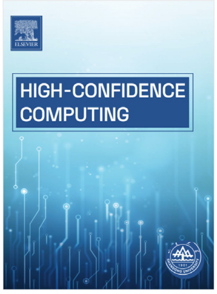

Privacy-preserving human activity sensing: A survey

Yanni Yang, Pengfei Hu, Jiaxing Shen, Haiming Cheng, Zhenlin An,
Xiulong Liu

PII: S2667-2952(24)00007-2
DOI: https://doi.org/10.1016/j.hcc.2024.100204
Reference: HCC 100204

To appear in: *High-Confidence Computing*

Received date : 23 August 2023
Revised date : 21 October 2023
Accepted date : 5 November 2023

Please cite this article as: Y. Yang, P. Hu, J. Shen et al., Privacy-preserving human activity sensing: A survey, *High-Confidence Computing* (2024), doi: https://doi.org/10.1016/j.hcc.2024.100204.

Privacy-Preserving Human Activity Sensing: A Survey

Yanni Yang[a], Pengfei Hu[a], Jiaxing Shen[b], Haiming Cheng[c], Zhenlin An[d], Xiulong Liu[e]

[a]*Shandong University, Qingdao, China*
[b]*Lingnan University, Hong Kong, China*
[c]*The Hong Kong Polytechnic University, Hong Kong, China*
[d]*Princeton University, New Jersey, USA*
[e]*Tianjin University, Tianjin, China*

Abstract

With the prevalence of various sensors and smart devices in people's daily lives, numerous types of information are being sensed. While using such information provides critical and convenient services, we are gradually exposing every piece of our behavior and activities. Researchers are aware of the privacy risks and have been working on preserving privacy while sensing human activities. This survey reviews existing studies on privacy-preserving human activity sensing. We first introduce the sensors and captured private information related to human activities. We then propose a taxonomy to structure the methods for preserving private information from two aspects: individual and collaborative activity sensing. For each of the two aspects, the methods are classified into three levels: signal, algorithm, and system. Finally, we discuss the open challenges and provide future directions.

Keywords: Human activity sensing, privacy-preserving sensing

1. Introduction

People enjoy various indispensable and convenient services enabled by the proliferation and development of smart devices and the Internet of Things. People's information is sensed to provide benefits and convenience, whereas privacy risks increase as we expose ourselves. Researchers have realized the importance of privacy issues during the emergence and popularity of human activity sensing [1]. Without proper solutions to preserving people's private information during activity sensing, not only are user's interests harmed, but

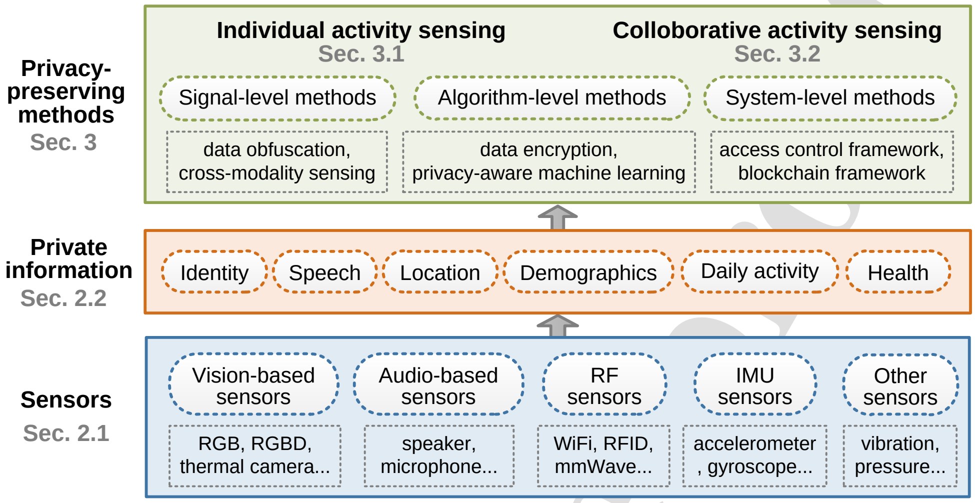

Figure 1: Taxonomy of the survey

the progress of the human activity sensing area is also hindered. Therefore, researchers have been devoted to tackling the privacy issue when sensing different activities.

This study presents a survey of existing studies on privacy-preserving human activity sensing. The survey taxonomy is shown in Fig. 1. We first introduce the sensors and the captured private information related to human activities. Then, we propose a new taxonomy to structure the methods to preserve private information from two aspects: individual and collaborative activity sensing. The methods for these two aspects are classified into three levels: signal, algorithm, and system. Finally, we discuss the open challenges and provide future directions.

1.1. Structure of the Survey

The survey is presented as follows: First, we introduce the common sensors used to sense human information and the types of signals and activities captured by these sensors in Section 2.1. Second, we demonstrate the private information involved in the sensed signals for human activity sensing in Section 2.2. Third, we propose a two-level taxonomy to classify existing methods for achieving private-preserving human activity sensing in Section 3. Specifically, the first-level methods are summarized as individual and collaborative activity sensing from the perspective of the scale of people. Second-level methods are categorized from the viewpoint of the pipeline for human activity sensing: signal-, algorithm-, and system-level methods. Then, we summarize the main features of different privacy-preserving methods and conduct a critical comparison. Finally, we propose and discuss future research directions in privacy-preserving human sensing.

1.2. Key Contributions

Some existing surveys related to privacy-preserving human activity sensing can be found in the literature [2, 3, 4]; however, they only focus on a specific aspect to preserve privacy. [2] mainly reviewed the privacy-preserving techniques for using deep learning techniques for human sensing. [3] summarized the studies applying federated learning to protect the privacy of user data. [4] presented a survey on privacy issues and corresponding approaches in human recognition and human activity recognition. No survey has yet presented a thorough introduction and summary of the state-of-the-art works for privacy-preserving human activity sensing. Therefore, we expand the scope of existing surveys to provide a systematic review of relevant works in privacy-preserving human activity sensing considering different aspects, including sensors, sensed information, human object scope, and methods for privacy preservation.

2. Sensors, Signals, and Private Information of Human Activity Sensing

This section first introduces the common sensors used to sense human information and the kinds of signals and activities captured by these sensors. Then, we present the private information involved in the sensed signals for human activity sensing.

2.1. Sensors and Signals

Various sensors are employed for sensing human activities. We classify the commonly used sensors into four categories: vision-based sensors, audio-based sensors, radio frequency (RF) sensors, inertial measurement unit (IMU) sensors, and other sensors. The captured signals are correspondingly introduced for different sensors.

2.1.1. Vision-based sensors

Many vision-based sensors, including RGB [5, 6, 7], RGB-D [8, 9, 10], and thermal [11] cameras, are widely used to sense human activities, e.g., human identification, pose recognition, and assisted living monitoring. Compared with the RGB camera, the RGB-D camera provides an extra dimension of information (i.e., coordinates). The thermal camera measures the light of a wavelength from 1,000 nm to 14,000 nm instead of the visible light. Vision-based sensors usually take videos to capture human movements. Therefore, instead of using a single image that only involves the spatial information of the human, the spatial-temporal information of the video is used to detect the activity.

2.1.2. Audio-based sensors

Audio-based sensors mainly refer to speakers and microphones. Current smart devices, like smartphones and laptops, are usually embedded with a pair of speaker and microphone. Audio-based sensors not only capture people's speech but also measure non-speech signals, e.g., coughing, sniffing, and breathing sounds, which can be used to detect human activities [12, 13, 14]. In addition, acoustic signal is one kind of wireless signal, which can be reflected by the human body. Thus, human movements can affect the propagation of the acoustic signal from the speaker to the microphone, from which the activity pattern can be observed. Therefore, the inaudible and ultrasound acoustic signals are also used to sense human activities, e.g., gesture recognition [15, 16, 17] and eyeblink [18, 19].

2.1.3. RF sensors

RF signals, such as RFID, WiFi, and mmWave signals, can be used not only for communication but also for human activity sensing. The principle behind using RF signals to detect human activities is that human body movements affect the propagation of the RF signal traveling from the transmitter to the receiver. By analyzing typical RF signal indicators, e.g., amplitude or phase, the human activity pattern can be revealed. Various RF signals, including Bluetooth [20], Zigbee [21], WiFi [22, 23, 24], RFID [25, 26], and radar signals [27, 28], have been investigated for human activity sensing.

