scientific reports

Check for updates

OPEN

Comprehensive analysis of security threats and privacy issues in indoor localization systems

Ayesha Ayub[1], Zuhairiah Zainal Abidin[1]✉, Abdulraqeb Alhammadi[2]✉, Muhammad Asim Khan[3], Naglaa F. Soliman[4], Nurul Bashirah Ghazali[1,5] & Abeer D. Algarni[4]

The growing use of indoor localization systems (ILS) in essential applications, including healthcare, smart buildings, and logistics, has created serious security and privacy concerns. This paper thoroughly analyzes the existing security and privacy concerns in ILS, emphasizing risks such as spoofing, signal jamming, and adversarial attacks. We explore defense strategies, such as federated learning, adversarial machine learning, and cryptographic protocols, emphasizing their efficacy and constraints. The study examines the trade-offs among privacy, accuracy, and efficiency in ILS while tackling significant difficulties such as non-Independent and Identically Distributed (non-IID) data, energy efficiency, and scalability in practical applications. This review provides a comprehensive overview of the state of the art in protecting ILS against growing adversarial threats by integrating major trends and approaches from the last five years. This survey paper will help researchers and industry professionals gain a deeper understanding of privacy and security concerns in ILS.

Keywords Adversarial machine learning, Indoor localization systems, Federated learning, Privacy, Security, Spoofing attacks, Signal jamming

Abbreviations

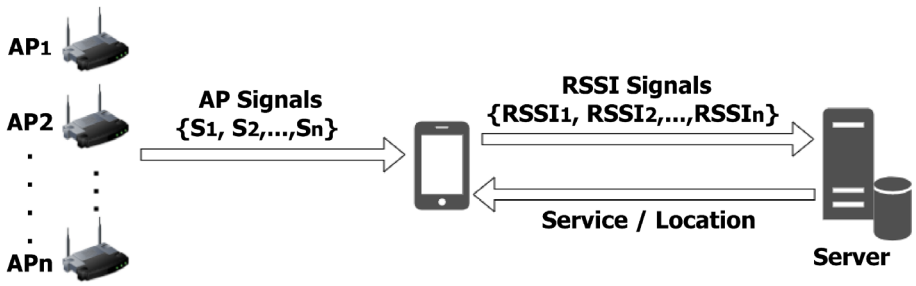
3D	Three-dimensional
ACTD	Abnormal crowd traffic detection
ADC	Analog-to-digital converter
AI	Artificial intelligence
AML	Adversarial machine learning
AP	Access point
BLE	Bluetooth low energy
CNNs	Convolutional neural networks
CSI	Channel state information
CV	Computer vision
DNN	Deep neural network
DPGANs	Differentially private generative adversarial networks
FD	Federated distillation
FGSM	Fast gradient sign method
FL	Federated learning
FMCW	Frequency modulated continuous wave
GAN	Generative adversarial network
GDPR	General data protection regulation
GNSS	Global navigation satellite system
GPS	Global positioning system
ILS	Indoor localization systems

[1]Advanced Telecommunication Research Center (ATRC), Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia, 86400 Parit Raja, Johor, Malaysia. [2]Faculty of Artificial Intelligence, Universiti Teknologi Malaysia, 54100 Kuala Lumpur, Malaysia. [3]School of Mathematical Sciences, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia. [4]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, 11671 Riyadh, Saudi Arabia. [5]Control Software Design Department, Daikin Research and Development Sdn. Bhd., P.O.Box 79, Taman Perindustrian, Lot 60334, Persiaran 3, 47000 Sungai Buloh, Selangor, Malaysia. ✉email: zuhairia@uthm.edu.my; abdulraqeb.alhammadi@utm.my

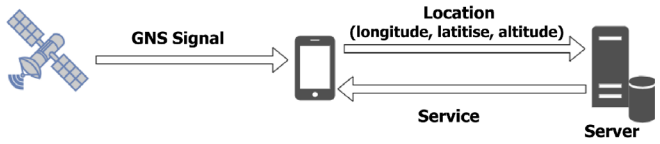
IoT	Internet of Things
KNN	K-nearest neighbor
LBS	Location-based services
LDP	Local differential privacy
LIDAR	Light detection and ranging
LoS	Line-of-sight
MAC	Media access control
MIM	Momentum iterative method
ML	Machine learning
NFC	Near-field communication
NLoS	Non-line-of-sight
ODE	Ordinary differential equation
PGD	Projected gradient descent
PST	Probability suffix trees
RF	Radio frequency
RFID	Radio-frequency identification
RL	Reinforcement learning
RNNs	Recurrent neural networks
RSS	Received signal strength
RSSI	Received signal strength indicator
SNR	Signal-to-noise ratio
SVM	Support vector machine
TDoA	Time difference of arrival
ToA	Time of arrival
UWB	Ultra-wideband
ZKP	Zero-knowledge proof
ZUPT	Zero-velocity update

Location-based services (LBS) are applications that deliver location-specific information regarding a user or device via mobile devices or communication networks. Recent years have seen an increase in demand due to their broad range of applications, which include navigation, mapping, social networking, targeted advertising, virtual reality, healthcare, transportation, smart cities, and gaming[1]. While outdoor localization largely depends on global navigation satellite systems (GNSS), many emerging services require accurate positioning indoors, where GNSS is unreliable. Indoor Localization Systems (ILS) fulfill this requirement by utilizing several technologies, including frequency modulation (FM), amplitude modulation (AM), Bluetooth, global system for mobile communications (GSM), Wi-Fi, and long-term evolution (LTE)[2,3].

Localization fundamentally involves determining the position of an object or individual in relation to reference points (RP) within a specified indoor environment[4], as depicted in Fig. 1, which emphasizes the difference between indoor and outdoor methodologies. The increasing dependence on ILS in essential sectors, such as healthcare, smart infrastructure, logistics, and emergency response, highlights the necessity for dependable, secure, and privacy-respecting systems. Indoor locations present distinct issues, including



(a) Indoor localization systems.



(b) Outdoor localization systems.

Fig. 1. Indoor versus outdoor localization systems.

signal blockage, multipath effects, and vulnerability to malicious interference. Security threats such as signal spoofing and jamming, along with privacy risks like unauthorized tracking, can result in significant real-world repercussions. It is therefore essential to understand and address these threats, which highlight the importance of a comprehensive review of existing vulnerabilities, defense mechanisms, and future research directions in this evolving field.

The study distinguishes itself from others[5–7] by providing a comprehensive examination of security and privacy concerns in ILS, something that is frequently overlooked in previous research. Numerous present assessments concentrate on security concerns or privacy troubles, although seldom do they examine the combination of both. Our analysis underscores the imperative for a dual approach, particularly in response to rising threats such as signal spoofing, jamming, and data privacy violations. This report highlights recent trends and offers a current view of the growing environment of ILS, including developments in FL and AML as defensive strategies. Unlike prior studies that narrow their scope to specific technologies, our paper broadens the scope by analyzing the latest developments across diverse ILS applications, providing insights into both attack prevention and defense mechanisms, and identifying gaps in the literature. The main contributions of this study are summarized as follows:

- *Comprehensive literature synthesis* We provide a structured and up-to-date review of recent developments (2020–2025) in ILS security and privacy, emphasizing the interplay between threats such as spoofing, jamming, and data breaches, which are often treated separately in prior surveys.
- *Methodological integration of defense paradigms* This study uniquely integrates discussions on federated learning (FL), adversarial machine learning (AML), and cryptographic protocols, offering a comparative analysis of their effectiveness and limitations across varied ILS scenarios.
- *Evaluation of privacy–utility trade-offs* We critically examine the trade-offs between privacy, accuracy, and computational efficiency in decentralized ILS architectures, offering insights into real-world applicability and constraints that are often overlooked in more theoretical studies.
- *Identification of open challenges and research Ddrections* The study highlights unresolved issues such as non-IID data handling, scalability limitations, and energy efficiency bottlenecks. Based on these, we propose concrete future research directions to support the design of more secure and privacy-preserving ILS frameworks.

While several prior reviews have discussed either security or privacy in indoor localization systems, few studies have offered an integrated perspective that systematically addresses both concerns in tandem. This gap is particularly significant given the increasing interdependence between privacy-preserving mechanisms and security defenses in real-world ILS deployments. Existing literature has tended to focus on isolated technical challenges–such as specific attack types, encryption techniques, or signal interference–but has often lacked a comprehensive view that maps these threats to emerging defensive strategies like federated learning and adversarial machine learning. In response, this study presents a structured and up-to-date synthesis of both vulnerabilities and countermeasures in ILS, covering technological trends from 2020 to 2025. Methodologically, this review differs from past works by bridging siloed research areas and offering a comparative analysis of ILS privacy and security solutions across a range of practical application scenarios. By doing so, it not only identifies unresolved challenges but also outlines future research directions to guide the development of robust and privacy-aware indoor localization architectures.

To conduct this comprehensive review, we systematically searched leading academic databases, including IEEE Xplore, Scopus, and Web of Science, for peer-reviewed journal and conference papers published between 2020 and 2025. Keywords such as indoor localization, privacy, security, federated learning, and adversarial machine learning guided our search. We included articles that specifically addressed either security or privacy concerns or both within the context of Indoor Localization Systems (ILS). Studies that focused exclusively on hardware-level improvements or unrelated positioning technologies were excluded. We restrict the time window to 2020–2025 to capture the rapid shift toward FL/AML and cryptographic defenses during these years, provide a coherent and up-to-date scope, and complement–rather than duplicate–pre-2020 surveys. For the detailed eligibility rules and screening workflow, see "earch Strategy and Eligibility Criteria"Section.

As a survey paper, this study aims to synthesize and evaluate existing research, without proposing new algorithms or experiments. Selected articles were analyzed and categorized based on attack types, defense mechanisms, and system architectures, as illustrated in Fig. 3, to support a structured exploration of current trends and open challenges in the field.

Unlike prior surveys, this work integrates recent advances and organizes threats and solutions using a taxonomy aligned with AI-driven and cryptographic methodologies, offering a novel perspective on the dual challenge of privacy and security in ILS.

Search strategy and eligibility criteria

To enhance transparency and reproducibility, we specify the eligibility rules governing study selection and outline the screening workflow used to assemble the final corpus. A concise summary appears in Table 1.

Inclusion criteria (all must be satisfied).

1. Peer-reviewed journal or conference papers published during 2020-2025.
2. English-language publications.
3. Full text available.
4. Studies focused on ILS that analyze security and/or privacy (e.g., threats, defenses, trade-offs).

Category	Rule
Include	Peer-reviewed journal or conference paper (2020–2025), English, full text available
Include	Focus on ILS with analysis of security and/or privacy (threats/defenses/trade-offs)
Include	Empirical, simulation, algorithm/framework, or survey with substantive ILS security/privacy content
Exclude	Hardware-only improvements without ILS security/privacy analysis
Exclude	Outdoor-only localization or unrelated positioning technologies
Exclude	Non–peer-reviewed items; abstracts only; non-English

Table 1. Eligibility criteria (summary).

5. Study designs including empirical evaluations, simulations, algorithmic/framework proposals, or surveys that substantively address ILS security or privacy.**Exclusion criteria (any single criterion is sufficient for exclusion)**

1. Works focused exclusively on hardware-level improvements with no ILS security/privacy analysis.
2. Studies on outdoor-only localization or otherwise unrelated positioning technologies.
3. Non–peer-reviewed items (e.g., theses, patents, white papers), abstracts without full text, or non-English publications.*Screening workflow* Records aggregated from the selected bibliographic sources were first deduplicated. We then conducted title/abstract screening against the eligibility rules above, followed by a full-text assessment of the remaining candidates. For transparency, reasons for exclusion were documented at the full-text stage. The subsequent taxonomy and synthesis consider only studies meeting the inclusion criteria.

The remainder of the paper is organized as follows: Section "Fundamentals of indoor localization systems" covers the basics of ILS, including their kinds, range methods, and localization algorithms. Section "Related work" summarizes current ILS security and privacy assessments and research. Section "Comparative study of privacy and security approaches in ILS" examines the strengths, weaknesses, and current trends of ILS security solutions and highlights key issues. Section "Security and privacy concerns in ILS" discusses ILS security and privacy issues, including spoofing and jamming attacks and their consequences. Section "Machine learning techniques for enhancing security and privacy in ILS" discusses the AI techniques that can be used for enhancing ILS privacy and security. Section "Discussion and synthesis of findings" synthesizes the findings from the previous sections by categorizing security and privacy techniques along the dimensions of effectiveness, scalability, and real-world applicability. Finally, sect. "Research gaps and future directions" provides a comprehensive discussion of gaps and future directions in the ILS study. Finally, sect. "Conclusion" concludes the paper by summarizing the findings and suggesting future research directions to improve ILS security and privacy. For a complete structure of this paper, refer to Fig. 2.

Fundamentals of indoor localization systems

Before delving into privacy and security challenges related to ILS, let us briefly look into these systems. ILS estimates the position of a target continuously in an indoor environment by first applying a distance estimation algorithm using different ranging techniques, followed by a localization algorithm[8]. To offer a structured understanding of the security and privacy landscape in ILS, Fig. 3 presents a taxonomy that categorizes the common threat types, corresponding defense mechanisms (e.g., federated learning, adversarial training, cryptographic solutions), and deployment models. This taxonomy serves as a conceptual anchor for the techniques reviewed in subsequent sections.

Types of indoor localization

Indoor environments are diverse, and each indoor environment requires ILS tailored to its needs in terms of accuracy and coverage. For example, ambient assisted living applications require room-level coverage with an accuracy of less than one meter, while law enforcement requires urban or rural coverage with an accuracy of a few meters. Because of these diverse needs, there is no single solution to indoor localization; different localization techniques coexist. Indoor localization can broadly be divided into two categories: active localization and passive localization. A more detailed sub-classification of active and passive localization techniques is shown in a flow chart in Fig. 4.

Active localization

Active localization is ideal for application that require high accuracy like asset tracking, robot navigation, etc., but demands users to carry a tag or device like a mobile phone, smartwatch, etc. Some of the techniques used for active detection include computer vision (CV)[9], light detection and ranging (LIDAR)[10–12], ultrasound[13], acoustic[14,15], geometric fingerprinting[16], wireless or radio frequency (RF)[17], visible light[18], and aroma fingerprinting[19,20].

Passive localization

Unlike active localization, passive localization suitable for scenarios like occupancy detection, with limitations in precision is due to the lack of active tags. Some of the applications of passive detection are intrusion detection, fall detection, remote monitoring, emergency evacuation, business analytics, accessibility aids for the visually impaired[21], etc. The techniques used in passive localization include camera- or vision-based localization[22,23],

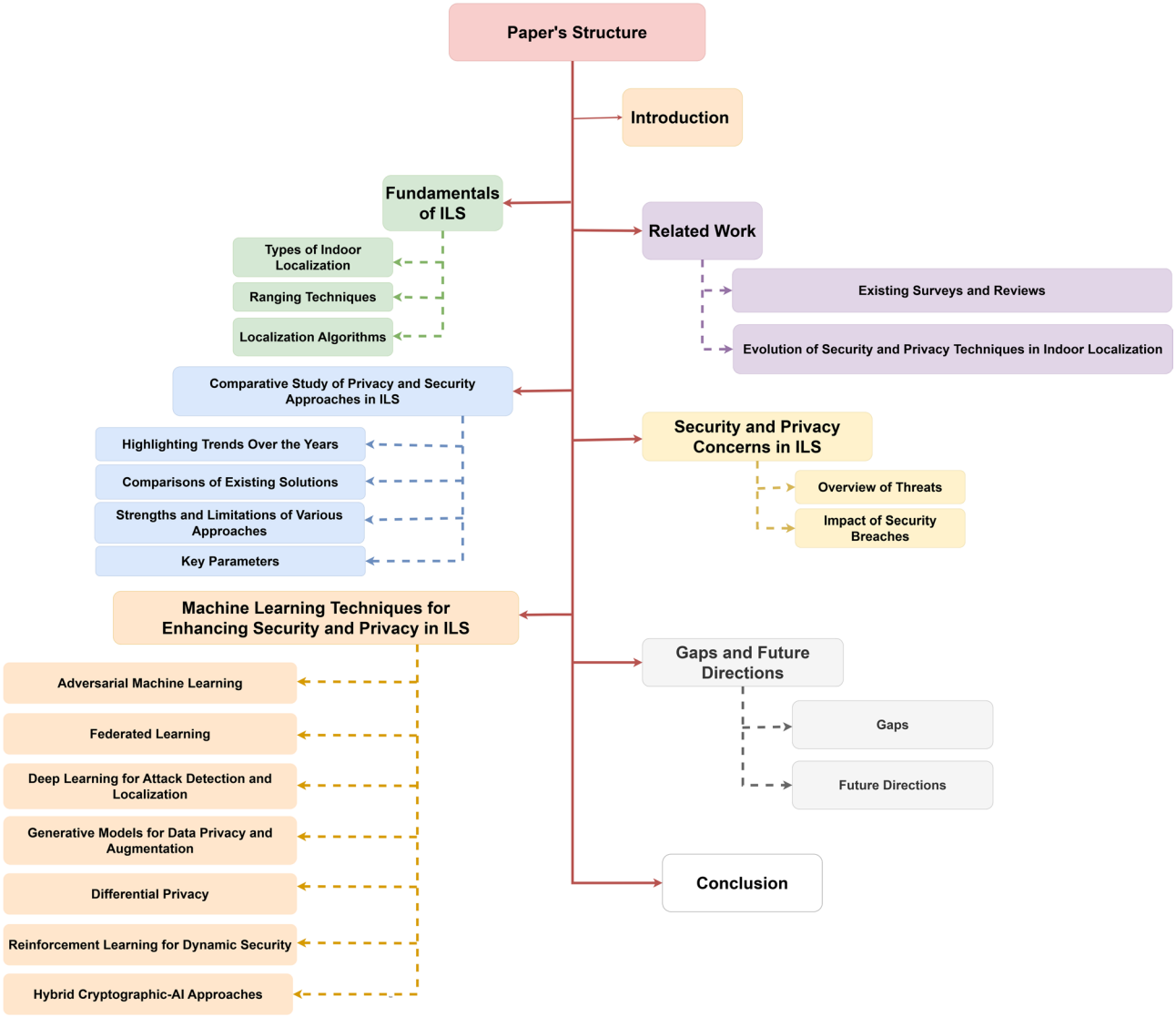


Fig. 2. Outline of the study.

RF-based localization[24], visual light-based localization[25,26], infrared-based localization[27,28], physical excitation[21], and electric field sensing[13,29].

Ranging techniques

Ranging techniques in ILS are different methods used to measure the distance between devices, such as beacons, sensors, or access points (AP), and a target object that could be a mobile device or person. These techniques are essential for determining the location of a target in an indoor environment. Different ranging techniques are used for ILS in the literature (Fig. 5); some of the common ones include the following:

Phase of arrival (PoA)

PoA is a ranging technique in which the phase difference of a signal that is received at multiple antennas or from multiple transmitters is measured. The phase information in PoA is used to estimate the target location. Although PoA can provide high accuracy, especially in environments with limited multipath path effects, it is challenging because it requires precise measurement and is sensitive to environmental factors and frequency offset[30,31].

The PoA is estimated by evaluating the phase difference of the signal received at various antennas. Mathematically, the phase difference $\Delta\phi$ between the two antenna positioned at a distance d is represented as

$$\Delta\phi = \frac{2\pi d \cos\theta}{\lambda}, \tag{1}$$

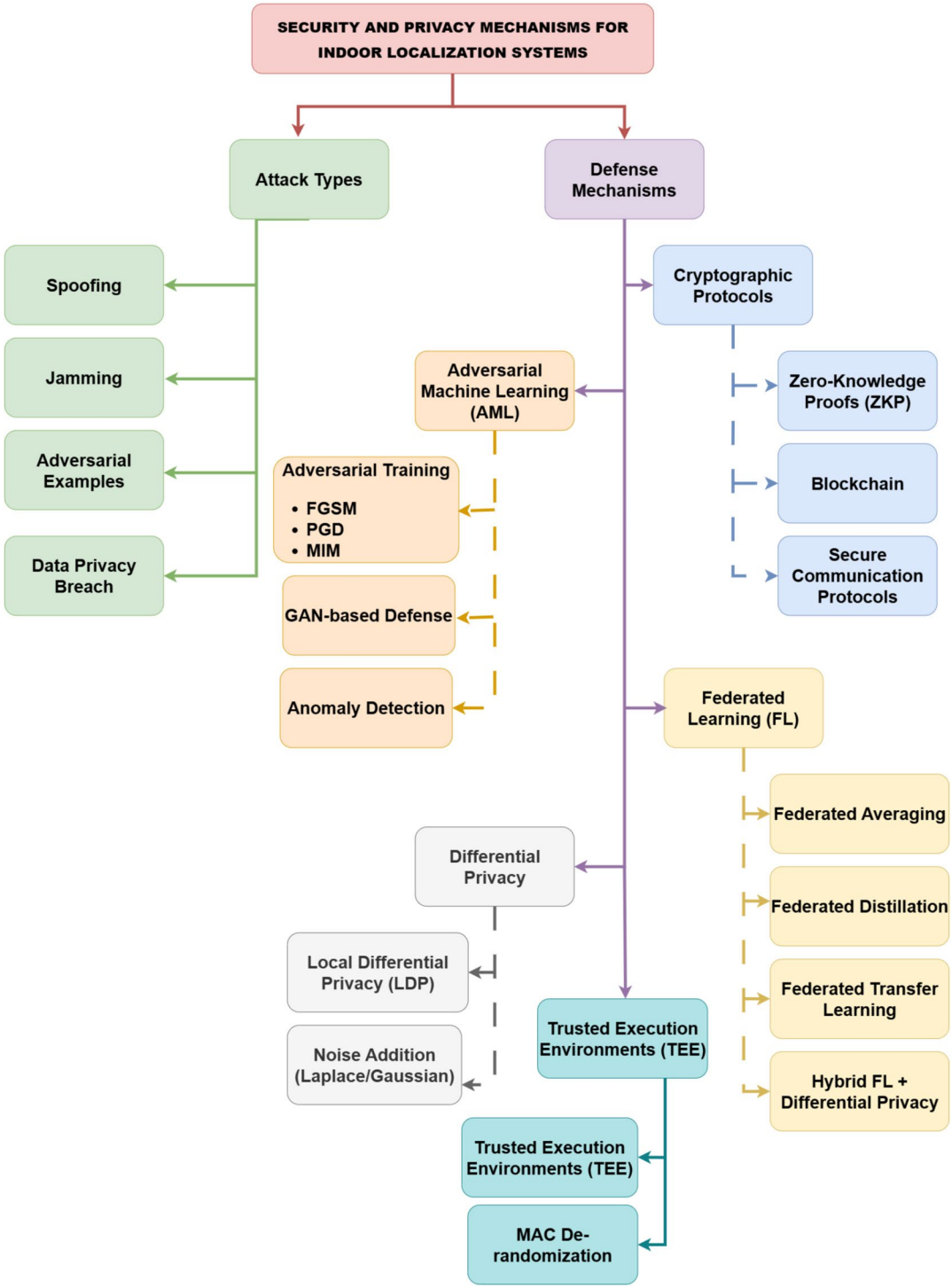


Fig. 3. Taxonomy of security and privacy mechanisms for indoor localization systems (ILS), classified by attack type, mitigation approach, and system architecture.

where, θ is the angle of arrival of the signal, λ represents the wavelength of the signal, and d denotes the distance between the antennas. The angle of arrival, θ, can be approximated using the measured phase difference $\Delta\phi$:

$$\theta = \cos^{-1}\left(\frac{\Delta\phi \cdot \lambda}{2\pi d}\right). \tag{2}$$

The approximated phase can then be used to determine the target's position in either a two or three dimensional space. The effectiveness of this method depends upon the accurate measurements and careful calibration, which

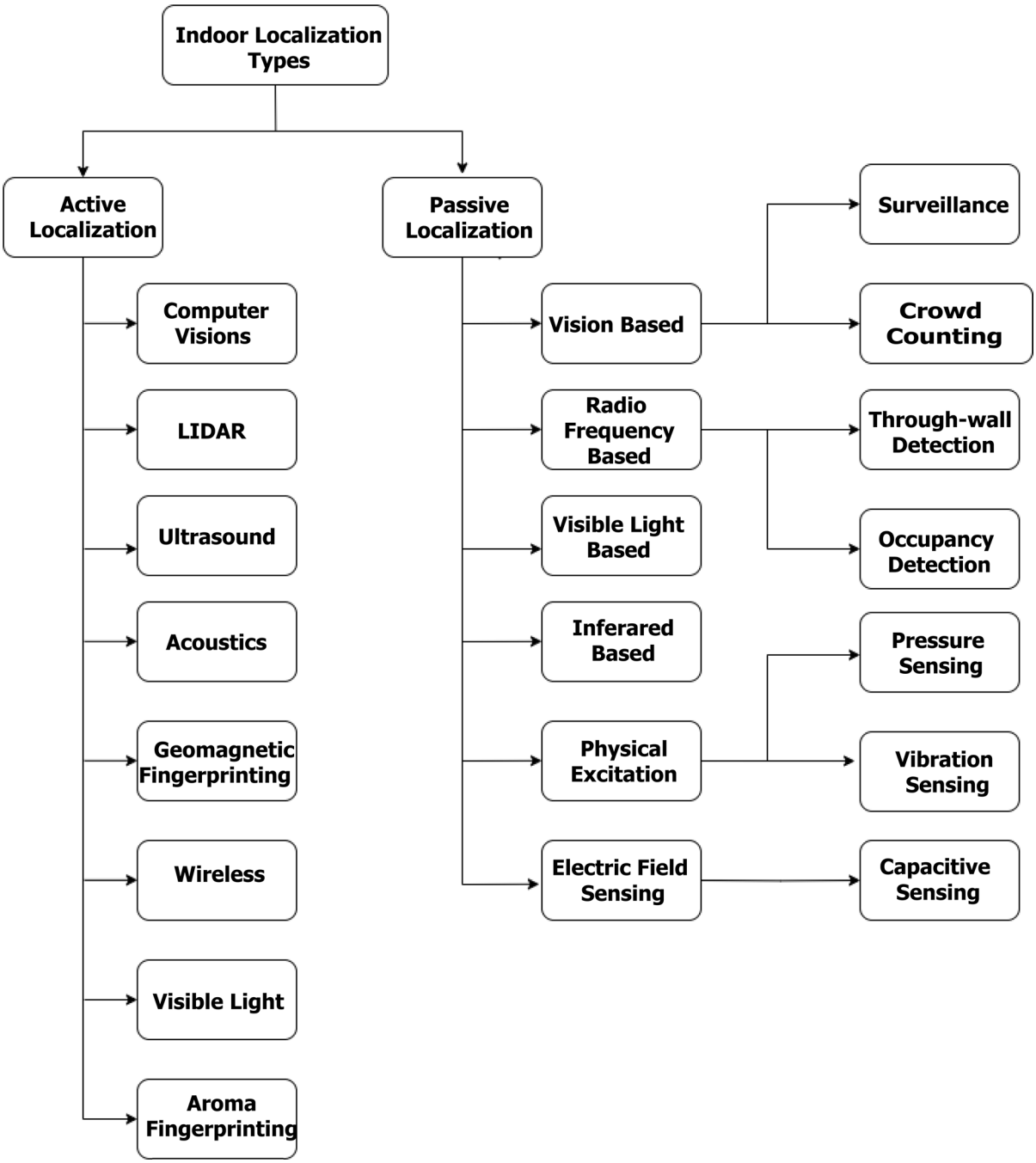


Fig. 4. Types of indoor localization.

help mitigate influences such as frequency offset and environmental noise. Although PoA provides high accuracy in controlled settings, its susceptibility to noise, frequency offsets, and calibration issues limits its practicality in dynamic or large-scale applications.

