PrivGait

An Energy Harvesting-based Privacy-Preserving User Identification System by Gait Analysis

Xu, Weitao; Xue, Wanli; Lin, Qi; Lan, Guohao; Feng, Xingyu; Wei, Bo; Luo, Chengwen; Li, Wei; Zomaya, Albert Y.

DOI
10.1109/JIOT.2021.3089618

Publication date
2022

Document Version
Final published version

Published in
IEEE Internet of Things Journal

PrivGait: An Energy-Harvesting-Based Privacy-Preserving User-Identification System by Gait Analysis

Weitao Xu, Wanli Xue, Qi Lin, Guohao Lan, Xingyu Feng, Bo Wei, Chengwen Luo, Wei Li, *Senior Member, IEEE*, and Albert Y. Zomaya, *Fellow, IEEE*

***Abstract*—Smart space has emerged as a new paradigm that combines sensing, communication, and artificial intelligence technologies to offer various customized services. A fundamental requirement of these services is person identification. Although a variety of person-identification approaches has been proposed, they suffer from several limitations in practical applications, such as low energy efficiency, accuracy degradation, and privacy issue. This article proposes an energy-harvesting-based privacy-preserving gait recognition scheme for smart space, which is named PrivGait. In PrivGait, we extract discriminative features from 1-D gait signal and design an attention-based long short-term memory (LSTM) network to classify different people. Moreover, we leverage a novel Bloom filter-based privacy-preserving technique to address the privacy leakage problem. To demonstrate the feasibility of PrivGait, we design a proof-of-concept prototype using off-the-shelf energy-harvesting hardware. Extensive evaluation results show that the proposed scheme outperforms state of the art by 6%–10% and incurs low system cost while preserving user's privacy.**

***Index Terms*—Gait recognition, IoT security, privacy preserving, smart space.**

Manuscript received 16 September 2020; revised 24 May 2021; accepted 7 June 2021. Date of publication 15 June 2021; date of current version 7 November 2022. This work was supported in part by the Early Career Scheme (ECS) Grant from Hong Kong Research Grants Council under Project 21201420; in part by the CityU New Research Initiatives/Infrastructure Support from Central (APRC) Grant under Project 9610485 and the Start-Up Grant under Project 7200642 from the City University of Hong Kong; and in part by the Chow Sang Sang Group Research Fund sponsored by Chow Sang Sang Holdings International Ltd. under Project 9229062. *(Corresponding author: Weitao Xu.)*

This work involved human subjects or animals in its research. Approval of all ethical and experimental procedures and protocols was granted by the corresponding organization under Approval Number HC15304 and HC17008.

Weitao Xu is with the Department of Computer Science, City University of Hong Kong, Hong Kong (e-mail: weitaoxu@cityu.edu.hk).

Wanli Xue is with Cyber Security Cooperative Research Centre, Joondalup, WA 6027, Australia (e-mail: wanli.xue@cybersecuritycrc.org.au).

Qi Lin is with the School of Computer Science, University of New South Wales, Sydney, NSW 2052, Australia (e-mail: qi.lin@unsw.edu.au).

Guohao Lan is with the Department of Software Technology, Delft University of Technology, 2628 CD Delft, The Netherlands (e-mail: g.lan@tudelft.nl).

Xingyu Feng is with the College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, China.

Bo Wei is with the Department of Computer and Information Sciences, Northumbria University, Newcastle upon Tyne NE1 8ST, U.K. (e-mail: bo.wei@northumbria.ac.uk).

Chengwen Luo is with the College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, China (e-mail: chengwen@szu.edu.cn).

Wei Li and Albert Y. Zomaya are with the School of Computer Science, University of Sydney, Sydney, NSW 2006, Australia (e-mail: weiwilson.li@sydney.edu.au; albert.zomaya@sydney.edu.au).

Digital Object Identifier 10.1109/JIOT.2021.3089618

I. Introduction

A SMART space is a physical environment that is embedded with sensors, actuators, and smart devices [1]. Leveraging sensing and communication technology provides proactive and augmented services to users based on contextual information. Smart spaces can greatly improve productivity, energy efficiency, and make daily life more convenient. Some common examples of smart spaces include smart home, smart building, and smart airport. Person identification is a prerequisite function for smart space to provide customized applications because it is hard to associate the corresponding context to a given person without knowing his/her identity. For example, without knowing who is in the room, a smart building application is unable to offer user-specific applications, such as adjust room brightness or temperature [2].

Gait recognition has recently emerged as a promising solution to identify people by analyzing their walking patterns. Compared to other biometrics, such as face [3] and fingerprint [4], gait-based approaches can identify different people continuously and unobtrusively. Based on the hardware used, gait recognition systems can be classified into four categories: 1) camera based [5]; 2) radio based [2]; 3) floor sensor based [6], [7]; and 4) wearable sensor based [8], [9]. Although extensive works have been done in each subcategory, some approaches still have limitations in practical application. For example, camera-based approaches need line-of-sight (LOS) view and are subject to high privacy concern. Radio-based approaches are susceptible to environmental changes [2], [10]. In floor sensor-based approaches, a number of sensors such as geophone sensor [6], [7] need to be installed on the floor. Unfortunately, the unavailability of such sensors on most building floors limits their wide application in real-world environments.

Thanks to the prevalence of sensor-equipped wearable devices, such as smartphone and smart watch, wearable sensors-based approach has become the most promising technology, and the most widely used sensor is accelerometer [11]–[13]. However, the major challenge of accelerometer-based gait recognition is the continuous sampling accelerometer will quickly drain the battery of wearable devices. Energy constraint has long been identified as the

bottleneck of IoT systems, especially for on-body wearable devices, such as smart clothing and smart shoes, because of their limited onboard resources. A recent vision is to use a kinetic energy harvesting (KEH) device to replace the accelerometer to sense user's context [14]–[18]. KEH is a technology that converts kinetic motions, such as walking and running, into energy. A number of prior works have demonstrated that the harvested voltage signal of KEH when the user is walking reflects his/her walking patterns. For example, KEH-Gait [14], [15] is a state-of-the-art energy-harvesting-based gait recognition system for wearable devices. The authors demonstrated that the output voltage signal of energy harvesting can be directly used for gait recognition and they can achieve significant power saving by not sampling accelerometer. Ma *et al.* [17] also designed an energy-harvesting-based smart shoe called SEHS to recognize different people based on the harvested signal.

Although these systems have demonstrated the feasibility of using KEH signal for gait recognition, there are two limitations in practical application, namely, accuracy and privacy. In terms of accuracy, both KEH-Gait [14], [15] and SEHS [17] are based on sparse representation-based classification (SRC) whose performance will decrease when the number of users increases. Therefore, these systems cannot be used to accurately identify a large number of people in a smart space. Privacy is an important but often overlooked issue in many IoT classification systems. Due to the limited processing capability of wearable devices, the collected gait data are usually uploaded to a server or edge device for further processing. However, it poses severe privacy issues because an adversary (e.g., internal attacker) can perform "reverse engineer" on the data to obtain important personal information. The privacy issue will exacerbate for gait data because gait analysis has been widely used in clinical evaluation and a person's gait signal can reflect his/her health condition [19]. Unfortunately, in existing gait recognition systems, the raw gait data or extracted features are uploaded to a server directly, which poses high privacy concerns.

To overcome the above two problems, we design a gait recognition as a service model for smart space, which is named PrivGait. To improve accuracy, PrivGait leverages a novel feature extraction method to extract discriminative features from 1-D gait signal. To address privacy issue, PrivGait applies a novel differentially private Bloom filter [20] on the extracted features. The primary advantage of the adopted privacy preserving technology is that it can provide a better tradeoff between utility and privacy than other privacy preserving approaches. Finally, we design an attention-based long short-term memory (AT-LSTM) classification model to obtain the identity of the users based on the processed features, which do not reveal users' private information but are still distinguishable for different persons. As we will show in the evaluation, the proposed system achieves privacy preserving by sacrificing recognition accuracy slightly (about 0.3%–1%). The designed gait recognition scheme can be used as a fundamental service in a smart space to provide identity information. In summary, we make the following contributions in this article.

1) We design a gait recognition as a service model for smart space, which features energy-harvesting-based wearables, novel feature extraction approach, privacy-preserving technique, and deep learning technology. The proposed framework can be easily integrated into smart space to enable high-level user-specific applications.
2) We provide a proof-of-concept implementation using off-the-shelf energy-harvesting hardware. We collect 24 subjects' gait data in a typically indoor environment. The data set has been made public available to facilitate research on KEH-based gait analysis.[1]
3) Extensive evaluation is conducted to evaluate the performance of our scheme. Evaluation results show that PrivGait protects user's privacy by sacrificing accuracy slightly. But PrivGait still outperforms state-of-the-art energy-harvesting-based gait recognition systems by 6%–10%. The energy consumption profile demonstrates that PrivGait incurs low system cost on our prototype.