2.1.4. IMU sensors

IMU sensors consist of accelerometers, gyroscopes, and magnetometers. Accelerometer measures object acceleration, and the gyroscope reports the object's angular velocity. The magnetometer is used to show the magnetic field strength around the object. Currently, various smart devices are commonly equipped with IMU sensors. Thus, people's movement acceleration, angular velocity, and the magnetic field of the surrounding environment can all be sensed when people carry smart devices while performing different activities. The IMU sensors can detect daily human activities [29, 30], e.g., gestures [31] and exercise [32].

2.1.5. Other sensors

Apart from the abovementioned mainstream sensors, researchers also investigate other sensor types, e.g., vibration [33, 34], pressure [35, 36], fiber [37, 38], and photoplethysmogram (PPG)/electrocardiogram (ECG)/electroencephalogram (EEG) sensors [39, 40, 41]. These sensors can either be worn by users on the body or installed in the environment for human activity sensing. Vibration sensors are used to capture muscle motions for human-computer interaction [42, 43]. Pressure sensors are used to sense the force from different body parts, e.g., the feet's force on shoes and hips' force on a seat cushion for gait analysis [44] and sitting posture recognition [45], respectively. Stretchable fiber sensors can be assembled into clothing, i.e., smart clothes, for activity monitoring, particularly for physiological signal measurement. PPG/ECG/EEG sensors are dedicatedly used for both physical and mental human information, particularly for cardiovascular and neurological diseases. Recently, portable and wearable PPG/ECG/EEF devices have been produced for daily human activity sensing, e.g., drowsiness detection during driving [41].

2.1.6. Discussion on the privacy intrusion of sensors

The level of privacy intrusion depends on various factors, such as the type of data collected, context in which the data is collected, and information sensitivity.

Vision-based sensors can capture visual information about people's bodies and movements, which can reveal sensitive information about their identity, appearance, and behavior. This can be particularly concerning in contexts where people have privacy expectations, such as in their homes and private spaces. Recent artificial intelligence (AI)-based image/video generation techniques can easily swap human faces to conduct fraud. Thus, information leakage from vision-based sensors is at a high-risk level concerning people's privacy and safety.

Acoustic-based sensors, such as microphones or sound sensors, can capture audio information, including people's conversations and other sounds in the environment. An unnoticed loudspeaker can also easily be turned into a microphone and eavesdrop on the surrounding sound without grabbing people's attention. Private conversations are a valuable source of information. Recent AI-based audio generation techniques can also mimic a person's tone and timbre. The acoustic leakage is also noteworthy in privacy protection.

RF-based sensors, such as RFID tags and Wi-Fi trackers, can capture information about people's movements and locations, potentially revealing sensitive information about one's daily routines and health conditions. Most importantly, RF signals, especially for signal frequencies below 10 GHz, can traverse through the wall, indicating that attackers can install RF transceivers outside people's homes and secretly monitor their behaviors. Thus, defenses against RF-based through-wall human monitoring should be well established.

Meanwhile, IMU-based sensors can capture information about people's movements and postures, potentially revealing sensitive information about one's physical activities, health status, and emotional state. Since IMU units are mainly wearable sensors, the corresponding sensory data are mostly collected from the user side. However, IMU signals are still vulnerable to privacy leakage while the data is sent to the cloud. Apart from the activity information, the user's personal information, e.g., age and gender, can also be inferred from the IMU sensory data. Recent studies on the Internet of Things (IoT) security have shown that IMU sensors in smartphones can also eavesdrop on the sound from the loudspeaker because the sound vibration can affect the accelerometer [46]. Thus, access to IMU sensors should be well-regulated.

2.2. Private Information

In general, private information can be any data that people do not want to disclose to others [47]. The information captured by the abovementioned sensors involves much private information, as listed in Table 1. This section introduces the key private information.

2.2.1. Identity information

Various types of signals can reveal a person's identity. Direct sensory data is the image and speech information because the current face and speech recognition approaches are widely used for human identification. Therefore, human activity sensing via vision- and audio-based sensors can easily lead to the disclosure of people's identity information. In recent studies, researchers have found that the sensory data collected for human activity recognition can indirectly expose the user's identity information [48]. In

Table 1: Sensors and involved private information

Sensors	Private information
Vision sensors	identity, location, demographics, activities, health
Audio sensors	identity, speech, activities, health
RF sensors	identity, location, speech, activities, health
IMU sensors	speech, location, demographics, activities, health
Others (GPS, pressure, etc.)	identity, speech, location, activities, health

addition, many biomarkers, including the fingerprint, palmprint, or heartbeat [49], can uniquely represent people's identities. A surge of physiological and behavioral features for human identification has been presented to enhance security. On the other hand, if these features are not properly protected, they will leave potential opportunities for adversaries to steal identity information.

2.2.2. Speech information

In addition to identity information, the speech content in the audio signal also involves private information. For long-term activity monitoring, the user's and bystander's speech during conversation can be secretly captured. The famous Watergate Scandal involved the installation of an automatic recording system in the White House to eavesdrop on conversations and phone calls. Many famous celebrities are plagued by eavesdropping. The high interest in speech information and its seriousness has made eavesdropping a hot topic for many years. Eavesdropping on speech via IMU sensors, RF signals, and side-channel signals is widely investigated [50, 51, 52, 53]. The unnotified recording poses more damage to public privacy with the prevalence of IoT devices. Therefore, anti-recording is also an important field to study and investigate.

2.2.3. Location information

The most popular way for localization nowadays is using GPS. Telecommunication operators and location-based service companies own a huge amount of GPS data. The GPS data play a significant role when used for social benefits, e.g., crowd control and disaster response. However, when exposed to adversaries, threats can range from personal safety to national security. Apart from GPS data for the outdoors, researchers have also shown the capability of audio and RF signals and IMU sensory data for indoor localization

[54, 55, 20]. Therefore, the location information can be contained in the signals initially used for other human sensing tasks. In a word, various human sensing techniques have woven a seamless web of location information, threatening people's privacy anytime and anywhere.

2.2.4. Demographic information

Demographic information, such as age, gender, and income, can be excavated from human activity sensing-related sensory data using big data mining techniques. For instance, group gender is detected using the audio signal, even if the audio signal is filtered to remove the sensitive information [56]. IMU sensory data during walking can be used to predict the user's age and gender with over 90% accuracy [57]. The place of residence and the places people visit every day can reveal their income levels [58]. Hidden information from human sensing data can be enormous. In addition, the sensory data specifically collected for one sensing task can be reused to dig out demographic information, which should not be overlooked.

2.2.5. Daily activity information

Tracking people's daily activities can be considered a privacy intrusion or even a security threat. Daily activity monitoring is useful for assisted living, especially in the era of global aging. This is one of the key motivations for developing diverse sensors for human activity recognition. On the other hand, it provides different ways to secretly acquire the activity information of a person of interest. Sometimes, adversaries only need to obtain a course-grained piece of information to reach their goals. For instance, the thief can simply take action by knowing if someone is in the room, which can be accomplished by sniffing the WiFi usage status. If more advanced techniques are employed, e.g., RF-based through-wall human sensing [23], adversaries can know how many people are in a home or who are at home. For business purposes, companies may leverage the activity information collected from smartphones, smartwatches, and voice assistants, for advertising. Thus, daily activity information requires appropriate safeguards.

2.2.6. Health information

Smart healthcare has become a popular and developing concept in recent decades. People have started caring for their health by monitoring their long-term physiological signals (e.g., heartbeat and blood pressure) and sleeping conditions (e.g., sleeping depth and length) using many wearable devices that usually contain certain health condition monitoring applications. These applications collect health information that enables users to monitor their physical and mental status. However, if people's disease information is leaked, they may be improperly treated with discrimination and social stigma. Disrespect of people's health information privacy is a serious breach of trust and can have negative consequences for affected individuals.