Angle of arrival (AoA)

Angle of arrival (AoA) is a method that measures the direction from which a signal reaches the receiver. This method triangulates the target location by combining multiple AoAs from different receiver locations. AoA provides high accuracy, especially when directional antennas are used. However, it requires specialized hardware and can be affected by multipath interference[32]. In practice, the AoA technique determines the angle θ of the incoming signal at each receiver, which can be calculated using the coordinates of the transmitter (x_t, y_t) and the receiver (x_r, y_r).

$$\theta = \tan^{-1}\left(\frac{y_t - y_r}{x_t - x_r}\right). \tag{3}$$

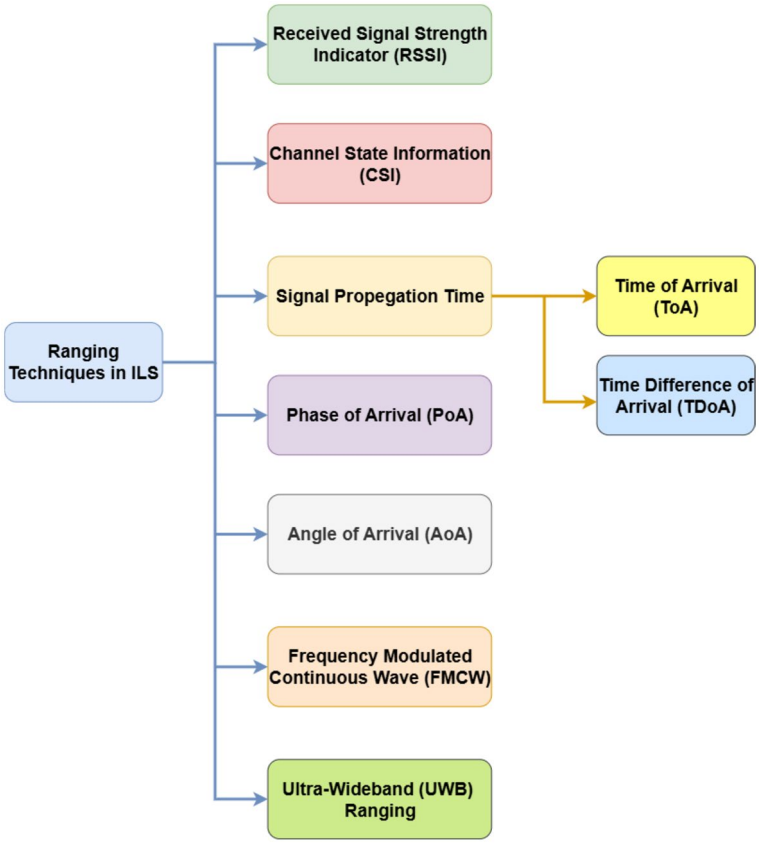


Fig. 5. Ranging techniques in ILS.

Several receivers with known positions are employed to determine the transmitter's location through triangulation. Using the AoA information θ_i at receiver i, the lines of bearing (LoB) can be described as

$$y - y_{r_i} = \tan(\theta_i) \cdot (x - x_{r_i}), \tag{4}$$

(x_{r_i}, y_{r_i}) denotes the coordinates of the i-th receiver. The intersection of these LoBs from various receivers yields the estimated location of the transmitter (x_t, y_t). In actual situations, noise and multipath effects can distort AoA readings, requiring error minimization strategies to enhance the accuracy of the estimated position.

Although AoA is highly accurate, it is especially susceptible to multipath effects. Additionally, the requirement for specialized directional antennas and noise reduction techniques can make its deployment in real-world situations more complex.

Signal propagation time

In the signal propagation time technique, the distance between the target and a reference point (RP) with a known location is estimated by measuring the time it takes for a signal to arrive between them. Based on this principle, two common techniques are used, namely time of arrival (ToA) and time difference of arrival (TDoA). ToA provides high accuracy in line of sight (LOS) environments but its performance decreases in no line of sight (NLOS) scenarios due to the multi-path effect and signal reflection[33]. A major challenge in ToA is the need for accurate time synchronization between the transmitter and receiver, which TDoA addresses. However, TDoA requires multiple receivers and the use of complex algorithms to estimate the target location, which introduces its own difficulties.

In the ToA method, the distance d between the transmitter and receiver is calculated as

$$d = c \cdot t, \tag{5}$$

where c is the speed of light (or more generally, the signal propagation velocity in a medium), and t represents the measured signal propagation duration. This equation presumes that the signal propagates on a linear trajectory without considerable delays caused by obstructions.

The TDoA technique uses the time difference of arrival (Δt) between two receivers at known locations to calculate the difference in distances (Δd) from the target to these receivers, expressed as $\Delta d = c \cdot \Delta t$. Here, Δt represents the time difference between the signals reaching the two receivers, defined as $\Delta t = t_2 - t_1$, where t_1

and t_2 denote the arrival times at the first and second receivers, respectively. The target's location is determined by integrating several measurements through trilateration or other geometric methods.

ToA and TDoA perform well under ideal line-of-sight conditions, but their accuracy decreases in non-line-of-sight environments. Beyond classical multilateration, a recent approach couples propagation modeling with a genetic algorithm to efficiently explore the position space and improve indoor localization under multipath constraints[34].

Received signal strength indicator (RSSI)

RSSI, as the name suggest, is a measure of the real signal power received by the receiver. It is calculated in decibel milliwatts (*dBm*) or milliwatts (*mW*)[35]. The RSSI technique estimates the distance between the transmitter and receiver based on the strength of the received signal. As the distance between the devices increases, the signal strength decreases, which is used to approximate the distance between them.

The received signal strength (RSS) is represented by the path loss equation:

$$P_r(d) = P_t - 10 \cdot n \cdot \log_{10}(d) + X_g, \tag{6}$$

where $P_r(d)$ represents the received power at a distance d (in dBm), P_t denotes the transmitted power (in dBm), n signifies the path loss exponent (typically ranging from 2 to 4 in indoor environments), d indicates the distance between the transmitter and receiver (in meters), and X_g refers to the Gaussian noise that accounts for environmental factors (e.g., obstacles and interference). The estimated distance $\hat{d}$ can be computed using the following equation:

$$\hat{d} = 10^{\frac{P_t - P_r(d) + X_g}{10 \cdot n}}. \tag{7}$$

RSSI based localization is easy to implement without requiring complex hardware or calculations. Another advantage of RSSI is that they are inexpensive and are widely supported by existing wireless technologies like Wi-Fi and Bluetooth. Accuracy of RSSI is directly influenced by environmental factors like obstacles, interference, and multi-path propagation[36]. Compared to other techniques RSSI is generally less accurate, especially in complex indoor environments.

RSSI provides ease of use and cost benefits; however, it faces challenges with accuracy in areas with many obstacles or interference, which reduces its reliability for accurate indoor localization.

Frequency modulated continuous wave (FMCW)

FMCW is a technique in which a continuous waveform is transmitted along with its frequency modulation over time. The transmitted signal can be represented as

$$s_{\mathrm{tx}}(t) = A \cos\left(2\pi f_0 t + \pi k t^2\right), \tag{8}$$

where A denotes the amplitude of the signal, f_0 represents the initial frequency, and $k = \frac{B}{T}$ represents the chirp rate, with B indicating the bandwidth and T the duration of the chirp. This signal reflects off an object and is received by the system. The received signal, delayed by the duration τ, is expressed as

$$s_{\mathrm{rx}}(t) = A \cos\left(2\pi f_0 (t-\tau) + \pi k (t-\tau)^2\right). \tag{9}$$

The system estimates the frequency shift f_Δ, defined as the difference between the transmitted and received signals. The frequency shift is expressed as

$$f_\Delta = k\tau = \frac{2kR}{c}, \tag{10}$$

where $\tau = \frac{2R}{c}$ denotes the round-trip time delay, R represents the distance from the transmitter to the object, and c signifies the speed of light. Hence, the distance R to the item can be calculated using the formula:

$$R = \frac{c f_\Delta}{2k}. \tag{11}$$

FMCW is a versatile technique that supports both short- and long-range sensing, making it suitable for a wide range of indoor applications[37]. While it offers high accuracy, its performance is sensitive to environmental factors and relies on advanced signal processing and sophisticated hardware. These requirements increase system cost and complexity, limiting its feasibility for large-scale or cost-sensitive deployments[38].

Channel state information (CSI)

CSI is an advanced technique for measuring distance in ILS. CSI holds detailed data about the propagation characteristics of a wireless communication channel like Wi-Fi. It includes information regarding the variations in signal as it passes through an environment, which can be affected by factors like walls, furniture, and people moving around[39]. CSI provides more precise data compared to traditional RSSI data which allows for a more accurate localization, device tracking, and environment sensing.

The CSI captures the frequency response of the channel, mathematically expressed as

$$H(f) = |H(f)|e^{j\phi(f)}, \tag{12}$$

where $H(f)$ denotes the complex channel frequency response at frequency f, $|H(f)|$ represents the amplitude response, and $\phi(f)$ indicates the phase response. The received signal can be expressed with the CSI as follows:

$$Y(f) = H(f) \cdot X(f) + N(f), \tag{13}$$

In the frequency domain, $Y(f)$ denotes the received signal, $X(f)$ signifies the broadcast signal, $H(f)$ represents the CSI, and $N(f)$ indicates noise. In a multipath environment, where signals arrive at the receiver via multiple routes, the CSI is generally represented as

$$H(f) = \sum_{i=1}^{L} \alpha_i e^{-j2\pi f \tau_i}, \tag{14}$$

where L denotes the number of propagation paths, α_i signifies the amplitude attenuation of the i-th path, and τ_i indicates the propagation delay of the i-th path.

CSI provides exceptional accuracy and depth in localization data through its comprehensive channel measurements. However, its substantial computational demands and sensitivity to environmental changes pose considerable challenges for real-time and resource-limited applications.

Localization algorithms

Indoor localization algorithms are used to determine the position of a target object based on factors like RSSI, CSI, ToA, etc. These algorithms are broadly classified as follows:

Proximity-based algorithms

Proximity-based localization algorithms determine the location of a device by measuring its closeness to some known fixed point[40]. Bluetooth beacons are a common proximity-based approach that measures device closeness by measuring the strength of the signals from the beacons set at known locations. This method is commonly implemented in indoor environments. Near-field communication (NFC) is another example of a proximity-based algorithm in which the location of the device is determined by directly interacting with NFC tags that are embedded in the area of interest.

Triangulation-based algorithms

Triangulation-based algorithms utilize the geometric relationship between the known RP or anchor. It includes methods like lateration[13], which determines the target distance from multiple anchors to calculate its location. TDoA and ToA are examples of lateration, which improves localization accuracy using signal travel times. Angulation (or AoA) is another triangulation-based algorithm that estimates the target location using the measure of the angle of the signal arriving from multiple anchors. Both lateration and angulation are widely used methods, and they balance accuracy and computational requirements based on the indoor environment and infrastructure.

Dead reckoning

Dead reckoning, though a navigation method, can be used for indoor localization. It estimates the current position of the target using previously known locations, along with its velocity measurement and direction of movement. Dead reckoning is sensitive to error accumulation over time[41]; hence, it is often combined with other localization techniques to improve its accuracy.

Trilateration/multilateration

Trilateration and multilateration are techniques that find an unknown node by using three (in the case of trilateration) or more (in the case of multilateration) reference nodes. In trilateration, the position of the target node is determined by finding the intersection of three imaginary circles that are centered at the reference nodes[42].

Magnetic field-based localization

In the magnetic field-based localization algorithm, distortions in the earth's magnetic field are used to pinpoint locations[43]. This distortion in the magnetic field is caused by the structural elements of the buildings. Magnetic field-based localization involves creating detailed maps of the indoor environment's magnetic field, which are then used as references in indoor localization.

Range-free

Range-free localization algorithms are methods that do not rely on distance or angle measurements to predict the position of the target and are used in wireless sensor networks (WSNs). Range-free localization algorithms use, instead, the connectivity information to infer the relative position of nodes in a network. Common range-free algorithms include distance vector-hop (DV-Hop)[44], centroid localization, approximate point-in-triangulation (APIT), and multidimensional scaling mapping (MDS-MAP).

Machine learning (ML)-based algorithms

ML-based algorithms use methods like neural networks, like deep neural networks (DNNs), convolutional neural networks (CNNs), and recurrent neural networks (RNNs), to improve localization accuracy by learning from a large dataset[35]. These neural networks effortlessly model complex relationships between the signal features and specific location coordinates. Support vector machines (SVMs) are another ML algorithm used for localization problems due to their robust classification capabilities. SVMs efficiently determine the position based on different signal attributes.

Fingerprinting

Fingerprinting in indoor localization is the process of creating a radio map (database) of signal characteristics like RSSI and CSI at multiple locations in the area of interest[45]. This radio map is used as a reference to match the current signal measurements with those in the database and predict the location based on this comparison. The most popular method, Wi-Fi fingerprinting, uses RSSI data from many APs to estimate the device location. Another method of fingerprinting is RFID fingerprinting, which builds complex signal maps using RFID tags and readers, allowing for more accurate localization (Fig. 6).

Related work

ILS security and privacy surveys and case studies are reviewed in this section, highlighting key findings and limitations. It includes case studies and real-world applications in indoor localization from 2020 to 2025.

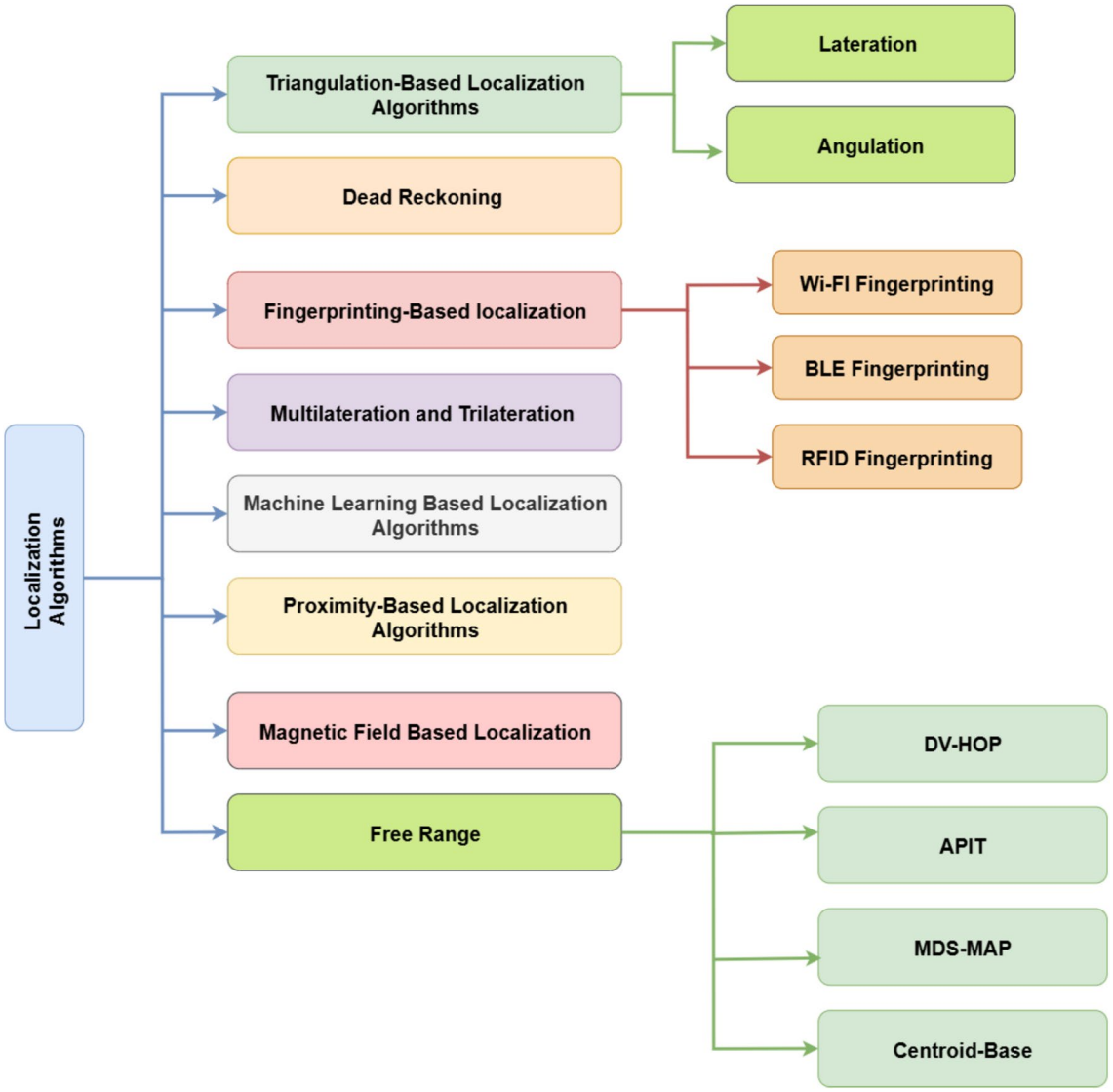


Fig. 6. Localization algorithms.

Existing surveys and reviews

Recent surveys on ILS have explored various aspects of security and privacy, yet gaps remain in their coverage and depth. Early reviews, such as[46], provided a foundational categorization of privacy concerns–device, transmission, and server-level–but their relevance is limited due to outdated datasets. More recent works have examined the intersection of machine learning and IoT security[47], as well as the broader landscape of indoor/outdoor localization in IoT[42]. Studies focusing on specific technologies, like BLE in wearable devices[48], and deep learning-based approaches using Wi-Fi, Bluetooth, and UWB[49], highlight ongoing challenges such as multipath interference, data scarcity, and environmental noise. While these surveys contribute valuable insights, particularly on hybrid techniques and device-free localization, standardization and efficiency remain critical concerns. More recent efforts[7] have introduced structured classifications based on collaboration and security principles but offer limited treatment of privacy-preserving methods. Privacy-specific surveys[5,50] have begun to explore novel attack models and protection strategies in location fingerprinting, though their scope is often narrow and lacks comprehensive analysis. Overall, existing literature reveals a fragmented approach to privacy in ILS, underscoring the need for more integrative and up-to-date reviews. For a cutting-edge 2025 synthesis of AI–cybersecurity fusion trends–spanning FL, AML, privacy mechanisms, and policy directions–see[51], which complements our ILS-focused review. Given that several pre-2020 surveys are limited or outdated with respect to modern datasets and techniques, our review focuses on 2020–2025 to provide an up-to-date synthesis that complements these earlier works.

Evolution of security and privacy techniques in indoor localization

2020

Several studies have explored privacy and security concerns in indoor positioning systems (IPS), particularly the handling of sensitive user data and resilience against adversarial behavior. Barsocchi et al.[52] propose a GDPR-compliant, privacy-by-design framework for location-based services, demonstrated through a Telegram-based proximity marketing application. While the architecture supports regulatory compliance, it remains limited in scope and reveals ongoing vulnerabilities in data protection. Addressing malicious data manipulation, Li et al.[53] introduce the ACTD framework, which employs machine learning and outlier detection to identify anomalous RSS fingerprint submissions. Although effective in simulations, the lack of real-world validation limits its practical reliability. To counter fraudulent check-ins, Li et al.[54] present an AP subset selection strategy that optimizes positioning accuracy and robustness; however, the method is sensitive to environmental variation, computationally demanding, and may struggle with emerging threats. Expanding on this, Li et al.[55] propose a boundary-based defense using fingerprint refinement and level-set methods to improve localization security. Despite promising simulated results, its effectiveness remains constrained by untested assumptions and partial mitigation of attack vectors.

Building on these efforts to strengthen IPS resilience, Yang et al.[56] focus on secure state estimation under sensor attacks, where measurements can be manipulated even with protected communication channels. Their map-based localization algorithm ensures robust estimation against such threats, though practical deployment under diverse attack scenarios remains unexplored. To address localization in large, multi-floor environments with limited labeled data, Li et al.[57] propose a decentralized federated learning (FL) approach combined with pseudo-labeling. Their centralized indoor localization method using the Pseudo-label(CRNP) method enhances accuracy while preserving privacy and reducing network costs, yet challenges persist with data heterogeneity, privacy sensitivity, and the computational burden of distributed training. In parallel, Ko et al.[58] introduce RFBSA, a random forest-based filter designed to mitigate localization errors caused by MAC spoofing. The technique proves effective against attacker-generated noise, outperforming traditional filters and deep learning models, but maintaining robustness against increasingly sophisticated spoofing remains a concern. Ciftler et al.[59] further explore privacy-preserving localization by applying FL to crowdsourced RSS fingerprint data. While achieving notable accuracy gains and safeguarding user privacy, their approach is constrained by scalability issues, slower convergence on non-IID data, and the performance limitations of low-power devices in real-time scenarios.

Further contributions focus on enhancing privacy and spoofing resistance in localization systems. Zhang et al.[60] propose a lightweight privacy-preserving solution (LWP^2) for Wi-Fi fingerprinting, utilizing the Paillier cryptosystem to perform secure computations in the encrypted domain. Although it improves localization accuracy and privacy, the method incurs higher processing and communication overhead and offers limited protection for the localization server itself. Shubina et al.[61] explore the privacy-accuracy trade-off in wearable networks, introducing metrics that allow users to manage location obfuscation. Their findings are informative for dense environments but may not generalize to sparse settings and highlight the ongoing challenge of balancing privacy with utility in location-based services. To detect physical-layer spoofing, Yan et al.[62] develop PHY-IDS, an RSSI-based system that performs well against both naïve and informed attackers. However, its scope is limited to wearable devices and does not address broader security threats. Similarly, Madani et al.[63] present a randomized moving target defense (RMTD) for detecting MAC spoofing in IoT systems. By dynamically altering network parameters, RMTD improves spoofing resistance but depends heavily on accurate modeling of advanced adversarial behavior, which may not always be feasible.

Privacy-preserving and three-dimensional localization techniques have also received notable attention. Nieminen et al.[64] propose a secure two-party computation method for indoor localization, integrating Wi-Fi fingerprinting with privacy models. While their Android-based proof-of-concept demonstrates feasibility with reasonable retrieval times, scalability is hindered by computational and communication overhead. Kordi et al.[65] offer a broad review of wireless IoT-based indoor localization methods, covering proximity, lateration, fingerprinting, and hybrid techniques. Although the study provides a useful taxonomy and highlights the potential of machine learning for optimization, it lacks empirical performance evaluations and real-world deployment considerations. Addressing the limitations of 2D systems, Alhammadi et al.[66] present a 3D Bayesian

graphical model (3D-BGM) that reduces reference point requirements while achieving competitive accuracy. Despite outperforming several baseline models, the system's reliance on static environments and challenges in scaling to multi-story buildings limit its generalizability. A related approach by the same authors[67] extends 3D-BGM with RF fingerprinting, leveraging existing Wi-Fi infrastructure to improve localization accuracy and efficiency. However, the system still requires frequent radio map updates and does not fully address scalability, security, or privacy in dynamic IoT environments.