The remainder of this article is organized as follows. Section III provides an overview of the designed gait recognition as a service model. Section IV describes the design details of the system and Section V presents the evaluation results. Then, Section II discusses related work before concluding this article in Section VI.

II. Related Work

Gait Recognition: The research on gait recognition can be categorized into four classes: 1) camera based; 2) wireless radio based; 3) floor sensor based; and 4) wearable sensor based. Camera-based approaches can achieve high accuracy, but they violate user's privacy especially when they are used in offices and homes. Moreover, their results are highly affected by external factors, such as occlusions, distance, and lighting conditions. Gait recognition based on wireless signal has attracted extensive attention in the past few years, such as WiWho [2] and WifiU [21]. However, radio-based approaches are susceptible to environmental changes. In comparison, both floor sensor-based and wearable sensor-based approaches can reflect the dynamics of gait more directly and faithfully.

In floor sensor-based approaches, a number of sensors need to be installed on the floor. Such sensors can measure people's walking pattern when people walk on the floor [6], [7], [22]. For example, Pan *et al.* [6], [7] proposed to use the vibration signal induced by people's footstep to identify different people. The advantage of floor sensor-based approaches lies in its unobtrusive data collection. But the unavailability of sensors on current building floors limits their wide application in real-world environments. In wearable sensor-based approaches, Ailisto *et al.* [12] conducted the first study on accelerometer-based gait recognition. Recently, with the popularity of wearable devices, many wearable devices-based gait recognition systems have been designed. For example, Lu *et al.* [13] developed a gait authentication system for mobile phone users. Xu *et al.* [11] proposed a context-aware gait recognition system on smart watch. It solves the problem of gait recognition when the user is performing different activities, such as walking upstairs, walking with hand in pocket, etc.

Our work differs from all of the above prior works in two aspects. First, we consider the privacy problem of a

[1] https://github.com/xuweitao005/Gait-dataset

gait recognition system. Second, in order to improve recognition accuracy, we adopt novel feature extraction approaches and design the attention-based LSTM model. The results show that our system can improve recognition accuracy by 6%–10% compared to KEH-Gait [14] and SEHS [17], which are state-of-the-art KEH-based gait recognition systems.

Apart from gait recognition, many person-identification systems based on user's activities or behaviors are also proposed. For example, in SonicDoor [23], the authors installed three ultrasonic sensors on a door to identify different people. SenseTribute proposed by Han *et al.* [24] utilized on-object sensors to identify different people. SenseTribute is based on the observation that different people interact with objects (e.g., knock a door) in different manners.

KEH-Based Sensing: Recently, researchers have started to use energy harvesters as self-powered sensors to address the energy consumption issue of accelerometer-based systems. Instead of consuming power, energy-harvesting-enabled IoT devices can generate power from user's motions, though the available power is still limited by the current technology. Different energy-harvesting prototypes have been designed to sense a variety of contexts. To name a few, Lan *et al.* [16] proposed to use the energy-harvesting signal to detect different transportation modes, such as bus, train, and ferry. The intuition is that the energy-harvesting device will be subjected to different vibration patterns when the user takes different vehicles. Xu *et al.* [14], [15], and Ma *et al.* [17] both used KEH signal for gait recognition, and they used the same classifier in their systems SRC. Our evaluation results show that PrivGait outperforms these two systems. Moreover, our system incorporates privacy-preserving technique to protect user's privacy.

Privacy Preserving in IoT: Privacy is an important but often overlooked issue in many IoT classification systems. Due to the energy constraints of IoT systems, complicated cryptographic-based methods are no longer the top priority options, such as fully homomorphic encryption, and deterministic and order-preserving encryption. Instead, more lightweight encryption primitives and privacy preserving methods [25]–[27], such as differential privacy-based noise addition and privacy preserving sparse coding, are emerging and considered. However, noise addition methods cannot be generalized well, and additional privacy calibration is always required. In this article, we adopt another category of lightweight "cryptographic" method: Bloom filter encoding. The Bloom filter encoding has been used in many areas such as patient medical information matching [28]. It can convert the data from raw domain to the binary but remaining the data utility like relative string distance. Xue *et al.* [20] made the Bloom filter encoding more generalized, which can be applied on sequence data instead of string or category data only. We adopt the Bloom filter encoding as the privacy-preserving conversion module to encode the data feature to binary data to prevent the potential privacy leakage. Our results show that the accuracy only drops slightly after applying the privacy preserving technique.

III. System Overview

Overview: Fig. 1 shows the architecture of the designed gait recognition as a service model for smart space. The

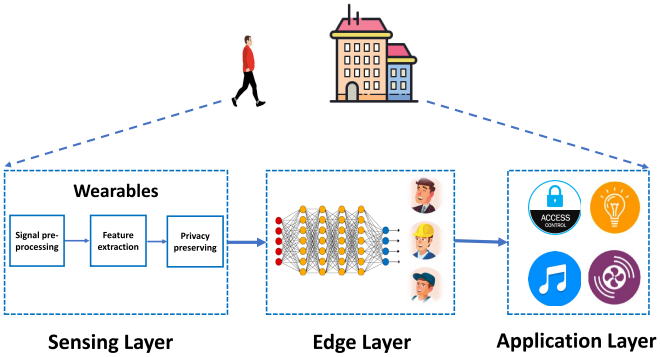


Fig. 1. Gait recognition as a service framework.

proposed model consists of three layers: 1) sensing layer; 2) edge layer; and 3) application layer. The sensing layer refers to various devices that can collect user's gait data for identification. We assume that these wearable devices are equipped with KEH technique to collect user's gait signal. This assumption is reasonable because there have been many KEH-equipped wearables in the IoT market, such as AMPY [29] and energy-harvesting-based smart shoe [30]. Although these wearable devices usually have limited processing capability, some simple signal preprocessing techniques can be performed in this layer to improve data quality and reduce transmission overhead. In this article, the filtering, feature extraction, and privacy-preserving technology will be run in this layer. As demonstrated in Section V-K, these operations incur low system cost on our prototype. The sensing layer will upload the processed data to edge layer, which will perform computationally expensive tasks. Different from cloud computing, edge computing can gather and process data in real time, allowing them to respond faster and more effectively. In this article, the deep learning model will run in edge layer to obtain user's identity. Because we apply privacy-preserving technique, the uploaded data will not reveal any private information of users. Finally, the identity information is transmitted to the application layer to enable customized applications such as access control.

Example Scenario: Suppose Jack is a manager of a company. In the morning, when he approaches the entrance of his company, the wearable devices on his body (e.g., smart shoe and smart watch) record his walking patterns for a few seconds and sends the data to an edge device. The edge device can be a local server or simply a router with programming capability. Next, the edge layer employs an AT-LSTM model to classify the uploaded gait data and knows the person is Jack. The gait recognition result is then sent to the application layer to enable a number of applications set by Jack or building manager. For example, he can walk through the access control system directly without swiping the access card because his identity has already been identified by his walking patterns. The lamp and fan in his office are adjusted to his preference automatically before he enters the office. After he enters the office, a smart speaker will play his favorite music. He enjoys these seamless services that are enabled by the designed gait recognition as a service framework.

Attack Model: The gait identification system is vulnerable to user spoofing attacks. For instance, an attacker may mimic the walking style of the target and try to spoof the system. Therefore, the adversary model considered in this article focuses on impersonation attacks. We assume the presence of two types of impersonation attacks.

1) *Passive Adversary:* The passive adversary tries to spoof the system by using his own walking pattern.
2) *Active Adversary:* The active spoofing attacker knows the identification scheme and will try his best to imitate the walking pattern of the genuine user to spoof the system.

The main goal of our system is to detect spoofing attacks. In fact, there are many other possible attacks to such identification system. We discuss these possible attacks and corresponding solutions.

1) *Replay Attack:* An adversary first records a measurement trace from another person, and then replays the data trace to fool the system. This attack can be easily detected by the method in [31].
2) *MITM Attack:* The attacker can eavesdrop the communication between the wearable device and cloud with the aim of modifying or inserting fake messages. This attack can be solved by using an encryption algorithm. In our system, we use a modern symmetric encryption algorithm advanced encryption standard (AES) [32] with 256-bit key.
3) *Video Analysis:* Further potential threats include deriving the walking patterns by studying a video of the target's gait through computer vision techniques. We believe this is a potential vulnerability of unknown severity and leave it as future work.

IV. System Design

Below, we will present the design details of PrivGait. Fig. 1 provides an overview of PrivGait, which consists of signal preprocessing, feature extraction, privacy preserving, and classification.