3. Privacy-Preserving Human Activity Sensing Methods

This section introduces methods for protecting and preserving private information during human activity sensing. We separately introduce the existing methods according to the scope of the human subjects, i.e., individual and collaborative activity sensing. The key difference between individual and collaborative human activity sensing lies in whether the sensing information can be exposed and shared. In many cases, user data does not need to be shared, e.g., presence detection and localization applications. For these scenarios, data from different individuals can be independent. In short, individual activity sensing is sufficient. Accordingly, the focus in realizing privacy-preserving individual human sensing is to prevent the sensed information from being exposed and shared with other parties. On the other hand, many activity sensing tasks, especially for activity recognition, aggregate different user data can significantly improve recognition performance. For instance, existing exercise recognition applications on smartwatches significantly benefit from the large amount of data collected from various users; thus, different users must share their data and collaboratively obtain a recognition model. The focus of privacy-preserving collaborative human sensing is to avoid the leakage of private information during data sharing. We summarize the privacy-preserving methods for individual and collaborative activity sensing in Fig. 2. For each of them, we further classify the privacy-preserving methods into three categories: signal-, algorithm-, and system-level methods.

3.1. Methods for Individual Activity Sensing

For many human activity sensing applications, the target person only uses his or her own activity data. For example, a person first collects training data for their own activities. He/she then uploads the data to the computation device to obtain an activity sensing model. Subsequently, this model can be used to infer future activities without the need for individuals to share

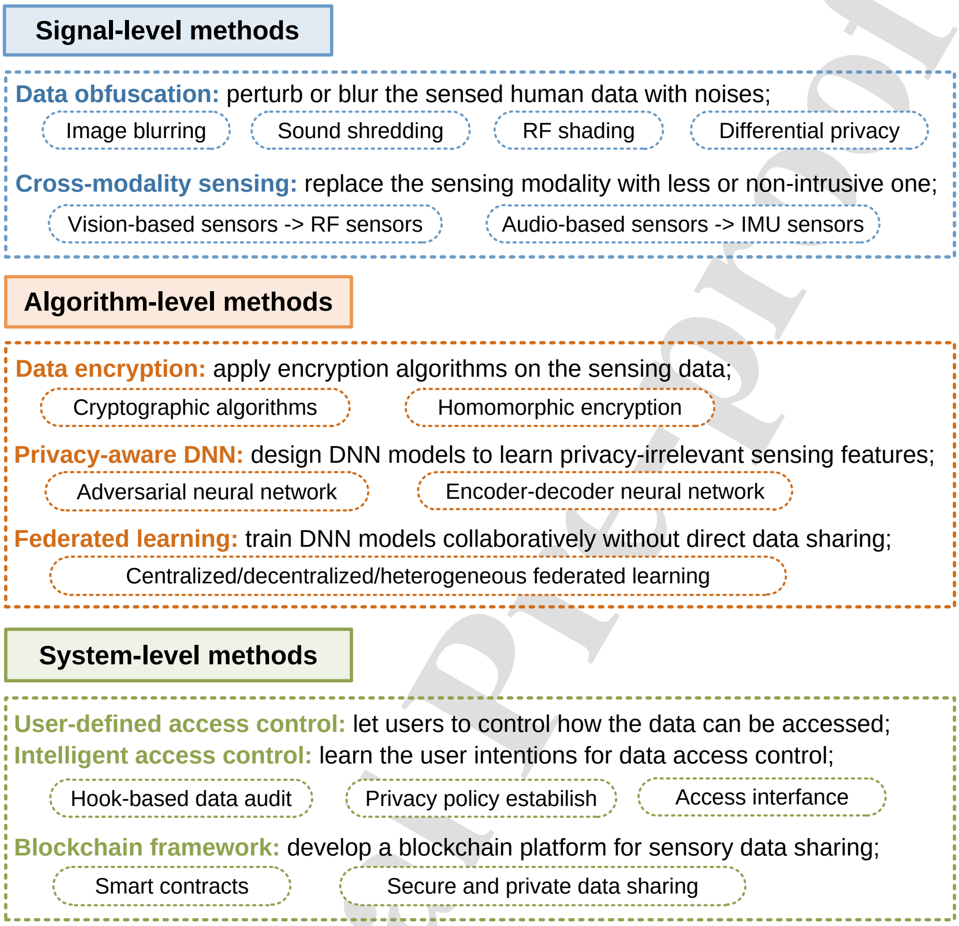
Signal-level methods
Data obfuscation: perturb or blur the sensed human data with noises;
Image blurring
Sound shredding
RF shading
Differential privacy
Cross-modality sensing: replace the sensing modality with less or non-intrusive one;
Vision-based sensors -> RF sensors
Audio-based sensors -> IMU sensors
Algorithm-level methods
Data encryption: apply encryption algorithms on the sensing data;
Cryptographic algorithms
Homomorphic encryption
Privacy-aware DNN: design DNN models to learn privacy-irrelevant sensing features;
Adversarial neural network
Encoder-decoder neural network
Federated learning: train DNN models collaboratively without direct data sharing;
Centralized/decentralized/heterogeneous federated learning
System-level methods
User-defined access control: let users to control how the data can be accessed;
Intelligent access control: learn the user intentions for data access control;
Hook-based data audit
Privacy policy estabilish
Access interfance
Blockchain framework: develop a blockchain platform for sensory data sharing;
Smart contracts
Secure and private data sharing

Figure 2: Privacy-preserving methods for human activity sensing

their sensed information. A naive method for preserving a person's individual private information is to store and process the data locally. Existing end devices, e.g., laptops and smartphones, are equipped with large storage and computation capabilities. Meanwhile, thanks to neural network design development, activity sensing models can now be made lightweight for running on end devices [59]. Local signal processing and activity inference preserve private information from misuse and poor data management. Many activity sensing systems have adopted this idea and are implemented on the local device [42, 55]. However, many activity monitoring applications can secretly collect sensory signals without notification. Thus, local data collection and processing cannot guarantee user privacy.

3.1.1. Signal-level methods

The first signal-level method involves perturbation or blurring of the sensed signal, i.e., deliberately adding noises in the raw signal to avoid leakage of important information. With regard to images, extremely low-resolution images [60, 6, 11, 61, 62], blur filtering [63], and face anonymizer [64] are used to protect the private information captured by cameras. For audio signals, sound shredding [65], sub-sampling [56], and filtering [66, 12] are performed to remove sensitive information. To impede unauthorized speech information recording, researchers have harnessed the nonlinearity of commodity microphones and designed active ultrasound for jamming [67]. For RF-based sensing, extra reflectors have been added in the room to prevent illegal through-wall shopping, which can generate fake humans to deceive adversaries [68]. However, the aforementioned solutions are proposed for a specific type of signal modality. To achieve generalized protection of sensitive information, researchers have also developed frameworks that support the obfuscation [69] and substitution [70] of human sensing data collected by smartphones and body-worn sensors. Differential privacy techniques, which add random noise to data, can also be applied to protect the individual's privacy in a dataset [71].

The second signal-level method changes the sensing modality for the same activity sensing task. Although each sensor can expose certain private information, they can complement each other by alternating the usage of different sensors. A typical example of this is human face authentication, which is commonly realized via cameras to capture facial images/videos. To avoid abuse of captured images/videos, we can substitute vision-based sensors with RF-based sensors. RFID and mmWave radars have been shown to be effective in face imaging and human identification [72, 73]. Another example is to replace audio-based human-computer interaction with gesture-based solutions using IMU sensors, vibration sensors, and so on, which can reduce the chances of speech information leakage.

3.1.2. Algorithm-level methods

This first algorithm-level method is to encrypt the collected sensory data. Traditional encryption methods simply apply cryptographic algorithms to the data, which needs further decryption before use. The decryption key is still vulnerable to being stolen during delivery. To achieve a double-win among convenience, data privacy, and smooth data usage, homomorphic encryption can be employed to perform computation on encrypted data without decryption. In other words, sensitive data can be stored and processed in an encrypted state, thereby reducing the risk of unauthorized access. Homomorphic encryption is particularly useful in human activity sensing situations, where privacy is paramount, such as in healthcare-related and biometric data [74, 4].