2021

Adversarial robustness and cross-technology attacks have emerged as critical challenges in indoor localization and activity recognition systems. Patil et al.[68] explore the vulnerability of RSSI-based systems to adversarial inputs, demonstrating that their deep learning model (DMLP) outperforms traditional methods and benefits from adversarial training. However, the model remains limited by its focus on white-box attacks, susceptibility to dynamic environments, and dependency on high-quality RSSI data. Similarly, Ambalkar et al.[69] investigate adversarial attacks on Wi-Fi CSI-based human activity recognition systems, proposing a defense framework using Projected Gradient Descent (PGD) and Momentum Iterative Method (MIM) techniques. While the framework enhances resilience, it shares limitations with Patil et al., including an exclusive focus on white-box scenarios, sensitivity to data quality, and lack of real-world validation. Addressing secure indoor localization at scale, Wang et al.[70] present RMBMFL, a multi-task collaborative learning approach achieving high accuracy in large building environments. Despite its strong performance, the method's generalizability is uncertain due to evaluation on a single, fixed site. In a related threat landscape, Na et al.[71] introduce Wi-attack, a cross-technology impersonation attack exploiting BLE advertising via Wi-Fi. Although their detection method based on power consumption variance shows promise, the approach suffers from high localization errors, low packet reception rates, and reliance on cross-technology interaction, limiting practical deployment.

Comparative evaluations of indoor localization technologies have revealed both performance differences and persistent security challenges. Dervicsouglu et al.[72] assess UWB and BLE systems, showing that UWB achieves superior accuracy (0.43 m vs. BLE's 1.54 m), but note that variations in standards and distance estimation methods introduce unpredictable security vulnerabilities, with BLE being less reliable for precise positioning. Expanding on BLE-based solutions, Sun et al.[73] propose a crowdsourced localization framework using dual BERT models–BERT-AD for adversarial sample detection and BERT-LOC for localization refinement. While the system improves robustness and accuracy, its reliance on BLE alone, environmental sensitivity, and scalability issues limit broader applicability. In parallel, Madani et al.[74] introduce an LSTM autoencoder-based method for detecting MAC-layer spoofing in IoT networks using RSSI data. The model handles real-time detection and adapts to signal volatility, but its applicability is constrained to specific topologies, lacks multi-node coordination, and depends on manual data labeling. Addressing data scarcity, Njima et al.[75] employ GAN-based augmentation with semi-supervised learning to improve RSSI-based localization. Their approach enhances accuracy on both simulated and real datasets, yet still falls short of optimal performance and faces limitations related to training data requirements and potential inaccuracies in synthetic samples.

Security vulnerabilities in Wi-Fi-based activity recognition and location privacy remain pressing concerns. Huang et al.[76] introduce IS-WARS, a stealthy adversarial attack that manipulates wireless interference from protocols like ZigBee and Bluetooth to mislead Wi-Fi-based recognition systems without detection. Their results expose the vulnerability of such systems to cross-protocol interference, which is often overlooked, compromising reliability in real-world environments. To address location privacy, Min et al.[77] propose a 3D geo-indistinguishability (3D-GI) mechanism that perturbs user coordinates while maintaining service quality. Although the method effectively adapts 2D privacy models to 3D settings, it remains simulation-based and lacks real-world validation, limiting its practical impact. Beko et al.[78] focus on secure localization in randomly deployed networks, combining clustering, weighted central mass, and a bisection-based GTRS approach to detect spoofing and improve localization accuracy. While outperforming existing methods in simulations, the framework's dependence on specific network assumptions may hinder its adaptability to dynamic, real-world scenarios.

2022

Privacy-preserving indoor localization continues to evolve through edge computing, federated learning, and anonymization frameworks. Zhang et al.[79] introduce Adp-FSELM, a federated stacked extreme learning model integrated with differential privacy within an edge computing framework. The system achieves robust ε–differential privacy and low localization error while minimizing calibration effort. However, fingerprint collection remains labor-intensive, and scalability is limited. Similarly, Navidan et al.[80] propose a local differential privacy (LDP)-based framework for population frequency estimation in indoor spaces. Though effective under moderate privacy settings, its performance degrades with increased noise and varies across datasets, limiting generalizability. Fathalizadeh et al.[81] address location privacy using a k-anonymity and l–diversity model combined with Dijkstra's algorithm, allowing secure data sharing while maintaining utility. Still, the method overlooks more sophisticated threats like poisoning and collusion and incurs computational overhead, reducing its adaptability to dynamic or sparsely covered environments. In a related study, Boora et al.[82] focus on adversarial robustness in large MIMO localization using DCNNs and neural ODEs. While adversarial training enhances resilience, models remain sensitive to noise and hyperparameters, and suffer from high computational costs, limiting scalability in real-world, evolving environments.

Adversarial training and federated learning continue to play a central role in enhancing the robustness of indoor localization and activity recognition systems. Yang et al.[83] propose SecureSense, which employs techniques like label smoothing and virtual adversarial training to improve defense against both black-box and white-box attacks in device-free human activity recognition. While it strengthens DNN resilience, challenges

such as training instability, hyperparameter sensitivity, and limited real-world validation restrict its deployment in dynamic or resource-constrained environments. In a similar direction, Ye et al.[84] introduce SE-Loc, a semi-supervised method that effectively combines labeled and unlabeled data for secure indoor localization. Despite high robustness under adversarial conditions, its accuracy is still affected by the presence of numerous malicious APs. Addressing adversarial threats in RSSI-based systems, Wang et al.[85] develop AdvLoc using DCNNs with adversarial training, demonstrating strong performance against first-order attacks. However, the method lacks evaluation against more advanced attacks and across diverse environments. Han et al.[86] present a CNN and ResNet-based defense for device-free localization that effectively detects spoofed signals and sensor faults, though it remains vulnerable to physical damage and tampering. Finally, Gao et al.[87] propose FedLoc3D, a federated learning framework for cross-building 3D localization. Their approach, combining CNN-based classification and regression models, shows improved accuracy and privacy preservation but faces challenges related to network unreliability, data heterogeneity, and scaling in 3D environments.

2023

Recent efforts have focused on enhancing the reliability, security, and privacy of indoor localization systems through trust modeling, blockchain, and decentralized authentication. Peterseil et al.[88] propose a trustworthiness score integrated with autoencoder neural networks and weighted non-linear least squares to reduce UWB localization errors by up to 50% in dynamic environments. While effective in controlled settings, the approach relies heavily on high-quality training data and requires calibration for varied deployments, limiting scalability and robustness under non-line-of-sight conditions. Shakerian et al.[89] introduce a blockchain-supported indoor navigation system combining dual IMU sensors and the ZUPT algorithm, achieving reliable navigation with a mean root mean square error (RMSE) of 1.2 m. Despite secure data handling through Hyperledger Fabric, challenges include limited energy capacity, dependence on Wi-Fi, and untested performance under complex movements or large-scale deployments. Addressing adversarial threats, Mitchell et al.[90] assess the vulnerability of learning-based localization models, showing that omniscient attacks significantly degrade accuracy. While adversarial training and outlier detection improve resilience, broader threat models and infrastructure-level vulnerabilities remain unexplored. Casanova et al.[91] propose a decentralized attribute-based authentication (ABA) protocol using BLE and zero-knowledge proofs to secure collaborative indoor positioning systems. The protocol improves privacy, untraceability, and unlinkability, offering a practical alternative to centralized schemes, though it highlights the limitations of existing CIPS protocols in safeguarding user identity.

Privacy, energy efficiency, and threat detection remain key themes in recent indoor localization research. Mohsen et al.[92] present PassiFi, a privacy-preserving system using passive Wi-Fi TDoA and deep learning regression to achieve sub-meter accuracy, outperforming traditional multilateration. However, its scalability and performance degrade under environmental changes, and privacy trade-offs–such as reliance on trusted entities and vulnerability to spatio-temporal attacks–remain unresolved. Focusing on secure 3D localization, Kalpana et al.[93] propose a hybrid method combining acoustic and distance-based approaches with cryptographic safeguards. Their solution reduces localization error and energy use while identifying Sybil and malicious nodes. Yet, computational overhead, sensitivity to RSSI fluctuations, and reliance on beacon nodes limit its real-time applicability. In a related effort, Gebremariam et al.[94] develop a hybrid machine learning framework for detecting routing threats in WSNs, achieving high localization precision and perfect threat detection in simulations. Nevertheless, the model's processing demands, dependency on accurate training data, and lack of validation in dynamic environments raise concerns about scalability and practical deployment. Addressing spoofing attacks, Chen et al.[95] introduce UnSpoof, a UWB-based system leveraging passive anchors and secure two-way ranging to detect and locate spoofed tags. While effective at distinguishing spoofed from genuine tags, its accuracy declines when devices fall outside the anchor-defined area, and its adaptability to diverse spoofing techniques remains uncertain.

Adversarial robustness, privacy, and federated learning continue to shape the advancement of indoor localization systems. Xiao et al.[96] propose FooLoc, an over-the-air adversarial attack that generates subtle yet effective perturbations to mislead Wi-Fi-based DNN localization models, achieving up to 90% success in untargeted attacks. Despite its efficiency, the method relies on downlink CSI and faces challenges in practical implementation due to the limitations of additive perturbation on CSI measurements. Addressing privacy, Fathalizadeh et al.[97] introduce GeoInd, a differential privacy-based framework that adds Gaussian noise to RSS data for geo-indistinguishability without relying on third parties. While effective in simulations, its lack of real-world deployment and limited scope raise concerns about broader applicability. In the realm of federated learning, Guo et al.[98] present FedPos, a federated transfer learning system that reuses feature extractors across domains to reduce training data needs by 65% and achieve a mean localization error of 42.18 cm. However, its performance may be insufficient for precision-critical applications and remains validated only in limited indoor environments. Gufran et al.[99] further advance this field with FedHIL, a heterogeneous FL framework incorporating stacked autoencoders and communication-efficient strategies to enhance accuracy while reducing latency. Though it outperforms existing models, its sensitivity to device heterogeneity, environmental noise, and generalization issues limits its scalability and robustness in dynamic settings.

Privacy-preserving indoor localization techniques have increasingly incorporated differential privacy, reinforcement learning, and federated learning. Xu et al.[100] utilize Wi-Fi fingerprints and extreme learning machines with local differential privacy (LDP) to reduce data exposure during model training, demonstrating improved privacy with lower data quality degradation than centralized approaches. However, their method still suffers from up to 7.2% data loss and potential performance trade-offs compared to established techniques. Addressing semantic location privacy, Min et al.[101] propose SALPPM, a reinforcement learning-based framework using modified geolocation data and semantic tags in 3D indoor environments. By leveraging D3QN and A3C algorithms, the system refines perturbation strategies and policy selection. Yet, its scope is limited to specific

RL methods, excluding alternative algorithms or continuous action spaces, which may hinder adaptability. Similarly, Kumar et al.[102] present f-ILC, a federated learning-based Wi-Fi fingerprinting framework combining CNN-LSTM to enhance localization accuracy and preserve user anonymity. The system performs well across IID and non-IID settings but faces challenges in hierarchical space modeling, resource demands, and real-time deployment feasibility. Finally, Shahbazian et al.[103] provide a broader examination of machine learning applications in IoT localization, highlighting both current limitations and future opportunities, though lacking specific experimental validations or frameworks.

Security and privacy remain central to recent innovations in indoor localization. Chen et al.[104] propose UnSpoof-Passive Ranging, a hybrid active-passive system that achieves 30 cm accuracy for legitimate tags and sub-meter precision for spoofed tags using ToF and TDoA measurements. While effective at detecting distance manipulation attacks even beyond the anchor convex hull, its performance is sensitive to anchor geometry, non-line-of-sight conditions, and multi-antenna spoofing. Additional limitations include high energy consumption, computational overhead, and limited scalability in multi-client deployments. In a parallel effort, Wang et al.[105] introduce a privacy-preserving localization method based on two-party computation and Paillier encryption, offering enhanced RSS protection and reduced communication costs. However, the computational complexity of encryption may hinder real-time performance, and the reliance on a two-party model restricts applicability in decentralized systems. Addressing access point vulnerabilities, Tiku and Pasricha[106] develop S-CNNLOC, a secure CNN-based framework that improves robustness against AP-level attacks, achieving up to 10 times greater resilience than conventional models. Despite its strong accuracy and security gains, challenges remain in scaling the framework and adapting it to diverse and dynamic network environments.

Recent advancements in indoor localization continue to address challenges related to security, privacy, and performance under dynamic conditions. Ma et al.[107] propose LENSER, a CSI-based system for detecting unauthorized devices, which improves localization accuracy by 86.1% and reduces time overhead by 58.2% compared to existing methods. Despite these gains, the system remains sensitive to environmental fluctuations, indicating a need for enhanced robustness. Brachmann et al.[108] examine privacy risks in XR localization using the LINDDUN framework, identifying threats such as identifiability and linkability in XR glasses and suggesting targeted mitigation strategies. However, the framework's reliance on static threat categories may limit its adaptability in evolving XR scenarios. To strengthen privacy in LBS, Yan et al.[109] introduce LDPORR, a local differential privacy method that applies Hilbert encoding and spatial decomposition to enhance both privacy and efficiency. While effective on real-world datasets, its processing complexity may hinder scalability in dynamic environments. Pandey and Patel[110] develop SLABLDA, a secure fingerprinting algorithm that models AP location diversity and compensates for RSSI variability, yielding improved accuracy in complex indoor environments. Nonetheless, reliance on offline evaluations may restrict responsiveness in rapidly changing conditions. Lastly, Billa et al.[111] offer a comprehensive review of indoor localization technologies for IoT systems, highlighting the trade-offs between cost and accuracy, particularly in hybrid and high-precision systems like UWB and VLC. Their work underscores the need for adaptable and cost-effective solutions that balance performance and practical deployment constraints.

2024

Recent research in 2024 has focused on enhancing indoor localization systems through federated learning, adversarial resilience, and cryptographic privacy-preserving techniques. Etiabi et al.[112] propose a federated distillation (FD) approach that reduces communication overhead in IoT networks by 98% while maintaining localization accuracy and improving energy efficiency. However, its applicability to regression-based tasks like localization remains limited, and transmission energy savings come at the cost of increased computational demand. Gufran et al.[113] introduce CALLOC, a lightweight, adversarial-resilient framework leveraging curriculum learning to improve localization robustness across devices and settings. Although it significantly reduces localization error, its performance depends heavily on curriculum design and has yet to be validated in dynamic real-world environments. Additionally, the computational load from attention mechanisms and adversarial training may hinder deployment on low-power devices. Eshun et al.[114] present a cryptographic localization framework that ensures mutual privacy between users and service providers by offloading encrypted computation to a third-party cloud server. While it achieves up to 99% cost reduction, the system's resilience against active adversaries remains unexplored. Huang et al.[115] examine vulnerabilities in off-device wireless positioning systems and demonstrate practical attacks using homomorphic encryption and oblivious transfer. Although defenses are proposed, the study is confined to specific wireless environments, and inherent privacy concerns in off-device architectures present challenges for secure deployment in future networks.

Privacy-preserving indoor localization systems in 2024 have increasingly leveraged generative models, differential privacy, and adversarial threat analysis. Moghtada et al.[116] propose DPGANs, a framework combining generative adversarial networks with differential privacy to protect user data while generating realistic synthetic fingerprints. While effective at preserving accuracy under moderate privacy constraints, performance degrades at higher privacy levels, and the reliance on a single generator-discriminator pair limits scalability and adaptability to complex environments. Fathalizadeh et al.[5] provide a comprehensive review of privacy-preserving fingerprinting techniques, offering a novel classification framework for adversary models, vulnerabilities, and evaluation metrics. The study highlights critical research gaps and encourages future exploration into unified privacy frameworks. Examining attack impacts, Machaj et al.[117] analyze Wi-Fi AP spoofing using KNN and the UJIIndoorLoc dataset, showing significant degradation in localization accuracy tied to the number of spoofed APs and reference points. However, the study's focus on a single method and dataset limits generalizability to broader contexts and techniques. Addressing task privacy in mobile crowdsensing, Hemkumar et al.[118] introduce a geo-obfuscation strategy combining local differential privacy, geo-indistinguishability, and k-means clustering to defend against inference attacks. Despite outperforming existing methods like Eclipse and PIVE,

its effectiveness depends on environmental conditions, clustering parameters, and AP density, and it lacks evaluation against more advanced or emerging attack models.

Emerging 2024 studies continue to explore privacy threats and adversarial defenses in indoor localization. Li et al.[119] propose RFTrack, a stealthy tracking attack that leverages RSSI time sequences and reinforcement learning to infer device locations using passive Wi-Fi sniffing. While it achieves high precision in structured environments, its effectiveness is limited by RSSI instability, bootstrap inaccuracies, and challenges in differentiating similar trajectories, particularly in open or dynamic settings. Pettorru et al.[6] offer a comprehensive review of IoT localization strategies, examining vulnerabilities and the potential of AI, blockchain, and quantum computing for improving security. Despite identifying key advancements, the study notes issues such as hybrid system complexity, high energy demands, and a lack of empirical validation across many proposed solutions. Addressing robustness in noisy environments, Yang et al.[120] introduce TRAIL, a three-phase adversarial architecture that combines transfer learning and adversarial interaction to improve accuracy in low SNR conditions. Though it outperforms existing methods, the model struggles with environmental variability and balancing offline-online data alignment during training. Lastly, Wang et al.[121] present a privacy-preserving scheme using inner product encryption to secure location data from untrusted cloud services. While it maintains accuracy with low computational overhead, its scalability and adaptability to real-time, large-scale deployments remain untested, particularly under frequent data updates.

Privacy-preserving and trustworthy localization frameworks have continued to evolve through encryption, blockchain, and probabilistic modeling. Wang et al.[122] propose a secure indoor localization framework using inner product encryption (IPE) and ranging transformation to protect user and anchor data in cloud-based systems. While it maintains localization accuracy with low overhead, its scalability in real-time, dynamic environments remains a concern. Zocca and Hasan[123] introduce a blockchain-based localization scheme using Hyperledger Fabric to ensure trust, data integrity, and privacy. The system shows strong security performance and leverages UWB for improved accuracy, but its reliance on centralized storage and blockchain transaction overhead may hinder scalability in large IoT networks. Verma et al.[124] highlight privacy risks from unauthorized geo-tracking using device sensors, presenting an attack model with 98% accuracy without GPS and recommending mitigation strategies for Android platforms. However, the approach lacks real-world deployment and generalization beyond Android ecosystems. Addressing physical-layer privacy, Li and Mitra[125] propose the DAIS method, which obfuscates delay and angle information to mislead eavesdroppers while preserving authorized localization accuracy. Though resilient to precoder leakage and effective under high SNR, its reliance on secure communication may be vulnerable in dynamic or adversarial conditions. Finally, Alhammadi et al.[126] present a 3D Bayesian graphical model that reduces localization error to 1.8 meters using Wi-Fi fingerprints and adaptive probabilistic reasoning. While it demonstrates scalability and efficiency, limitations include dependence on static access points, lack of built-in security features, and computational intensity during sampling in resource-constrained settings.

2025

Recent studies in 2025 have emphasized privacy, efficiency, and robustness in Wi-Fi and BLE-based localization and sensing systems. Abuhoureyah et al.[127] provide a comprehensive review of CSI-based human activity recognition (HAR), highlighting CSI's advantages in mitigating signal distortion for location-independent sensing. However, transmission and reception noise remain key limitations, especially in constrained environments. David et al.[128] explore privacy vulnerabilities in BLE beacons and propose a quasi-periodic randomized scheduling method to counter battery insertion attacks. While effective at obfuscating initialization timestamps, the study does not fully address power trade-offs or large-scale deployment feasibility. Enhancing secure location queries, Li et al.[129] introduce ROLQ-TEE, a TEE-based framework that supports privacy-preserving and revocable location queries via cryptographic RNN techniques. Despite improved performance over traditional schemes, TEE-related processing overhead raises concerns for scalability in larger systems. Boudlal et al.[130] present a low-cost, non-intrusive HAR system using existing Wi-Fi CSI and deep learning to detect activities without wearables or cameras. While demonstrating strong performance, the system faces challenges related to hardware variability, environmental sensitivity, and computational demand. Finally, Nie et al.[131] propose MS.Id, a mobile single-station identification method leveraging spatiotemporal data and MAC de-randomization to improve user identification. Achieving 95.24% accuracy and reduced localization error, the system offers scalable, infrastructure-light deployment but may encounter issues in dynamic environments, device heterogeneity, and potential privacy concerns from MAC-level data handling.

As shown in Table 2, security and privacy solutions in ILS vary widely in trade-offs between robustness, scalability, and efficiency. Cryptographic methods ensure strong confidentiality but often introduce significant latency and overhead, limiting real-time deployment[64,114]. Federated learning enhances data privacy in decentralized settings, yet remains vulnerable to poisoning and struggles with non-IID data[59,87]. Differential privacy offers theoretical guarantees but often degrades localization accuracy in dense environments [77], [114]. Adversarial training and GAN-based defenses improve resilience against spoofing but lack generalizability and are resource-intensive[79,116]. Blockchain solutions add transparency but suffer from scalability and energy constraints[89,123]. Lightweight approaches like MAC de-randomization and TEE-assisted queries are promising for real-time IoT deployments, though they trade off latency and coverage[127–131]. Overall, no single approach offers a balanced solution across privacy, accuracy, and computational efficiency–highlighting the need for hybrid, adaptive frameworks.

To provide a clearer overview of the existing research landscape, Table 3 presents a comparative summary of key studies in the domain of ILS security and privacy. It highlights the respective threat models, techniques, datasets or environments, main results, and known limitations, enabling readers to identify major trends and remaining gaps in the field.

Study	Attack type	Defense method	Dataset	Accuracy	Privacy	Performance
Ciftler et al.[59]	Privacy breach	Federated learning	Real	1.8 m	✓ Strong	Low (scalability issues)
Ko et al.[58]	MAC spoofing	Random forest filtering	Real	Improved vs baseline	✗	Medium
Li et al.[55]	Malicious check-ins	Fingerprinting + AP subset	Simulated + Real	High	✗	Medium
Li et al.[54]	Fraudulent check-ins	Optimal boundary + LSM	Simulated	High	✗	Medium
Nieminen et al.[64]	Privacy breach	Secure two-party computation	Real	2.2 s query time	✓ Moderate	High
Shubina et al.[61]	Privacy vs Accuracy trade-off	Obfuscation control	Real	Moderate	✓ Moderate	Medium
Yan et al.[62]	Physical-layer spoofing	RSSI-based detection	Real	99.8%	✗	Medium
Zhang et al.[60]	Privacy exposure	Paillier encryption	Simulated	Efficient (no exact error)	✓ Moderate	High (processing cost)
Ambalkar et al.[69]	Adversarial ML	PGD + MIM + Defense	Simulated	Good (exact N/A)	✗	High
Beko et al.[78]	Spoofing	WCM + GTRS bisection	Simulated	Improved	✗	Low
Dervicsouglu et al.[72]	Security comparison	UWB vs BLE	Real	UWB: 0.43 m, BLE: 1.54 m	✗	Medium
Min et al.[77]	Privacy leak	3D geo-indistinguishability	Simulated	Good (no error given)	✓ Strong	Medium
Na et al.[71]	Cross-tech impersonation	Detection by power variance	Real	>20 m error	✗	Low
Njima et al.[75]	Data scarcity	GAN + Semi-supervised	Sim + Real	21.7%/15.3% ↑	✗	Medium
Patil et al.[68]	Adversarial ML	Adversarial training + DNN	Simulated	84.18%	✗	High
Wang et al.[70]	General security	Multi-task learning	Real	<2 m	✗	Medium
Boora et al.[82]	Adversarial ML	Neural ODE + Adversarial defense	Simulated	High	✗	High
Fathalizadeh et al.[81]	Anonymization	k-Anonymity + Dijkstra	Sim + Real	Moderate	✓ Moderate	High
Gao et al.[87]	Data privacy	FL (FedLoc3D)	Real	Improved	✓ Strong	Medium
Han et al.[86]	Spoofing/Faulty Sensors	CNN/ResNet filter	Real	High	✗	Medium
Wang et al.[85]	First-order adversarial	AdvLoc (DCNN)	Simulated	<1 m	✓ Moderate	Medium
Yang et al.[83]	Adversarial ML	SecureSense	Simulated	High (not exact)	✗	High
Ye et al.[84]	Adversarial APs	SE-loc semi-supervised	Simulated	8.9 m	✓ Weak	Medium
Zhang et al.[79]	Privacy leakage	FL + DP (Adp-FSELM)	Real	2.22% MAE	✓ Strong	Low
Casanova et al.[91]	Tracking	Zero-knowledge ABA	Real	Secure Auth (no loc error)	✓ Strong	Medium
Chen et al.[95,104]	Spoofing	UnSpoof (UWB + ToA)	Real	30 cm	✓ Strong	Medium
Kalpana et al.[93]	Node attacks	3D DV-Hop + Cryptography	Simulated	<2m	✓ Strong	High
Mitchell et al.[90]	Adversarial ML	Adversarial training + Outlier detection	Simulated	Improved vs baseline	✗	High
Mohsen et al.[92]	Privacy leakage	PassiFi (DL + TDoA)	Real	Sub-meter	✓ Strong	Medium
Peterseil et al.[88]	Signal tampering	Autoencoder + Trust score	Real	50% RMSE reduction	✗	Medium
Shakerian et al.[89]	Privacy, Tampering	Blockchain + IMU + ZUPT	Real	1.2 m	✓ Strong	High
Xiao et al.[96]	OTA adversarial	FooLoc perturbations	Real	70–90% attack success	✗	High
Eshun et al.[114]	Data leakage	Cloud Offload + Crypto	Real	Good	✓ Strong	Medium
Etiabi et al.[112]	Communication privacy	Federated distillation	Simulated	Good (no value)	✓ Moderate	Low
Fathalizadeh et al.[5]	Privacy	Survey + Framework	N/A	N/A	✓ Strong	N/A
Gufran et al.[113]	Adversarial ML	CALLOC + Curriculum FL	Simulated	6× Error Reduction	✓ Strong	Medium
Hemkumar et al.[118]	Geo-inference	LDP + Clustering	Real	Good (empirical)	✓ Strong	Medium
Li et al.[119]	Tracking	RFTrack + RL agent	Simulated	Improved	✗	Medium
Machaj et al.[117]	AP spoofing	KNN accuracy degradation	Real	Impacted	✗	Low
Moghtada et al.[116]	Privacy leakage	DPGAN	Simulated	Balanced	✓ Strong	Medium
Boudlal et al.[130]	Passive tracking	Wi-Fi CSI + DL	Real	26.4 cm	✓ Moderate	Medium
David et al.[128]	BLE beacon privacy	Randomized ID timing	Real	Tracked avoidance	✓ Moderate	Low
Nie et al.[131]	User identification	MAC de-randomization + DR.LIE	Real	1.15 m	✗	Medium
Abuhoureyah et al.[127]	Signal distortion	CSI-enhanced HAR analysis	Literature review	Not specified	✗	Medium
Li et al.[129]	Location query privacy	TEE + RNN + Key revocation	Real	<1 m	✓ Strong	Medium

Table 2. Comparative analysis of indoor localization studies (2020–2025). The accuracy values are presented exactly as reported in the original studies. As different works adopt diverse metrics–such as horizontal or vertical error (in meters), relative improvements, percentages, or qualitative descriptions– no post-standardization was applied in order to preserve the fidelity of the original results. Readers should interpret the values in the context of each study's methodology and evaluation criteria.