A. Signal Preprocessing

When the user is walking, a KEH-equipped wearable device will record his or her gait signals. KEH device, however, is not originally designed for accurate motion recording. The recorded signals, therefore, contain much noise that need to be filtered out. In this article, we use the Savitzky–Golay (SG) filter to remove noise and smooth data. The adoption of the SG filter is based on the following two observations. First, the SG filter is a low-pass filter well adapted for data smoothing. It is able to follow the underlying slow-moving features of people's walking, while providing a controllable reduction in the bandwidth of high-frequency fluctuations and noise. Second, the SG filter is a linear algorithm that can be easily implemented in resource-constrained wearable devices. There is a tradeoff between noise suppression and signal distortion. As the frequency of most people's walking is less than 10 Hz [11], the cutoff frequency of the SG filter is set to 10 Hz. The cutoff frequency of the SG filter is determined by two parameters N and M [33]

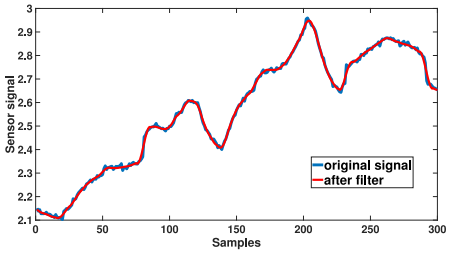


Fig. 2. Signal preprocessing.

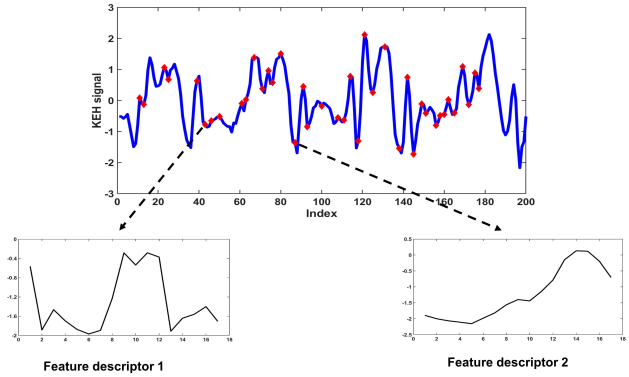


Fig. 3. Extract features from gait signal. (a) Red circles represent the locations of key points. (b) Bottom figures are two examples of extracted descriptors.

$$f_c \approx \frac{N+1}{3.2M-4.6}. \tag{1}$$

One may notice that different combinations of N and M can obtain the same cutoff frequency. Based on the study by Schafer [33], the above formula becomes more accurate with larger M and N. Therefore, we use $N = 1553$ and $M = 50$, which results in 10 Hz cutoff frequency. Fig. 2 compares the signal with and without SG filter. We can see that the gait signal becomes more smoothing after filtering.

B. Feature Extraction

Conventionally, gait-based recognition systems are based on template or statistical features, such as mean, median, and variance [34]. But we find that these features do not work well for a KEH-based gait recognition system because of two reasons. First, as mentioned above, the KEH technology is not originally designed for precise motion tracking purpose. Although filtering can remove noise, the recorded signal is still not as precise as the accelerometer-based gait recognition system as stated in KEH-Gait [14], [15]. Moreover, despite the fact that different people have distinct walking styles, the overall shapes or patterns of different people's gait signals are similar. So the template or statistical features cannot reflect the key difference of different people's walking patterns. Instead, in the proposed system, we adopt a novel feature extraction approach that can extract fine-grained and discriminative features for different subjects.

In the computer vision community, scale-invariant feature transform (SIFT) is a popular feature detection algorithm to

detect and describe local features in images [35]. SIFT, however, only works for 2-D image. To overcome this limitation, Xu *et al.* [11] transformed it to apply for 1-D signal. In this article, we adopt the feature extraction method proposed in [11]. Below, we briefly describe the process of this method.

We first divide the time-series gait signals into consecutive windows with nonoverlap. The window size is set to 1.3 s because most people's gait cycle varies from 0.8 to 1.3 s [11]. So a window of size 1.3 s can capture a complete gait cycle of most people. Suppose the 1-D gait signal in a window is $x(t)$. The first step of the feature extraction method is to identify locations and scales of features that can be repeatably detected from multiple gait cycles of the same person. To this end, we first define the scale space of a gait signal as a function $L(t, \delta)$, which can be obtained from the convolution of a variable-scale Gaussian $G(t, \delta)$ $L(t, \delta) = G_\delta(t, \delta) * x(t)$, where $*$ is the convolution operation and $G_\delta(t, \delta)$ is the zero-mean Gaussian function with variance δ^2

$$G_\delta(t, \delta) = \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2\delta^2}\right). \tag{2}$$

Next, we need to calculate $D(t, \delta)$, the difference of two nearby scales that is separated by a constant multiplication factor of ν for the detection of stable keypoint locations in scale space

$$\begin{aligned} D^\nu(t, \delta) &= (G(t, \nu\delta) - G(t, \delta)) * x(t) \\ &= L(t, \nu\delta) - L(t, \delta). \end{aligned} \tag{3}$$

Then, the DoG responses of the input 1-D gait signal $x(t)$ can be expressed as $E(t, \delta) = (a * D^\nu_\delta)(t)$. The next step is to find the locations of keypoints, which can be done by finding the extrema of $E(t, \delta)$. Instead of searching $E(t, \delta)$ continuously, the method proposed by Xu *et al.* finds extrema in a κ-layer pyramid based on the following discrete series:

$$E[t, i] = E\left(t, \nu^{i-1}\delta_0\right) \quad \text{for} \quad i = 1, 2, \ldots, \kappa \tag{4}$$

where t is the sampling timestamp, i is the layer index, and δ_0 is the base scale. To detect the local maxima and minima, each point in $E(t, i)$ is compared to its eight neighbors. If it is larger or smaller than all of their neighbors, the extremum in $E(t, i)$ is regarded as a feature keypoint. Finally, the descriptor function $\Psi(t, \delta)$ is obtained by calculating the gradient, which contains ρ points sampled uniformly around t

$$\begin{aligned} \Psi(t, \delta) &= \nabla\left(\frac{(v_1, v_2, \ldots, v_\rho)}{\|v_1, v_2, \ldots, v_\rho\|_2}\right) \\ \text{where} \quad v_i &= (a * G_\delta)\left(t + i - \frac{\rho + 1}{2}\right). \end{aligned} \tag{5}$$

The feature descriptors extracted from the above methods present two advantages. First, these features are more discriminative than traditional statistical features. Second, in gait recognition, one of the challenges is that the same person will walk in different speeds at different times. However, the feature descriptors used in our system are invariant to changes in amplitude induced by different walking speed. The changes in amplitude caused by different walking speed means the magnitude is multiplied by the same constant. It can be canceled by the normalization of the vector. Additionally, the gradient values will not be affected by speed change, as they are calculated from differences.

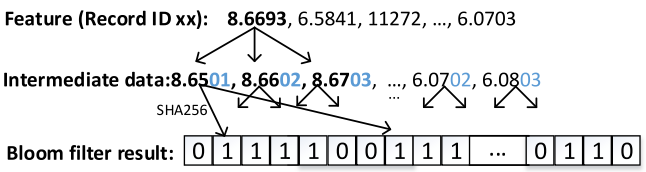


Fig. 4. Adding sequence information into Bloom filter.

In our system, the length of the feature vector is empirically set to 17 (i.e., $\rho = 17$). Fig. 3 illustrates two feature extractors from time-series gait signal of the same person. Although it is generally agreed that deep learning approaches can use the raw gait signal as input directly and hence, relax the burden of manual feature extraction, we find that our system can achieve higher accuracy by using more discriminative features (see Section V-H).

C. Privacy Preserving

As mentioned earlier, most gait recognition systems pose privacy issues. This is because the malicious attacker can obtain critical information from the raw gait signal or extracted features, for example, the health status of the walker [36]. Besides, the gait information itself can be used as the personally identifiable information, which emphasizes that gait data require significant protection. Thus, allowing not-fully-trusted party/server (e.g., honest-but-curious server) access the gait information without privacy protection will cause severe privacy concerns.

To address this problem, we adopt the Bloom filter-based privacy preserving approach proposed in [20]. The selected feature is hashed and fed into Bloom filter bins before uploaded o the server. After hashing, there will only be binary bits ("0" or "1" s) in the Bloom filter data structure instead of raw features. Because the hash (e.g., SHA-256) is a one-way function, the Bloom filter result cannot be reversed to reconstruct the users' gait data or select features. The challenge here is to remain the key useful information while Bloom filter encoding. This is done by following the adding-sequence information step in [20].

