturbs and cloaks the transmitted data in these two stages and utilizes k-anonymity and differential privacy to provide privacy. The main benefit is that it does not rely on any previous knowledge of the underlying localization algorithms, and it guarantees the anonymity of the position of both users and the data of the server.

Alikhani N. et al. [50] suggested a framework for protecting user privacy in both the training and position estimation stages of data fingerprinting. In the training process, by using the Hilbert curve, when users are active in the crowdsourcing network, their privacy is maintained. Then, the privacy of users is protected in the location estimation stage by using both the double encryption technique and the Hilbert curve. The proposed method includes an anonymizer that is unaware of the real user's position and a server that is unaware of the user's identity.

Wang Y. et al. [51] suggest a Differential Privacy

(DP)-based indoor localization system DP3, composed of four different stages: client-side access point (AP) fuzzification and position retrieval, and server-side DP finger clustering and finger permutation. The localization server then divides the fingerprints related to the AP sequence into k clusters using DP-enabled clustering, permutes these reference points in each cluster using an exponential mechanism to mask the true positions of these fingerprints, and sends the modified data set to the to-be-localized (TBL) client. The location retrieval step on the client side calculates the client's location. Theoretical and experimental findings reveal that DP3 can safeguard both the TBL client's location and the localization server's data privacy.

Table 4. Features of privacy-preserving Wi-Fi based indoor localization

Paper	Year	Technology	Signal Property	Algorithm	Used Method for Providing Location Privacy
[77]	2022	Wi-Fi	RSS	Fingerprinting	• Paillier's Homomorphic Encryption
[76]	2022	Wi-Fi and BLE	RSSI	Fingerprinting	• ε-Differential Privacy
[75]	2022	Wi-Fi	RSS	Fingerprinting	• Secure Two-Party Computation • Yao's Garbled Circuits
[74]	2022	Wi-Fi	TDOA	Ranging	• Inner Product Encryption • k-Anonymity
[73]	2021	Wi-Fi	RSSI	Fingerprinting	• Bloom Filter-based Partial Radio Map
[42]	2020	Wi-Fi	RSSI	Fingerprinting	• Secure Two-Party Computation • Paillier's Homomorphic Encryption
[43]	2020	Wi-Fi	RSSI	Fingerprinting	• Paillier's Homomorphic Encryption
[44]	2019	Wi-Fi	RSSI	Fingerprinting	• Asymmetric Scalar-Product • Preserving Encryption kNN Search
[45]	2019	Wi-Fi	RSSI	Fingerprinting	• Paillier's Homomorphic Encryption • Secure Two-Party Computation • Spatial Bloom Filter
[46]	2019	Wi-Fi	RSSI	Fingerprinting	• Secure Two-Party Computation • Depth-Optimized Circuits
[47]	2019	Wi-Fi	RSSI	Fingerprinting	• Differential Privacy Edge Computing
[48]	2019	Wi-Fi	RSSI	Fingerprinting	• Secure Two-Party Computation • Paillier's Homomorphic Encryption
[49]	2018	Wi-Fi	RSSI	Fingerprinting Model Dead-Reckoning	• Differential Privacy k-Anonymity
[50]	2018	Wi-Fi	RSSI	Fingerprinting	• Hilbert curve Double encryption
[51]	2018	Wi-Fi	RSSI	Fingerprinting	• Differential Privacy Based Clustering

5. Conclusions

Today, the number of indoor spaces such as airports, hospitals and universities has increased considerably. Therewithal, locating people or an object in these interiors has become much more important. Although human life has become easier with the widespread use of positioning systems if positioning data cannot be protected, people's actions and information can be easily detected and people can be harmed. Because Wi-Fi access points are so widely used, wireless-based technologies are preferred more than Bluetooth, ultra-broadband and RFID technologies in indoor localization [52-53]. Based on the importance of indoor localization systems, their data privacy and the widespread use of wireless technology in the field, we wanted to examine the privacy-preserving wireless indoor localization systems in this study.

In the wireless indoor localization systems we have examined, we see that RSSI and fingerprinting techniques are generally chosen. Studies based on RSSI values o Wi-Fi technologies rely on the fact that the devices implementing these devices spread signals to a certain

distance. Our research firstly revealed that Wi-Fi technologies perform better than other technologies when used with RSSI as signal property and fingerprinting as positioning algorithms. Secondly, it revealed that for solving data privacy, the majority of studies have used secure two-party computation and homomorphic encryption methods. With homomorphic encryption, without breaking the encrypted data, different operations can be performed. Also, the client and the server provide complete security. But there is serious energy consumption for operations. For privacy protection, a hybrid approach can be built with Wi-Fi using other technologies, so the performance rate and client-server protection can be improved without the need for high energy consumption.