Reference	Threat model	Technique used	Dataset/ Environment	Results	Limitations
Barsocchi et al.[52],	Privacy leakage in indoor navigation	GDPR-compliant access control	Telegram-based proximity marketing	Highlighted security/privacy issues in current frameworks	Specific to one use-case; lacks broader validation
Ko et al.[58],	MAC spoofing attacks	Random Forest-based filtering (RFBSA)	Real-world Wi-Fi data	Improved filtering accuracy over baselines	Vulnerable to advanced spoofing tactics
Ciftler et al.[59],	Data leakage in federated learning	Federated Learning (FL)	Crowdsourced RSS fingerprint dataset	Improved privacy with modest accuracy trade-off	Scalability and convergence challenges with non-IID data
Patil et al.[68],	Adversarial RSSI perturbations	Deep learning with adversarial training	Simulated/real RSSI data	Enhanced robustness over traditional ML	Limited to white-box attacks; environment-sensitive
Na et al.[71],	Cross-technology impersonation (BLE–Wi-Fi)	Power variance-based detection	BLE advertising + Wi-Fi interference	Detected impersonation via power consumption	High localization error; low packet reception rates
Zhang et al.[79],	Data leakage in FL	Differentially private FL (Adp-FSELM)	Edge computing testbeds	Achieved ε-privacy with low error	High fingerprinting cost; limited scalability
Yang et al.[83],	Black-box and white-box adversarial attacks	Virtual adversarial training + label smoothing	Device-free HAR datasets	Strengthened DNN resilience	Instability and hyperparameter sensitivity
Peterseil et al.[88],	UWB signal manipulation	Trust score + autoencoder models	Real-world UWB datasets	50% error reduction in dynamic settings	Heavy reliance on training data quality
Casanova et al.[91],	Privacy/identity leaks in CIPS	Decentralized attribute-based authentication (ABA)	BLE + zero-knowledge proofs	Improved untraceability and unlinkability	Scalability and deployment complexity
Etiabi et al.[112],	High communication overhead in FL	Federated distillation (FD)	IoT networks	Reduced comm. cost by 98%	Limited support for regression tasks
Moghtada et al.[116],	Data leakage in fingerprinting	Differentially private GANs (DPGANs)	Wi-Fi fingerprint datasets	Preserved privacy with synthetic fingerprints	Degraded performance under strict privacy budgets
Li et al.[119],	Passive Wi-Fi sniffing attacks	Reinforcement learning (RFTrack)	Controlled Wi-Fi environments	Accurate stealthy tracking	Limited in dynamic/open spaces
David et al.[128],	BLE beacon battery insertion attacks	Quasi-periodic randomized scheduling	BLE beacon testbed	Obfuscated initialization timestamps	Power trade-offs; scaling issues
Li et al.[129],	Privacy leakage in location queries	ROLQ-TEE (TEE + cryptographic RNN)	Simulated query workloads	Secure + revocable queries with efficiency gains	TEE overhead hinders scalability
Nie et al.[131],	MAC address de-randomization	MS.Id (spatiotemporal + MAC-level)	Mobile Wi-Fi devices	95.24% ID accuracy; reduced error	Privacy risks; heterogeneity challenges

Table 3. Summary of key ILS security and privacy studies (2020–2025).

Privacy–accuracy trade-offs with case examples

A recurring theme in ILS research is the tension between preserving user privacy and maintaining localization accuracy. While theoretical discussions highlight this balance, concrete case studies illustrate the trade-offs more vividly.

For example, healthcare applications often require strict privacy guarantees when handling patient movement data. Zhang et al.[79] demonstrate that integrating differential privacy into federated edge learning frameworks substantially reduces the risk of individual data leakage. However, they also report up to a 7–10% decline in localization accuracy in dense hospital environments, underscoring the performance cost of strong ε–privacy guarantees. Similarly, Moghtadaiee et al.[116] show that differentially private GANs (DPGANs) can protect patient location traces, but accuracy deteriorates sharply as the privacy budget tightens.

In the financial services sector, federated learning has been explored for collaborative location-based authentication without centralizing sensitive user trajectories. Ciftler et al.[59] and Gao et al.[87] both show that federated models achieve comparable accuracy to centralized methods under controlled conditions. However, when different institutions contribute heterogeneous datasets, it is common for their performance to drastically deteriorate in non-IID data scenarios. This points to an important trade-off in which statistical differences across sites can be reduced accuracy, while at the same time privacy is enhanced by keeping the data decentralized.

Real-time IoT applications provide practical examples of these challenges. David et al. [128] show that stochastical scheduling of BLE beacons can improve privacy by obscuring timestamps to reduce the risk of tracking attacks. However, in large-scale deployments, this approach often comes at a cost of reduced coverage and increased latency. Similarly, Li et al. [129] employed trusted execution environments (TEEs) to protect location queries. While their method offers strong security guarantees, the added processing overhead limits its scalability for real-world applications.

Taken all together, these findings point to a clear pattern in which privacy-preserving solutions almost always come with a cost. Common challenges include higher latency, limited scalability, and reduced accuracy. This highlights the need for adaptable hybrid frameworks that can dynamically balance accuracy, privacy and efficiency to address the requirements of different applications.

Comparative study of privacy and security approaches in ILS

Security threats in ILS

From 2020 to 2025, ILS security and privacy measures progressed from encryption approaches and GDPR-compliant access controls to sophisticated methods such as FL and adversarial training. Initial techniques, such as the Paillier cryptosystem and fast gradient sign method (FGSM), facilitated the development of contemporary methods such as GAN-based data augmentation and LD for safeguarding privacy. Primary priorities encompass

precision, confidentiality, practical applicability, and energy efficiency. CNN-based and UWB systems have enhanced accuracy of over 90%; however privacy-preserving solutions frequently compromise accuracy for security. Energy efficiency and communication overhead continue to pose issues, especially for federated learning and IoT systems[59,82,89,112].

In 2025, ILS privacy and security research expanded to wireless sensing, BLE beacon tracking, and privacy-preserving location queries. Key advancements include CSI-based human activity recognition[127], BLE beacon privacy enhancements[128], TEE-based location queries[129], Wi-Fi CSI-based indoor activity detection[130], and mobile Wi-Fi user identification[131]. These developments highlight emerging privacy challenges, emphasizing the need for improved obfuscation, efficiency, and scalability.

To orient the reader, Table 2 synthesizes prominent ILS papers by threat/attack type, countermeasure, data setting, and utility trade-offs, providing a quick map of the security landscape before deeper discussion.

Highlighting trends over the years

Indoor localization research from 2020 to 2025 shows a clear evolution from privacy preservation to advanced machine learning integration. In 2020, emphasis was placed on privacy and federated learning (FL)[59], with growing interest in encryption (Paillier cryptosystem[60]) and GDPR-compliant access control[52]. By 2021, adversarial training methods (FGSM, PGD, MIM[69]) gained traction, complemented by GAN-based data augmentation[75] and BERT for adversarial recognition[73]. In 2022, noise-based privacy (LDP[80]), adversarial robustness[82], and differential privacy techniques[79] were consolidated. The year 2023 advanced deep learning with CNNs[100] and FL[98], while blockchain[89] and UWB systems[88] emerged for secure localization. In 2024, adversarial learning and FD dominated privacy-preserving localization[112], reinforced by cryptographic protocols[114] and GAN-driven synthetic data[116]. Finally, 2025 studies furthered privacy and security with CSI-based sensing for HAR[127], BLE beacon analysis[128], TEE-based queries[129], Wi-Fi CSI activity detection[130], and mobile station Wi-Fi user identification[131].

Overall, the field has progressively integrated FL, adversarial training, privacy-preserving mechanisms, GANs, cryptographic protocols, and deep learning. Each methodology offers unique strengths and trade-offs, shaping the trajectory of modern indoor positioning systems. Table 4 concisely summarizes these developments from 2020–2025.

Privacy issues in ILS

Comparisons of existing solutions

An analysis of current privacy and security solutions for ILS shows various methods, each with unique advantages and disadvantages depending on particular use cases and system needs. FL provides a decentralized approach to preserving privacy by not sharing sensitive data during the training process[57,59,79]. This method improves scalability and minimizes data-sharing risks, making it appropriate for dynamic settings such as crowdsourced localization and smart cities. However, it encounters challenges related to the scalability of large datasets, significant communication overhead, and vulnerability to model poisoning[87,99]. Conversely, differential privacy (DP) methods[79,97] safeguard privacy by introducing noise to data, which helps keep individual location traces anonymous. Although differential privacy ensures robust privacy protection, finding the right balance between added noise and the accuracy of the system is a considerable challenge[116]. Cryptographic techniques like homomorphic encryption[60,122] ensure strong data confidentiality and are resistant to unauthorized access. Nonetheless, their significant computational cost and communication overhead restrict their use in real-time systems and large-scale environments[64,114].

Blockchain offers a reliable and transparent solution for location data due to its immutable ledger capabilities[89,123]. This ensures the authentication and verification of location-based transactions, making it suitable for systems that need clear data integrity, like IoT-based localization and supply chain tracking. Blockchain faces challenges related to scalability, significant energy consumption in its consensus mechanisms, and difficulties with integration[89]. Adversarial training[83,85] improves model robustness by protecting against data manipulation. However, it comes with high computational costs and can result in overfitting when trained on adversarial examples. This approach is especially beneficial in applications where security is crucial, such as autonomous vehicles and AI-based navigation systems.

Year	Key focus	Methodology highlights	Privacy/Security techniques	Key trends /Development
2020[52,53,55,59,60]	Privacy preservation	FL, Encryption (Paillier), GDPR Access Control	Pseudonymization, Dummy Locations	Privacy with encryption methods
2021[68,69,71,73,75]	Adversarial attacks	GAN-based Augmentation, BERT, FGSM, PGD, MIM	Adversarial Learning, Anonymization	Adversarial attacks, GANs for data
2022[79,80,82,83]	Robustness in adversarial scenarios	Neural Networks, LDP, Differential Privacy	Adversarial Training, Noise Addition	Adversarial defenses, Differential privacy
2023[89–91,98,100]	Advanced ML for security	CNNs, Blockchain, UWB, FL	Cryptographic Protocols, ZKP	ML models, UWB, FL
2024[112–114,116]	FL & Cryptography	FD, GANs, Cryptographic Privacy	Adversarial Training, Cryptographic Protocols	Privacy-focused cryptography, Efficient FD
2025[127–131]	Wireless sensing & Privacy in BLE	CSI, TEE, BLE Privacy Analysis, Wi-Fi-based HAR, RNN Queries	MAC De-randomization, Key Refresh, Quasi-periodic Randomization	Privacy in BLE, CSI-based Sensing, TEE for Secure Queries

Table 4. Trends over the years in ILS.

Recent research in 2025 has further advanced privacy-preserving solutions for ILS. CSI-based sensing has been explored for human activity recognition (HAR) in wireless sensing, where Abuhoureyah et al.[127] highlight the potential of Wi-Fi-based CSI for improving signal processing accuracy while recognizing challenges such as noise interference. Similarly, Boudlal et al.[130] propose a cost-effective, privacy-preserving Wi-Fi CSI-based activity detection system, eliminating the need for wearable sensors or visual monitoring, making it a viable solution for smart environments.

Privacy concerns with BLE beacon tracking have been critically examined by David et al.[128], who demonstrate the Battery Insertion Attack on BLE beacon randomization and propose quasi-periodic randomized scheduling as a countermeasure. However, their solution may introduce trade-offs in power consumption. In privacy-preserving location queries, Li et al.[129] introduce ROLQ-TEE, a TEE-based framework for securely handling outsourced location queries, ensuring location confidentiality while allowing for revocable query authorization. Nonetheless, TEE-based computations impo higher server-side processing costs, which may limit large-scale applicability.

se Efforts in Wi-Fi-based indoor localization have also been expanded by Nie et al.[131], who propose MS.Id, a mobile single-station user identification approach leveraging IE-based MAC de-randomization. Their findings indicate improved accuracy over multi-station techniques while reducing infrastructure overhead, though potential privacy concerns regarding MAC de-randomization remain.

Privacy-preserving frameworks that integrate methods such as FL, cryptography, and anonymization (for example, *k*-anonymity) provide thorough protection[81,116]. These frameworks keep location data secure while maintaining system performance.

Each solution offers distinct advantages and limitations within the ILS context. While FL, DP, and cryptographic methods ensure privacy, they face scalability and real-time application challenges. Blockchain enhances transparency but struggles with energy efficiency and integration. Adversarial training improves robustness but increases computational costs. Recent 2025 advancements–CSI-based sensing, BLE beacon privacy, TEE-secured location queries, and MAC de-randomization for user identification–broaden privacy-preserving options in ILS, each with distinct benefits and challenges. The summary of current trends, their advantages, disadvantages, and suitability in ILS is presented in Table 5.

Defense mechanisms in ILS

Strengths and limitations of various approaches

Upon conducting a thorough examination of the present methodologies, it becomes evident that there are several strengths and limits. Significant advancements have been made in adapting privacy-preserving and adversarial-attack-resistant models for real-world applications, especially in the fields of IoT, GNSS-denied environments, and indoor localization employing UWB systems[88]. FL and its advanced variations, such as FD, show great potential in facilitating safe and decentralized learning while avoiding privacy vulnerabilities[112]. Furthermore, there have been consistent advancements in localization accuracy, especially in the presence of noise and adversarial conditions[82]. These advancements have been particularly notable in solutions that utilize CNN-based and blockchain-based technologies[75,85,86,89]. Moreover, cryptographic protocols have been used to ensure security in collaborative localization tasks[91].

Nevertheless, there are significant constraints. Methods such as adversarial training[68], GAN data generation[75], and cryptographic protocols[91] often impose computational overhead, necessitating substantial processing capacity. Consequently, their implementation becomes challenging in situations with limited resources. Scalability is still a problem, as solutions that work well in simulations or small real-world settings may not adequately handle large systems[82,93,104]. FL models, in particular, have difficulty converging when dealing with non-IID data[87,98]. Privacy-preserving strategies, such as differential privacy[97], include a trade-off between privacy and accuracy. Increasing privacy levels can sometimes result in decreased localization accuracy, a challenge that remains unresolved[79]. Table 6 summarizes the strengths and limitations of various approaches. However, challenges related to scalability and adaptability in dynamic environments persist. Combining location fingerprinting with anonymization techniques effectively protects user privacy[117]. However, it is susceptible to attacks such as Wi-Fi AP spoofing, which can undermine security.In conclusion, UWB-based systems for detecting spoofing attacks[95,104] achieve high accuracy but face challenges in real-time detection and scalability in large networks.

Key parameters

The publications have identified accuracy, privacy, real-world feasibility, and energy efficiency as the main parameters. Accuracy remains the paramount factor, with the majority of approaches striving for a success rate of above 90%, namely in UWB-based and CNN-based positioning systems[55,70,82]. These systems attempt to enhance performance in both challenging and real-life situations. Privacy is a critical aspect, and differential privacy and encryption methods have a substantial impact[52,80]. Techniques such as adding noise to data[81,97] and employing cryptographic methods[60,114] were extensively investigated to improve privacy safeguards. The emphasis on real-world viability increased as research transitioned from solely simulated environments in 2020-2021[53,68] to tangible applications by 2024, particularly in the fields of IoT and ILS[112]. Finally, the issue of energy efficiency has become a significant problem, specifically in the context of blockchain-based and FL systems[89,113]. By 2024, the primary goal is to minimize communication overhead and increase energy consumption[112].

In 2025, research continued to refine privacy-preserving techniques, especially in BLE beacon-based tracking and Wi-Fi CSI-based activity recognition. David et al.[128] demonstrated vulnerabilities in BLE beacons, highlighting the need for improved temporal obfuscation mechanisms. Similarly, Li et al.[129] introduced ROLQ-TEE, leveraging Trusted Execution Environments (TEEs) to safeguard location-based queries while minimizing computational costs. Meanwhile, Wi-Fi CSI-based sensing gained traction as an energy-efficient and privacy-

Solution	Approach	Strengths	Limitations and challenges	Key findings	Adversarial risks addressed	Addressed practical applications
Federated learning (FL) for privacy and security[57,59,79,87,98,99,112,113]	Federated learning for decentralized model training with differential privacy or transfer learning.	Protects privacy by not sharing sensitive data, improves scalability, and reduces data-sharing risks.	Challenges with large dataset scalability, high communication overhead, and limited labeled data for training.	FL enhances privacy-preserving localization while ensuring data accuracy and robustness across multiple devices. FL frameworks like FedLoc3D and FedPos improve accuracy and reduce communication overhead.	Vulnerable to model poisoning and data poisoning attacks where adversaries can inject false data to corrupt the model.	Crowdsourced localization, smart cities, healthcare, multi-building indoor navigation systems, location-based services.
Differential privacy (DP) for privacy preservation[79,97,100,116,116,118]	Uses differential privacy to add noise to data and ensure individual privacy during localization.	Strong privacy protection, maintains system utility with noise addition, widely applicable in decentralized systems.	Balancing privacy and accuracy, especially when dealing with high levels of noise. Computational cost for large-scale systems.	DP ensures privacy in localization systems by using noise addition (e.g., Gaussian noise, local DP) to mask user data. It allows geo-indistinguishability for location privacy without significant degradation in query precision.	Attacks targeting the noise mechanism, such as reconstructing individual data from aggregate outputs, can reduce privacy.	Indoor location-based services, mobile crowdsensing, geospatial data privacy, privacy-preserving query systems, and healthcare.
Cryptographic techniques for secure localization[60,64,114,115,121,122]	Cryptographic techniques (e.g., Paillier cryptosystem, homomorphic encryption) for securing location data during transmission and processing.	High level of confidentiality and security protects against unauthorized access or manipulation of data.	High computational cost and communication overhead, especially for large-scale systems. May not be scalable for real-time applications.	Secure cryptographic methods like homomorphic encryption and Paillier ensure confidentiality and prevent unauthorized access to sensitive location data. They can protect both user and service provider privacy.	Vulnerable to side-channel attacks and cryptanalysis, where attackers can exploit computational or transmission weaknesses.	Secure wireless positioning, IoT-based localization, secure mobile networks, cryptographically protected location-based services.
Blockchain for trust and security[89,123]	Blockchain (e.g., Hyperledger Fabric) for providing immutable ledgers to authenticate and verify location data transactions.	Immutable ledger, increased trust and accountability, and provides transparency in location data transactions.	Scalability issues in large-scale environments, high energy consumption in consensus mechanisms, and integration complexity with existing systems.	Blockchain solutions ensure trust and security in localization systems by providing decentralized verification of location data. The use of permissioned blockchain (e.g., Hyperledger Fabric) addresses privacy concerns.	Susceptible to 51% attacks, where adversaries control the majority of the network and can manipulate the blockchain.	Secure navigation, supply chain tracking, transparent location-based data transactions, IoT, and data integrity in mobile and indoor localization systems.
Adversarial training and robustness[82,83,85,90,120]	Adversarial training to improve system robustness by defending against attacks that manipulate sensor data or mislead models.	Improves model robustness, enhances resilience to adversarial attacks, and improves data integrity.	High computational cost, potential overfitting on adversarial examples, and scalability in real-time systems	Adversarial training techniques like label smoothing and feature squeezing improve the model's resistance to adversarial inputs, even under low signal-to-noise ratio conditions.	Adversarial risks include adversarial examples designed to evade detection and fool the model, potentially causing mislocalization.	Robust indoor and outdoor localization, autonomous vehicles, security in AI-driven navigation, and defense against data manipulation attacks in wireless networks.
Privacy-preserving frameworks[5,81,116]	Frameworks combining cryptography, anonymization (e.g., *k*-anonymity, *l*-diversity), and federated learning for privacy protection.	Comprehensive protection against unauthorized access, combines multiple privacy-preserving techniques.	Trade-off between privacy, accuracy, and system performance; scalability in dynamic environments.	Privacy-preserving frameworks that combine multiple techniques (e.g., *k*-anonymity, federated learning, and differential privacy) ensure that location data remains secure without compromising system performance.	Vulnerable to attacks targeting anonymization algorithms (e.g., re-identification attacks) and federated learning poisoning.	Indoor localization, mobile applications, location-based services, and data privacy in crowdsensing and IoT systems.
Location fingerprinting and anonymization[117]	Uses location fingerprinting combined with anonymization techniques to protect user privacy in vulnerable fingerprint-based systems.	Protects user privacy by anonymizing location fingerprints, preventing tracking or reidentification.	Vulnerable to attacks like Wi-Fi AP spoofing that can disrupt the fingerprinting accuracy and compromise security.	Location fingerprinting can be enhanced with anonymization techniques, such as *k*-anonymity, to mitigate risks of tracking or re-identification in Wi-Fi-based systems.	Spoofing attacks can mislead fingerprint matching and reduce system reliability.	Indoor navigation, Wi-Fi-based positioning systems, and secure location fingerprinting in public and private spaces.
Spoofing attack detection and prevention[95,104]	Detection of spoofed tags using UWB-based systems and time-of-arrival (ToA) or time-difference-of-arrival (TDoA) methods.	High accuracy in detecting spoofed tags with sub-meter precision prevents malicious manipulation of location data.	Limited to specific technologies (e.g., UWB), real-time detection may be challenging, and scalability for large networks is difficult.	Spoofing detection systems using ToA and TDoA methods provide sub-meter localization accuracy and help mitigate the impact of spoofing attacks.	Vulnerable to advanced spoofing techniques that manipulate time-of-arrival or signal-to-noise ratios, potentially evading detection.	High-precision localization in IoT systems, security in navigation systems, anti-spoofing for UWB-based location systems, secure positioning in military or asset tracking applications.