The feature records used to fed into the classifier (e.g., LSTM model) are first processed and transferred into Bloom filter data. The hash function apparently cannot hold all the original information since there is information loss while mapping from original feature space (floating point data) to Bloom filter space (binary data). In order to remain as much information as possible, we convert the floating point features to string data by adding two neighbors to each floating point (round to two decimals) as illustrated in Fig. 4. Then, each new element is appended a timestamp (2 bits) before hash mapping into the final Bloom filter result. In Fig. 4, we use two hash functions; thus, each element in the intermediate data type will be put into two places (turn the original "0" to "1").

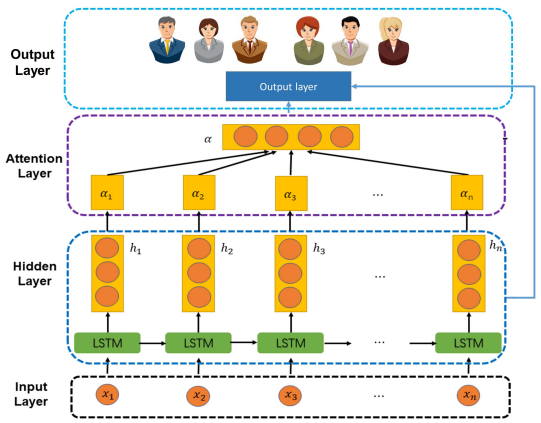


Fig. 5. Attention-based LSTM model.

The final Bloom filter results are fed into the classifier instead of original feature data.

However, the hash in Bloom filter also comes with false positive events (collisions), i.e., it happens that two different elements maybe hash mapped into one "bin" in the Bloom filter with a possibility [false positive rate (fp)]. The fp can be estimated via the equation from [37]

$$\text{fp} = \left(1 - (1 - \frac{1}{n})^{kp}\right)^k = \left(1 - e^{-kp/n}\right)^k \tag{6}$$

where k represents for the number of hash functions, n represents for the Bloom filter length, and p is cardinality of the key. Thus, we can control the fp to a very low rate such as 0.01 to avoid the collision with a high possibility. Our experiments illustrate the collision that rarely (never) occurs in our experimental setting.

Most importantly, this adapted Bloom filter data structure can also hold the set-based distance between the raw feature data and the projected Bloom filter data (the proof can be referred in [20]). Therefore, sufficient information is still remained for the classifier and the evaluation result in Section V-E shows that the accuracy only drops slightly after using this technique. This step is performed before uploading the data to an edge or cloud server, ensuring there is no privacy leakage problem. Moreover, the adapted Bloom filter, which only use hash functions and limit temporary storage (to store the Bloom filter results), will not involve much overhead to our system's efficiency as we will demonstrate in Section V-K.

D. Attention-Based LSTM Classification

After the data are uploaded to an edge or cloud server, an attention-based LSTM model will be performed on the data to obtain user's identity. LSTM is a popular neural network based on the recurrent neuron network (RNN) [38], [39]. We adopt the LSTM network because it is well adapted for the sorting, analysis, and forecasting of time-series data. The standard LSTM, however, cannot detect which part is necessary for the recognition of fine-grained gait features. To address this drawback, we design an attention system that can catch the main information of the input gait features. The attention scheme is used to simulate how human brain thinks, that is, give high attention to important information, and assign low attention to unimportant information.

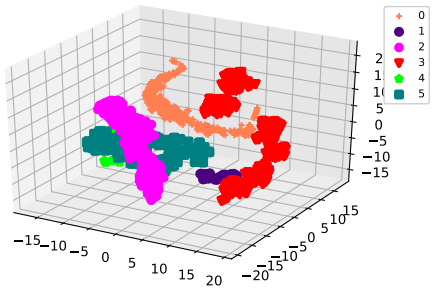


Fig. 6. t-SNE projection of six different subjects.

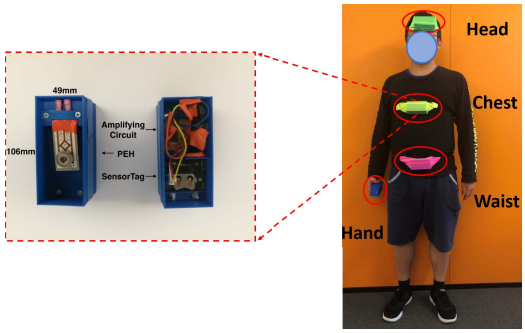
As shown in Fig. 5, the designed AT-LSTM model consists of four layers: 1) input layer; 2) hidden layer; 3) attention layer; and 4) output layer. As discussed in Section IV-B, we extract a number of discriminative features from a segment of gait signal. Therefore, these extracted features will be used as the input of the first layer. Then, after we feed these features into the LSTM network, we can get a series of hidden states $\{h_1, h_2, \ldots, h_n\}$. Next, the output of the hidden layer is used as an input of the attention layer. Different feature vectors have different weights because they are extracted from different locations of the gait signal and they carry different levels of information about user's walking pattern. So if we suppose the feature importance vector is u_t, we can obtain the normalized weights α_t for each feature vector by

$$u_t = \tanh(Wh_t + b) \tag{7}$$

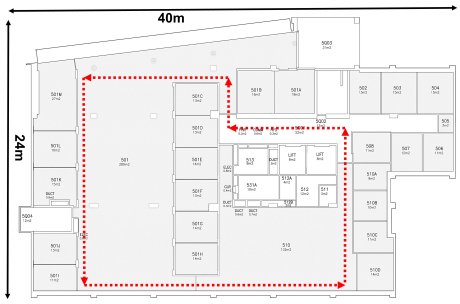
$$\alpha_t = \frac{\exp(u_t^T u)}{\sum_t \exp(u_t^T u)} \tag{8}$$

where W and b are two parameters determined in the training process. Next, the weighted sum for every hidden state h_t is then determined, with its corresponding weight α_t: $v = \sum_t a_t h_t$. Finally, to get the probabilities of each class, we enter v in the output layer with softmax activation. The testing signal identity is the class that has the highest probability. The loss function used in the designed network is cross-entropy.

The number of neurons in the input layer, hidden layer, and output layer is 17, 200, and 24, respectively. The designed network is trained on the features extracted from user's gait data in order to minimize the loss function by gradient descent. The loss is reached with repeated training and repair until the loss reaches convergence. The calculated error is optimized by the AdamOptimizer algorithm. In deep learning, the dropout strategy is widely used to enhance the generalization of a machine learning model and prevent overfitting. The dropping out rate of the proposed system is empirically set to 20%, which means we randomly select 20% of the neurons and drop them. To visualize the results, we plot t-distributed stochastic neighbor (t-SNE) project of six different subjects' gait data in Fig. 6. It is evident that the designed AT-LSTM model can differentiate different people' gait signals effectively.



(a)



(b)

Fig. 7. Prototype and data collection. (a) Prototype. (b) Indoor walking path.

V. Evaluation

A. Goals, Metrics, and Methodology

In this section, we conduct extensive evaluation to investigate the performance of PrivGait. The goals of evaluation are threefold: 1) to evaluate the performance of the proposed gait recognition system in different conditions; 2) to analyze the impact of privacy preserving technology on recognition accuracy; and 3) to compare our system with state-of-the-art KEH-based gait recognition system KEH-Gait [14].

1) KEH Prototype: To validate the performance of the proposed gait recognition service, we have built four proof-of-concept prototype devices. The KEH device used in the prototype is PPA 1001 piezoelectric cantilevers produced by MIDE technology. The PPA 1001 is connected to the analog-to-digital converters (ADCs) of a TI SensorTag board.[2] The MCU of SensorTag is Cortex-M4 microcontroller and it also has an onboard 3-axis accelerometer—MPU9250. During data collection, the accelerometer signal is also recorded for comparison purpose. The resonance frequency of PPA 1001 is tuned to be 20 Hz by adding weights to the piezoelectric cantilevers. The sampling rate is 128 Hz for both KEH and accelerometer. The data are stored in internal flash memory during data collection and imported to laptop via USB after data collection. The size of our prototype device is 49 $\times$ 52 $\times$ 104 mm^3, and the weight is about 90 g [see Fig. 7(a)].

2) Data Collection: The data collection is conducted in an indoor environment because our system aims to recognize people in a smart space, which is usually an indoor environment. In total, there were 24 volunteers participating in data collection, of which 14 of them are males and the rest ten volunteers are females.[3] More details of the gait data set are summarized in Table I. All participants wore four prototypes on their chest, waist, head, and hand as shown in Fig. 7(a). The floor plan and walking path are shown in Fig. 7(b). During data collection, they were asked to walk for two loops at their normal speed. The data set has been made public available.

3) Metrics: The proposed gait recognition system can also be used for authentication purpose based on the classification result. That is, we can choose one or multiple users as genuine users and treat the others as illegal users. If the identification result belongs to the genuine users, the authentication result is "accept," otherwise, it is "reject." Therefore, we use the following three evaluation metrics that are commonly used in prior gait recognition or authentication works [14], [15], [40], [41].