Declaration of Ethical Standards

The author(s) of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

Conflict of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Alinsavath K.N., Nugroho L.E., and Hamamoto K., 2019. The Seamlessness of Outdoor and Indoor Localization Approaches based on a Ubiquitous Computing Environment: A Survey. In Proceedings of the 2019 2nd International Conference on Information Science and Systems, Tokyo, 16-19 March, pp. 316-324.

[2] Sakpere W., Adeyeye-Oshin M., Mlitwa N.B., 2017. A state-of-the-art survey of indoor positioning and navigation systems and technologies. South African Computer Journal, **29(3),** pp. 145-197.

[3] Zafari F., Gkelias A., Leung K.K., 2019. A survey of indoor localization systems and technologies. IEEE Communications Surveys and Tutorials, **21(3)**, pp. 2568-2599.

[4] Yassin A., Nasser Y., Awad M., Al-Dubai A., Liu R., Yuen C., Aboutanios E., 2016. Recent advances in indoor localization: A survey on theoretical approaches and applications. IEEE Communications Surveys and Tutorials, **19(2)**, pp. 1327-1346.

[5] Rahman A. B. M., Li T., Wang, Y., 2020. Recent Advances in Indoor Localization via Visible Lights: A Survey. Sensors, **20(5)**, pp. 1382.

[6] Morar A., Moldoveanu A., Mocanu I., Moldoveanu F., Radoi I. E., Asavei V., Butean, A., 2020. A Comprehensive Survey of Indoor Localization Methods Based on Computer Vision. Sensors, **20(9)**, 2641.

[7] Liu M., Cheng L., Qian K., Wang J., Wang J., and Liu, Y., 2020. Indoor acoustic localization: a survey. Human-Centric Computing and Information Sciences, **10(1)**, pp. 1-24.

[8] Gaber H., Marey M., Amin S., Tolba M.F., 2020. Localization and Mapping for Indoor Navigation: Survey. In Robotic Systems: Concepts, Methodologies, Tools, and Applications, **1**, pp.930-954.

[9] Bai X., Huang M., Prasad N. R., Mihovska A.D., 2019. A Survey of Image-Based Indoor Localization using Deep Learning. In 2019 22nd International Symposium on Wireless Personal Multimedia Communications, Lisbon, 24-27 November, pp. 1-6.

[10] Gu F., Hu X., Ramezani M., Acharya D., Khoshelham K., Valaee S., Shang J., 2019. Indoor localization improved by spatial context—A survey. ACM Computing surveys (CSUR), **52(3)**, pp. 1-35.

[11] Mieth C., Humbeck P., Herzwurm G., 2019. A Survey on the Potentials of Indoor Localization Systems in Production. In Interdisciplinary Conference on Production, Logistics and Traffic, Dortmund, pp. 42-154.

[12] Sumitra I. D., Supatmi S., Hou R., 2018. Enhancement of Indoor Localization Algorithms in Wireless Sensor Networks: A Survey. In IOP Conference Series: Materials Science and Engineering, **407(1)**, pp. 1-8.

[13] Liu Y., Liu W., Luo, X., 2018. Survey on the Indoor Localization Technique of Wi-Fi Access Points. International Journal of Digital Crime and Forensics (IJDCF), **10(3)**, pp. 27-42.

[14] Zhou M., Bulgantamir O., Wang, Y., 2018. Highly Available Localization Techniques in Indoor Wi-Fi Environment: A Comprehensive Survey. In International Conference on Machine Learning and Intelligent Communications, Hangzhou, pp. 460-469.

[15] Zhou X., Chen T., Guo D., Teng X., Yuan B., 2018. From one to crowd: A survey on crowdsourcing-based wireless indoor localization. Frontiers of Computer Science, **12(3)**, pp. 423-450.

[16] Zakhary S., Benslimane A., 2018. On location-privacy in opportunistic mobile networks, a survey.

Journal of Network and Computer Applications, **103**, pp. 157-170.

[17] Brena R. F., García-Vázquez J. P., Galván-Tejada C. E., Muñoz-Rodriguez D., Vargas-Rosales C., and Fangmeyer J., 2017. Evolution of indoor positioning technologies: A survey. Journal of Sensors, **2017**.