The second algorithm-level method stems from the advances in neural networks. Privacy-preserving neural networks refer to the machine learning models designed to protect the privacy of sensitive data used to train models or make predictions [75]. As discussed in Section 2.1.6, neural network models are good at learning the user's underlying domestic information. Thus, we need to deal with privacy leakage in neural network models. The emergence of adversarial neural network brings opportunities to realize privacy-preserving neural networks. The adversarial neural network model comprises two neural networks, namely, the generator and the discriminator, which combat each other to achieve an optimal result. It can be applied to allow the human activity recognition model to learn representations that promote the classification of various activities, meanwhile preventing the model from accessing user-discriminative information [48, 76, 77]. In addition to adversarial neural networks, convolutional neural networks have also been investigated to transform sensor data into a new format in which private information is forgotten after transformation [78].

Some studies have combined the two abovementioned types of algorithm-level methods. However, homomorphic encryption can be time-consuming. A fully homomorphic encrypted wavelet neural network has been proposed to preserve data privacy and maintain the model's time efficiency [79]. On the other hand, most neural network models offer insufficient protection of sensitive information. Privacy-preserving neural network models using homomorphic encryption are often utilized [80].

3.1.3. System-level methods

The first system-level method is to provide a privacy control framework and let users decide the kind of information forbidden to use and share [81, 82]. To reach this goal, the first step is to monitor and track the sensor usage conditions. Researchers have designed hook-based methods to audit the sensor signal flow, frequency, duration, and invoker, meanwhile performing quantitative analysis of the signal usage in real time [83]. Frameworks for recognizing sensor data tussles in the operating system have also been proposed [84]. The second step is to establish privacy policies or rules for sensor data control. Various data control policies, which are mostly related to permission over sensors, have been proposed for mobile human sensing systems [85, 86, 87]. The final step is to offer tools to users for applying these policies. This can be achieved by designing a set of libraries [88], assigning privacy-guaranteed regions [89], inserting hooks into applications [86], or providing secure log sealing on live sensors [90]. To achieve flexible privacy control, framework developers usually allow users to select and customize data permission choices in the interface [91].

The second system-level methods are more intelligent than the previous ones. Instead of requiring users to select privacy control policies and permissions, it would be more convenient if the system could predict user intentions in data control during runtime. Besides, the rigidity of existing permission control frameworks on mobile devices suffers from poor matching of users' privacy preferences; thus, researchers have leveraged contextual information to dynamically learn user intentions over time. Accordingly, machine learning techniques have been used for prediction purposes [92, 93].

3.1.4. Comparison of different methods for privacy-preserving individual activity sensing

Signal-level privacy-preserving methods generally obfuscate, filter, or change the sensed signal to remove sensitive information. They aim to mitigate the private information from the signal source. Signal-level methods are widely used in anti-eavesdropping and anti-recording tasks. For example, researchers have designed ultrasonic devices to prevent speech from being secretly recorded. However, this can lead to extra information loss for the activity sensing task, which can degrade the sensing performance. Besides, extra hardware is required to generate noises or disturbances, increasing the cost and complexity of the sensing system.

Compared with signal-level methods, algorithm-level methods manage to balance the trade-off between the privacy and utility of the sensed signal using encryption algorithms or neural network models. Algorithm-level methods mainly encrypt sense information. Encryption algorithms are widely applied in sensitive data storage, such as demographic data and health records. However, the widely used homomorphic encryption method has an extremely high time complexity, which may not be applicable to real-time sensing applications and resource-constrained devices. Neural networks can be relatively lightweight in computation for small-scale models and datasets; however, they are also susceptible to adversarial attacks, during which an attacker can deliberately manipulate the input data to cause the model to make incorrect predictions.

Different from the former two methods that only preserve part of the sensing data, system-level methods cut off the collection of sensor data as user specifies over the operation system. This forbids the malicious collection of sensor data from the background. System-level methods are mostly adopted by software and operating systems for data control. For instance, when applications on smartphones and smartwatches need to collect user data, reminders of information usage and control pop up for users to select. However, designating sensor permission can be inconvenient to users in practice because it requires the user's involvement from time to time. Furthermore, the forbidden sensor data collection also disables the corresponding human sensing function.

3.2. Methods for Collaborative Activity Sensing

Collaborative activity sensing refers to scenarios involving multiple sensing devices working together to detect and recognize human activities in a shared environment. By combining sensor data from multiple devices, collaborative activity sensing can improve the accuracy and robustness of activity recognition systems. With the development of cloud and edge computing, human sensing systems can leverage rich computation resources from a powerful central server or offload computation tasks to nearby available edge devices. In the meantime, the activity recognition models obtained based on the sensor data from different parties can be generalized to enhance the sensing performance. We also divided the privacy-preserving methods for collaboration activity sensing depicted in Fig. 2 into the signal-, algorithm-, and system-level methods presented below.

3.2.1. Signal-level methods

The software-based signal and data obfuscation methods mentioned in Section 3.1.1 to blur the sensitive information for individual activity sensing can be borrowed here [94, 95, 96]. Consequently, the shared data will not involve relevant private information. The idea of changing the sensor modality can also be adopted in collaborative activity sensing. If the sensing application requires sharing sensitive sensor data, people can resort to less privacy-sensitive sensors. However, hardware-based signal jamming methods are usually not applied in collaborative sensing because they tend to completely damage the sensing utility, making it difficult for later collaborative use.

3.2.2. Algorithm-level methods

The first algorithm-level method still employs the idea of encryption over data that is to be shared, similar to that of individual activity sensing. Encryption algorithms are utilized, designed, and enhanced in various ways in privacy-preserving participatory sensing. Researchers have adopted symmetric key cryptography and homomorphic encryption to achieve a sum aggregation of data from different parties [97, 98]. The differential privacy strategy has also been combined with encryption algorithms to enhance the trust between multiple parties and the central server [99]. Secure multi-party computation, which allows multiple parties to compute a function on their private data without revealing their data to each other, has been used in social human sensing, as well [100]. Since encryption algorithms are computationally expensive, researchers have harnessed the inherent signal noise caused by hardware imperfections to achieve efficient distributed differential privacy [101].

The second algorithm-level method lies in the presence of federated learning. Federated learning allows multiple devices or parties to collaboratively train a neural network model without sharing their raw data. They only share the model parameters which are aggregated in a central server to generate the global model. Before federated learning, privacy-preserving collaborative learning was proposed to achieve accurate activity recognition after data perturbation from end devices [102]. However, it only works for traditional machine learning models, e.g., the support vector machine and logistic regression. Federated learning promotes the prevalence of neural networks in collaborative sensing. Adopting federated learning for human activity sensing, however, encounters many challenges owing to various sensor modalities and different environments [103]. The first challenge stems from the balance between sensing performance and privacy. Sharing model parameters can also result in privacy leakage. Thus, researchers have proposed a group optimization technique in the federated learning framework to achieve a better balance between performance and privacy [104]. The second challenge arises from the data issues of multiple parties, e.g., data heterogeneity and scarcity. To deal with these issues, cluster and representation modules have been introduced in the federated learning framework [105]. The clustering-based federated learning strategy has also been employed to achieve semi-supervised learning that speeds up the convergence process [106, 107].

3.2.3. System-level methods

The first system-level method is to provide options for users to determine data access permissions for other parties. Many studies have been conducted using this methodology route. Users can customize the data collection rules using the operating system [108]. A trust network, a library of rules for defining access control over data, and the compressive sensing technique have been combined into a framework for privacy-aware data sharing [109]. Other frameworks jointly consider various data issues, e.g., data heterogeneity, privacy, security, and reliability in collaborative and crowd sensing scenarios [110, 111, 112].

The second system-level method benefits from advances in blockchain techniques. By leveraging the security and immutability of blockchain, it is possible to create a decentralized network of sensors that can collect data on human activities without compromising personal privacy. Meanwhile, smart contracts can be used to govern the data collection and usage, ensuring that data is collected only for authorized purposes and that the individual privacy is protected. For example, a decentralized privacy-preserving trajectory data mining framework based on blockchain has been developed, in which a privacy-preserving proposal is implemented as a proof-of-concept for consensus [113]. Traditional central servers can also be replaced by edge devices and blockchain for data audit [114]. Considering the importance of human health-related data, blockchain is widely applied to healthcare data exchange [115].