1) *Recognition Accuracy:* It means the number of correct classifications over the total number of classifications.
2) *False Acceptance Rate (FAR):* It refers to the possibility that our system incorrectly classifies an illegal user to be a genuine user (i.e., accept an attacker's authentication request).
3) *False Rejection Rate (FRR):* It represents the possibility that our system incorrectly recognizes a genuine user as an attacker (i.e., reject a genuine user's authentication request).

Baseline: We compare PrivGait with KEH-Gait [14], which is state-of-the-art KEH-based gait recognition systems. Note that KEH-Gait uses sparse representation-based classification (SRC). Therefore, we use SRC to represent the accuracy of KEH-Gait in the rest of evaluation. We randomly divide the whole data set into three parts: 1) training set; 2) validation set; and 3) test set. The training set is used to train the model and occupies 60% of the whole data set. The validation set is used to tune the hyperparameters and occupies 20% of the whole data set. The test set is used to test the performance of the model on new data and accounts for 20% of the whole data set. In the evaluation, we let W denote the length of the window size (e.g., 1 and 2 s). We plot the average and 95% confidence level of the results obtained from ten runs. Since the whole data set is collected from four different body locations, it can be divided into four subdata sets: 1) hand data set; 2) waist data set; 3) chest data set; and 4) head data set. Unless otherwise stated, the model is trained and tested on the whole data set without partitioning it into four parts. Therefore, the accuracy indicates the overall performance of four different locations. To investigate the impact of different locations, we also analyze the accuracy of each independent data set. In this case, the model is trained and tested on each subdata set. The results can be found in Section V-G.

B. Impact of Parameters

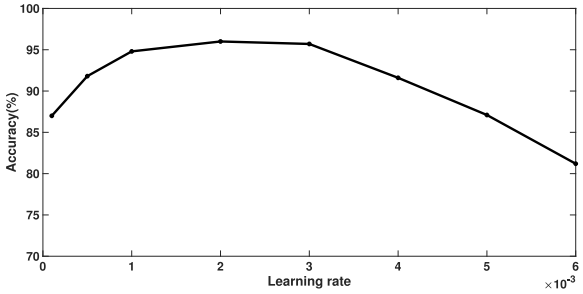
In the first experiment, we evaluate the impact of important parameters, including learning rate and number of iterations in training. The learning rate is a hyperparameter that controls

[2]SensorTag: https://au.mouser.com/new/texas-instruments/ti-sensor-tag-kits/.

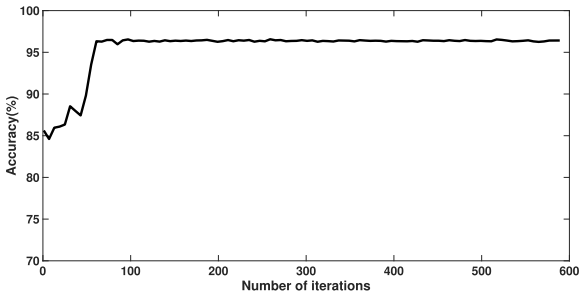
[3]Ethical approval for carrying out this experiment has been granted by the corresponding organization (Approval Number HC15304 and HC17008).

TABLE I
DATA SET INFORMATION

Property	Value
Subjects	24 (14 males, 10 females)
Age	18-44
Height	155-181 cm
Weight	47-96 kg
Duration of each record	≈ 5 minutes
Sample frequency	128 Hz



(a)



(b)

Fig. 8. Impact of parameters on accuracy. (a) Impact of learning rate. (b) Impact of iterations.

how much we are adjusting the weights of the neuron network with respect to the loss gradient. The number of iterations determines how fast our proposed system can achieve stable accuracy. Fig. 8(a) and (b) shows the impact of different learning rate and number of iterations evaluated on our data set. We can see that the best learning rate on the data set is 0.002. Meanwhile, from Fig. 8(b), we can see that the proposed classification system can achieve stable and high accuracy quickly within 80 iterations.

C. Impact of Preprocessing

As mentioned in Section IV-A, the energy-harvesting signal contains much noise because energy harvester is not designed for precise motion tracking purpose. To eliminate the impact of noise, we use a S-G filter to smooth the signal. In this experiment, we evaluate the effectiveness of the signal preprocessing step. We calculate the accuracy of our system with and without preprocessing and plot the results in Fig. 9. We can see that the signal preprocessing step help improve the recognition accuracy by 2.6%–6%.

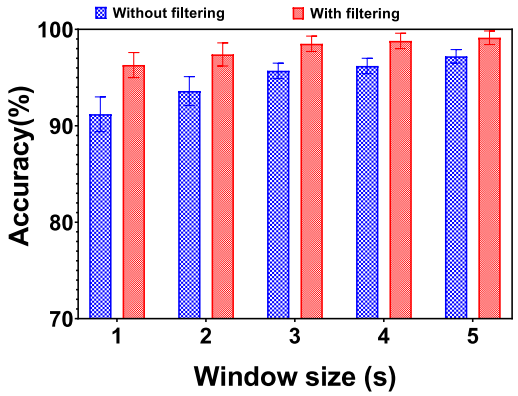


Fig. 9. Impact of preprocessing on accuracy.

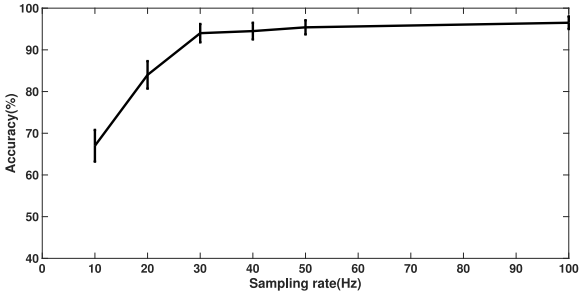


Fig. 10. Impact of sampling rate on accuracy.

D. Impact of Sampling Rate

After determining important hyperparameters, we now investigate the impact of sampling rate on recognition accuracy. The aim of this experiment is to study the relationship between recognition accuracy and the consumed power by sampling KEH, as the power consumption is directly related to the sampling rate. We downsample the data from original 128 to 10 Hz and calculate the recognition accuracy of different sampling rates. As shown in Fig. 10, the classification accuracy increases as the sampling rate grows. This is easy to understand because the more measurements are sampled, the more information is available, and thus, enabling more accurate classification. However, after the sampling rate is greater than 30 Hz, we find that the accuracy starts to level off. The results indicate that to achieve high recognition accuracy, a sampling rate of 30 Hz is sufficient. Therefore, we use 30-Hz sampling rate in the rest of the evaluation. Note that the window size used in this experiment is 1 s and later, we will show the accuracy can be further improved by using larger window size.

E. Impact of Privacy Preserving

The adoption of privacy preserving will decrease the recognition accuracy, but can provide a good tradeoff between privacy and utility. As mentioned in [20], different parameters be used to provide privacy protection for different applications, and they provide different levels of utility and privacy tradeoff. In this experiment, we tried different combinations of parameters and found the following combination that achieves the best performance: the length of Bloom filter $m = 500$,

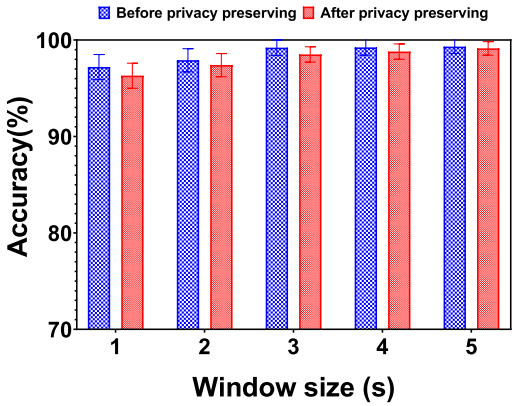


Fig. 11. Impact of privacy preserving on accuracy.