Continued

Solution	Approach	Strengths	Limitations and challenges	Key findings	Adversarial risks addressed	Addressed practical applications
Energy efficiency and scalability solutions[58,79,93,94]	Focus on improving the energy efficiency and scalability of privacy-preserving localization systems.	Reduces energy consumption, improves system efficiency, and addresses scalability issues in dynamic environments.	Computational and communication overheads may still hinder real-time performance in large-scale, dynamic environments.	Energy-efficient techniques can significantly improve system scalability, though challenges in real-time computation and communication efficiency remain.	Attacks that drain energy resources or exploit system inefficiencies can cause service disruptions.	Energy-efficient positioning systems, smart grid applications, low-power IoT networks, and real-time localization in large-scale environments.
Privacy-preserving wireless sensing and BLE security (2025)[127–131]	CSI-based sensing for human activity recognition (HAR), BLE beacon privacy protection, TEE-based privacy-preserving location queries, and MAC de-randomization for single-station user identification.	Leverages existing Wi-Fi and BLE infrastructure, enhances privacy without requiring additional hardware, enables privacy-preserving location queries with revocability.	CSI-based sensing may suffer from noise interference, BLE beacon security solutions may introduce power consumption trade-offs, and TEE-based queries require higher server-side processing costs.	Wi-Fi CSI can improve signal processing precision in HAR applications. BLE beacons require improved randomization techniques to avoid tracking risks. TEE-based solutions can securely handle location queries while maintaining revocability. Mobile single-station identification techniques reduce infrastructure requirements while improving accuracy.	Privacy concerns in CSI-based HAR, BLE beacon tracking vulnerabilities, security challenges in outsourced location queries, and MAC de-randomization risks.	Smart environments, privacy-preserving BLE-based tracking, secure location-based services, privacy-aware IoT-based indoor positioning, and non-intrusive human activity recognition.

Table 5. Existing privacy and security solutions in ILS (Part 1).

Aspect	Strengths	Limitations
Privacy solutions	Strong privacy protection (encryption, differential privacy)[5,79,91]	Higher privacy levels may reduce accuracy (trade-off)[79,97]
Adversarial defenses	Advanced defenses via GANs, CNNs, adversarial learning[85,86,116]	High computational overhead and energy consumption[68,85,115]
FL	Decentralized and privacy-preserving[87,98,112]	Challenges in handling non-IID data, higher convergence time[98,112]
Real-world feasibility	Tested in real-world (IoT, GNSS-denied, large-scale systems)[88,89,93]	Some solutions remain simulation-based, scalability concerns[82,104,113]

Table 6. Strengths and limitations of various approaches.

Parameter	Importance	Key techniques	Real-world feasibility
Accuracy [55,57,68–70,82,86,87,98,100]	Essential for localization	Neural Networks, FL, CNNs	Achieved up to 99% accuracy across years
Privacy preservation [5,52,60,79–81,89,91,97,100,114]	Key in IoT and Localization	Differential Privacy, Cryptographic Protocols	Cryptographic techniques proved feasible in IoT systems
Real-world feasibility [52,53,55,68,88,89,95,112]	Increasing focus over years	Blockchain-based localization, UWB, Adversarial training	Tested in real-world environments, especially IoT and GNSS-denied scenarios
Energy efficiency [98,112–114,116]	Focus in resource-limited devices	FD, Cryptographic Techniques	Optimized for low-power environments like IoT
Scalability [89,95,112]	Crucial for applicability across different sizes and complexities of environments	Decentralized architectures (e.g., Blockchain), Federated Learning	Verified with large-scale deployments, capable of adapting to various building sizes and user densities
Security robustness [57,68,70,88]	Essential for protecting against spoofing, jamming, and other cyberattacks	Adversarial Training, Blockchain, Cryptographic Protocols	Proven to mitigate common threats, effectiveness depends on network size and attack sophistication
Latency and responsiveness [55,69,100]	Important for real-time applications such as augmented reality and emergency response	Edge Computing, Low-latency Communication Protocols (e.g., 5G)	Achieved low latency through edge computing, suitable for time-sensitive applications
Temporal privacy and obfuscation [128–130]	Critical for preventing tracking based on timing patterns in BLE and Wi-Fi-based localization	Quasi-periodic randomized scheduling, TEE-based encryption, CSI-based obfuscation	Demonstrated effectiveness but requires optimization for scalability and power consumption

Table 7. Key parameters in ILS.

conscious alternative for indoor activity recognition[130]. Furthermore, Nie et al.[131] proposed MS.Id, a mobile single-station Wi-Fi-based user identification approach that achieves high accuracy while reducing reliance on extensive infrastructure deployment. These developments underscore the growing intersection of accuracy, privacy, and feasibility in ILS research. Table 7 summarizes the key parameters in ILS.

Security and privacy concerns in ILS

ILS are becoming increasingly crucial in numerous applications; however, they have multiple weaknesses that might jeopardize the accuracy and reliability of location data. An important weakness is the proneness to signal interference and spoofing. Many ILS systems, dependent on RF signals like Wi-Fi, Bluetooth, or RFID, are vulnerable to disruption from other devices and ambient conditions. This vulnerability allows malicious attackers to launch adversarial assaults. These attacks can result in substantial inaccuracies in position monitoring or

unlawful entry into restricted areas, creating security risks, particularly in sensitive settings such as hospitals, military installations, or financial organizations.

The risk associated with ILS increased with the emergence of wearable technology. Wearable devices, such as smartwatches, fitness trackers, and AR glasses, frequently come with sensors and networking features that can be integrated with ILS. Although these devices improve the user experience by offering customized LBS, they also bring new opportunities for attacks. Attackers can exploit weaknesses in wearable devices to carry out side-channel assaults, or they can use them as entry points to compromise the entire localization system. For instance, attackers can intercept or alter information from wearable devices, leading to inaccurate location data, privacy violations, or even potential threats to physical security if they exploit the compromised data to gain unlawful entry[132].

Overview of threats

ILS are essential for accurately identifying the location of objects or humans within buildings, but they are susceptible to several forms of malicious attacks. Spoofing and signal jamming are two prominent attacks in this context, both of which affect the RSSI data and undermine localization accuracy, as illustrated in Fig. 7.

Spoofing attacks

As categorized under 'Spoofing Attacks' in the taxonomy in Fig. 3 these attacks involve the intentional transmission of counterfeit signals by a perpetrator, with the aim of making them undetectable from authentic signals to the ILS. Typically, the perpetrator transmits the faked signals with modified parameters like adjusted RSSI values, timestamps, or even variations in frequency. Attackers can change the apparent distance between a transmitter and receiver by faking the RSSI values[133]. This manipulation causes the device to look as if it is located at a different location than it actually is[134]. Figure 8 shows a spoofing attack.

Technically speaking, the majority of ILS utilize trilateration, a method that calculates the position of a device by estimating its distance from several predetermined reference points. In Wi-Fi fingerprinting-based ILS, the distance is estimated based on the RSSI values, which decrease proportionally to the square of the distance from the signal source. If an assailant transmits a forged signal with a strong RSSI from a considerable distance, the ILS may incorrectly perceive it as a signal emanating from nearby. Conversely, the ILS may misinterpret a faintly modified signal originating from a short distance as emanating from a far place. Information distortion can cause significant localization errors, leading to inaccurate monitoring of resources or individuals. As a result, there may be significant security vulnerabilities or operational inefficiencies.

Signal jamming

Signal jamming transpires when an attacker employs identical frequency channels as the ILS to transmit undesirable or disruptive messages, so obscuring genuine communications. This may diminish the signal-to-noise ratio (SNR), complicating the ILS's ability to detect and assess genuine signals. Jammer attacks diminish the accuracy of RSSI measurements by introducing random fluctuations, complicating the localization of objects. The modifications render the calculated distances less dependable, hence diminishing the accuracy of the trilateration process. Interference can hinder the ILS system's ability to maintain consistent RSSI data. If an attacker continuously alters the signal strength, disrupting the ILS, it may impede the system's ability to effectively counteract the interference, potentially resulting in inaccurate location predictions. Intense jamming signals can saturate the receiver's analog-to-digital converters (ADCs), resulting in further distortion of signal measurements. Significant interference may necessitate the ILS to employ alternative methods or cease operation entirely, hence diminishing its efficacy. Figure 9 shows how the signal jamming attack works in the ILS.

Recent real-world incidents reinforce the practical impact of these threats on deployed Indoor Localization Systems (ILS). For example, the UWBAD attack demonstrated how commercially available ultra-wideband (UWB) hardware could be used to selectively jam ranging signals, effectively disrupting Apple's AirTag devices and automotive keyless entry systems in operational environments[135]. This incident drew responses from major vendors, including Volkswagen and Audi, who acknowledged the system-level vulnerability. Similarly, an extensive BLE spoofing campaign was analyzed in Taipei Main Station, where attackers used cloned iBeacons to confuse indoor navigation services used by over 300,000 daily commuters. The study showed that without encrypted, time-varying identifiers, location services were easily deceived[136]. Furthermore, adversarial perturbations to Wi-Fi signal strength have been shown to trick deep learning models used in fingerprinting-based systems, causing significant localization errors even with imperceptible input changes[68]. These examples clearly illustrate the operational risks of spoofing, jamming, and adversarial attacks in real-world ILS deployments.

Impact of security breaches

ILS breaches have significant consequences, including user privacy, operational integrity, and safety in critical applications. A compromised ILS may permit unauthorized individuals to monitor and track users within a building, thus intruding upon their privacy. The violation of privacy may disclose personal information, including medical records in healthcare institutions or the movements of individuals in secure locations. The risk of data theft, corporate espionage, and stalking is greatly increased by unauthorized tracking. Therefore, security and privacy are the primary objectives in the context of ILS.

Attacks like spoofing and jamming are a big threat to the proper functioning of ILS. In retail transportation services, spoofing and jamming assaults can lead to wrong asset tracking, bad inventory management, and broken customer navigation systems. This can cause big problems with operations and cost a lot of money. Companies who need reliable indoor monitoring to run their businesses may have big problems because of these breaches. Moreover, security breaches can lead to incidents that jeopardize human life in sectors that are largely reliant on safety, such as industrial automation, emergency response, and healthcare. In industrial contexts, ILS

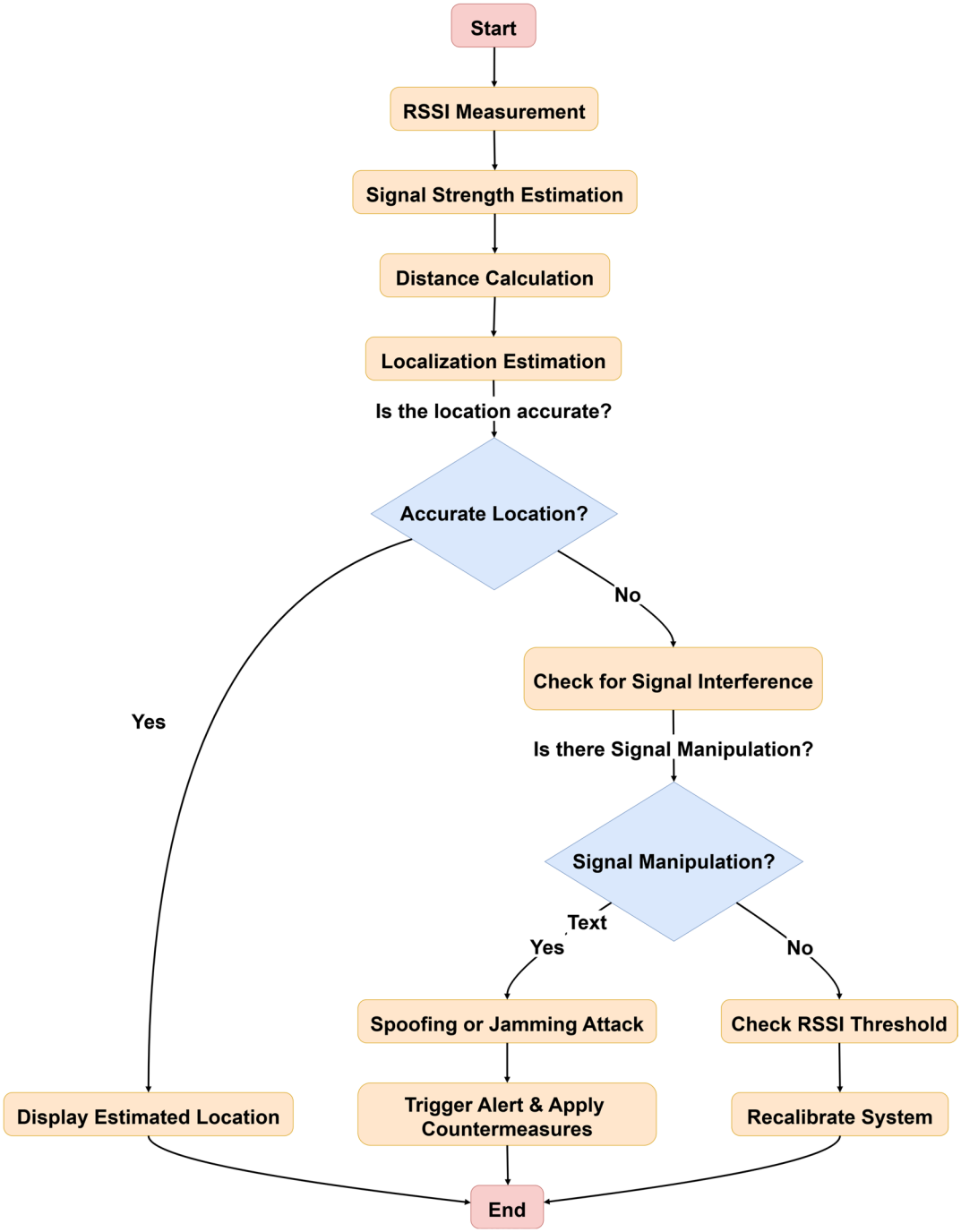


Fig. 7. End-to-end indoor localization workflow: from RSSI-based location estimation to spoofing and jamming detection.

may provide patients, emergency personnel, or machinery with inaccurate location data, potentially leading to errors or fatalities. For localization technology to work well and reliably in these settings, ILS integrity and security are very important.

Machine learning techniques for enhancing security and privacy in ILS

ML approaches significantly improve the security and privacy of ILS. As ILS systems spread into more sensitive domains like healthcare, smart buildings, and industrial installations, the necessity of protecting them from risks such as signal spoofing, jamming, and unauthorized access grows. This section looks at various AI-based technologies that have been proved to have the capacity to increase the levels of both security and privacy in ILS.

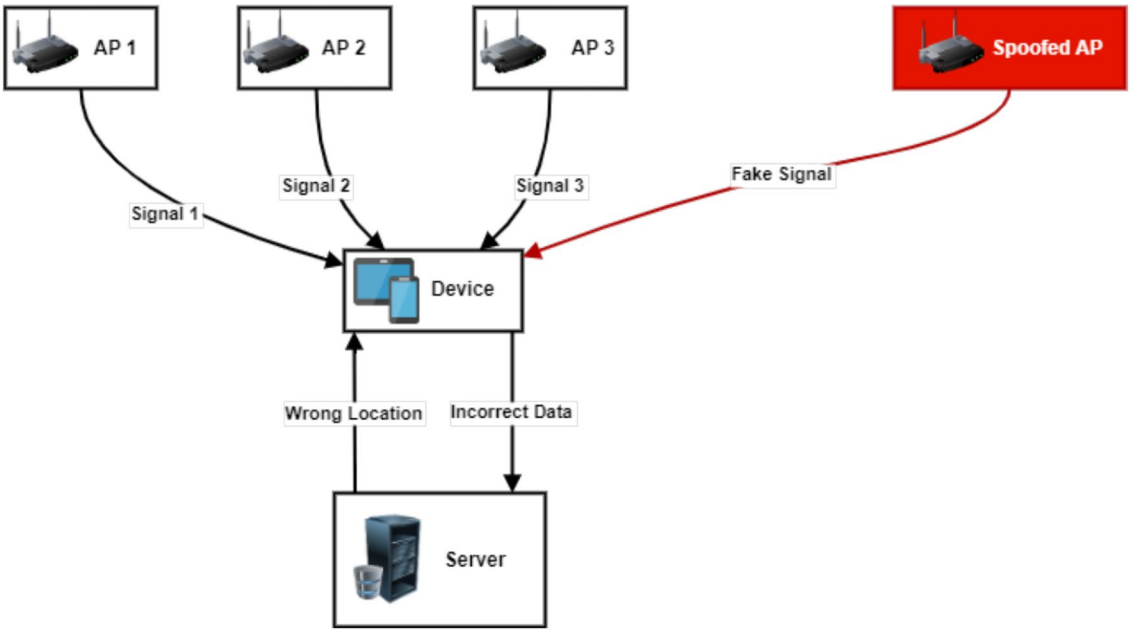


Fig. 8. Spoofing attack.

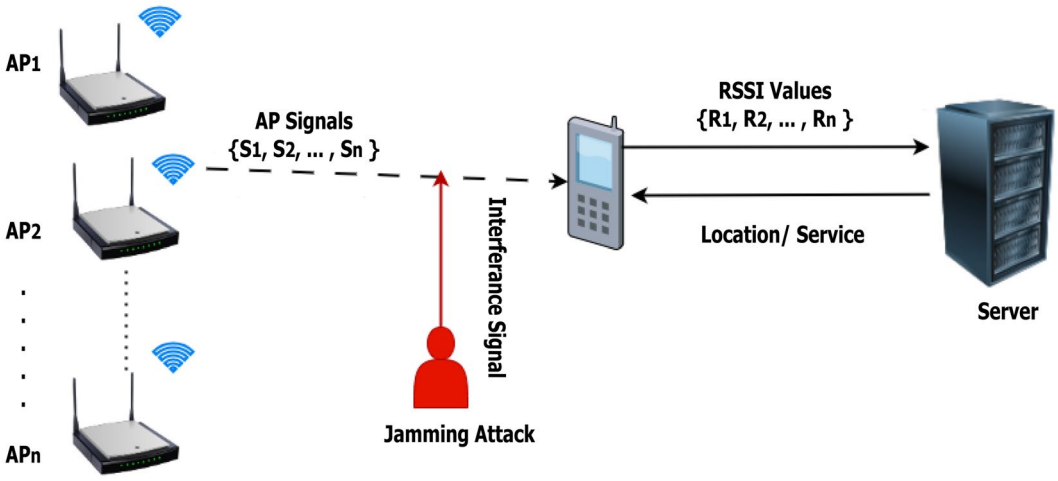


Fig. 9. Signal jamming attack.

Adversarial machine learning

AML aims to make ILS better at standing up against adversarial attacks. In such systems, adversarial attacks introduce deliberate modification to the input data that misguides the learning model, causing it to degrade the localization accuracy to a large extent.

Adversarial Training Techniques Adversarial training is a robust defense method aimed at enhancing the resilience of ILS against adversarial attacks. This process includes training models with adversarial examples, which are specifically designed inputs that increase the model's prediction error. This subsection describes three important adversarial training methods: FGSM, PGD, and MIM, including their mathematical formulations.

- *FGSM* FGSM creates adversarial examples by applying perturbations to the input, following the direction of the gradient of the loss function. The adversarial example is calculated as follows:

$$\mathrm{x}_{\mathrm{adv}} = \mathrm{x} + \epsilon \cdot \mathrm{sign}(\nabla_{\mathrm{x}} J(\theta, \mathrm{x}, y)), \tag{15}$$

where x is the original input, ϵ is the perturbation magnitude, $J(\theta, \mathrm{x}, y)$ is the loss function, $\nabla_{\mathrm{x}} J$ is the gradient of the loss with respect to x, θ is the model parameters, and y is the true label.

- *PGD* PGD builds on FGSM by repeatedly applying gradient steps and projecting the adversarial example back onto the ϵ-ball surrounding the original input. The iterative update is expressed as follows:

$$x_{\text{adv}}^{(t+1)} = \text{Proj}_{\mathscr{B}_\epsilon}(x_{\text{adv}}^{(t)} + \alpha \cdot \text{sign}(\nabla_x J(\theta, x_{\text{adv}}^{(t)}, y))), \tag{16}$$

- $x_{\text{adv}}^{(t)}$ is the adversarial example at iteration t, α the step size, and $\text{Proj}_{\mathscr{B}_\epsilon}$ is the projection onto the ϵ-ball.
- *MIM* MIM enhances PGD by adding a momentum term that stabilizes the direction of the gradient updates. The gradient update with momentum is:

$$g^{(t+1)} = \mu \cdot g^{(t)} + \frac{\nabla_x J(\theta, x_{\text{adv}}^{(t)}, y)}{\|\nabla_x J(\theta, x_{\text{adv}}^{(t)}, y)\|_1}, \tag{17}$$

$$x_{\text{adv}}^{(t+1)} = \text{Proj}_{\mathscr{B}_\epsilon}(x_{\text{adv}}^{(t)} + \alpha \cdot \text{sign}(g^{(t+1)})), \tag{18}$$

where $g^{(t)}$ is the accumulated gradient at step t and μ is the decay factor for momentum.*Real-world attack scenarios and implications* The theoretical construction of adversarial scenarios is significant, although their practical implications are of greater importance to assess. Minor disturbances to input signals can substantially interfere with ILS, resulting in mislocalization. An attacker can add carefully crafted noise in the RSSI measurements, causing the system to misplace a user's location. For example, showing them on the wrong floor of the hospital. Mistakes like these can have serious consequences, from delaying medical staff to hindering emergency response. Similarly, interference with Wi-Fi CSI data leads to inaccurate activity recognition, putting applications like elderly care monitoring and surveillance at risk. In smart buildings attackers can carry out spoofing attacks that copy and mimic real signals, potentially granting unauthorized access or hindering indoor navigation. These examples highlight that adversarial attacks on ILS are not just theoretical but pose a real threat to safety, security, and privacy.

To reduce these risks, ILS needs to be designed with strong resilience. Adversarial training methods like FGSM, PGD, and MIM provide protection by exposing models to realistic adversarial examples during training. This allows the models to learn how to recognize and adapt to signal disruptions that could otherwise reduce their accuracy and reliability. The training process follows a strict cycle as demonstrated by Fig. 10. It starts with clean data, then generates adversarial examples, followed by adding these adversarial examples to the training set and retraining the models. By repeating this cycle, the system gradually becomes more resilient against adversarial examples generated by attackers.

Anomaly detection Machine learning-based systems detect unusual patterns in signal behavior that could indicate security breaches. These systems analyze real-time data for violations of established signal standards,

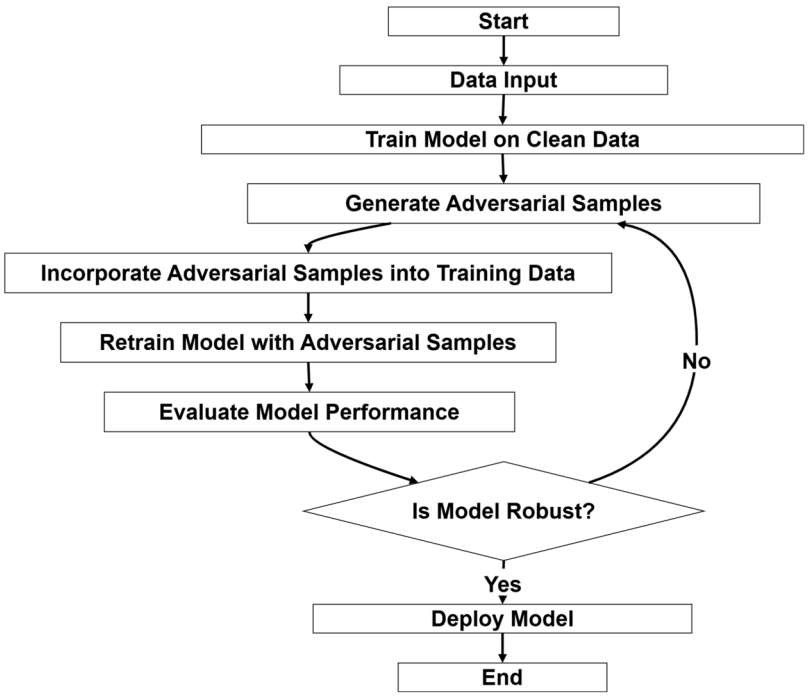


Fig. 10. Adversarial training workflow illustrating how iterative inclusion of adversarial samples strengthens ILS models against real-world attack scenarios such as signal spoofing, floor misclassification, and adversarial noise injection.

facilitating the early detection of threats such as signal manipulation and unauthorized localization. Anomaly detection can be formulated as a problem of identifying deviations δ between real-time observations $\mathrm{x}_{\mathrm{real}}$ and the expected behavior $\mathrm{x}_{\mathrm{expected}}$:

$$\delta = \|\mathrm{x}_{\mathrm{real}} - \mathrm{x}_{\mathrm{expected}}\|_p, \tag{19}$$

where $\|\cdot\|_p$ denotes the p-norm (e.g., Euclidean distance for $p = 2$) used to quantify the deviation. An anomaly is flagged if $\delta > \tau$, where τ is a predefined threshold.

Integrating AML techniques into ILS can greatly strengthen their defense against complex attacks. For example, Patil et al.[68] demonstrates that using adversarial training with FGSM and PGD improves both floor classifications and localization accuracy under attack. This is especially critical in environments like hospitals, where a misclassification could delay emergency response. Ambalkar et al.[69] demonstrated that the use of MIM and PGD to Wi-Fi CSI data improved resistance against adversarial interference in human activity recognition, therefore diminishing the likelihood of false alarms in surveillance and assisted living contexts. Li et al.[53] presented the Abnormal Crowd Traffic Detection (ACTD) system to detect abnormalities in crowdsourced positioning data, demonstrating that real-time anomaly detection can thwart extensive manipulation of indoor mobility data in public spaces.