3.2.4. Comparison of different for privacy-preserving collaborative activity sensing

For collaborative human activity sensing, signal-level data obfuscation approaches are useful for blocking the major information from leakage. However, the data utility issue is more prominent in collaborative human activity sensing. Thereby, perturbing the data without considering the data utility over shared parties will significantly degrade the sensing performance. Algorithm-level data encryption solutions suffer less from undesirable data loss than signal-level methods. While the issue of excessive computation required by encryption still exists. Another type of algorithm-level method, i.e., federated learning, has emerged as a promising solution. One of its key advantages is that it allows for privacy-preserving machine learning without sacrificing data utility. Local models are trained using raw data. The global

Table 2: Capability of different privacy-preserving methods

	privacy protect	**data utility**	**computation**	**convenience**
Signal-level	high	low	low	medium
Algorithm-level	medium	high	high	high
System-level	medium	medium	medium	low

model can learn from the collective knowledge of all parties without ever accessing their raw data. This ensures that sensitive data is kept private while enabling the development of accurate neural network models. At the bottom of federated learning, the collaborative human activity sensing system can be strengthened in terms of security and privacy if the system-level method, i.e., blockchain-enabled solutions, is combined. However, introducing blockchain into the sensing system requires a careful incentive design to tempt more users to join in.

We summarize the capabilities of different privacy-preserving methods in terms of the level of privacy protection, data utility, required computation, and convenience in Table 2.

4. Future Directions in Privacy-preserving Human Sensing

This section discusses promising topics that require further improvement or potential attention.

4.1. Privacy-Preserving Wireless Human Sensing

Wireless human sensing is famous for its non-intrusiveness, in other words, people do not need to wear any on-body sensors. This preferable feature is enabled by the propagation properties (i.e., signal reflection, scattering, refraction, etc.) of the wireless signal over the air. However, the side effect of employing wireless signals for human sensing is that wireless signals, especially RF signals, can be easily overheard and sniffed, even through walls. Various types of RF signals, e.g., WiFi, LoRa, and FMCW radar, have been shown the capability to successfully sense human presence and activities through walls [116, 117, 118]. Researchers have proposed preliminary countermeasures to impede malicious human sensing [68, 119]. However, these solutions are dedicatedly designed for a certain type of RF signal. RF-Protect is specifically proposed for the FMCW radar sensing system at a frequency band of approximately 10 GHz [68]. RF-Veil is specifically devised to resist the impersonation attack on the WiFi radiometric fingerprint [68]. Considering the variety of RF signals, a generalized framework to combat attacks on wireless human sensing systems is desirable. This framework should provide plug-in modules such that signal- and algorithm-level methods fitting different RF signals can be alternated.

4.2. Pay Attention to Attacks on Human Sensing-related AI models

Attacks on human sensing-related AI models are becoming increasingly common [120, 121]. One of the primary concerns with these attacks on sensing-related AI models is the potential for adversaries to manipulate sensor data to cause the model to produce incorrect or misleading results. For example, an attacker can present a face recognition system with an image modified in such a way as to cause the system to misidentify a legitimate user or attacker. Researchers have recognized these issues. In SecureSense, an adversarial defense method, that leverages the prediction consistency between normal and adversarial examples as a regularization. It was designed for better model robustness [122]. Another promising approach for improving the security of sensing-related AI models is the use of explainable AI (XAI) techniques. XAI techniques enable users to understand how AI models arrive at decisions, which can help identify potential vulnerabilities or attacks. XAI techniques can also help improve the transparency and accountability of AI models, which is increasingly important in applications that use AI models to make critical decisions.

4.3. Formulation of Personal/Family Edge for Sensing

One of the key motivations of collaborative human sensing approaches is the requirement of high-computation resources and better sensing performance from large-scale AI models. With the increasing number of computing end devices around people, we are now able to convert to another approach that can fully utilize the computation resources of personal end devices in our daily lives, e.g., smartphones, smartwatches, smart pads, laptops, and voice assistants. These devices can jointly form a personal edge network to offload human sensing computation tasks. The network can be further expanded into a family edge which integrates the end devices for all family members. As such, more computation resources are available to use and share, meanwhile preserving personal/home privacy. The personal/family edge sounds like a good alternative to existing human activity sensing frameworks; however, it faces a performance bottleneck because the upper limit of personal end devices is still low compared with the powerful cloud server. We may adopt the model segmentation technique to divide the sensing task into several parts and then separately offload each part to different devices.

5. Conclusion

This work presents a systematic survey of research on privacy-preserving human activity sensing. We comprehensively introduce and review existing studies on human activity sensing from different perspectives, including sensors, sensed signals, and involved privacy information. We also propose a new taxonomy to categorize the previous solutions for privacy-preserving human sensing, i.e., signal-level, algorithm-level, and system-level methods. Then, we present representative methods and compare their pros and cons. Furthermore, we discuss several promising directions in this field for the research community to investigate. Our survey can serve as a valuable reference for researchers and practitioners interested in privacy-preserving human activity sensing.

6. Acknowledgement

This work was supported by the National Key Research and Development Program of China (No. 2021YFB3100400), National Natural Science Foundation of China (Grant No. 62302274, 62202276, 62232010), Shandong Science Fund for Excellent Young Scholars (No. 2022HWYQ-038), Natural Science Foundation of Shandong (No. ZR2023QF113), and financial support of Lingnan University (LU) (DB23A4) and Lam Woo Research Fund at LU (871236).

References

[1] A. Acquisti, L. Brandimarte, G. Loewenstein, Privacy and human behavior in the age of information, Science 347 (6221) (2015) 509–514.

[2] A. Boulemtafes, A. Derhab, Y. Challal, A review of privacy-preserving techniques for deep learning, Neurocomputing 384 (2020) 21–45.

[3] C. Briggs, Z. Fan, P. Andras, A review of privacy preserving federated learning for private iot analytics, arXiv preprint arXiv:2004.11794 (2020).

[4] I. Y. Jung, A review of privacy-preserving human and human activity recognition (2020).

[5] M. Xu, A. Sharghi, X. Chen, D. J. Crandall, Fully-coupled two-stream spatiotemporal networks for extremely low resolution action recognition, in: IEEE Winter Conference on Applications of Computer Vision, 2018, pp. 1607–1615.

[6] J. Chen, J. Wu, J. Konrad, P. Ishwar, Semi-coupled two-stream fusion convnets for action recognition at extremely low resolutions, in: IEEE Winter Conference on Applications of Computer Vision, 2017, pp. 139–147.

[7] M. S. Ryoo, B. Rothrock, C. Fleming, H. J. Yang, Privacy-preserving human activity recognition from extreme low resolution, arXiv preprint arXiv:1604.03196 (2016).

[8] E. Cippitelli, S. Gasparrini, E. Gambi, S. Spinsante, A human activity recognition system using skeleton data from rgbd sensors, Computational intelligence and neuroscience (2016).

[9] E. Chou, M. Tan, C. Zou, M. Guo, A. Haque, A. Milstein, L. Fei-Fei, Privacy-preserving action recognition for smart hospitals using low-resolution depth images, arXiv preprint arXiv:1811.09950 (2018).

[10] V. Srivastav, A. Gangi, N. Padoy, Human pose estimation on privacy-preserving low-resolution depth images, in: International Conference on Medical Image Computing and Computer-Assisted Intervention, Springer, 2019, pp. 583–591.

[11] T. Kawashima, Y. Kawanishi, I. Ide, H. Murase, D. Deguchi, T. Aizawa, M. Kawade, Action recognition from extremely low-resolution thermal image sequence, in: 14th IEEE International Conference on Advanced Video and Signal Based Surveillance, 2017, pp. 1–6.

[12] H. Zhang, C. Song, A. Wang, C. Xu, D. Li, W. Xu, Pdvocal: Towards privacy-preserving parkinson's disease detection using non-speech body sounds, in: The 25th Annual International Conference on Mobile Computing and Networking, 2019, pp. 1–16.

[13] X. Sun, Z. Lu, W. Hu, G. Cao, Symdetector: detecting sound-related respiratory symptoms using smartphones, in: Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing, 2015, pp. 97–108.

[14] K. Yatani, K. N. Truong, Bodyscope: a wearable acoustic sensor for activity recognition, in: Proceedings of the ACM Conference on Ubiquitous Computing, 2012, pp. 341–350.