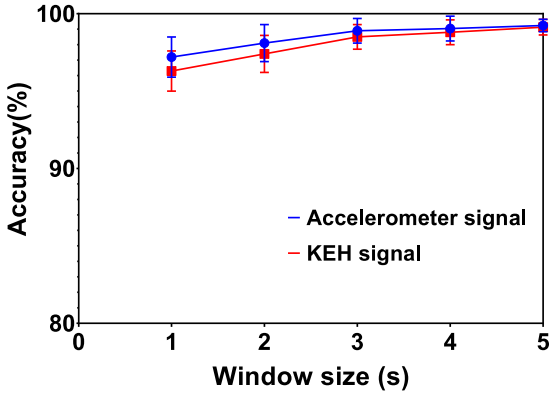


Fig. 12. KEH signal versus accelerometer signal.

neighbor size $b = 10$, neighbor distance $d = 0.03$, and the number of hash $N_{\text{hash}} = 2$. For the detailed explanation of these parameters, refer to [20]. Fig. 11 plots the accuracy of different window sizes before and after applying the privacy-preserving technology. We can see that by using fine-tuned parameters, the accuracy only drops slightly (about 0.3%–1%). The results suggest that we can preserve user's privacy by sacrificing accuracy slightly. Moreover, from Fig. 11, we notice that the accuracy degradation decreases when the window size increases from 1 to 5 s. In particular, we can see the accuracy of window size of 4 and 5 s is close to each other. This is because we use a specially designed Bloom filter in our system, which can reserve the set-based distance between the raw feature data and the projected Bloom filter data. Therefore, the impact of privacy preserving on recognition accuracy is minimized with more data collected (i.e., larger window size). In the following evaluations, the accuracy is obtained based on the data processed by privacy-preserving technique.

F. KEH Versus Accelerometer

In this experiment, we investigate whether the proposed system can achieve comparable accuracy in comparison with the accelerometer signal. We vary the window size from 1 to 5 s and the results are plotted in Fig. 12. We can see that the recognition accuracy of using voltage signal is slightly lower than that of using raw accelerometer signal. This is because the original purpose of KEH is not designed for precise motion tracking. But we find that the recognition accuracy is improved significantly when the window size increases. This is because more knowledge can be gathered to identify the subject with more measurements (e.g., longer window size). In practical applications, the window size W trades off security and user experience, and it can be tailored to satisfy various security requirements. For example, a larger W makes the system more accurate, but it requires users to walk for a longer time (i.e., sacrifice user experience).

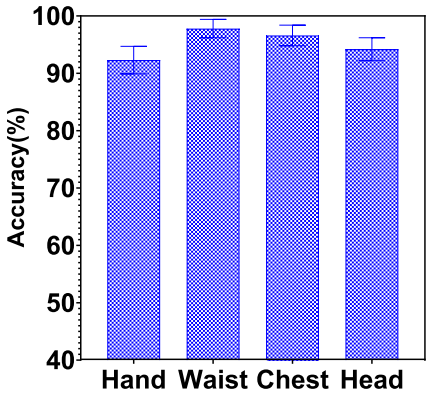


Fig. 13. Accuracy of different locations.

G. Accuracy of Different Locations

As mentioned in Section V-A2, we collected data from four different body locations: 1) hand; 2) waist; 3) chest; and 4) head. We now evaluate the accuracy of different locations. The purpose of this experiment is to understand which body part has the best performance. For each location, we only use the data collected from this location to train and test the model. To be specific, the whole data set is divided into four subsets based on the location they are collected from: 1) hand data set; 2) waist data set; 3) chest data set; and 4) head data set. Then, we use each subset to train and test the model, respectively. Finally, we can obtain the accuracy of these four body locations. From the result in Fig. 13, we can see that different locations produce different accuracy. The device on waist achieves the highest accuracy while the device hold in hand has the lowest accuracy. This is because the torso (trunk of the main body) is more responsible for the human gait than the arms, since the movement of the arms is primarily for maintaining balance and can be changed without having a major impact on people's regular walking [9]. Several previous studies also studied the impact of different locations. For example, Zhang *et al.* [9] found that pelvis can achieve better performance than wrist, leg, and arm, but their combination can significantly improve accuracy. Primo *et al.* [42] studied the impact of hand and pocket. Their results suggested that we can achieve higher accuracy by holding device in the hand than putting it in the pocket.

H. Comparison With State of the Art

We now evaluate whether the proposed system outperforms state-of-the-art KEH-based gait classification algorithms (i.e., SRC). We also evaluate the accuracy with and without feature

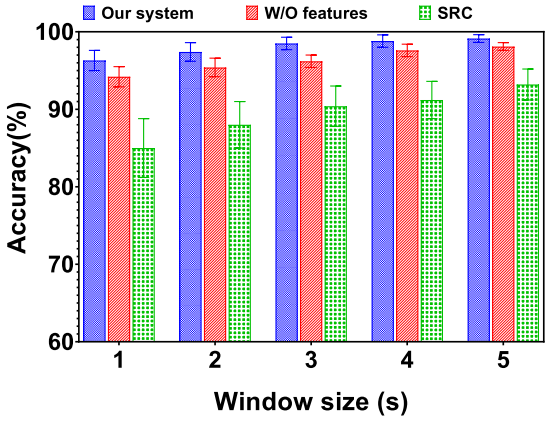


Fig. 14. Comparison with other classification methods.

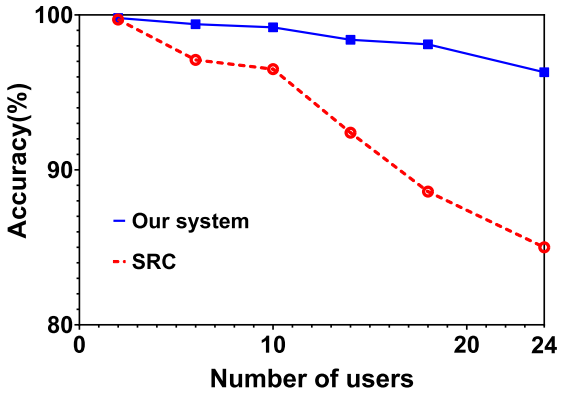


Fig. 15. Impact of number of users on accuracy.

extraction to demonstrate the advantage of extracting discriminative features. We perform the comparison on the collected data set and the results are shown in Fig. 14. We can see that our system consistently achieves the best performance. It is 2%–4% more accurate than AT-LSTM without extracting features, and 6%–10% more accurate than SRC. The improvement comes from two aspects. First, we apply a novel feature extraction method to extract discriminative features. Second, we design an attention scheme-based LSTM model to further improve the recognition accuracy. The attention mechanism tries to mimic the human's perception process, which focuses attention selectively on parts of the input signal to obtain more details while suppressing other useless information. Therefore, it can further improve accuracy based on the extracted features.

I. Impact of Number of Users

In order to understand the scalability of the system, we further investigate the performance of our system when the number of users changes. We evaluate the accuracy by increasing the number of users from 2 to 24 with a step of 4. The order of users is chosen randomly. As the results shown in Fig. 15, the classification accuracy of SRC decreases gradually, indicating that it does not scale well for large group of people. Although the accuracy of our scheme also drops slightly, we can see it maintains a relative stable accuracy around 96.7% in the end. The results suggest that our system is more robust and scalable in multiuser scenarios. Nevertheless, the accuracy still drops with increasing number of enrolled users. There are several methods to address this limitation. First, current off-the-shelf energy-harvesting hardware can provide 1-D signal only, but recent advances have made three axis energy harvesting possible [43]. Therefore, we can use a 3-D energy-harvesting hardware to achieve higher accuracy. Second, since most wearable devices are equipped with IMU, which can provide information about user's walking patterns, we can use the IMU sensor signal as a complement to improve the accuracy. Third, more complex and advanced deep learning technologies can be used to further improve accuracy, such as transfer learning.

J. Security Against Spoofing Attack

As a gait recognition system, one important security issue is that an attacker may spoof the system by mimicking others' walking pattern. The aim of this experiment is to evaluate the robustness of PrivGait against the spoofing attacker. To this end, we group the 24 subjects into 12 pairs: in each pair, one of them is a genuine user and the other is treated as an attacker. During evaluation, the attacker was instructed to imitate the walking style of his/her partner. The attacker physically analyzed the target's walking style, which can be achieved conveniently in a real-life environment because gait cannot be disguised. The gender of the genuine user and attacker was the same to maximize the attacking ability of attacker. The result, which is represented by FAR and FRR, is plotted in Fig. 16. For comparison purpose, we also plot the result of SRC.

An important point in the mistake trading decision (DET) is the equivalent error rate (EER) where FAR = FRR. For example, a 10% EER means 10 of 100 legitimate trials are wrongly denied and 10 of 100 impostor trials are wrongly admitted. The crossover (marked as a diamond) of the black dash line and FRR-FAR curve stands for the location of the EER. From Fig. 16, we notice that the EER of our system is 6%, which means out of 100 mimicking attack trials, only six are wrongfully accepted. In comparison, the EER of SRC is 13.5%, indicating that our system is more secure than SRC. In this experiment, the window size W is set to 1 s. The accuracy can be further improved by using larger window size. To mitigate the threats of false positives, our scheme can be combined with other authentication methods such as two-factor authentication to further improve the security of smart space.

K. Energy Consumption

In this section, we analyze the energy consumption of the proposed scheme. PrivGait includes two parts: 1) wearable device on user's body and 2) an edge device in the smart space. The wearable device is used to collect data, extract features, apply privacy-preserving technology, and upload data to edge server. Then, on the server's side, the classification is performed to obtain user's identity. The edge device can be viewed as a powerful computer; therefore, we only focus on evaluating the energy consumption of PrivGait on resource-limited wearable devices.