Furthermore, anomaly detection is essential for recognizing unusual trends in signal behavior that suggest adversary manipulation, including signal spoofing and jamming attempts. Li et al.[53] created the Abnormal Crowd Traffic Detection (ACTD) system, utilizing machine learning methods, including probability suffix trees (PST), to identify anomalies in crowdsourced indoor positioning data. Extending this form of anomaly detection for monitoring real-time RSSI and CSI signals in ILS could allow prompt detection of signal modifications that adversarial attacks depend upon. Ko et al.[58] developed a random forest-based filter (RFBSA) to eliminate noise resulting from MAC spoofing. This makes localization more accurate in systems that are vulnerable to spoofing attacks. Incorporating these anomaly detection methods will provide dynamic, real-time ILS defenses, ensuring system stability under hostile conditions.

Federated learning

In alignment with the mitigation strategies outlined in Fig. 3, FL is a decentralized machine learning methodology that addresses privacy concerns by ensuring that sensitive user information, such as location, remains on the local device. A central server receives model updates, thereby maintaining data privacy and improving model training efficacy. For an overview of FL schematics, refer to Fig. 11.

- Local Model Updates: Within the framework of ILS, FL enhances privacy by retaining location data on the user's device. This method is particularly advantageous in multi-building configurations where data privacy is paramount. FL models integrate data from several devices while preserving the privacy of individual users. The local updates at device k is computed as

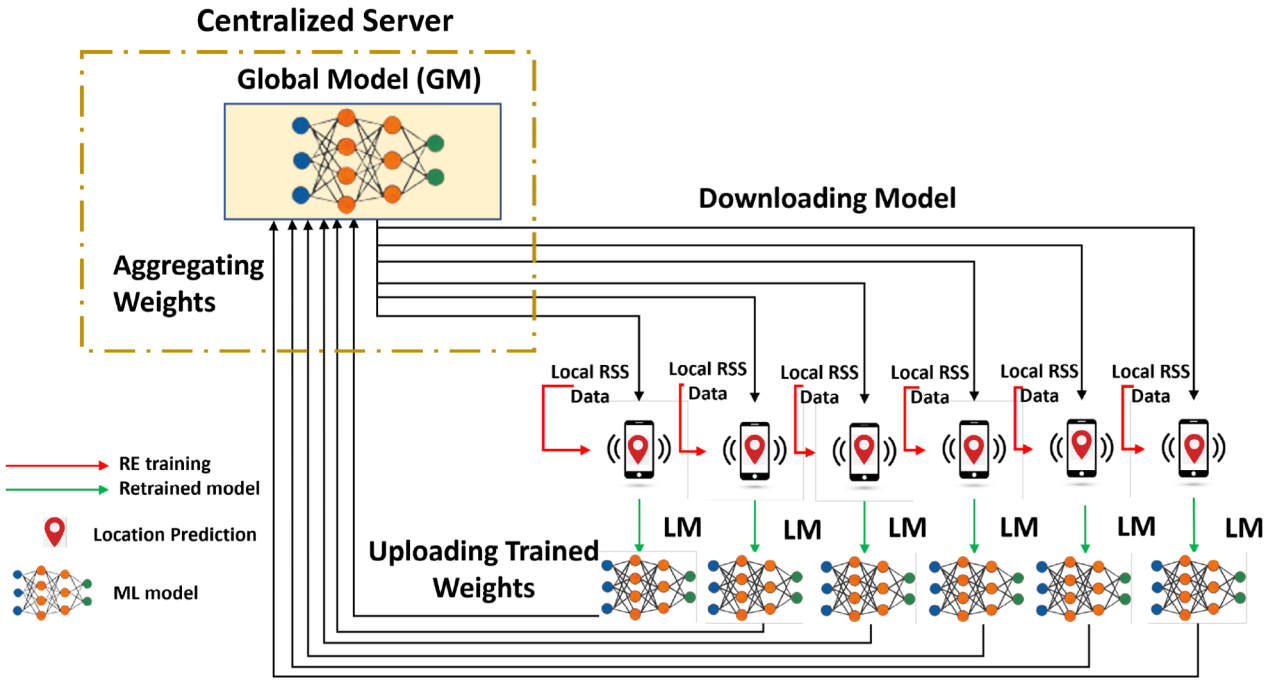


Fig. 11. Overview of FL in ILS[99].

$$\mathrm{w}_k^{t+1} = \mathrm{w}_k^t - \eta \nabla L_k(\mathrm{w}_k^t), \tag{20}$$

where w_k^t represents the local model weights at device k during iteration t, η is the learning rate, and $\nabla L_k(\mathrm{w}_k^t)$ is the gradient of the loss function L_k on the local data of device k.

- Managing Non-IID Data: In practical FL systems, addressing non-IID (independent and identically distributed) data is a considerable problem. Numerous advanced FL methodologies have been established to tackle these challenges, notably FD, which reduces communication overhead while maintaining high model accuracy. The global model aggregation in FL is given as

$$\mathrm{w}^{t+1} = \frac{1}{K} \sum_{k=1}^{K} \mathrm{w}_k^{t+1}, \tag{21}$$

where w^{t+1} is the updated global model, K is the total number of participating devices, and w_k^{t+1} are the updated weights from each device. This ensures that the global model benefits from diverse device data without transferring raw data.

To provide a clearer understanding of the overall FL workflow in indoor localization, we present the Algorithm 1 outlining the process.

Require: Initial global model M_0, number of communication rounds T, set of devices $\{D_1, D_2, \ldots, D_n\}$
Ensure: Final global model M_T
Initialize global model M_0
for $t = 1$ to T **do**
  Broadcast current global model M_t to all devices
  for all devices D_i in parallel **do**
    Train model locally: $M_i \leftarrow \text{Train}(M_t, \text{data}_i)$
    Send updated model M_i to the server
  end for
  Aggregate local models at server: $M_{t+1} \leftarrow \text{Aggregate}(\{M_i\})$
end for
return Final global model M_T

Algorithm 1. Federated learning for privacy-preserving Indoor localization[137]

FL has shown great promise in improving privacy-preserving ILS solutions. A significant use is its capacity to preserve location data on local devices, guaranteeing that sensitive user information remains on the user's device. Ciftler et al.[59] came up with an FL strategy for crowdsourcing RSS fingerprint-based localization that protects user privacy while still ensuring accurate localization. This method aggregates model updates from several devices, enabling collaborative learning while protecting individual user data. Li et al.[57] examined FL in ILS inside multi-building and multi-floor environments, employing pseudo-label-driven training to augment labeled data and address the challenge of insufficient labeled data in these scenarios. The decentralized nature of FL facilitates data aggregation across various locations or systems while complying with privacy regulations, as illustrated by Barsocchi et al.'s privacy-by-design framework for indoor navigation systems in alignment with GDPR standards[52]. Additionally, Gao et al.[87] established a FL framework tailored for extensive indoor localization, appropriate for multi-floor and multi-building settings, therefore augmenting the relevance of FL in strengthening privacy preservation. This decentralized method also tackles issues related to the administration of non-IID data, frequently encountered in varied localization contexts, and is alleviated using sophisticated techniques such as FD[112], which reduces communication overhead while maintaining model accuracy. The ability of FL to disseminate knowledge across devices while preserving privacy, as demonstrated by these instances, underscores its increasing significance in safe and efficient ILS.

While several advanced techniques have been proposed to mitigate security risks in ILS, their deployment in real-world systems presents significant challenges. FL, for instance, enables decentralized training without sharing raw data but suffers from non-IID data across clients. This heterogeneity can impair model convergence and degrade accuracy. To address this, SimDeep introduced similarity-aware aggregation strategies that improved accuracy to 92.9% despite client diversity [138]. Similarly, adversarial defenses such as CALLOC apply curriculum learning and lightweight attention mechanisms to resist adversarial examples, but still require retraining and computational resources that may not be feasible for constrained IoT environments [113]. Cryptographic approaches like TESLA and privacy-preserving schemes such as Sillcom [139] show promise in securing location information through authentication and secret sharing. However, these methods often increase communication overhead, introduce latency, and complicate synchronization–factors that can limit their scalability in dense or time-sensitive ILS applications. Therefore, while effective solutions exist in principle, translating them into robust, deployable systems remains an ongoing challenge.

Deep learning for attack detection and localization

Deep learning models, especially CNNs and RNNs, are increasingly used in ILS for precise localization and attack detection. These models have demonstrated a robust capacity to learn intricate spatial and temporal patterns from signal data, including Wi-Fi and Bluetooth signals.

- CNNs for Localization: ILS has employed CNNs to analyze RSSI or CSI data for accurate location prediction. These algorithms have effectively identified signal anomalies that may indicate an attack, including spoofing attempts or interference.
- RNNs for Temporal Data: RNNs are highly proficient at modeling sequential data, including movement patterns inside indoor environments. Through the analysis of these temporal sequences, RNNs can identify anomalies that signify security vulnerabilities, enabling them to predict attacks such as signal jamming.

CNNs and RNNs are deep learning models that have demonstrated significant potential in enhancing ILS performance regarding security improvements and localization precision. CNNs have effectively predicted user locations by examining signal strength data, such RSSI or CSI. This method, illustrated by Ko et al.[58], utilizes a random forest-based filter to detect and remove fraudulent signals that compromise localization accuracy. Likewise, Yang et al.[56] devised a CNN-based map localization method to facilitate the assessment of a secure condition during hostile assaults. This illustrates the identification and resolution of signal difficulties with deep learning techniques.

The capability of RNNs to identify sequential movement patterns in temporal data enables real-time detection of anomalies such as signal jamming or movement disparities. Li et al.[53] utilized machine learning approaches, such as probability suffix trees, to detect anomalous crowd traffic by analyzing temporal trends in signal data. RNNs may boost this by enhancing the prediction of temporal sequences within the signal data. Furthermore, Madani et al.[63] illustrated the application of deep learning for the detection of MAC layer spoofing. This approach could be enhanced by employing RNNs to identify anomalous temporal patterns in wireless signals, so aiding in the prediction of possible attacks. These pictures exemplify how deep learning models can be customized to tackle both temporal and spatial difficulties in ILS.

Generative models for data privacy and augmentation

ILS use generative models, namely GANs, shown in Fig. 12, to produce synthetic data that improves the system's privacy and resilience. GANs improve model training by producing realistic data samples while safeguarding the privacy of genuine user information. In ILS, GANs are utilized to generate synthetic training datasets that replicate various signal environments, including potential attack scenarios. This allows models to get insights from a larger dataset while protecting user privacy. Furthermore, GANs have been utilized to augment model resilience against adversarial attacks by producing adversarial samples for training purposes.

A GAN includes two neural networks: a generator G and a discriminator D, which compete against each other in a zero-sum game. The generator accepts random noise z drawn from a prior distribution $p_z(\mathrm{z})$ and produces synthetic data $G(\mathrm{z})$. The discriminator analyzes whether the data is authentic ($x \sim p_{\mathrm{data}}(x)$) or fabricated ($G(\mathrm{z})$). The objective function for GANs can be defined as follows:

$$\min_G \max_D V(G,D) = \mathbb{E}_{x\sim p_{\mathrm{data}}(x)}[\log D(x)] + \mathbb{E}_{\mathrm{z}\sim p_z(\mathrm{z})}[\log(1-D(G(\mathrm{z})))]. \tag{22}$$

Within this paradigm, the discriminator attempts to optimize the likelihood of accurately distinguishing between real and synthetic data. The generator seeks to reduce the likelihood of the discriminator differentiating between generated data and real data. The application of GANs in ILS may improve privacy, robustness, and overall efficacy of these systems. In the field of crowdsourced location systems, as noted by Li et al.[53], GANs can produce synthetic RSS signatures that replicate authentic data. This approach can improve the system's resilience to anomalous traffic detection and spoofing assaults while safeguarding user privacy. GANs, by generating authentic synthetic data, can augment datasets for ILS and reduce dependence on user-provided data, hence

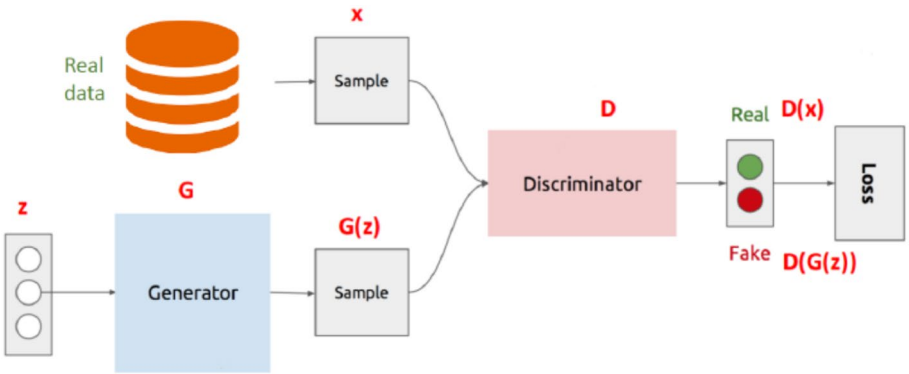


Fig. 12. GAN schematics[116].

diminishing the danger of privacy violations. Ciftler et al.[59] showed that FL may be integrated with GANs to enhance the privacy of indoor localization, enabling several devices to train on a common dataset without the necessity of revealing the raw data. In this context, GANs can generate synthetic training data that local models employ to improve system performance when labeled data is unavailable. Recent work shows that differentially private GANs can synthesize realistic indoor location fingerprints with formal privacy guarantees, enabling data sharing and model training without exposing raw trajectories[140].

Furthermore, GANs can enhance defenses against adversarial attacks. Patil et al.[68] investigate the vulnerability of deep learning models to attacks that modify signal strength data, hence reducing localization precision. GANs can generate adversarial instances during model training, enabling ILS to identify and counteract such attacks in practical applications. GANs enhance model training resilience by generating adversarial samples, safeguarding against deceptive inputs intended to compromise localization accuracy. Njima et al.[75] noted that employing GANs to provide authentic adversarial inputs in RSSI vector augmentation markedly enhances the model's accuracy and security, particularly in settings with less labeled data. In conclusion, the application of GANs in ILS, whether for privacy-preserving data production or adversarial defense, might significantly enhance both the security and efficiency of ILS.

Differential privacy

Differential privacy is a method that protects individual users' privacy even when their data is being used for system training or decision-making. It accomplishes this by introducing noise (Figure 13) into the data in a way that preserves broad patterns while safeguarding individual items. ILS employs differential privacy techniques to introduce appropriately calibrated noise to user location data, therefore obstructing the identification of individual movements linked to a specific user. This approach is highly effective in scenarios requiring significant amounts of location data, such as smart buildings or retail environments.

Differential privacy guarantees that noise is incorporated according to a defined process, such as the Laplace mechanism or the Gaussian mechanism. For instance, in the Laplace mechanism. noise is sampled from the Laplace distribution as

$$\text{Noise} \sim \text{Laplace}\left(0, \frac{\Delta f}{\epsilon}\right), \tag{23}$$

where Δf denotes the sensitivity of the query (i.e., the greatest extent to which a single individual's data can influence the output), and ϵ represents the privacy budget, governing the balance between privacy and accuracy. The output characterized by noise then becomes $\tilde{f}(x) = f(x) + \text{Noise}$. Similarly, in the Gaussian mechanism, noise is sampled from a Gaussian (normal) distribution as

$$\text{Noise} \sim \mathcal{N}\left(0, \sigma^2\right), \tag{24}$$

where σ is the standard deviation of the noise, calibrated based on ϵ and δ (a parameter for approximate differential privacy).

Incorporating noise into the data safeguards privacy by guaranteeing that the presence or absence of an individual's data in the dataset does not substantially influence the analysis results. For instance, with carefully adjusted noise, two datasets that differ solely by one individual's data yield statistically indistinguishable outcomes. This makes it almost impossible for attackers to derive sensitive information on particular individuals while still enabling the dataset to yield accurate aggregate insights. The noise conceals individual contributions, preventing identification while preserving the overall data's utility.

ILS can effectively integrate differential privacy by introducing noise to location data, so obscuring individual movements while maintaining the overall value of the data. This methodology has been implemented in various contexts, including smart buildings and retail environments, where substantial location data is essential for operations yet requires meticulous control of privacy concerns. Navidan et al.[80] introduced a privacy-focused

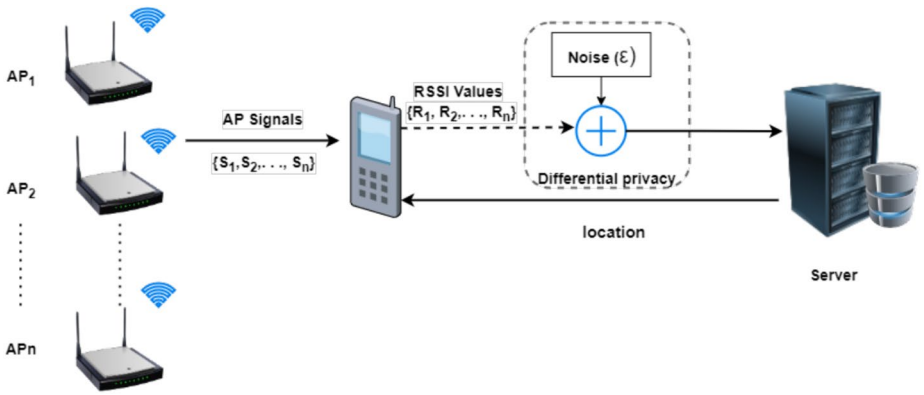


Fig. 13. Differential privacy process.

architecture utilizing LDP to safeguard users' indoor location data. Their method breaks down the indoor environment into distinct zones and monitors user presence within each zone, employing binary noise to protect individual privacy while preserving the precision of aggregate data. Zhang et al.[79] investigated a cloud-based collaborative localization framework that integrates FSELM and differential privacy methodologies. This guarantees the confidentiality of users' raw location data throughout the training process, especially relevant in crowdsourcing systems that aggregate vast datasets from users. Utilizing differential privacy, such systems can provide accurate geolocation while mitigating the danger of disclosing sensitive personal movements. Moreover, Fathalizadeh et al.[81] introduced anonymization methods employing differential privacy to preserve the utility of location data while protecting individual identities. This method is especially beneficial in settings requiring enhanced security and privacy, such as hospitals or corporate campuses, as it restricts the use of location data for illicit surveillance of persons. These examples demonstrate the adaptation of differential privacy for various indoor localization contexts, seeking to balance privacy concerns with the practical requirements of systems.

Reinforcement learning for dynamic security

Reinforcement learning (RL) offers a dynamic approach to improve ILS by enabling systems to adapt over time to changing surroundings and security threats. Rather than depending solely on established rules, RL models acquire knowledge through ongoing contact with their environment and adjust their behavior based on previous results. As seen in Fig. 14, reinforcement learning can improve real-time dynamic security in indoor localization systems.

In the presence of threats like jamming or spoofing, RL algorithms can dynamically adjust system parameters, thereby enhancing the resilience of localization models in uncertain or adversarial environments. Through real-time modifications, RL significantly enhances the robustness of integrated logistics systems. It can identify anomalous patterns in RSSI or atypical user movements, thereby detecting suspicious activities and preventing fraudulent check-ins. This methodology corresponds with the research conducted by Li et al.[54], who employed algorithmic strategies to identify aberrant behaviors.

In addition to accuracy and security, RL also facilitates privacy preservation. Barsocchi et al.[52] demonstrate that privacy-by-design frameworks can be improved when RL dynamically reconciles accuracy with data protection requirements, modifying privacy policies in response to the intensity of the threat. In FL contexts, RL can direct distributed models to enhance their learning techniques by utilizing inputs from many clients, as suggested by Ciftler et al.[59].

Yan et al.[62] have emphasized the significance of RL in interpreting RSS fluctuations and alleviating the effects of physical-layer attacks, thus enhancing the security and reliability of localization. Collectively, these attributes highlight RL as a promising approach for enhancing the precision, adaptability, and security of indoor localization systems.

Hybrid cryptographic-AI approaches

The integration of AI with cryptographic techniques is attracting considerable interest for the enhancement of ILS. These methodologies offer robust safeguarding of sensitive information, thus guaranteeing both privacy and security during the localization process.

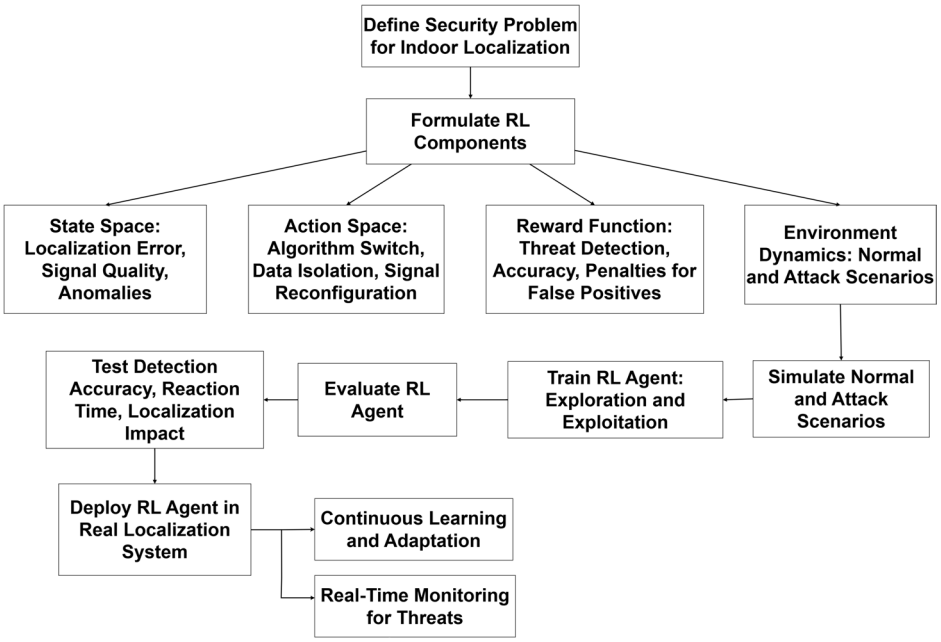


Fig. 14. RL for real-time dynamic security in ILS.

- Homomorphic Encryption with AI: Homomorphic encryption safeguards user location data by allowing computations to be executed directly on encrypted information. This technology, when combined with AI methodologies like FL, facilitates secure and privacy-preserving localization without compromising system speed.
- Zero-Knowledge Proofs: AI-enhanced applications of zero-knowledge proofs (ZKPs) facilitate safe device connectivity while preserving confidential information. These methods are especially efficient in collaborative indoor localization contexts, where numerous users must collaborate without revealing their raw data.

ILS can leverage hybrid frameworks that combine AI with cryptographic mechanisms such as ZKPs and homomorphic encryption to enhance privacy and security. Homomorphic encryption enables the processing of sensitive location data without decryption, so it maintains confidentiality while facilitating rapid computing. Ciftler et al.[59] emphasize this concept in FL, wherein data resides on the local device while aiding in the development of a collective global model.

In ILS, AI-augmented ZKP procedures facilitate secure verification and communication. Casanova et al.[91] proposed a BLE-based collaborative positioning method that safeguards user anonymity, particularly beneficial when various stakeholders (e.g., users and service providers) need to collaboratively ascertain locations without jeopardizing privacy.

Furthermore, Patil et al.[68] illustrate that the integration of AI into cryptographic solutions can alleviate adversarial assaults aimed at signal strength data. Na et al.[71] demonstrate that ZKPs can mitigate spoofing and cross-technology impersonation threats, wherein adversaries seek to distort the localization process. Integrating AI with cryptographic protections enables ILS to attain increased resilience and reliability, improving end-user security and privacy in applications like asset tracking and indoor navigation.

Discussion and synthesis of findings

This section synthesizes the reviewed literature by categorizing security and privacy techniques for Indoor Localization Systems (ILS) across three dimensions: effectiveness, scalability, and real-world applicability. The synthesis draws upon empirical results and conceptual trends identified in Sects. "Related work"–"Machine learning techniques for enhancing security and privacy in ILS".

Effectiveness

Effectiveness refers to how well a technique defends against specific threats such as spoofing, signal jamming, and adversarial manipulation. Approaches like adversarial machine learning (AML) and anomaly detection mechanisms show high accuracy and robustness in controlled conditions. For instance, AML-based frameworks demonstrated resilience against white-box attacks, particularly with adversarial training strategies[68,83]. Similarly, cryptographic solutions such as secure two-way ranging protocols, zero-knowledge proofs, and blockchain-based methods provide strong theoretical guarantees of confidentiality and integrity[89,104,114].

However, many methods exhibit context sensitivity. Their effectiveness may deteriorate under complex conditions like non-line-of-sight environments or dynamic user mobility. Several defenses also rely heavily on accurate signal models and high-quality training data, which may not generalize well across deployments.

Scalability

Scalability involves the adaptability of security and privacy solutions to large or heterogeneous environments. Federated learning (FL) and decentralized models appear promising in this regard[87,99]. These frameworks reduce the need for centralized data aggregation, thereby supporting edge-based intelligence and reducing latency.

Nonetheless, FL techniques face practical limitations including non-IID data distributions, communication overhead, and energy consumption in battery-constrained devices. Many studies highlighted convergence issues in FL models and the need for compression techniques or hierarchical architectures to ensure efficient scalability[59,99].

Real-world applicability

Although many solutions report high accuracy in simulated or laboratory settings, their real-world deployment remains limited. For example, approaches involving homomorphic encryption, blockchain integration, or differential privacy often introduce computational complexity that impairs responsiveness in real-time localization tasks[89,97].