[15] Y. Wang, J. Shen, Y. Zheng, Push the limit of acoustic gesture recognition, IEEE Transactions on Mobile Computing 21 (5) (2020) 1798–1811.

[16] D. Li, J. Liu, S. I. Lee, J. Xiong, Lasense: Pushing the limits of fine-grained activity sensing using acoustic signals, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 6 (1) (2022) 1–27.

[17] Y. Jin, Y. Gao, Y. Zhu, W. Wang, J. Li, S. Choi, Z. Li, J. Chauhan, A. K. Dey, Z. Jin, Sonicasl: An acoustic-based sign language gesture recognizer using earphones, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 5 (2) (2021) 1–30.

[18] J. Liu, D. Li, L. Wang, J. Xiong, Blinklistener: " listen" to your eye blink using your smartphone, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 5 (2) (2021) 1–27.

[19] D. Li, J. Liu, S. I. Lee, J. Xiong, Lasense: Pushing the limits of fine-grained activity sensing using acoustic signals, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 6 (1) (2022) 1–27.

[20] Z. Li, J. Cao, X. Liu, J. Zhang, H. Hu, D. Yao, A self-adaptive bluetooth indoor localization system using lstm-based distance estimator, in: 29th IEEE International Conference on Computer Communications and Networks, 2020, pp. 1–9.

[21] B. Mrazovac, M. Z. Bjelica, D. Kukolj, B. M. Todorovic, D. Samardzija, A human detection method for residential smart energy systems based on zigbee rssi changes, IEEE Transactions on Consumer Electronics 58 (3) (2012) 819–824.

[22] Y. Li, T. Zhu, Gait-based wi-fi signatures for privacy-preserving, in: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, 2016, pp. 571–582.

[23] Y. Yang, J. Cao, X. Liu, X. Liu, Wi-count: Passing people counting with cots wifi devices, in: 27th IEEE International Conference on Computer Communication and Networks, 2018, pp. 1–9.

[24] K. Zhang, X. Liu, X. Xie, J. Zhang, B. Niu, K. Li, A cross-domain federated learning framework for wireless human sensing, IEEE Network 36 (5) (2022) 122–128.

[25] Y. Yang, J. Cao, Y. Wang, Robust rfid-based respiration monitoring in dynamic environments, IEEE Transactions on Mobile Computing (2021).

[26] Y. Yang, J. Cao, X. Liu, Er-rhythm: Coupling exercise and respiration rhythm using lightweight cots rfid, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 3 (4) (2019) 1–24.

[27] Y. Yang, J. Cao, X. Liu, X. Liu, Multi-breath: Separate respiration monitoring for multiple persons with uwb radar, in: IEEE 43rd Annual Computer Software and Applications Conference, Vol. 1, 2019, pp. 840–849.

[28] L. Fan, L. Xie, X. Lu, Y. Li, C. Wang, S. Lu, mmmic: Multi-modal speech recognition based on mmwave radar, in: The 42nd International IEEE Conference on Computer Communications, 2023.

[29] M. J. Mathie, B. G. Celler, N. H. Lovell, A. C. Coster, Classification of basic daily movements using a triaxial accelerometer, Medical and Biological Engineering and Computing 42 (2004) 679–687.

[30] M. Zhang, A. A. Sawchuk, A preliminary study of sensing appliance usage for human activity recognition using mobile magnetometer, in: Proceedings of the ACM Conference on Ubiquitous Computing, 2012, pp. 745–748.

[31] J. Liu, L. Zhong, J. Wickramasuriya, V. Vasudevan, uwave: Accelerometer-based personalized gesture recognition and its applications, Pervasive and Mobile Computing 5 (6) (2009) 657–675.

[32] C. Crema, A. Depari, A. Flammini, E. Sisinni, T. Haslwanter, S. Salzmann, Imu-based solution for automatic detection and classification of exercises in the fitness scenario, in: IEEE Sensors Applications Symposium, 2017, pp. 1–6.

[33] I. V. Gabriel, P. Anghelescu, Vibration monitoring system for human activity detection, in: 7th IEEE International Conference on Electronics, Computers and Artificial Intelligence, 2015, pp. AE–41.

[34] R. Madarshahian, J. M. Caicedo, D. A. Zambrana, Benchmark problem for human activity identification using floor vibrations, Expert Systems with Applications 62 (2016) 263–272.

[35] G. Xu, Q. Wan, W. Deng, T. Guo, J. Cheng, Smart-sleeve: A wearable textile pressure sensor array for human activity recognition, Sensors 22 (5) (2022) 1702.

[36] K. Li, W. Yang, M. Yi, Z. Shen, Graphene-based pressure sensor and strain sensor for detecting human activities, Smart Materials and Structures 30 (8) (2021) 085027.

[37] J. Guo, B. Zhou, R. Zong, L. Pan, X. Li, X. Yu, C. Yang, L. Kong, Q. Dai, Stretchable and highly sensitive optical strain sensors for human-activity monitoring and healthcare, ACS applied materials & interfaces 11 (37) (2019) 33589–33598.

[38] T. Q. Trung, N.-E. Lee, Flexible and stretchable physical sensor integrated platforms for wearable human-activity monitoringand personal healthcare, Advanced materials 28 (22) (2016) 4338–4372.

[39] E. D. Übeyli, D. Cvetkovic, I. Cosic, Analysis of human ppg, ecg and eeg signals by eigenvector methods, Digital Signal Processing 20 (3) (2010) 956–963.

[40] K. Vandecasteele, T. De Cooman, Y. Gu, E. Cleeren, K. Claes, W. Van Paesschen, S. Van Huffel, B. Hunyadi, Automated epileptic

seizure detection based on wearable ecg and ppg in a hospital environment, Sensors 17 (10) (2017) 2338.

[41] T. Hwang, M. Kim, S. Hong, K. S. Park, Driver drowsiness detection using the in-ear eeg, in: 2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), IEEE, 2016, pp. 4646–4649.

[42] W. Chen, M. Guan, Y. Huang, L. Wang, R. Ruby, W. Hu, K. Wu, Vitype: A cost efficient on-body typing system through vibration, in: 15th Annual IEEE International Conference on Sensing, Communication, and Networking, 2018, pp. 1–9.

[43] X. Xu, J. Yu, Y. Chen, Q. Hua, Y. Zhu, Y.-C. Chen, M. Li, Touchpass: towards behavior-irrelevant on-touch user authentication on smartphones leveraging vibrations, in: Proceedings of the 26th Annual International Conference on Mobile Computing and Networking, 2020, pp. 1–13.

[44] G.-M. Jeong, P. H. Truong, S.-I. Choi, Classification of three types of walking activities regarding stairs using plantar pressure sensors, IEEE Sensors Journal 17 (9) (2017) 2638–2639.

[45] G. Liang, J. Cao, X. Liu, Smart cushion: A practical system for fine-grained sitting posture recognition, in: IEEE International Conference on Pervasive Computing and Communications Workshops, 2017, pp. 419–424.

[46] P. Hu, H. Zhuang, P. S. Santhalingam, R. Spolaor, P. Pathak, G. Zhang, X. Cheng, Accear: Accelerometer acoustic eavesdropping with unconstrained vocabulary, in: IEEE Symposium on Security and Privacy, 2022, pp. 1757–1773.

[47] Personal data (Oct 2020).
URL https://en.wikipedia.org/wiki/Personal$_{d}ata$

[48] Y. Iwasawa, K. Nakayama, I. Yairi, Y. Matsuo, Privacy issues regarding the application of dnns to activity-recognition using wearables and its countermeasures by use of adversarial training, in: IJCAI, 2017, pp. 1930–1936.

[49] J. M. Irvine, S. A. Israel, W. T. Scruggs, W. J. Worek, eigenpulse: Robust human identification from cardiovascular function, Pattern Recognition 41 (11) (2008) 3427–3435.

[50] Y. Chen, J. Yu, L. Kong, H. Kong, Y. Zhu, Y.-C. Chen, Rf-mic: Live voice eavesdropping via capturing subtle facial speech dynamics leveraging rfid, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 7 (2) (2023) 1–25.

[51] C. Wang, L. Xie, Y. Lin, W. Wang, Y. Chen, Y. Bu, K. Zhang, S. Lu, Thru-the-wall eavesdropping on loudspeakers via rfid by capturing submm level vibration, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 5 (4) (2021) 1–25.