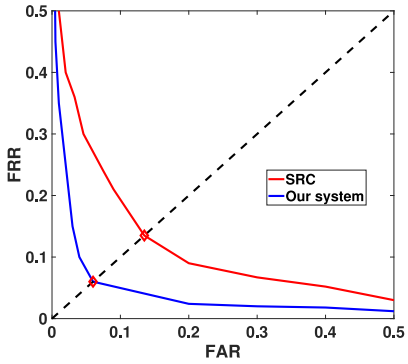


Fig. 16. Security against spoofing attack.

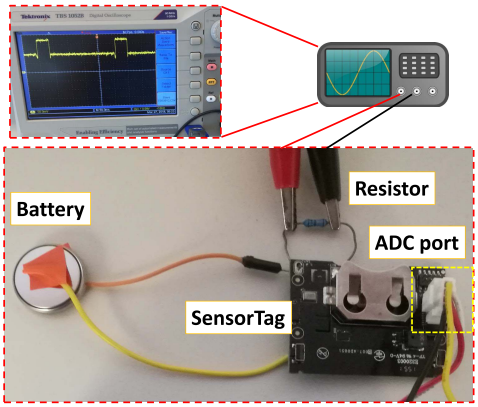


Fig. 17. Setup of energy profiling.

An illustration of the energy profiling setup is shown in Fig. 17. We connect the designed prototype to an oscilloscope through an external resistor. The SensorTag is installed with the up-to-date version of Contiki OS and the MCU is duty cycled to save energy. All the unnecessary components of the system are disabled, such as LED, SPI bus, and onboard sensors. The sampling frequency of the ADC is 30 Hz and the data are uploaded to a local laptop via BLE. Our measurements show that the sampling rate of 30 Hz leads to a power consumption of 12.6 μW. If we assume the window size is 1 s (i.e., we collect gait signal for 1 s), the energy consumption of the signal processing parts is shown in Table II. We can see the proposed scheme incurs low energy consumption. As demonstrated in Fig. 14, we can improve recognition accuracy by taking more samples. Suppose we ask the user to walk for 5 s, our system consumes approximately 282.25 mJ. The battery of a SensorTag board is 3 V 225 mAh, which is equivalent to 2430 J. With 1% budget, a typical battery can support our system continuously that run for about 87 times. If we further assume that the user enters the smart space (e.g., his company) once per day, then our system can run for 87 days.

Many studies [14]–[16] have demonstrated that sampling KEH is more energy efficient than sampling accelerometer; therefore, we do not compare the energy consumption of sampling KEH device with sampling 3-axis accelerometer in this article. Interested readers are encouraged to refer to prior work [14]–[16].

TABLE II
SYSTEM OVERHEAD

	Computation time	Energy consumption
Local processing	182 ms	56.4 mJ
Data transmission	14 ms	38 μJ
Total	196 ms	≈ 56.4 mJ

VI. CONCLUSION

This article presents PrivGait, a KEH-based privacy-preserving gait recognition scheme for smart space. PrivGait adopts a novel feature extraction approach, privacy-preserving technology, and deep learning technique to achieve high recognition accuracy while protecting user's privacy. We design a proof-of-concept prototype and collect data to evaluate the performance of PrivGait. The evaluation results show it can achieve 96.7% recognition accuracy, which is 6%–10% higher than state of the arts. Security analysis shows that the EER of our system against an active spoofing attacker is 6%. The proposed scheme features privacy preserving, high accuracy, energy efficiency, and nonobtrusiveness. Therefore, it has great potential in future smart space applications.

REFERENCES

[1] J. Zeng, L. T. Yang, H. Ning, and J. Ma, "A systematic methodology for augmenting quality of experience in smart space design," *IEEE Wireless Commun.*, vol. 22, no. 4, pp. 81–87, Aug. 2015.
[2] Y. Zeng, P. H. Pathak, and P. Mohapatra, "WIWHO: WiFi-based person identification in smart spaces," in *Proc. IEEE IPSN*, 2016, pp. 1–12.
[3] M. Turk and A. Pentland, "Face recognition using eigenfaces," in *Proc. CVPR*, 1991, pp. 586–587.
[4] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New York, NY, USA: Springer, 2009.
[5] J. Han and B. Bhanu, "Individual recognition using gait energy image," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 2, pp. 316–322, Feb. 2005.
[6] S. Pan, N. Wang, Y. Qian, I. Velibeyoglu, H. Y. Noh, and P. Zhang, "Indoor person identification through footstep induced structural vibration," in *Proc. 16th Int. Workshop Mobile Comput. Syst. Appl.*, 2015, pp. 81–86.
[7] S. Pan *et al.*, "FootPrintID: Indoor pedestrian identification through ambient structural vibration sensing," *ACM Interact. Mobile Wearable Ubiquitous Technol.*, vol. 1, no. 3, pp. 1–31, 2017.
[8] Y. Shen *et al.*, "GaitLock: Protect virtual and augmented reality headsets using gait," *IEEE Trans. Depend. Secure Comput.*, vol. 16, no. 3, pp. 484–497, May/Jun. 2019.
[9] Y. Zhang, G. Pan, K. Jia, M. Lu, Y. Wang, and Z. Wu, "Accelerometer-based gait recognition by sparse representation of signature points with clusters," *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 1864–1875, Sep. 2015.
[10] S. Tan and J. Yang, "WiFinger: Leveraging commodity WiFi for fine-grained finger gesture recognition," in *Proc. 17th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2016, pp. 201–210.
[11] W. Xu, Y. Shen, W. Cheng, J. Li, W. Li, and A. Y. Zomaya, "Gait-Watch: A gait-based context-aware authentication system for smart watch via sparse coding," *Ad Hoc Netw.*, vol. 107, Oct. 2020, Art. no. 102218.
[12] H. J. Ailisto, M. Lindholm, J. Mantyjarvi, E. Vildjiounaite, and S.-M. Makela, "Identifying people from gait pattern with accelerometers," in *Proc. Defense Security*, 2005, pp. 7–14.
[13] H. Lu, J. Huang, T. Saha, and L. Nachman, "Unobtrusive gait verification for mobile phones," in *Proc. ACM ISWC*, 2014, pp. 91–98.
[14] W. Xu *et al.*, "KEH-Gait: Towards a mobile healthcare user authentication system by kinetic energy harvesting," in *Proc. NDSS*, 2017. [Online]. Available: http://dx.doi.org/10.14722/ndss.2017.23023
[15] W. Xu *et al.*, "KEH-gait: Using kinetic energy harvesting for gait-based user authentication systems," *IEEE Trans. Mobile Comput.*, vol. 18, no. 1, pp. 139–152, Jan. 2019.

[16] G. Lan, W. Xu, D. Ma, S. Khalifa, M. Hassan, and W. Hu, "EnTrans: Leveraging kinetic energy harvesting signal for transportation mode detection," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 7, pp. 2816–2827, Jul. 2020.

[17] D. Ma, G. Lan, W. Xu, M. Hassan, and W. Hu, "SEHs: Simultaneous energy harvesting and sensing using piezoelectric energy harvester," in *Proc. IEEE IoTDI*, 2018, pp. 201–212.

[18] G. Lan, W. Xu, S. Khalifa, M. Hassan, and W. Hu, "Transportation mode detection using kinetic energy harvesting wearables," in *Proc. IEEE PerCom Workshops*, 2016, pp. 1–4.

[19] J. Marín, T. Blanco, J. J. Marín, A. Moreno, E. Martitegui, and J. C. Aragüés, "Integrating a gait analysis test in hospital rehabilitation: A service design approach," *PLoS ONE*, vol. 14, no. 10, 2019, Art. no. e0224409.

[20] W. Xue, D. Vatsalan, W. Hu, and A. Seneviratne, "Sequence data matching and beyond: New privacy-preserving primitives based on bloom filters," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2973–2987, Mar. 2020. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9037114

[21] W. Wang, A. X. Liu, and M. Shahzad, "Gait recognition using WiFi signals," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput.*, 2016, pp. 363–373.

[22] R. J. Orr and G. D. Abowd, "The smart floor: A mechanism for natural user identification and tracking," in *Proc. CHI*, 2000, pp. 275–276.

[23] N. Khalil, D. Benhaddou, O. Gnawali, and J. Subhlok, "SonicDoor: Scaling person identification with ultrasonic sensors by novel modeling of shape, behavior and walking patterns," in *Proc. BuildSys*, 2017, pp. 1–10.

[24] J. Han, S. Pan, M. K. Sinha, H. Y. Noh, P. Zhang, and P. Tague, "SenseTribute: Smart home occupant identification via fusion across on-object sensing devices," in *Proc. BuildSys*, 2017, pp. 1–10.

[25] W. Fan, J. He, M. Guo, P. Li, Z. Han, and R. Wang, "Privacy preserving classification on local differential privacy in data centers," *J. Parallel Distrib. Comput.*, vol. 135, pp. 70–82, Jan. 2020.

[26] W. Xue *et al.*, "Towards a compressive-sensing-based lightweight encryption scheme for the Internet of Things," *IEEE Trans. Mobile Comput.*, early access, May 6, 2020, doi: 10.1109/TMC.2020.2992737.

[27] P. Wang and H. Zhang, "Differential privacy for sparse classification learning," *Neurocomputing*, vol. 375, pp. 91–101, Jan. 2020.

[28] P. Christen, R. Schnell, D. Vatsalan, and T. Ranbaduge, "Efficient cryptanalysis of bloom filters for privacy-preserving record linkage," in *Proc. Pac.–Asia Conf. Knowl. Disc. Data Min.*, 2017, pp. 628–640.

[29] (2018). *AMPY*. [Online]. Available: https://www.kickstarter.com/projects/1071086547/ampy-power-your-devices-from-your-motion

[30] (2017). *Ch. Frequency Response (Channel Quality)*. [Online]. Available: http://rfmw.em.keysight.com/wireless/helpfiles/89600B/WebHelp/Subsystems/chanqual/content/trc_ch_frequency_response.htm

[31] L. Guan *et al.*, "From physical to cyber: Escalating protection for personalized auto insurance," in *Proc. Sensys*, 2016, pp. 42–55.

[32] J. Daemen and V. Rijmen, "The Rijndael block cipher: AES proposal," in *Proc. 1st Candidate Conf. (AeS1)*, 1999, pp. 343–348.

[33] R. W. Schafer, "On the frequency-domain properties of Savitzky–Golay filters," in *Proc. IEEE Digit. Signal Process. Signal Process. Educ. Meeting (DSP/SPE)*, 2011, pp. 54–59.

[34] S. Sprager and M. B. Juric, "Inertial sensor-based gait recognition: A review," *Sensors*, vol. 15, no. 9, pp. 22089–22127, 2015.

[35] D. G. Lowe, "Object recognition from local scale-invariant features," in *Proc. IEEE ICCV*, vol. 2, 1999, pp. 1150–1157.

[36] J. Juen, Q. Cheng, V. Prieto-Centurion, J. A. Krishnan, and B. Schatz, "Health monitors for chronic disease by gait analysis with mobile phones," *Telemedicine e-Health*, vol. 20, no. 11, pp. 1035–1041, 2014.

[37] M. Mitzenmacher and E. Upfal, *Probability and Computing: Randomization and Probabilistic Techniques in Algorithms and Data Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 2017.

[38] F. A. Gers, J. Schmidhuber, and F. Cummins, "Learning to forget: Continual prediction with LSTM," *Neural Comput.*, vol. 12, no. 10, pp. 2451–2471, 2000.

[39] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, 1997.

[40] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait recognition," in *Proc. IEEE 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, 2010, pp. 306–311.

[41] Y. Ren, Y. Chen, M. C. Chuah, and J. Yang, "Smartphone based user verification leveraging gait recognition for mobile healthcare systems," in *Proc. IEEE SECON*, 2013, pp. 149–157.

[42] A. Primo, V. V. Phoha, R. Kumar, and A. Serwadda, "Context-aware active authentication using smartphone accelerometer measurements," in *Proc. CVPR Workshops*, 2014, pp. 98–105.

[43] M. Han *et al.*, "Three-dimensional piezoelectric polymer microsystems for vibrational energy harvesting, robotic interfaces and biomedical implants," *Nat. Electron.*, vol. 2, no. 1, pp. 26–35, 2019.

Weitao Xu received the B.E. degree in communication engineering and the M.E. degree in communication and information system (advised by Prof. D. Yuan) from the School of Information Science and Engineering, Shandong University, Jinan, China, in 2010 and 2013, respectively, and the Ph.D. degree from the University of Queensland, Brisbane, QLD, Australia, in 2017 (advised by Prof. N. Bergmann and Dr. W. Hu).

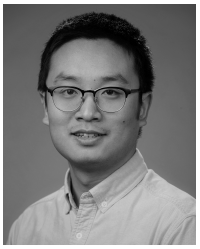
He is an Assistant Professor with the Department of Computer Science, City University of Hong Kong, Hong Kong. Before that, he was a Postdoctoral Research Associate with the School of Computer Science and Engineering, University of New South Wales, Sydney, NSW, Australia, from June 2017 to August 2019. His research areas include mobile computing, sensor network, and IoT.

Wanli Xue received the Ph.D. degree from the School of Computer Science and Engineering, University of New South Wales, Sydney, NSW, Australia.

He is currently a Research Fellow with the Cyber Security CRC, Joondalup, WA, Australia, and the School of Computer Science and Engineering, University of New South Wales. His research interests include security and privacy issues in cyber–physical systems and IoT, including highly efficient privacy-preserving techniques for IoT as well as IoT-related sensing systems and data analytic services.

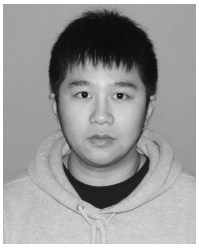
Qi Lin received the bachelor's degree in automation from Zhejiang University, Hangzhou, China, in 2007, the first master's degree in mechatronics from the University of Adelaide, Adelaide, SA, Australia, in 2010, the second master's degree in information technology from the University of New South Wales (UNSW), Sydney, NSW, Australia in 2016, and the Ph.D. degree from the School of Computer Science and Engineering, UNSW, in 2020.

He is currently a Research Associate with UNSW.



Guohao Lan received the B.E. degree in software engineering from Harbin Institute of Technology, Harbin, China, in 2012, the M.S. degree in computer science from KAIST, Daejeon, South Korea, in 2015, and the Ph.D. degree in computer science and engineering from the University of New South Wales, Sydney, NSW, Australia, in 2018.

He is an Assistant Professor with the Embedded and Networked Systems Group, Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, The Delft, The Netherlands. From 2018 to 2021, he was a Postdoctoral Research Associate with the Department of Electrical and Computer Engineering, Duke University, Durham, NC, USA. His research interests include wireless sensing and mobile computing.



Xingyu Feng received the bachelor's degree from Jiangxi University of Finance and Economics, Nanchang, China, in 2017, and the master's degree from Shenzhen University, Shenzhen, China, in 2020. He is currently pursuing the Ph.D. degree in computer science with Shenzhen University.

His current research interests mainly include Internet of Things, data analysis, and deep learning.

Bo Wei received the Ph.D. degree in computer science and engineering from the University of New South Wales, Sydney, NSW, Australia, in 2015.

He has been a Senior Lecturer with the Department of Computer and Information Sciences, Northumbria University, Newcastle upon Tyne, U.K. He was a Postdoctoral Research Assistant with the University of Oxford, Oxford, U.K. His research interests are mobile computing, Internet of Things, and wireless sensor networks.

Chengwen Luo received the Ph.D. degree from the School of Computing, National University of Singapore, Singapore, in 2015.

He was a Postdoctoral Researcher with CSE, University of New South Wales, Sydney, NSW, Australia. He is currently an Associate Professor with the College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, China. His research interests include mobile and pervasive computing and security aspects of Internet of Things.

Wei Li (Senior Member, IEEE) received the Ph.D. degree from the School of Information Technologies, University of Sydney, Sydney, NSW, Australia, in 2014.

He is currently a Research Fellow with Centre for Distributed and High Performance Computing, School of Computer Science, University of Sydney. His research interests include edge computing, sustainable computing, task scheduling, energy efficiency, and Internet of Things.

Dr. Li is the recipient of four IEEE or ACM Conference Best Paper Awards. He received the IEEE TCSC Award for Excellence in Scalable Computing for Early Career Researchers in 2018, and the IEEE Outstanding Leadership Award in 2018. He is a Senior Member of the IEEE Computer Society and a member of the ACM.

Albert Y. Zomaya (Fellow, IEEE) received the B.S. degree in electrical engineering from Kuwait University, Kuwait City, Kuwait, in 1987, and the Ph.D. degree in control engineering from Sheffield University, Sheffield, U.K., in 1990.

He is currently the Chair Professor of High Performance Computing and Networking with the School of Computer Science, University of Sydney, Sydney, NSW, Australia. He is also the Director of the Centre for Distributed and High Performance Computing which was established in late 2009. He was an Australian Research Council Professorial Fellow from 2010 to 2014 and held the CISCO Systems Chair Professor of Internetworking from 2002 to 2007 and also was the Head of School for 2006–2007 in the same school.