Several studies also emphasize the lack of validation in diverse or dynamic environments. Techniques that excel in static testbeds frequently underperform when faced with variable signal conditions, user density changes, or multipath propagation. Moreover, data availability and labeling constraints hinder the deployment of machine learning-based solutions in commercial-scale systems.

The synthesis presented above offers a critical perspective on the security and privacy techniques employed in ILS by evaluating them along dimensions of effectiveness, scalability, and real-world applicability. While several solutions show promise in controlled settings, their real-world feasibility is hindered by computational, architectural, and contextual limitations. Emerging hybrid frameworks that integrate FL, AML, and cryptographic primitives appear to be the most resilient, but they, too, require empirical validation at scale. These findings align with and are further elaborated upon in Section , where we detail key research gaps and propose future directions for advancing secure and privacy-preserving indoor localization.

Practical challenges

Despite the promising potential of the proposed approach, several practical challenges remain that may hinder its widespread adoption[5,65,111]. A key concern relates to cost considerations. Implementing advanced computational

frameworks and infrastructure often demands significant financial investment in hardware, software licensing, and continuous system maintenance[64,89,111,123]. For many organizations, particularly small- and medium-sized enterprises, these expenses may pose barriers to initial adoption and long-term sustainability. Furthermore, training personnel to effectively manage and operate the system adds an additional layer of resource demand.

Another important limitation concerns scalability. While the framework performs effectively in controlled or medium-scale environments, scaling it to handle large and complex datasets or high-throughput operations introduces performance bottlenecks[59,82,87,99]. Issues such as increased latency, higher storage demands, and greater energy consumption need to be addressed to ensure that the system can function efficiently under real-world, large-scale deployment conditions[79,89,105,123]. Research into distributed architectures, cloud integration, and optimization techniques will be essential to mitigate these scalability challenges[79,87,112,114].

Finally, interoperability remains a critical barrier. The integration of the proposed solution into existing technological ecosystems requires compatibility with heterogeneous platforms, standards, and legacy systems[71,72]. Achieving seamless data exchange and ensuring compliance with industry-specific regulations can be complex and time-consuming[52,108]. Without careful design to promote interoperability, adoption across diverse environments may be restricted, ultimately limiting the impact of the approach. Addressing these interoperability concerns through standardized protocols and modular architectures will be crucial to supporting practical implementation[91,123].

Research gaps and future directions

Despite ILS privacy, security, and performance improvements, several issues and research gaps remain. FL, AML, and cryptographic approaches have shown potential in simulations, but their real-world deployment is constrained. The complexity of managing non-IID data, the privacy-performance trade-off, energy efficiency concerns, and scalability in decentralized situations like IoT remain obstacles. To address these difficulties, creative methods like enhancing FL efficiency, strengthening adversarial defenses, and optimizing cryptographic protocols for low-power contexts are needed. The next sections identify these shortcomings and suggest ILS research directions.

Research gaps

Scalability and real-world feasibility

Although several research projects undertaken in 2020 and 2021[59,68,69,83] investigated solutions in simulated environments, their feasibility for implementation in extensive real-world systems remains limited. Various methodologies, including FL[87,112], adversarial training[68,85], and cryptographic techniques[104,114], have yet to exhibit substantial scalability in diverse, dynamic, and expanding environments such as smart cities or large organizations. Whilst simulation-based techniques demonstrate encouraging results, they are deficient in extensive real-world validations that consider discrepancies in devices, sensors, and networks.

Handling non-IID data in FL

FL has been recognized as a vital framework for safeguarding privacy in indoor localization. Nonetheless, the management of non-IID (independent and identically distributed) data across decentralized devices remains a considerable difficulty. In diverse real-world settings, such as IoT-based localization systems, numerous FL algorithms have difficulties in attaining stable convergence. Additional investigation is necessary to enhance FL models in non-IID environments and to reduce communication overhead while maintaining accuracy[87,98,99]. Even though ILS has made progress in becoming more secure and private, this gap shows that there is still a lot of room for improvement.

Trade-off between privacy and accuracy

A persistent difficulty in privacy-preserving methodologies, such as differential privacy, is achieving a balance between robust privacy assurances and high location accuracy. Methods like noise addition and encryption, although protecting sensitive data, also diminish accuracy, potentially undermining system effectiveness. This problem is especially pronounced in high-density or resource-constrained settings, where even little reductions in accuracy can dramatically affect system performance[79–81,97,116].

Adversarial attack robustness

Adversarial training is commonly utilized to enhance the resilience of machine learning models in indoor localization; nevertheless, existing methodologies are insufficient in mitigating sophisticated or adaptable adversarial attacks. Common methods like FGSM, PGD, and MIM only provide limited protection against more advanced or tailored strategies[68,69,85]. Additionally, the continual requirement for retraining and the significant computational burden of adversarial defenses impede their use in real-time IoT and GNSS-denied contexts[83,113].

Energy efficiency in cryptographic solutions

Cryptographic methods, such as mutual privacy protocols and encryption processes, usually need a lot of processing power and energy. This problem is especially bad in IoT scenarios when resources are limited. Blockchain-based solutions can make data more reliable, but they also require more processing power and energy, which makes them less useful for devices that need to work in real time or use less power[89,114,115].

Future directions

Enhancing resilience against advanced adversarial attacks

The review of current literature has pinpointed some critical domains for future study in ILS. A significant trend that is occurring is the improvement of ILS's ability to withstand advanced attacks from attackers. Adversarial

training strategies like FGSM, PGD, and MIM have shown some success as current defense mechanisms. They still have trouble dealing with more advanced and complicated attacks, especially in complicated IoT settings[68,69]. For instance, while adversarial training is effective against fundamental attack vectors, recent studies demonstrate that systems remain vulnerable to informed attacks and emerging techniques such as cross-technology interference[71,76]. Further study may investigate sophisticated methodologies, such as adversarial curriculum learning or hybrid models that integrate adversarial training with differential privacy methods or FL to improve robustness. Curriculum Adversarial Learning and other hybrid methods try to protect systems from assaults and keep users' privacy safe[113]. These strategies can make the system stronger, protecting it from attacks and breaches of privacy.

Improving privacy-preserving methods

A major area of research is finding better ways to safeguard privacy. Differential privacy and cryptographic protocols like ZKP have made privacy safeguards better, but they typically come with trade-offs in terms of accuracy and computational cost[91]. Studies such as[79] have demonstrated that the use of differential privacy can markedly reduce the likelihood of privacy violations. However, it also has problems, such as the cost of labor for site surveys and effects on performance. Future research may concentrate on refining these methodologies to attain greater accuracy while minimizing computational and transmission costs, particularly in resource-constrained settings like IoT systems[5,116]. Investigating LDP techniques alongside FL has demonstrated potential in improving privacy while reducing performance degradation[79,100]. Methods like federated averaging[87] and the combination of differential privacy have been shown to work well for protecting user privacy and improving localization performance.

Scalability and efficiency in FL systems

FL and its advanced versions, such as federated distillation, show promise for decentralized learning in several scenarios. However, challenges like data heterogeneity (non-IID data) and connection costs limit their scalability in real-world applications. FedLoc3D was accurate for indoor localization, but it had trouble with distributed and diverse data. This shows that we need to find ways to solve model convergence problems in non-IID situations[87]. Future research should focus on enhancing the scalability and efficiency of FL systems, particularly in extensive IoT contexts where reducing power consumption is essential[112]. Furthermore, the integration of FL with GANs to generate realistic synthetic data for training, while preserving privacy, may enhance system resilience[5,116].

Improving energy efficiency in blockchain-based localization systems

Blockchain systems developed for secure navigation and localization in GNSS-deficient locations often encounter issues related to substantial computational and energy expenditures. Blockchain systems, as outlined in[89], have highlighted the energy constraints, particularly regarding IMU sensors. Future developments should concentrate on improving blockchain protocols to reduce supplementary expenses while preserving data integrity and security[89,114]. Lightweight consensus techniques and off-chain strategies can reduce the computational burden, rendering these systems more appropriate for resource-constrained settings[115].

Empirical validation of machine learning models in real-world settings

Numerous proposed solutions, including Anomalous Crowd Traffic Detection (ACTD) and various machine learning-based detection frameworks, predominantly depend on simulations for validation. The ACTD framework and methodologies such as IS-WARS[53,76] have shown encouraging outcomes in controlled environments; yet, their effectiveness in unpredictable, real-world contexts remains largely unvalidated. Future investigation should focus on implementing these systems in real-world settings to assess their effectiveness under varying situations, including environmental changes and adversarial capabilities[53,58].

Robust privacy mechanisms for crowdsourced data

The increasing reliance on crowdsourced indoor location data raises substantial privacy issues, especially in IoT environments where users could unintentionally reveal sensitive information. Privacy-enhancing approaches, like LDP and FL, together with anonymization methods such as *k*-anonymity, require more refinement for dynamic crowdsourcing applications[80,81]. The application of LDP in frameworks like Navidan et al.'s research has shown encouraging outcomes; however it encounters difficulties with noise control and scalability. Investigating methods that reconcile privacy with location precision in dynamic contexts may yield significant progress in this domain.

Hybrid security solutions for robustness against novel attacks

Numerous current protections, such as MAC spoofing detection and adversarial training, falter when faced with novel attack vectors that were not foreseen during the model training phase. To enhance resilience against known and unknown threats, a potential strategy is to create hybrid security mechanisms that include several detection layers, such as physical-layer metrics and RSS fingerprinting[71,85]. Recent research indicates that employing multi-layered detection, which integrates signal features with statistical models, enhances defense against novel attack vectors[78]. This approach corresponds with cross-layer, multi-modal neural network defense frameworks that provide end-to-end robustness improvements across sensing and protocol layers[141].

Advanced sensor fusion for indoor localization

Future study should investigate the amalgamation of several sensor data types, including BLE, Wi-Fi, inertial sensors, and acoustic signals, to enhance the dependability of localization systems, especially in regions lacking GNSS accessibility. Kalpana et al.[93] demonstrated that the integration of public and private key cryptography

Future direction	Method	Design	Baselines	Metrics
Enhancing resilience against advanced adversarial attacks	Curriculum adversarial training (FGSM→ PGD→MIM) + strong attack battery incl. cross-technology interference	White/black-box settings; OTA/ physical-layer stress; report robust error at fixed ℓ_∞ budgets; retraining overhead	Standard adversarial training; no-AT	Robust error; attack success rate; retraining time; edge energy
Improving privacy-preserving methods	Local DP (randomized response/Gaussian) integrated with FL; lightweight ZKP where needed	ϵ-grid $\{0.1, 0.3, 1, 3, 8\}$; noise-mechanism sweep on IoT devices	FL without DP; centralized DP only; plaintext	Privacy–utility frontier (ϵ vs. error); bytes/round; latency; mWh/inference
Scalability and efficiency in FL systems	FedAvg/FedProx with federated distillation; gradient compression; adaptive client selection	Dirichlet non-IID splits (vary α); cross-building holdout; comms-round budgeting	Centralized training; naive FedAvg	Convergence rounds; mean error; participation rate; bytes/ round; device energy
Improving energy efficiency in blockchain-based localization systems	Lightweight consensus (e.g., PoA); off-chain commitments/channels; TEE-assisted verification	Microbenchmarks on constrained nodes; spoof/jam scenarios	Default Hyperledger-style stacks	Energy/tx; end-to-end latency; throughput; accuracy drop vs. plaintext
Empirical validation in real-world settings	Multi-site field trials with standardized logging	Hold-out by building/time-of-day; environment-shift stress tests	Simulation-only and lab-only validations	Mean/90th-pct error; drift over time; failure rate under shift
Robust privacy mechanisms for crowdsourced data	LDP + FL with per-user privacy budgets and adaptive noise; k-anonymity fallback	Dynamic crowdsourcing with churn; context-aware noise calibration	No privacy; server-side DP only; naive anonymization	Error vs. privacy; user participation/retention; communication cost
Hybrid security solutions for novel attacks	Multi-layer detector (physical-layer CSI/phase + protocol/RSS) with ensemble ML	Evaluate on unseen/novel attack families	Single-layer detectors	AUC; FPR@TPR; detection latency; compute overhead
Advanced sensor fusion for indoor localization	Probabilistic 3D fusion (EKF/UKF/factor-graph) and/or GNN-based fusion of BLE/Wi-Fi/UWB/ IMU/acoustic	Modality ablations; NLoS stress tests	Best single-modality models	Mean/floor-aware error; robustness under NLoS/ occlusion
Real-time performance and scalability testing	Model compression (quantization/distillation); operator fusion; batching	Profiling on edge devices with p50/ p95 latency targets	Full-precision, unoptimized pipeline	Latency; throughput; mWh/ query; accuracy drop
Transfer learning and adaptability	Federated transfer learning with domain adaptation (feature alignment, adversarial DA)	Few-shot adaptation to new building with K labeled samples	From-scratch; no adaptation	Error after K samples; adaptation time; communication cost
Secure and scalable blockchain for localization	Permissioned ledger with lightweight consensus and off-chain data paths; anchor attestation	Tune block size/epoch and membership; test under load/faults/ jam	Default Fabric-like configuration	Tx latency/throughput; energy/ tx; integrity under fault/jam
RL for adaptive privacy management	RL-based LPPM adjusting ϵ, sampling rate, on-device compute by context	Sim-to-real training with limited on-site calibration; online policy updates	Static privacy policies	Privacy–utility reward; regret; latency/energy overhead
Trustworthiness in crowdsourced ILS	Per-source trust scoring + autoencoder outlier detection; robust aggregation	Inject label noise and adversarial contributions at controlled rates	Unweighted aggregation	Error under contamination; precision/recall for bad-source detection
Energy-efficient FL for large-scale systems	Federated distillation; sparse/partial updates; adaptive round frequency; TinyML quantization/ distillation at edge	Energy profiling across device tiers; workload scaling	Full-precision, full-model updates	Energy/round; total energy to target accuracy; accuracy delta vs. baseline

Table 8. Actionable plans for each future direction. When a year appears in a table, it denotes the publication year of the cited paper/parameter; when not shown, the scope is 2020–2025.

with acoustic localization significantly improves system resilience. Emphasis should be directed on improving sensor fusion algorithms to achieve high precision, particularly in diverse IoT systems.

Real-time performance and scalability testing

The computational demands and energy usage of several proposed methodologies, including FL, blockchain solutions, and differential privacy, constrain their implementation in real-time, large-scale systems. Research, including[59,79], underscores concerns such as energy consumption and prolonged convergence times, signifying a significant obstacle for practical implementation. The future path may involve optimizing these approaches to decrease energy usage and increase processing speeds, thereby rendering them more suitable for real-time applications.[92,113].

Transfer learning and adaptability in diverse environments

A major problem in ILS is the adaptation of systems to diverse contexts, such as large buildings and shopping centers, without necessitating complete retraining. Transfer learning, particularly in FL contexts, demonstrates potential. Guo et al.[98] have effectively shown that federated transfer learning may diminish localization error and training time in indoor localization. Additional investigation into domain adaptation and transfer learning techniques may enable localization systems to adjust to new surroundings with minimal data, hence diminishing the necessity for retraining while maintaining high precision.

Secure and scalable blockchain systems for localization

Blockchain technology is suggested as a secure and decentralized method for indoor localization. Nonetheless, the substantial computational and energy requirements provide considerable hurdles, as evidenced in frameworks like Hyperledger Fabric, which encounter constraints due to processing overheads[89]. Subsequent investigation can concentrate on lightweight blockchain protocols that are more appropriate for IoT settings, where energy efficiency is critical[114].

Integration of reinforcement learning for adaptive privacy management
RL offers a method to regulate privacy in fluctuating indoor localization environments. Min et al.[101] presented an RL-based local privacy protection system for three-dimensional indoor environments, demonstrating its efficacy in selecting policies and adapting to environmental changes. Through these techniques, computers may dynamically modify and update privacy regulations in real time according to context, thus providing both usability and privacy in intricate multi-story structures. Employing RL-driven local privacy protection mechanisms (LPPMs) can markedly improve flexibility and fortify privacy in these contexts.

Trustworthiness in crowdsourced ILS
A crucial next step is to guarantee the dependability of data in crowdsourced localization systems. Existing techniques, such as trustworthiness assessments and autoencoder-based anomaly detection, demonstrate potential but require more refining and optimization[88]. Formulating ways to guarantee data consistency and correctness while safeguarding user privacy will improve the trustworthiness of crowdsourced ILS systems.

Energy-efficient FL for large-scale systems
FL has demonstrated potential for privacy-preserving localization. Nonetheless, the energy expenditure linked to model updates, especially in extensive IoT networks, continues to pose a significant barrier. Additional research is required to enhance FL protocols, including federated distillation, to minimize communication and energy expenditures[112]. Methods like energy-efficient aggregation and selective model updates can enhance the scalability of FL, rendering it more appropriate for IoT applications, including ILS. Recent advancements in complementary TinyML indicate that the quantization and knowledge distillation of transformer/Mamba models can achieve precise indoor localization on limited edge devices while minimizing computational and memory requirements[142]. In order to facilitate thorough and repeatable studies, Table 8 combines the indicated future directions into a structured research agenda, outlining the methodological approach, experimental design, comparison baselines, and assessment criteria for each theme.

Conclusion
This paper has provided an in-depth review of the security and privacy issues in ILS, with particular attention to major threats such as spoofing, signal jamming, and adversarial attacks. The analysis shows that while techniques such as Federated Learning (FL), Adversarial Machine Learning (AML), and cryptographic protocols can each strengthen system resilience, privacy, and efficiency, they also face critical challenges.

FL addresses privacy concerns but faces difficulties with non-IID data and increased transmission costs. AML improves robustness against attacks but requires significant computational resources. Cryptographic procedures provide data integrity; nevertheless, they also include computational expenses. The findings collectively suggest that no one method may sufficiently meet the complex demands of ILS.

This research highlights the importance of a balanced approach that combines lightweight privacy-preserving strategies with strong security measures. Future research should focus on integrating these approaches to tackle challenges related to scalability, energy efficiency, and adaptability. This will enable the creation of a secure, privacy-conscious, and flexible ILS capable of functioning in diverse and dynamic environments.

Data availability
All data generated or analysed during this study are included in this published article.

Received: 26 July 2025; Accepted: 26 September 2025
Published online: 11 December 2025

References
1. Pascacio, P., Casteleyn, S., Torres-Sospedra, J., Lohan, E. S. & Nurmi, J. Collaborative indoor positioning systems: A systematic review. *Sensors* **21**, 1002. https://doi.org/10.3390/s21031002 (2021).
2. Liu, W., Zhang, Y., Deng, Z. & Zhou, H. Low-cost indoor wireless fingerprint location database construction methods: A review. *IEEE Access* **11**, 37535–37545 (2023).
3. Rahman, M. M., Moghtadaiee, V. & Dempster, A. G. Design of fingerprinting technique for indoor localization using am radio signals. In *2017 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, 1–7, https://doi.org/10.1109/IPIN.2017.8115949 (2017).
4. Geng, J., Xia, L. & Wu, D. Attitude and heading estimation for indoor positioning based on the adaptive cubature Kalman filter. *Micromachines* **12**, 79. https://doi.org/10.3390/mi12010079 (2021).
5. Fathalizadeh, A., Moghtadaiee, V. & Alishahi, M. Indoor location fingerprinting privacy: A comprehensive survey. *arXiv preprint* arXiv:2404.07345 (2024).
6. Pettorru, G., Pilloni, V. & Martalò, M. Trustworthy localization in IoT networks: A survey of localization techniques, threats, and mitigation. *Sensors* **24**, 2214 (2024).
7. Sartayeva, Y. & Chan, H. C. A survey on indoor positioning security and privacy. *Comput. Secur.* **131**, 103293 (2023).
8. Liu, H., Darabi, H., Banerjee, P. & Liu, J. Survey of wireless indoor positioning techniques and systems. *IEEE Trans. Syst. Man Cybernet. Part C Appl. Rev.* **37**, 1067–1080. https://doi.org/10.1109/TSMCC.2007.905750 (2007).
9. Morar, A. et al. A comprehensive survey of indoor localization methods based on computer vision. *Sensors* **20**, 2641. https://doi.org/10.3390/s20092641 (2020).
10. Xiang, Y., Yang, X. Q., Yang, W. W. & Miao, W. H. Localization and mapping algorithm for the indoor mobile robot based on lidar. *IOP Conf. Ser.: Mater. Sci. Eng.* **831**, 012021. https://doi.org/10.1088/1757-899X/831/1/012021 (2020).
11. Zhou, G. et al. Design of supercontinuum laser hyperspectral light detection and ranging (LIDAR)(SCLaHS LIDAR). *Int. J. Remote Sens.* **42**, 3731–3755 (2021).
12. Billa, A., Shayea, I., Alhammadi, A., Abdullah, Q. & Roslee, M. An overview of indoor localization technologies: Toward IoT navigation services. In *2020 IEEE 5th International Symposium on Telecommunication Technologies (ISTT)*, 76–81, https://doi.org/10.1109/ISTT50966.2020.9279369 (2020).

13. Andò, B., Baglio, S., Crispino, R. & Marletta, V. An introduction to indoor localization techniques case of study: A multi-trilateration-based localization system with user-environment interaction feature. *Appl. Sci.* **11**, 7392. https://doi.org/10.3390/app11167392 (2021).
14. Jekateryńczuk, G. & Piotrowski, Z. A survey of sound source localization and detection methods and their applications. *Sensors* **24**, 68. https://doi.org/10.3390/s24010068 (2024).
15. Sun, Y. et al. Indoor drone localization and tracking based on acoustic inertial measurement. *IEEE Trans. Mob. Comput.* **23**, 7537–7551. https://doi.org/10.1109/TMC.2023.3335860 (2024).
16. Al-homayani, F. & Mahoor, M. H. Improved indoor geomagnetic field fingerprinting for smartwatch localization using deep learning. *2018 International Conference on Indoor Positioning and Indoor Navigation (IPIN)* 1–8 (2018).
17. Subedi, S. & Pyun, J.-Y. A survey of smartphone-based indoor positioning system using RF-based wireless technologies. *Sensors* **20**, 7230. https://doi.org/10.3390/s20247230 (2020).
18. Maheepala, M., Kouzani, A. Z. & Joordens, M. A. Light-based indoor positioning systems: A review. *IEEE Sens. J.* **20**, 3971–3995. https://doi.org/10.1109/JSEN.2020.2964380 (2020).
19. Lee, C.-H., Chen, I.-T., Yang, H.-C. & Chen, Y. J. An AI-powered electronic nose system with fingerprint extraction for aroma recognition of coffee beans. *Micromachines* **13**, 1313. https://doi.org/10.3390/mi13081313 (2022).
20. Aghili, N. S. et al. Aromatic fingerprints: VOC analysis with E-nose and GC-MS for rapid detection of adulteration in sesame oil. *Sensors* **23**, 6294. https://doi.org/10.3390/s23146294 (2023).
21. Alam, F., Faulkner, N. & Parr, B. Device-free localization: A review of non-RF techniques for unobtrusive indoor positioning. *IEEE Internet Things J.* **8**, 4228–4249. https://doi.org/10.1109/JIOT.2020.3030174 (2021).
22. Choutri, K. et al. Vision-based UAV detection and localization to indoor positioning system. *Sensors* **24**, 4121. https://doi.org/10.3390/s24134121 (2024).
23. Zhao, W. et al. Vivid: Augmenting vision-based indoor navigation system with edge computing. *IEEE Access* **8**, 42909–42923. https://doi.org/10.1109/ACCESS.2020.2978123 (2020).
24. Ngamakeur, K., Yongchareon, S., Yu, J. & Rehman, S. U. A survey on device-free indoor localization and tracking in the multi-resident environment. *ACM Comput. Surv.* **53**, 1. https://doi.org/10.1145/3396302 (2020).
25. Chen, Y. et al. Led based high accuracy indoor visible light positioning algorithm. *Optik* **243**, 166853. https://doi.org/10.1016/j.ijleo.2021.166853 (2021).
26. Chen, Y., Zheng, H., Liu, H., Han, Z. & Ren, Z. Indoor high precision three-dimensional positioning system based on visible light communication using improved hybrid bat algorithm. *IEEE Photonics J.* **12**, 1–13. https://doi.org/10.1109/JPHOT.2020.3017670 (2020).
27. Bregar, K., Hrovat, A., Mohorčič, M. & Javornik, T. Self-calibrated UWB based device-free indoor localization and activity detection approach. In *2020 European Conference on Networks and Communications (EuCNC)* 176–181, https://doi.org/10.1109/EuCNC48522.2020.9200968 (2020).
28. Ngamakeur, K., Yongchareon, S., Yu, J. & Islam, S. Passive infrared sensor dataset and deep learning models for device-free indoor localization and tracking. *Pervasive Mob. Comput.* **88**, 101721. https://doi.org/10.1016/j.pmcj.2022.101721 (2023).
29. Faulkner, N., Parr, B., Alam, F., Legg, M. & Demidenko, S. Caploc: Capacitive sensing floor for device-free localization and fall detection. *IEEE Access* **8**, 187353–187364. https://doi.org/10.1109/ACCESS.2020.3029971 (2020).
30. Kim Geok, T. et al. Review of indoor positioning: Radio wave technology. *Appl. Sci.* **11**, 279. https://doi.org/10.3390/app11010279 (2021).
31. Roy, P. & Chandreyee, C. A survey of machine learning techniques for indoor localization and navigation systems. *J. Intell. Robot. Syst.* **101**, 63 (2021).
32. Sakpere, W., Adeyeye-Oshin, M. & Mlitwa, N. B. A state-of-the-art survey of indoor positioning and navigation systems and technologies. *S. Afr. Comput. J.* **29**, 145–197 (2017).
33. Guvenc, I., Chong, C.-C. & Watanabe, F. Analysis of a linear least-squares localization technique in LOS and NLOS environments. In *2007 IEEE 65th Vehicular Technology Conference - VTC2007-Spring*, 1886–1890, https://doi.org/10.1109/VETECS.2007.391 (2007).
34. Assayag, Y. et al. Efficient exploration of indoor localization using genetic algorithm and signal propagation model. *Computing* **107**, 30 (2025).
35. Singh, N., Choe, S. & Punmiya, R. Machine learning based indoor localization using Wi-Fi RSSI fingerprints: An overview. *IEEE Access* **9**, 127150–127174. https://doi.org/10.1109/ACCESS.2021.3111083 (2021).
36. Du, J., Yuan, C., Yue, M. & Ma, T. A novel localization algorithm based on RSSI and multilateration for indoor environments. *Electronics* **11**, 289. https://doi.org/10.3390/electronics11020289 (2022).
37. Park, J.-K., Park, J.-H. & Kim, K.-T. Multipath signal mitigation for indoor localization based on MIMO FMCW radar system. *IEEE Internet of Things J.* **11**(2), 2618–2629 (2023).
38. Yu, C., Fang, S.-H., Lin, L., Chien, Y.-R. & Xu, Z. The impact of environmental factors on mm-wave radar point-clouds for human activity recognition. 1–2, https://doi.org/10.1109/iWEM49354.2020.9237398 (2020).
39. Che, R. & Chen, H. Channel state information based indoor fingerprinting localization. *Sensors* **23**, 5830. https://doi.org/10.3390/s23135830 (2023).
40. Bouchard, K., Ramezani, R. & Naeim, A. Features based proximity localization with bluetooth emitters. In *2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 1–5 (IEEE, 2016).
41. Gharib, M. R., Fard, M. A. & Koochi, A. Error analysis of dead reckoning navigation system by considering uncertainties in an underwater vehicle's sensors. *J. Navig.* **77**, 18. https://doi.org/10.1017/S0373463324000183 (2024).
42. Asaad, S. M. & Maghdid, H. S. A comprehensive review of indoor/outdoor localization solutions in IoT era: Research challenges and future perspectives. *Comput. Netw.* **212**, 109041 (2022).
43. Ouyang, G. & Abed-Meraim, K. A survey of magnetic-field-based indoor localization. *Electronics* **11**, 864 (2022).
44. Jia, W., Qi, G., Liu, M. & Zhou, J. A high accuracy localization algorithm with dv-hop and fruit fly optimization in anisotropic wireless networks. *J. King Saud Uni. Comput. Inf. Sci.* **34**, 8102–8111 (2022).
45. Reyes, J. M. R., Ho, I.W.-H. & Mak, M.-W. WI-FI CSI fingerprinting-based indoor positioning using deep learning and vector embedding for temporal stability. *Expert Syst. Appl.* **264**, 125802 (2025).
46. Holcer, S., Torres-Sospedra, J., Gould, M. & Remolar, I. Privacy in indoor positioning systems: A systematic review. In *2020 International Conference on Localization and GNSS (ICL-GNSS)*, 1–6, https://doi.org/10.1109/ICL-GNSS49876.2020.9115496 (2020).
47. Al-Garadi, M. A. et al. A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Commun. Surv. Tutor.* **22**, 1646–1685 (2020).
48. Barua, A., Al Alamin, M. A., Hossain, M. S. & Hossain, E. Security and privacy threats for bluetooth low energy in IoT and wearable devices: A comprehensive survey. *IEEE Open J. Commun. Soc.* **3**, 251–281 (2022).
49. Kordi, K. A. et al. Survey of indoor localization based on deep learning. *Comput. Mater. Continua* **79**, 3261 (2024).
50. Adanur Dedturk, B., Kolukısa, B. & Tonyali, S. Privacy-preserving wireless indoor localization systems. *Kocaeli J. Sci. Eng.* **6**, 114 (2023).
51. Ali, S., Wang, J. & Leung, V. C. M. Ai-driven fusion with cybersecurity: Exploring current trends, advanced techniques, future directions, and policy implications for evolving paradigms-a comprehensive review. *Inf. Fus.* **118**, 102922 (2025).

52. Barsocchi, P. *et al.* A privacy-by-design architecture for indoor localization systems. In *International Conference on the Quality of Information and Communications Technology*, 358–366 (Springer, 2020).
53. Li, W., Su, Z., Li, R., Zhang, K. & Xu, Q. Abnormal crowd traffic detection for crowdsourced indoor positioning in heterogeneous communications networks. *IEEE Trans. Netw. Sci. Eng.* **7**, 2494–2505 (2020).
54. Li, W., Su, Z., Zhang, K., Benslimane, A. & Fang, D. Defending malicious check-in using big data analysis of indoor positioning system: An access point selection approach. *IEEE Trans. Netw. Sci. Eng.* **7**, 2642–2655 (2020).
55. Li, W., Su, Z., Zhang, K. & Benslimane, A. Defending malicious check-in based on access point selection for indoor positioning system. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, 1–6 (IEEE, 2020).
56. Yang, Y. & Huang, G. Map-based localization under adversarial attacks. In *Robotics Research: The 18th International Symposium ISRR*, 775–790 (Springer, 2019).
57. Li, W., Zhang, C. & Tanaka, Y. Pseudo label-driven federated learning-based decentralized indoor localization via mobile crowdsourcing. *IEEE Sens. J.* **20**, 11556–11565 (2020).
58. Ko, D., Choi, S.-H., Ahn, S. & Choi, Y.-H. Robust indoor localization methods using random forest-based filter against mac spoofing attack. *Sensors* **20**, 6756 (2020).
59. Ciftler, B. S., Albaseer, A., Lasla, N. & Abdallah, M. Federated learning for RSS fingerprint-based localization: A privacy-preserving crowdsourcing method. In *2020 International Wireless Communications and Mobile Computing (IWCMC)*, 2112–2117 (IEEE, 2020).
60. Zhang, G., Zhang, A., Zhao, P. & Sun, J. Lightweight privacy-preserving scheme in Wi-Fi fingerprint-based indoor localization. *IEEE Syst. J.* **14**, 4638–4647 (2020).
61. Shubina, V., Ometov, A., Andreev, S., Niculescu, D. & Lohan, E. S. Privacy versus location accuracy in opportunistic wearable networks. In *2020 International Conference on Localization and GNSS (ICL-GNSS)*, 1–6 (IEEE, 2020).
62. Yan, W., Hylamia, S., Voigt, T. & Rohner, C. PHY-IDS: A physical-layer spoofing attack detection system for wearable devices. In *Proceedings of the 6th ACM Workshop on Wearable Systems and Applications*, 1–6 (2020).
63. Madani, P., Vlajic, N. & Sadeghpour, S. Mac-layer spoofing detection and prevention in IoT systems: Randomized moving target approach. In *Proceedings of the 2020 Joint Workshop on CPS &IoT Security and Privacy*, 71–80 (2020).
64. Nieminen, R. & Järvinen, K. Practical privacy-preserving indoor localization based on secure two-party computation. *IEEE Trans. Mob. Comput.* **20**, 2877–2890 (2020).
65. Kordi, K. A., Alhammadi, A., Roslee, M., Alias, M. Y. & Abdullah, Q. A review on wireless emerging IoT indoor localization. In *2020 IEEE 5th International Symposium on Telecommunication Technologies (ISTT)*, 82–87 (IEEE, 2020).
66. Alhammadi, A., Hashim, F., Rasid, M. F. A. & Alraih, S. A three-dimensional pattern recognition localization system based on a Bayesian graphical model. *Int. J. Distrib. Sensor Netw.* **16**(9), 1550147719884893 (2020).
67. Alhammadi, A., Alraih, S., Hashim, F. & Rasid, M. F. A. Robust 3d indoor positioning system based on radio map using Bayesian network. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, 107–110 (IEEE, 2019).
68. Patil, M. *Adversarial Attack on RSSI-Based Indoor Localization Using Deep Learning*. Master's thesis, California State University, Sacramento (2021).
69. Ambalkar, H., Wang, X. & Mao, S. Adversarial human activity recognition using Wi-Fi CSI. In *2021 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 1–5 (IEEE, 2021).
70. Wang, C., Luo, J., Liu, X. & He, X. Secure and reliable indoor localization based on multitask collaborative learning for large-scale buildings. *IEEE Internet Things J.* **9**, 22291–22303 (2021).
71. Na, X., Guo, X., He, Y. & Xi, R. Wi-attack: Cross-technology impersonation attack against ibeacon services. In *2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, 1–9 (IEEE, 2021).
72. DERVİŞOĞLU, İ. & YAVANOĞLU, U. Security threats and performance evaluation of ultra wideband and bluetooth low energy technologies for indoor positioning. In *2021 International Conference on Information Security and Cryptology (ISCTURKEY)* 22–27 (IEEE, 2021).
73. Sun, X., Ai, H., Tao, J., Hu, T. & Cheng, Y. BERT-ADLOC: A secure crowdsourced indoor localization system based on BLE fingerprints. *Appl. Soft Comput.* **104**, 107237 (2021).
74. Madani, P. & Vlajic, N. BERT-ADLOC: A secure crowdsourced indoor localization system based on BLE fingerprints. *J. Cybersecur. Privacy* **1**, 453–469 (2021).
75. Njima, W., Chafii, M., Chorti, A., Shubair, R. M. & Poor, H. V. Indoor localization using data augmentation via selective generative adversarial networks. *IEEE Access* **9**, 98337–98347 (2021).
76. Huang, P., Zhang, X., Yu, S. & Guo, L. Is-wars: Intelligent and stealthy adversarial attack to Wi-Fi-based human activity recognition systems. *IEEE Trans. Dependable Secure Comput.* **19**, 3899–3912 (2021).
77. Min, M. et al. 3d geo-indistinguishability for indoor location-based services. *IEEE Trans. Wirel. Commun.* **21**, 4682–4694 (2021).
78. Beko, M. & Tomic, S. Toward secure localization in randomly deployed wireless networks. *IEEE Internet Things J.* **8**, 17436–17448 (2021).
79. Zhang, X. et al. A differentially private indoor localization scheme with fusion of WiFi and bluetooth fingerprints in edge computing. *Neural Comput. Appl.* **34**, 4111–4132 (2022).
80. Navidan, H., Moghtadaiee, V., Nazaran, N. & Alishahi, M. Hide me behind the noise: Local differential privacy for indoor location privacy. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS &PW)*, 514–523 (IEEE, 2022).
81. Fathalizadeh, A., Moghtadaiee, V. & Alishahi, M. On the privacy protection of indoor location dataset using anonymization. *Comput. Secur.* **117**, 102665 (2022).
82. Boora, U., Wang, X. & Mao, S. Robust massive MIMO localization using neural ode in adversarial environments. In *ICC 2022-IEEE International Conference on Communications*, 4866–4871 (IEEE, 2022).
83. Yang, J., Zou, H. & Xie, L. Securesense: Defending adversarial attack for secure device-free human activity recognition. *IEEE Trans. Mob. Comput.* **23**, 823–834 (2022).
84. Ye, Q. et al. Se-loc: security-enhanced indoor localization with semi-supervised deep learning. *IEEE Trans. Netw. Sci. Eng.* **10**, 2964–2977 (2022).
85. Wang, X. et al. Adversarial deep learning for indoor localization with channel state information tensors. *IEEE Internet Things J.* **9**, 18182–18194 (2022).
86. Han, Z. et al. Cnn-based attack defense for device-free localization. *Mob. Inf. Syst.* **2022**, 2323293 (2022).
87. Gao, B. et al. A federated learning framework for fingerprinting-based indoor localization in multibuilding and multifloor environments. *IEEE Internet Things J.* **10**, 2615–2629 (2022).
88. Peterseil, P., Etzlinger, B., Khanzadeh, R. & Springer, A. Trustworthiness score for uwb indoor localization. In *GLOBECOM 2023-2023 IEEE Global Communications Conference* 189–194 (IEEE, 2023).
89. Shakerian, A., Eghmazi, A., Goasdoué, J. & Landry, R. J. A secure ZUPT-aided indoor navigation system using blockchain in GNSS-denied environments. *Sensors* **23**, 6393 (2023).
90. Mitchell, F., Smith, P., Bhaskara, A. & Kasera, S. K. Exploring adversarial attacks on learning-based localization. In *Proceedings of the 2023 ACM Workshop on Wireless Security and Machine Learning* 15–20 (2023).
91. Casanova-Marqués, R., Torres-Sospedra, J., Hajny, J. & Gould, M. Maximizing privacy and security of collaborative indoor positioning using zero-knowledge proofs. *Internet of Things* **22**, 100801 (2023).
92. Mohsen, M., Rizk, H. & Youssef, M. Privacy-preserving by design: Indoor positioning system using Wi-Fi passive TDOA. In *2023 24th IEEE International Conference on Mobile Data Management (MDM)* 221–230 (IEEE, 2023).

93. Kalpana, A. V., Geetha, A. V., Jagadeesh, M. S. & Shobana, J. Secure 3d: Secure and energy efficient localization in 3d environment using wireless sensor networks. *Wirel. Pers. Commun.* **136**, 1375–1402 (2024).
94. Gebremariam, G. G., Panda, J. & Indu, S. Secure localization techniques in wireless sensor networks against routing attacks based on hybrid machine learning models. *Alex. Eng. J.* **82**, 82–100 (2023).
95. Chen, H. & Dhekne, A. Unspoof: Distance spoofing-evident localization using UWB. In *2023 13th International Conference on Indoor Positioning and Indoor Navigation (IPIN)* 1–6 (IEEE, 2023).
96. Xiao, F., Huang, Y., Zuo, Y., Kuang, W. & Wang, W. Over-the-air adversarial attacks on deep learning Wi-Fi fingerprinting. *IEEE Internet Things J.* **10**, 9823–9835 (2023).
97. Fathalizadeh, A., Moghtadaiee, V. & Alishahi, M. Indoor geo-indistinguishability: Adopting differential privacy for indoor location data protection. *IEEE Trans. Emerg. Top. Comput.* **12**, 293–306 (2023).
98. Guo, J., Ho, I.W.-H., Hou, Y. & Li, Z. Fedpos: A federated transfer learning framework for CSI-based Wi-Fi indoor positioning. *IEEE Syst. J.* **17**, 4579–4590 (2023).
99. Gufran, D. & Pasricha, S. Fedhil: Heterogeneity resilient federated learning for robust indoor localization with mobile devices. *ACM Trans. Embedded Comput. Syst.* **22**, 1–24 (2023).
100. Xu, J. *et al.* An indoor localization mechanisms based on local differential privacy. In *2023 4th Information Communication Technologies Conference (ICTC)* 121–126 (IEEE, 2023).
101. Min, M. *et al.* Indoor semantic location privacy protection with safe reinforcement learning. *IEEE Transactions on Cognitive Communications and Networking* (2023).
102. Kumar, R., Popli, R., Khullar, V., Kansal, I. & Sharma, A. Confidentiality preserved federated learning for indoor localization using Wi-Fi fingerprinting. *Buildings* **13**, 2048 (2023).
103. Shahbazian, R., Macrina, G., Scalzo, E. & Guerriero, F. Machine learning assists IoT localization: A review of current challenges and future trends. *Sensors* **23**, 3551 (2023).
104. Chen, H. & Dhekne, A. Spoofing evident and spoofing deterrent localization using ultra-wideband (uwb) active-passive ranging. *IEEE J. Indoor Seamless Position. Navig.* **2**, 12 (2023).
105. Wang, X. *et al.* Secure two-party computation for fingerprinting-based indoor localization. In *2023 IEEE/CIC International Conference on Communications in China (ICCC)* 1–5 (IEEE, 2023).
106. Tiku, S. & Pasricha, S. Secure indoor localization on embedded devices with machine learning. In *Embedded Machine Learning for Cyber-Physical, IoT, and Edge Computing: Use Cases and Emerging Challenges* 343–375 (Springer, 2023).
107. Ma, Y., Luo, X., Li, R., Du, S. & Liu, W. Lenser: A channel state information based indoor localization scheme for malicious devices. In *2023 IEEE 20th International Conference on Mobile Ad Hoc and Smart Systems (MASS)* 461–470 (IEEE, 2023).
108. Brachmann, M., Phillips, G., Gülen, U. & Tudor, V. Toward privacy-preserving localization and mapping in extended reality: A privacy threat model. In *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)* 635–640 (IEEE, 2023).
109. Yan, Y., Chen, J., Mahmood, A., Qian, X. & Yan, P. Ldporr: A localized location privacy protection method based on optimized random response. *J. King Saud Univ. Comput. Inf. Sci.* **35**, 101713 (2023).
110. Pandey, A. K. & Patel, Y. Domestic security clustering algorithm based on ap's capability to discriminate location: A survey. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* 1767–1771 (IEEE, 2023).
111. Billa, A., Shayea, I., Alhammadi, A., Abdullah, Q. & Roslee, M. An overview of indoor localization technologies: Toward IoT navigation services. In *2020 IEEE 5th International Symposium on Telecommunication Technologies (ISTT)* 76–81 (IEEE, 2020).
112. Etiabi, Y. & Amhoud, E. M. Federated distillation based indoor localization for IoT networks. *IEEE Sensors J.* **2**, 12 (2024).
113. Gufran, D. & Pasricha, S. Calloc: Curriculum adversarial learning for secure and robust indoor localization. In *2024 Design, Automation & Test in Europe Conference & Exhibition (DATE)* 1–6 (IEEE, 2024).
114. Eshun, S. N. & Palmieri, P. A cryptographic protocol for efficient mutual location privacy through outsourcing in indoor Wi-Fi localization. *IEEE Trans. Inf. Forens. Secur.* **19**, 4086–4099 (2024).
115. Huang, P. et al. Attacking and defending deep-learning-based off-device wireless positioning systems. *IEEE Trans. Wirel. Commun.* **23**(8), 8883–8895 (2024).
116. Moghtadaiee, V., Alishahi, M. & Rabiei, M. Differentially private gans for generating synthetic indoor location data. *arXiv preprint* arXiv:2404.07366 (2024).
117. Machaj, J., Brida, P. & Adamec, B. Effect of Wi-Fi access points spoofing on fingerprinting localization. In *2024 34th International Conference Radioelektronika (RADIOELEKTRONIKA)* 1–5 (IEEE, 2024).
118. Hemkumar, D. Preserving location privacy against inference attacks in indoor positioning system. *Peer-to-Peer Network. Appl.* **17**, 784–799 (2024).
119. Li, R., Hu, H. & Ye, Q. Rftrack: Stealthy location inference and tracking attack on Wi-Fi devices. *IEEE Trans. Inf. Forens. Secur.* **19**, 5925 (2024).
120. Yang, Y. et al. Trail: A three-step robust adversarial indoor localization framework. *IEEE Sensors J.* **24**, 10462 (2024).
121. Wang, Z., Xu, Y., Zhang, B. & Ouyang, X. Privacy-preserving indoor localization in cloud environments based on ranging transformation and inner product encryption. *Int. Arch. Photogramm. Remote. Sens. Spat. Inf. Sci.* **48**, 711–716 (2024).
122. Wang, J. *et al.* A trustworthy AIOT-enabled localization system via federated learning and blockchain. *arXiv preprint* arXiv:2407.07921 (2024).
123. Zocca, G. & Hasan, O. Privacy-preserving and trustworthy localization in an IoT environment. *arXiv preprint* arXiv:2406.16182 (2024).
124. Verma, H., Naval, S., Killi, B. R. & Vinod, P. Indoor localization using device sensors: A threat to privacy. *Microprocess. Microsyst.* **106**, 105041 (2024).
125. Li, J. & Mitra, U. Channel state information-free location-privacy enhancement: Delay-angle information spoofing. In *ICC 2024-IEEE International Conference on Communications* 3767–3772 (IEEE, 2024).
126. Alhammadi, A., Shamsan, Z. A. & De, A. Enhancing indoor user localization: An adaptive Bayesian approach for multi-floor environments. *Comput. Mater. Continua* **80**, 1889 (2024).
127. Abuhoureyah, F., Wong, Y. C., Al-Taweel, M. H. & Abdullah, N. I. Challenges and opportunities to location independent human activity recognition utilizing Wi-Fi sensing. *Int. J. Electr. Comput. Eng. (2088–8708)* **15**, 1 (2025).
128. David, L., Hassidim, A., David, Y. & Yung, M. The battery insertion attack: Is periodic pseudo-randomization sufficient for beacon privacy? *Proceedings on Privacy Enhancing Technologies* (2025).
129. Li, B. et al. ROLQ-TEE: Revocable and privacy-preserving optimal location query based on trusted execution environment. *Appl. Sci.* **15**, 1641 (2025).
130. Boudlal, H., Serrhini, M. & Tahiri, A. Towards a low-cost and privacy-preserving indoor activity recognition system using wifi channel state information. *Multimed. Tools Appl.* **84**, 1–32 (2025).
131. Nie, W. et al. Pervasive indoor user identification leveraging mobile single station localization. *IEEE Internet of Things J.* **12**, 15224–15237. https://doi.org/10.1109/JIOT.2025.3528447 (2025).
132. Salehzadeh Niksirat, K. et al. Wearable activity trackers: A survey on utility, privacy, and security. *ACM Comput. Surv.* **56**, 1–40 (2024).
133. Babalola, O. P. & Balyan, V. Wifi fingerprinting indoor localization based on dynamic mode decomposition feature selection with hidden Markov model. *Sensors* **21**, 6778 (2021).

134. Wang, Z., Wang, Z., Fan, L. & Yu, Z. A hybrid Wi-Fi fingerprint-based localization scheme achieved by combining fisher score and stacked sparse autoencoder algorithms. *Mob. Inf. Syst.* **2020**, 5710450 (2020).
135. Yang, Y. *et al.* UWBAD: Towards effective and imperceptible jamming attacks against uwb ranging systems with COTS chips. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, https://doi.org/10.1145/3658644.3670349 (2024).
136. Huang, C., Chi, C. & Hung, W. Hybrid-AI-based iBeacon indoor positioning cybersecurity: Attacks and defenses. *Sensors* **23**, 2159. https://doi.org/10.3390/s23042159 (2023).
137. Etiabi, Y., Njima, W. & Amhoud, E. M. Federated learning based hierarchical 3d indoor localization. In *2023 IEEE Wireless Communications and Networking Conference (WCNC)* 1–6 (IEEE, 2023).
138. Jaheen, A., Elsamanody, S., Rizk, H. & Youssef, M. Simdeep: An efficient federated learning indoor localization system with similarity aggregation strategy. In *Proceeding of the 32nd ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (GIS)*, https://doi.org/10.1145/3678717.3695763 (2024).
139. Song, S., Liu, L. & Peng, W. Sillcom: A communication-efficient privacy-preserving scheme for indoor localization. *Appl. Sci.* **15**, 6439. https://doi.org/10.3390/app15126439 (2025).
140. Moghtadaiee, V., Alishahi, M. & Rabiei, M. Differentially private GANs for generating synthetic indoor location data. *Int. J. Inf. Secur.* **24**, 111 (2025).
141. Ali, S. et al. CLDM-MMNNS: Cross-layer defense mechanisms through multi-modal neural networks fusion for end-to-end cybersecurity-issues, challenges, and future directions. *Inf. Fus.* **122**, 103222 (2025).
142. Suwannaphong, T., Jovan, F., Craddock, I. & McConville, R. Optimising tinyml with quantization and distillation of transformer and mamba models for indoor localisation on edge devices. *Sci. Rep.* **15**, 10081 (2025).

Acknowledgements
This research was supported by the Ministry of Higher Education (MoHE) Malaysia through the Fundamental Research Grant Scheme (FRGS/1/2023/ICT02/UTHM/02/3) and Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R51).

Author contributions
Ayesha Ayub : writing final draft, software, analyzed the results, and analysis, Writing - original draft. Dr. Zuhairiah Zainal Abidin: interpretation of data, Supervision, Writing - review & editing. Dr. Abdulraqeb Alhammadi: Supervision, Writing - review & editing. Dr. Muhammad Asim khan : Writing - review & editing and Software. Dr. Naglaa F. Soliman: Project administration, Resources, Writing - Review & Editing. Nurul Bashirah Ghazali: Writing- Review & Editing. Dr. Abeer D. Algarni :Project administration, Resources, Writing - Review & Editing.

Funding
The research was supported by the Fundamental Research Grant Scheme (FRGS/1/2023/ICT02/UTHM/02/3) and Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R51).

Declarations

Competing interests
The authors declare no competing interests.

Additional information
Correspondence and requests for materials should be addressed to Z.Z.A. or A.A.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.