[52] P. Hu, W. Li, R. Spolaor, X. Cheng, mmecho: A mmwave-based acoustic eavesdropping method, in: IEEE Symposium on Security and Privacy, 2022, pp. 836–852.

[53] J. Zhang, X. Liu, T. Gu, X. Tong, S. Chen, K. Li, Siloc: A speed inconsistency-immune approach to mobile rfid robot localization, in: IEEE INFOCOM 2021-IEEE Conference on Computer Communications, IEEE, 2021, pp. 1–10.

[54] F. Hong, Y. Zhang, Z. Zhang, M. Wei, Y. Feng, Z. Guo, Wap: Indoor localization and tracking using wifi-assisted particle filter, in: 39th Annual IEEE Conference on Local Computer Networks, 2014, pp. 210–217.

[55] Y. Zhao, Z. Zhang, T. Feng, W.-C. Wong, H. K. Garg, Graphips: Calibration-free and map-free indoor positioning using smartphone crowdsourced data, IEEE Internet of Things Journal 8 (1) (2020) 393–406.

[56] J. Shen, O. Lederman, J. Cao, F. Berg, S. Tang, A. Pentland, Gina: Group gender identification using privacy-sensitive audio data, in: IEEE International Conference on Data Mining, 2018, pp. 457–466.

[57] T. Van Hamme, G. Garofalo, E. Argones Rúa, D. Preuveneers, W. Joosen, A systematic comparison of age and gender prediction on imu sensor-based gait traces, Sensors 19 (13) (2019) 2945.

[58] S. Ding, X. Gao, Y. Dong, Y. Tong, X. Fu, Estimating multiple socioeconomic attributes via home location—a case study in china, Journal of Social Computing 2 (1) (2021) 71–88.

[59] R. Mishra, H. Gupta, Transforming large-size to lightweight deep neural networks for iot applications, ACM Computing Surveys 55 (11) (2023) 1–35.

[60] M. Xu, A. Sharghi, X. Chen, D. J. Crandall, Fully-coupled two-stream spatiotemporal networks for extremely low resolution action recognition, in: IEEE Winter Conference on Applications of Computer Vision, 2018, pp. 1607–1615.

[61] M. S. Ryoo, B. Rothrock, C. Fleming, H. J. Yang, Privacy-preserving human activity recognition from extreme low resolution, arXiv preprint arXiv:1604.03196 (2016).

[62] J. Dai, J. Wu, B. Saghafi, J. Konrad, P. Ishwar, Towards privacy-preserving activity recognition using extremely low temporal and spatial resolution cameras, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2015, pp. 68–76.

[63] M. Dimiccoli, J. Marín, E. Thomaz, Mitigating bystander privacy concerns in egocentric activity recognition with deep learning and intentional image degradation, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 1 (4) (2018) 1–18.

[64] Z. Ren, Y. Jae Lee, M. S. Ryoo, Learning to anonymize faces for privacy preserving action detection, in: Proceedings of the European Conference on Computer Vision, 2018, pp. 620–636.

[65] S. Kumar, L. T. Nguyen, M. Zeng, K. Liu, J. Zhang, Sound shredding: Privacy preserved audio sensing, in: Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications, 2015, pp. 135–140.

[66] D. Liaqat, E. Nemati, M. Rahman, J. Kuang, A method for preserving privacy during audio recordings by filtering speech, in: IEEE Life Sciences Conference, 2017, pp. 79–82.

[67] X. Ma, Y. Song, Z. Wang, S. Gao, B. Xiao, A. Hu, You can hear but you cannot record: Privacy protection by jamming audio recording, in: IEEE International Conference on Communications, 2021, pp. 1–6.

[68] J. Shenoy, Z. Liu, B. Tao, Z. Kabelac, D. Vasisht, Rf-protect: privacy against device-free human tracking, in: Proceedings of the ACM SIGCOMM Conference, 2022, pp. 588–600.

[69] H. Choi, S. Chakraborty, M. B. Srivastava, Design and evaluation of sensorsafe: A framework for achieving behavioral privacy in sharing personal sensory information, in: IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012, pp. 1004–1011.

[70] N. Saleheen, S. Chakraborty, N. Ali, M. M. Rahman, S. M. Hossain, R. Bari, E. Buder, M. Srivastava, S. Kumar, msieve: differential behavioral privacy in time series of mobile sensor data, in: Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing, 2016, pp. 706–717.

[71] C. Lin, P. Wang, H. Song, Y. Zhou, Q. Liu, G. Wu, A differential privacy protection scheme for sensitive big data in body sensor networks, Annals of Telecommunications 71 (2016) 465–475.

[72] W. Xu, W. Song, J. Liu, Y. Liu, X. Cui, Y. Zheng, J. Han, X. Wang, K. Ren, Mask does not matter: Anti-spoofing face authentication using mmwave without on-site registration, in: Proceedings of the 28th Annual International Conference on Mobile Computing and Networking, 2022, pp. 310–323.

[73] W. Xu, J. Liu, S. Zhang, Y. Zheng, F. Lin, J. Han, F. Xiao, K. Ren, Rface: anti-spoofing facial authentication using cots rfid, in: IEEE Conference on Computer Communications, 2021, pp. 1–10.

[74] K. A. Kumari, M. Indusha, D. Dharani, Enhanced human activity recognition based on activity tracker data using secure homomorphic encryption techniques, in: 2nd International Conference for Emerging Technology, 2021, pp. 1–7.

[75] H. Chabanne, A. De Wargny, J. Milgram, C. Morel, E. Prouff, Privacy-preserving classification on deep neural network, Cryptology ePrint Archive (2017).

[76] Z. Ren, Y. J. Lee, M. S. Ryoo, Learning to anonymize faces for privacy preserving action detection, in: Proceedings of the european conference on computer vision, 2018, pp. 620–636.

[77] A. Boutet, C. Frindel, S. Gambs, T. Jourdan, R. C. Ngueveu, Dysan: Dynamically sanitizing motion sensor data against sensitive inferences through adversarial networks, in: Proceedings of the ACM asia conference on computer and communications security, 2021, pp. 672–686.

[78] D. Zhang, L. Yao, K. Chen, Z. Yang, X. Gao, Y. Liu, Preventing sensitive information leakage from mobile sensor signals via integrative transformation, IEEE Transactions on Mobile Computing 21 (12) (2021) 4517–4528.

[79] S. I. Ahamed, V. Ravi, Privacy-preserving wavelet neural network with fully homomorphic encryption., CoRR (2022).

[80] B. Pulido-Gaytan, A. Tchernykh, J. M. Cortés-Mendoza, M. Babenko, G. Radchenko, A. Avetisyan, A. Y. Drozdov, Privacy-preserving neural networks with homomorphic encryption: Challenges and opportunities, Peer-to-Peer Networking and Applications 14 (3) (2021) 1666–1691.

[81] S. Chakraborty, C. Shen, K. R. Raghavan, Y. Shoukry, M. Millar, M. Srivastava, ipshield: a framework for enforcing context-aware privacy, in: 11th USENIX Symposium on Networked Systems Design and Implementation, 2014, pp. 143–156.

[82] H. Choi, S. Chakraborty, Z. M. Charbiwala, M. B. Srivastava, Sensorsafe: a framework for privacy-preserving management of personal sensory information, in: Workshop on Secure Data Management, 2011, pp. 85–100.

[83] W. Han, C. Cao, H. Chen, D. Li, Z. Fang, W. Xu, X. S. Wang, sendroid: Auditing sensor access in android system-wide, IEEE Transactions on Dependable and Secure Computing 17 (2) (2017) 407–421.

[84] R. P. Singh, B. Cassell, S. Keshav, T. Brecht, Tussleos: Managing privacy versus functionality trade-offs on iot devices, ACM SIGCOMM Computer Communication Review 46 (3) (2018) 1–8.

[85] P. Arjunan, N. Batra, H. Choi, A. Singh, P. Singh, M. B. Srivastava, Sensoract: a privacy and security aware federated middleware for building management, in: Proceedings of the Fourth ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings, 2012, pp. 80–87.