[18] Samu G. W., Kadam P., 2017. Survey on Indoor Localization: Evaluation Performance of Bluetooth Low Energy and Fingerprinting Based Indoor Localization System. International Journal of Computer Engineering & Technology (IJCET), **8(6)**, pp. 23-35.

[19] Basri C., El Khadimi A., 2016. Survey on indoor localization system and recent advances of Wi-Fi fingerprinting technique. In 2016 5th International Conference on Multimedia Computing and Systems (ICMCS), Marrakesh, pp. 253-259.

[20] Xiao J., Zhou Z., Yi Y., Ni L. M., 2016. A survey on wireless indoor localization from the device perspective. ACM Computing surveys (CSUR), **49(2),** pp. 1-31.

[21] Khudhair A. A., Jabbar S. Q., Sulttan M. Q., Wang, D., 2016. Wireless indoor localization systems and techniques: survey and comparative study. Indonesian Journal of Electrical Engineering and Computer Science, **3(2)**, pp. 392-409.

[22] Kim C. M., Jang B., 2016. "Indoor Localization Technology Survey", Journal of The Korea Society of Computer and Information, **21(1)**, pp. 17-24.

[23] Stojkoska B. R., Kosovic I. N., Jagust T., 2016. "A Survey of Indoor Localization Techniques for Smartphones. Web Proceedings of ICT Innovations, Ohrid, pp. 11-22.

[24] Pei L., Zhang M., Zou D., Chen R., Chen Y., 2016. A survey of crowd sensing opportunistic signals for indoor localization. Mobile Information Systems, **2016**, pp. 1-16.

[25] Xi R., Li Y. J., Hou M. S., 2016. Survey on indoor localization. Computer Science, **43(4),** pp. 1-6.

[26] Yang Z., Wu C., Zhou Z., Zhang X., Wang X., Liu Y., 2015. Mobility increases localizability: A on wireless indoor localization using inertial sensors. ACM Computing Surveys (Csur), **47(3)**, pp. 1-34.

[27] Shandilya S., Idate S. R., 2015. Survey on Localization of Smartphone User in an Indoor Environment Using Wi-Fi and Navigation through Layout of the Floor Plans. International Journal of Innovative Research in Computer and Communication Engineering, **3(5)**, pp. 3784-3789.

[28] Minmin C., 2015. A survey of indoor localization using Pedestrian Dead Reckoning. Microcomputer & Its Applications, **13**, pp. 9-11.

[29] Ji H., Xie L., Wang C., Yin Y., Lu S., 2015. CrowdSensing: A crowd-sourcing based indoor navigation using RFID-based delay tolerant network. Journal of Network and Computer Applications, **52**, pp. 79-89.

[30] Luo C., Hong H., Cheng L., Chan M. C., Li J., Ming Z., 2016. Accuracy-aware wireless indoor localization: Feasibility and applications. Journal of Network and Computer Applications, **62**, pp. 128-136.

[31] Bianchi V., Ciampolini P., De Munari I., 2018. RSSI-based indoor localization and identification for ZigBee wireless sensor networks in smart homes. IEEE Transactions on Instrumentation and Measurement, **68(2)**, pp. 566-575.

[32] Ni L. M., Zhang D., Souryal M.R., 2011. RFID-based localization and tracking technologies. IEEE Wireless Communications, **18(2)**, pp. 45-51.

[33] García E., Poudereux P., Hernández Á., Ureña J., Gualda D., 2015. A robust UWB indoor positioning system for highly complex environments. In 2015 IEEE International Conference on Industrial Technology (ICIT), Seville, pp. 3386-3391.

[34] Hassan N. U., Naeem A., Pasha M. A., Jadoon T., and Yuen C., 2015. Indoor positioning using visible led lights: A survey. ACM Computing Surveys (CSUR), **48(2)**, pp. 1-32.

[35] Moutinho J. N., Araújo R. E., Freitas D., "Indoor localization with audible sound—Towards practical implementation. Pervasive and Mobile Computing, **29**, pp. 1-16.

[36] Luo X., O'Brien W. J., Julien C.L., 2011. Comparative evaluation of Received Signal-Strength Index (RSSI) based indoor localization techniques for construction jobsites. Advanced Engineering Informatics, **25(2)**, pp. 355-363.

[37] Kulshrestha T., Saxena D., Niyogi R., Raychoudhury V., Misra M., 2017. SmartITS: Smartphone-based identification and tracking using seamless indoor-outdoor localization. Journal of Network and Computer Applications, **98**, pp. 97-113.

[38] Al-Ammar M. A., Alhadhrami S., Al-Salman A., Alarifi A., Al-Khalifa H. S., Alnafessah A., Alsaleh, M., 2014. Comparative survey of indoor positioning technologies, techniques, and algorithms. In 2014 International Conference on Cyberworlds, Cantabria, pp. 45-252.

[39] Zegeye W. K., Amsalu S. B., Astatke Y., Moazzami, F., 2016. WiFi RSS fingerprinting indoor localization for mobile devices". In 2016 IEEE 7th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, pp. 1-6.

[40] Li H., Sun L., Zhu H., Lu X., Cheng, X., 2014. Achieving privacy preservation in WiFi fingerprint-based localization. In IEEE INFOCOM 2014-IEEE Conference on Computer Communications, Toronto, pp. 2337-2345.

[41] Ziegeldorf J. H., Viol N., Henze M., Wehrle K., 2014. Poster: Privacy-preserving indoor localization. 7th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec'14), Oxford, pp. 1-2.

[42] Nieminen R., Järvinen K., 2020. Practical Privacy-Preserving Indoor Localization based on Secure Two-Party Computation. IEEE Transactions on Mobile Computing, **20**, pp. 2877-2890.

[43] Zhang G., Zhang A., Zhao P., Sun, J., 2020. Lightweight Privacy-Preserving Scheme in Wi-Fi Fingerprint-Based Indoor Localization. IEEE Systems Journal, **14(3)**, pp. 4638-4647.

[44] Wang W., Gong Z., Zhang J., Lu H., Ku W. S., 2019. On Location Privacy in Fingerprinting-based Indoor Positioning System: An Encryption Approach. In Proceedings of the 27th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, Chicago, pp. 289-298.

[45] Eshun S. N., Palmieri P., 2019. A privacy- preserving protocol for indoor Wi-Fi localization. In Proceedings of the 16th ACM International Conference on Computing Frontiers, Alghero, pp. 380-385.

[46] Järvinen K., Leppäkoski H., Lohan E. S., Richter P., Schneider T., Tkachenko O., Yang Z., 2019. PILOT: practical privacy-preserving indoor localization using outsourcing. In 2019 IEEE European Symposium on Security and Privacy (EuroSandP), Stockholm, pp. 448-463.

[47] Zhang X., Chen Q., Peng X., Jiang X., 2019. Differential Privacy-Based Indoor Localization Privacy Protection in Edge Computing. In 2019 IEEE (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Leicester, pp. 491-496.

[48] Yang Z., Järvinen K., 2019. Towards Modeling Privacy in WiFi Fingerprinting Indoor Localization and its Application. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), **10(1),** pp. 4-22.

[49] Zhao P., Jiang H., Lui J. C., Wang C., Zeng F., Xiao F., Li Z., 2018. P3-LOC: A privacy-preserving paradigm-driven framework for indoor localization. IEEE/ACM Transactions on Networking, **26(6)**, pp. 2856-2869.

[50] Alikhani N., Moghtadaiee V., Sazdar A. M., Ghorashi S. A., 2018. A Privacy Preserving Method for Crowdsourcing in Indoor Fingerprinting Localization. In 2018 8th International Conference on Computer and Knowledge Engineering (ICCKE), Iran, pp. 58-62.

[51] Wang Y., Huang M., Jin Q., Ma J., 2018. DP3: A differential privacy-based privacy-preserving indoor localization mechanism. IEEE Communications Letters**, 22(12)**, pp. 2547-2550.

[52] Altintas B., Tacha, S., 2011. Improving RSS-based indoor positioning algorithm via k-means clustering. 17th European Wireless 2011-Sustainable Wireless Technologies. VDE, Vienna, pp. 1-5.

[53] Halder S., Ghosal A., 2016. A survey on mobility-assisted localization techniques in wireless sensor networks. Journal of Network and Computer Applications, **60**, pp. 82-94.

[54] Motroni A., Buffi A., Nepa P., 2021. A survey on indoor vehicle localization through RFID technology. IEEE Access, ***9***, pp. 17921-17942.

[55] Obeidat H., Shuaieb W., Obeidat O., Abd-Alhameed R., 2021. A review of indoor localization techniques and wireless technologies. Wireless Personal Communications, **119(1)**, pp. 289-327.

[56] Roy P., Chowdhury C., 2021. A survey of machine learning techniques for indoor localization and navigation systems. Journal of Intelligent & Robotic Systems, **101(3)**, pp. 1-34.

[57] Singh N., Choe S., Punmiya R., 2021. Machine learning based indoor localization using Wi-Fi RSSI fingerprints: an overview. IEEE Access, **9**, pp. 127150 – 127174.

[58] Yang T., Cabani A., Chafouk H., 2021. A Survey of Recent Indoor Localization Scenarios and Methodologies. Sensors, **21(23)**, 8086.

[59] Ouyang G., Abed-Meraim K., 2022. Survey of Magnetic-Field-Based Indoor Localization. Electronics, **11(6)**, 864.

[60] Farahsari P. S., Farahzadi A., Rezazadeh J., Bagheri A., 2022. A Survey on Indoor Positioning Systems for IoT-based Applications. IEEE Internet of Things Journal, **9(10)**, pp. 7680-7699.

[61] Roy P., Chowdhury C., 2022. A survey on ubiquitous

WiFi-based indoor localization system for smartphone users from implementation perspectives. CCF Transactions on Pervasive Computing and Interaction, pp. 1-21.

[62] Sorour S., Lostanlen Y., Valaee S., Majeed K., 2015. Joint indoor localization and radio map construction with limited deployment load. IEEE Trans. Mobile Comput., **14(5)**, pp. 1031-1043.

[63] Gu Z., Chen Z., Zhang Y., Zhu Y., Lu M., Chen A., 2016. Reducing fingerprint collection for indoor localization. Comput. Commun., **83**, pp. 56-63.

[64] Lee W. H., Ozger M., Challita U., Sung K.W., 2021. Noise learning based denoising autoencoder. In IEEE Communications Letters, **25(9),** pp. 2983-2987.

[65] Jia B., Huang B., Gao H., Li W., 2018. Dimension reduction in radio maps based on the supervised kernel principal component analysis. Soft Comput., **22(23)**, pp. 7697-7703.

[66] Lian L., Xia S., Zhang S., Wu Q., Jing C., 2019. Improved indoor positioning algorithm using KPCA and ELM. In Proc. 11th Int. Conf. Wireless Commun. Signal Process. (WCSP), 23-25 October, pp. 1-5.

[67] Imran S., Ko Y. B., 2018. A novel indoor positioning system using kernel local discriminant analysis in Internet-of-Things. Wireless Commun. Mobile Comput., **2018**, pp. 1-9.

[68] Adege A., Lin H. P., Tarekegn G., Jeng S. S., 2018. Applying deep neural network (DNN) for robust indoor localization in multi-building environment. Appl. Sci., **8(7)**, 1062.

[69] Lopez-de-Teruel P., Canovas O., Garcia F. J., 2017. Using dimensionality reduction techniques for refining passive indoor positioning systems based on radio fingerprinting," Sensors, **17(4)**, 871.

[70] Bengio Y., 2012. Practical recommendations for gradient-based training of deep architectures. In Neural Networks: Tricks Trade. Berlin, Germany: Springer, 2012, pp. 437-478.

[71] Bruha I., Famili A., 2000. Postprocessing in machine learning and data mining. ACM SIGKDD Explor. Newslett., **2(2)**, pp. 110-114.

[72] Zhuang F., Qi Z., Duan K., Xi D., Zhu Y., Zhu H., Xiong H., He Q., 2021. A comprehensive survey on transfer learning. Proc. IEEE, **109(1)**, pp. 43-76.

[73] Sazdar A. M., Alikhani N., Ghorashi S. A., Khonsari A., 2021. Privacy preserving in indoor fingerprint localization and radio map expansion. Peer-to-Peer Networking and Applications, **14(1)**, pp. 121-134.

[74] Wang Z., Xu Y., Yan Y., Zhang Y., Rao Z., Ouyang X, 2022. Privacy-preserving indoor localization based on inner product encryption in a cloud environment. Knowledge-Based Systems, **239**, 108005.

[75] van der Beets C., Nieminen R., Schneider T., 2022. FAPRIL: Towards Faster Privacy-Preserving Fingerprint-Based Localization. In: *SECRYPT*. 2022.

[76] Zhang X., He F., Chen Q., Jiang X., Bao J., Ren T., Du X., 2022. A differentially private indoor localization scheme with fusion of WiFi and bluetooth fingerprints in edge computing. Neural Computing and Applications, **34**, pp. 4111–4132.

[77] Hu Z., Li Y., Jiang G., Zhang R., Xie M., 2022. PriHorus: Privacy-Preserving RSS-Based Indoor Positioning. In ICC 2022-IEEE International Conference on Communications, pp. 5627-5632.