[86] X. Bai, J. Yin, Y.-P. Wang, Sensor guardian: prevent privacy inference on android sensors, EURASIP Journal on Information Security (2017) 1–17.

[87] Z. Alkindi, M. Sarrab, N. Alzidi, Cupa: a configurable user privacy approach for android mobile application, in: 7th IEEE International Conference on Cyber Security and Cloud Computing /2020 6th IEEE International Conference on Edge Computing and Scalable Cloud, 2020, pp. 216–221.

[88] I. Gasparis, Z. Qian, C. Song, S. V. Krishnamurthy, R. Gupta, P. Yu, Figment: Fine-grained permission management for mobile apps, in: IEEE Conference on Computer Communications, 2019, pp. 1405–1413.

[89] E. Yigitoglu, M. E. Gursoy, L. Liu, M. Loper, B. Bamba, K. Lee, Privacyzone: a novel approach to protecting location privacy of mobile users, in: IEEE International Conference on Big Data, 2018, pp. 1238–1247.

[90] N. Panwar, S. Sharma, G. Wang, S. Mehrotra, N. Venkatasubramanian, M. H. Diallo, A. A. Sani, Iot notary: Attestable sensor data capture in iot environments, ACM Transactions on Internet of Things 3 (1) (2021) 1–30.

[91] J. Huang, Y. Xiong, W. Huang, C. Xu, F. Miao, Sievedroid: Intercepting undesirable private-data transmissions in android applications, IEEE Systems Journal 14 (1) (2019) 375–386.

[92] H. Fu, Z. Zheng, S. Zhu, P. Mohapatra, Inspired: Intention-based privacy-preserving permission model, arXiv preprint arXiv:1709.06654 (2017).

[93] K. Olejnik, I. Dacosta, J. S. Machado, K. Huguenin, M. E. Khan, J.-P. Hubaux, Smarper: Context-aware and automatic runtime-permissions for mobile devices, in: IEEE Symposium on Security and Privacy, 2017, pp. 1058–1076.

[94] J. W. Bos, K. Lauter, M. Naehrig, Private predictive analysis on encrypted medical data, Journal of biomedical informatics 50 (2014) 234–243.

[95] P. Xie, M. Bilenko, T. Finley, R. Gilad-Bachrach, K. Lauter, M. Naehrig, Crypto-nets: Neural networks over encrypted data, arXiv preprint arXiv:1412.6181 (2014).

[96] L. Lyu, X. He, Y. W. Law, M. Palaniswami, Privacy-preserving collaborative deep learning with application to human activity recognition, in: Proceedings of the ACM on Conference on Information and Knowledge Management, 2017, pp. 1219–1228.

[97] Q. Li, G. Cao, Privacy-preserving participatory sensing, IEEE Communications Magazine 53 (8) (2015) 68–74.

[98] D. Christin, Privacy in mobile participatory sensing: Current trends and future challenges, Journal of Systems and Software 116 (2016) 57–68.

[99] K. Owusu-Agyemeng, Z. Qin, H. Xiong, Y. Liu, T. Zhuang, Z. Qin, Msdp: multi-scheme privacy-preserving deep learning via differential privacy, Personal and Ubiquitous Computing (2021) 1–13.

[100] Y. Tian, X. Li, A. K. Sangaiah, E. Ngai, Z. Song, L. Zhang, W. Wang, Privacy-preserving scheme in social participatory sensing based on secure multi-party cooperation, Computer Communications 119 (2018) 167–178.

[101] A. I. K. Kalupahana, A. N. Balaji, X. Xiao, L.-S. Peh, Serandip: Leveraging inherent sensor random noise for differential privacy preservation in wearable community sensing applications, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 7 (2) (2023) 1–38.

[102] B. Liu, Y. Jiang, F. Sha, R. Govindan, Cloud-enabled privacy-preserving collaborative learning for mobile sensing, in: Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems, 2012, pp. 57–70.

[103] Y. Zhao, H. Haddadi, S. Skillman, S. Enshaeifar, P. Barnaghi, Privacy-preserving activity and health monitoring on databox, in: Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking, 2020, pp. 49–54.

[104] J. Feng, C. Rong, F. Sun, D. Guo, Y. Li, Pmf: A privacy-preserving human mobility prediction framework via federated learning, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 4 (1) (2020) 1–21.

[105] X. Zhang, Q. Wang, Z. Ye, H. Ying, D. Yu, Federated representation learning with data heterogeneity for human mobility prediction, IEEE Transactions on Intelligent Transportation Systems (2023).

[106] X. Ouyang, Z. Xie, J. Zhou, G. Xing, J. Huang, Clusterfl: A clustering-based federated learning system for human activity recognition, ACM Transactions on Sensor Networks 19 (1) (2022) 1–32.

[107] X. Ouyang, Z. Xie, J. Zhou, J. Huang, G. Xing, Clusterfl: a similarity-aware federated learning system for human activity recognition, in: Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services, 2021, pp. 54–66.

[108] A. Clarke, R. Steele, Local processing to achieve anonymity in a participatory health e-research system, Procedia-Social and Behavioral Sciences 147 (2014) 284–292.

[109] S. Chakraborty, Z. Charbiwala, H. Choi, K. R. Raghavan, M. B. Srivastava, Balancing behavioral privacy and information utility in sensory data flows, Pervasive and Mobile Computing 8 (3) (2012) 331–345.

[110] M. Gheisari, H. E. Najafabadi, J. A. Alzubi, J. Gao, G. Wang, A. A. Abbasi, A. Castiglione, Obpp: An ontology-based framework for privacy-preserving in iot-based smart city, Future Generation Computer Systems 123 (2021) 1–13.

[111] L. Luceri, F. Cardoso, M. Papandrea, S. Giordano, J. Buwaya, S. Kundig, C. M. Angelopoulos, J. Rolim, Z. Zhao, J. L. Carrera, et al., Vivo: A secure, privacy-preserving, and real-time crowd-sensing framework for the internet of things, Pervasive and mobile computing 49 (2018) 126–138.

[112] C. Miao, W. Jiang, L. Su, Y. Li, S. Guo, Z. Qin, H. Xiao, J. Gao, K. Ren, Privacy-preserving truth discovery in crowd sensing systems, ACM Transactions on Sensor Networks 15 (1) (2019) 1–32.

[113] R. Talat, M. S. Obaidat, M. Muzammal, A. H. Sodhro, Z. Luo, S. Pirbhulal, A decentralised approach to privacy preserving trajectory mining, Future generation computer systems 102 (2020) 382–392.

[114] L. Wang, C. Zhao, K. Zhao, B. Zhang, S. Jing, Z. Chen, K. Sun, Privacy-preserving collaborative computation for human activity recognition, Security and Communication Networks 2022 (2022).

[115] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, J. He, Blochie: a blockchain-based platform for healthcare information exchange, in: IEEE international conference on smart computing, 2018, pp. 49–56.

[116] F. Zhang, Z. Chang, K. Niu, J. Xiong, B. Jin, Q. Lv, D. Zhang, Exploring lora for long-range through-wall sensing, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 4 (2) (2020) 1–27.

[117] M. Zhao, T. Li, M. Abu Alsheikh, Y. Tian, H. Zhao, A. Torralba, D. Katabi, Through-wall human pose estimation using radio signals, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2018, pp. 7356–7365.

[118] F. Adib, D. Katabi, See through walls with wifi!, in: Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM, 2013, pp. 75–86.

[119] R. Ayyalasomayajula, A. Arun, W. Sun, D. Bharadia, Users are closer than they appear: Protecting user location from wifi aps, in: Proceedings of the 24th International Workshop on Mobile Computing Systems and Applications, 2023, pp. 124–130.

[120] S. Kaviani, K. J. Han, I. Sohn, Adversarial attacks and defenses on ai in medical imaging informatics: A survey, Expert Systems with Applications (2022) 116815.

[121] Z. Yang, Y. Zhao, W. Yan, Adversarial vulnerability in doppler-based human activity recognition, in: IEEE International Joint Conference on Neural Networks, 2020, pp. 1–7.

[122] J. Yang, H. Zou, L. Xie, Securesense: Defending adversarial attack for secure device-free human activity recognition, IEEE Transactions on Mobile Computing (2022).

Declaration of interests

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

☐The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: