Computer Modeling in
Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2023.028656

ARTICLE

A Secure Device Management Scheme with Audio-Based Location Distinction in IoT

Haifeng Lin[1,2], Xiangfeng Liu[2], Chen Chen[2], Zhibo Liu[2], Dexin Zhao[3], Yiwen Zhang[4], Weizhuang Li[4] and Mingsheng Cao[5,6,*]

[1]College of Economics and Management, Nanjing University of Aeronautics and Astronautics, Nanjing, 211106, China

[2]Chengdu Aircraft Industrial (Group) Co., Ltd., Chengdu, 610073, China

[3]Academy of Military Sciences of PLA, Beijing, 100091, China

[4]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, 610054, China

[5]Ningbo WebKing Technology Joint Stock Co., Ltd., Ningbo, 315000, China

[6]The Network and Data Security Key Laboratory of Sichuan Province, University of Electronic Science and Technology of China, Chengdu, 610054, China

*Corresponding Author: Mingsheng Cao. Email: cms@uestc.edu.cn

Received: 30 December 2022 Accepted: 05 May 2023 Published: 22 September 2023

ABSTRACT

Identifying a device and detecting a change in its position is critical for secure devices management in the Internet of Things (IoT). In this paper, a device management system is proposed to track the devices by using audio-based location distinction techniques. In the proposed scheme, traditional cryptographic techniques, such as symmetric encryption algorithm, RSA-based signcryption scheme, and audio-based secure transmission, are utilized to provide authentication, non-repudiation, and confidentiality in the information interaction of the management system. Moreover, an audio-based location distinction method is designed to detect the position change of the devices. Specifically, the audio frequency response (AFR) of several frequency points is utilized as a device signature. The device signature has the features as follows. (1) Hardware Signature: different pairs of speaker and microphone have different signatures; (2) Distance Signature: in the same direction, the signatures are different at different distances; and (3) Direction Signature: at the same distance, the signatures are different in different directions. Based on the features above, a movement detection algorithm for device identification and location distinction is designed. Moreover, a secure communication protocol is also proposed by using traditional cryptographic techniques to provide integrity, authentication, and non-repudiation in the process of information interaction between devices, Access Points (APs), and Severs. Extensive experiments are conducted to evaluate the performance of the proposed method. The experimental results show that the proposed method has a good performance in accuracy and energy consumption.

KEYWORDS

Acoustic hardware fingerprinting; device management; IoT; location distinction

1 Introduction

With the rapid development of emerging technologies (e.g., 5G Communications and beyond [1–3], Artificial Intelligence [4–6], and Information Security [7–9]), the Internet of Things (IoT) have become an important part of people's life and work which provide people with intelligent, secure and privacy-protected services, such as smart medical care [10,11], smart city [12], and intelligent manufacturing [13,14]. As we all know, massive smart devices are extremely important in the IoT, as they undertake a variety of high-precision and difficult tasks [15–17]. It is noted that a lot of smart devices in IoT are extremely expensive. To reduce the acquisition cost of smart devices and improve their utilization of them, a large number of smart devices have been realized as mobile and portable [18–21]. It is necessary to manage smart devices, such that they can be accurately located when we need them [22–24]. Moreover, as the number of IoT nodes continue to increase, the risks associated with malicious attacks on the IoT also continue to rise [25,26]. When an IoT device is compromised, it is critical to locate the device among the vast number of IoT devices. However, the mobility and portability of devices have brought great challenges to secure device management [27–29]. In the midst of existing challenges, identifying an IoT device and detecting a change in its position are critical challenges in many IoT applications (e.g., intelligent logistics, intelligent transportation, and intelligent manufacturing [30,31]).

There are several existing methods to realize the identification and movement detection of devices. In [32], the radio frequency identification devices (RFID) based device tracking method was proposed, in which, RFID tags can be used to identify and track devices. In this method, the devices are attached with an RFID tag, which can be identified by an RFID reader. However, using the RFID-based method requires a large number of readers. This will come at a high cost, as the RFID reader is expensive. In [33], an IoT device management system was designed by using cloud computing to realize the dynamic task scheduling of devices. In [34], a single pixel tracking system is proposed for the microfluidic device monitoring without image processing. Other related works also include [35–37], which considers the secure management of smart devices. However, both of them focus on the security in smart device management and lack device tracking.

In this paper, a device management scheme is proposed, which includes device identification and movement detection by using audio-based location distinction techniques. In our system, a set of devices $\mathscr{D} = \{Dev_1, Dev_2, \ldots, Dev_s\}$ and a set of Access Points (APs) $\mathscr{A} = \{AP_1, AP_2, \ldots, AP_t\}$ are distributed in different rooms. A sever is included in our system to manage all the devices, such as, recoding the trajectory and current position of each device, and assisting in mutual authentication between device and AP. The APs are responsible for detecting the movement of a device in their rooms, and report it to the sever for tracking devices. Both of the devices and APs are equipped with communication module based on microphone and loudspeaker. It is worth noting that these modules are extremely inexpensive [38].

The proposed scheme includes three main stages: Device Registration, Position Report, and Location Distinction. We utilize traditional cryptographic techniques to realize the integrity, authentication, and non-repudiation of information transmitted between devices, APs, and Severs. Moreover, the audio-based location distinction method is designed to identify the devices and detect the position change of them. The audio frequency response (AFR) at several frequency points are utilized as the signature of a device [39,40] to identify the devices and detect the movements because of the following features. (1) Hardware Signature: the obtained signatures of different loudspeaker and microphone pairs are difference [41]; and (2) Location Signature: the obtained signatures are completely different for different distances in the same direction and the obtained signatures are different for different directions in the same distances. To evaluate the performance of the proposed scheme, extensive experiments are conducted. In our experiments, several mobile phones (i.e., HUAWEI Mate 40, HUAWEI nova 9pro, and HUAWEI nova 9SE) are used as devices and APs. We selected 31 frequency points ranging from 10 to 16 KHz with steps length of 0.2 KHz in our experiments. Extensive experiments show that the audio-based location distinction method has a good performance in security, accuracy and energy consumption.

The main contributions of this paper are shown as follows:

- We propose a secure IoT device management scheme with audio-based location distinction and traditional cryptographic techniques.
- We design an audio-based location distinction method to identify the IoT devices and detect the position change of them.
- We conduct extensive experiments to evaluate the performance of the proposed scheme. The results show that our scheme has a good performance in security, accuracy and energy consumption.

The structure of the paper is as follows. The system model is introduced in Section 2. Section 3 describes the proposed the details of IoT device management scheme. Audio-based location distinction method is discussed in Section 4. The experimental results are pretended in Section 5. Finally, Section 6 concludes this paper.

2 System Model

There are three entities involved in our system, as shown in Fig. 1, e.g., IoT device, Access Point, and Sever. Specifically, in the proposed system, there is a set of ***devices*** $\mathscr{D} = \{Dev_1, Dev_2, \ldots, Dev_s\}$, which are distributed in different rooms. There is also a set of Access Points (***AP***s) $\mathscr{A} = \{AP_1, AP_2, \ldots, AP_t\}$, where each room is equipped with an AP for identifying and monitoring devices. Moreover, a ***sever*** is included in our system to manage all the devices, e.g., recoding the trajectory and current position of each device, assisting in mutual authentication between device and AP, etc. The main objective of this paper is that, the APs are responsible for detecting the movement of a device in their rooms, and report it to sever for tracking.

The audio frequency response (AFR) at several frequency points is used as the location signature of a device for movement detection. It is necessary to introduce the acoustic propagation model. As sound wave is a kind of energy, its energy will gradually decline with the increase of the transmission distance owing to the diffusion, absorption and scattering, when it propagates in certain medium. Actually, the received energy is related to the propagation distance, the gain of the built-in loudspeaker at sender and the built-in microphone at receiver, and the frequency of the sound wave. The acoustic attenuation model is shown as follows:

$$P_r(d,f) = P_t(f)L_r(f)L_t(f)e^{-a_0 d(2\pi f)^{n_f}} \tag{1}$$

where d is the distance from the sound source, f is the acoustic frequency, $P_t(f)$ is the audio transmission power, $P_r(d,f)$ is the audio frequency receiving power, $L_r(f)$ is the loss of the microphone, $L_t(f)$ is the loss of loudspeaker, n_f is the attenuation factor independent of distance and related to frequency, *exp* is the exponential function.

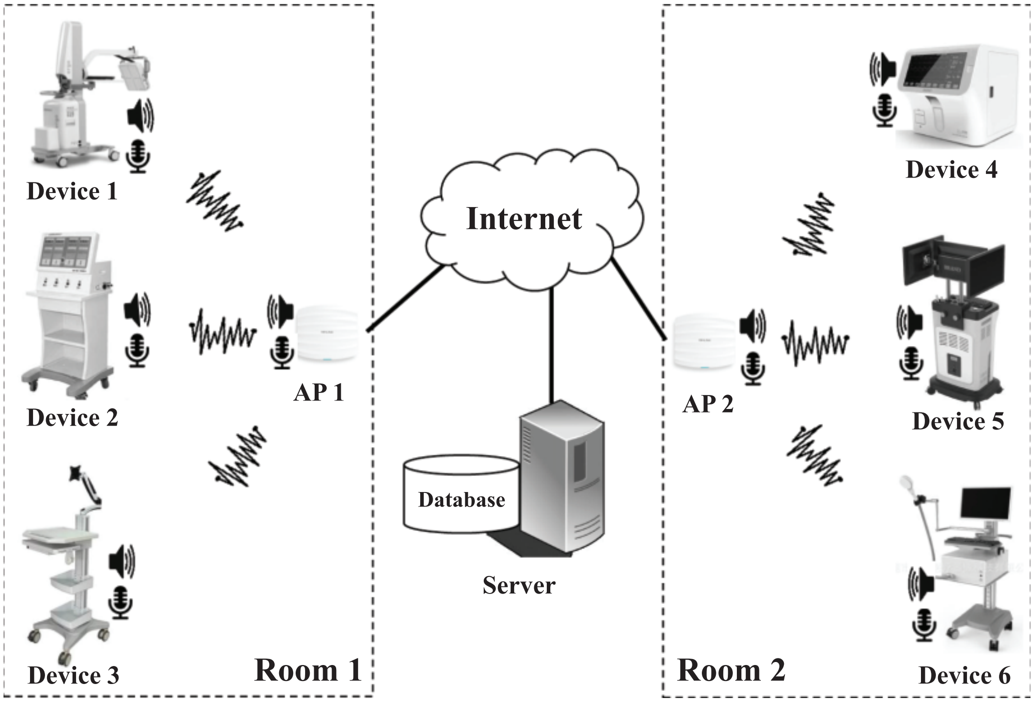


Figure 1: The system model

The audio frequency response (AFR) at frequency point f can be defined as:

$$AFR(f) = 20\log\left(\frac{P_r(d,f)}{P_t}\right) = 20\log[L_r(f)L_t(f)] - a_0 d\log(e)(2\pi f)^{n_f} \tag{2}$$

It is clear that the frequency response at f is a function of the distance between the sender and receiver, and loss at the microphone and loudspeaker. Accordingly, the set of frequency response $\{AFR(f_1), \ldots, AFR(f_n)\}$ at different frequency points $f_1, f_2, \ldots$, and f_n can be regarded as the hybrid signature of location and audio-hardware fingerprints. However, it is difficult for a receiver to obtain the audio transmission power $P_t(f_i)$. To solve the problem, the audio signal *AudSig* transmitted by sender for hybrid signature extraction can be fixed during the location distinction phase. In this case, the vector

$$\Phi = < 20\log P_r(d,f_1), \ldots, 20\log P_r(d,f_n) > \tag{3}$$

can be used as the hybrid signature.

In our system, it is assumed that there is an adversary who is equipped with loudspeaker and microphone. The adversary can obtain all the parameters of the proposed system, know the position of a target IoT device, and access to such devices. The adversary can record the sound of the target IoT device with its loudspeaker, and launch replay attacks with its microphone through adaptive selection of the appropriate positions to trick the AP into recognizing it as the target IoT device.

3 The Proposed Scheme

3.1 Device Registration

Assumed that there is a device manager who has a handhold smart terminal device (e.g., a mobile phone) and is in charge of assisting device registration during the registration phase and inputting basic information of the devices into the server database. The manager and server have a pair of public/private key (PK_M, SK_M) and (PK_S, SK_S), respectively.

In order to register a new device Dev_{new} with ID ID_{Dev} in the system, the manager and the sever perform the following steps:

Step 1. The manager first transmits the identification number ID_M (resp. ID_{Dev}) of the manager (resp. the device), time stamp T_0, and basic information of device *BasicInf* (e.g., model, function, price, manufacturer, etc.) to the sever with the handhold smart terminal device by using symmetric encryption algorithm AES [42] and RSA-based signcryption scheme RSA-TBOS [43] as follows:

- Defining $M =< ID_M \| ID_{Dev} \| T_0 \| BasicInf >$, the manager sends encrypted registration information

$$Reg = Enc_{K_{sec}}(M) \| SignCry\big(K_{sec} \| hash(M)\big) \tag{4}$$

to the sever, where $Enc_{K_{sec}}$ is the encoding algorithm of AES with secret key K_{sec}, $hash(\cdot)$ is a hash function, and *SignCry* is the signcryption algorithm of RSA-TBOS.

Step 2. After receiving registration information *Reg*, the Sever performs the following steps to complete registration:

- The sever checks the validity of $SignCry\big(K_{sec} \| hash(M)\big)$.
- If so, the sever can obtain the key K_{sec} and the hah values $hash(M)$; if not, the registration is failed.
- Then, the sever decrypts M from $Enc_{K_{sec}}(M)$, computes $hash(M)$, and checks if the two hash values are equal.
- If so, the sever chooses an initial section key K_0 and transmits $Enc_{K_{sec}}(ID_{Dev} \| K_0)$ to the manager, and puts M and K_0 in its database; if not, the registration is failed.

Step 3. The device manager decrypts $ID_{Dev} \| K_0$ from $Enc_{K_{sec}}(ID_{Dev} \| K_0)$, and then transmits $ID_{Dev} \| K_0$ to Dev_{new} with an audio-based secure D2D communication [44,45]. The device Dev_{new} stores the section key K_0.

3.2 Position Report

If a device Dev_i is moved from one room (room j_1) to another room (room j_2), it is required to report it's position to the Sever through the AP_{j_2} in the current room as follows:

Step 1. Dev_i first generates a randomness R_0 and transmits the encrypted report information *Rep* to AP_j:

$$Rep = ID_{Dec_i} \| R_0 \| Enc_{K_0}\big(M_{Rep} \| hash(M_{Rep})\big) \tag{5}$$

where $M_{Rep} = R_0 \| ID_{Dec_i} \| ID_{AP_{j_1}} \| Time$, $ID_{AP_{j_1}}$ is the ID of the AP in the last room, and *Time* is the time stamp. If Dev_i is in use for the first time, set $ID_{AP_{j_1}}$ to null.

Step 2. After obtaining *Rep* from Dev_i, AP_{j_2} sends

$$RepSign = ID_{AP_{j_2}} \| Rep \| Sign_{AP_{j_2}}\big(hash(ID_{AP_{j_2}} \| Rep)\big) \tag{6}$$

where $ID_{AP_{j_2}}$ is the ID of the AP in the current room, and $Sign_{AP_{j_2}}(\cdot)$ is the signature algorithm [46] with it is private key.

Step 3. When the sever received *RepSign* from AP_{j_2}, it performs the following step to complete the location report.

- First of all, it verifies the validity of the signature $Sign_{AP_{j_2}}(hash(ID_{AP_{j_2}} \| Rep))$ with AP_{j_2}'s public key.
- Then, it obtains M_{Rep} and $hash(M_{Rep})$ with current session key K_0 of Dev_i and checks the consistency between them (if not, returning *Failure* to Dev_i through AP_{j_2}).
- Finally, it verifies the consistency between $ID_{Dec_i} \| R_0$ and M_{Rep}. If so, it sends a feedback *EncSK* (which includes a new session key K_1 for Dev_i) to Dev_i through AP_{j_2} (if not, it returns *Failure* to Dev_i through AP_{j_2}), where

$$EncSK = Enc_{K_0}\left(ID_{Dev_i} \| ID_{AP_{j_2}} \| K_1 \| hash(ID_{AP_{j_2}} \| K_1)\right) \tag{7}$$

Step 4. After receiving *EncSK*, Dev_i decrypts $ID_{AP_{j_2}} \| K_1$ and $hash(ID_{AP_{j_2}} \| K_1)$ with session key K_0, and checks the consistency between them. If so, Dev_i stores $ID_{AP_{j_2}}$ and K_1 (as the new session key), and sends response

$$Enc_{K_1}\left(R_1 \| ID_{AP_{j_2}} \| hash(R_1 \| ID_{AP_{j_2}})\right) \tag{8}$$

to sever through AP_{j_2}, in which, R_1 is a random number; if not, it returns *Failure* to sever through AP_{j_2}.

Step 5. The sever decrypts $R_1 \| ID_{AP_{j_2}}$ and $hash(R_1 \| ID_{AP_{j_2}})$ from Dev_i's response, and verifies the consistency between them. If so, the sever stores $ID_{AP_{j_2}}$ as Dev_i's new position, K_1 as the new session key, and *Time* as the time stamp; if not, it reports *Failure* to Dev_i through AP_{j_2}.

3.3 Location Distinction

If the device Dev_i has been moved in room j and finished the position report, AP_j needs to monitor if Dev_i has changed its position and report to the sever if a position change of Dev_i occurs. In our system, an audio-based location distinction method is proposed, and the framework of the proposed method is shown as follows:

- **Audio Signal Generation.** After finishing the position report, Dev_i generates an audio signal *AudSig* and transmits it with it is loudspeaker to AP_j.
- **Hybrid Signature Extraction.** When AP_j received the audio signal with it's microphone, it extracts the fingerprints of location and hardware from the received audio signal as a hybrid signature.
- **Movement Detection.** Dev_i intermittently sends the same audio signal *AudSig* to AP_j for signature extraction, and AP_j compares current signature with the previous signatures to determine whether AP_j has been moved.

For the details of the audio-based location distinction method, please refer to the next section.

4 Audio-Based Location Distinction Method

4.1 Location and Audio-Hardware Fingerprints

From the discussion above, the vector Φ generated from the received signal is strong correlated with audio-hardware and location. To verify the theoretic result in a real scenario, three experiments are conducted, in which the selected frequencies are from 10 to 16 KHz with the step length 0.2 KHz, and the transmitted audio signal *AudSig* is the sum of the sine wave at the selected frequencies (i.e., 10, 10.2, . . . , 16 KHz).

Hardware Signature. In the first experiment, three different smart phones are used to investigate the hardware differences, in which the phone i equipped with $Loudspeaker_i$ and $Microphone_i$ ($i = 1, 2, 3$). Fig. 2 plots the vectors $\Phi(L_1, M_2)$, $\Phi(L_2, M_3)$ and $\Phi(L_3, M_3)$, where $\Phi(L_i, M_j)$ is used to denote the obtained value of Φ with $Loudspeaker_i$ and $Microphone_j$. As shown in Fig. 2, the hardware signatures of different loudspeaker and microphone pairs are very clear difference.

Location Signature. In the second experiment, two smart phones (i.e., Phone 1 and Phone 2) are used to study the location differences. Fig. 3 plots the vectors $\Phi(L_1, M_2)$ under four different distances between sender to receiver in the same direction, in which the distances are set to 20, 40, 60, and 80 cm. From Fig. 3, the obtained vectors are completely different in different distances at the same direction. Fig. 4 shows the vectors $\Phi(L_1, M_2)$ in three different directions from receiver in the same distance. It can be seen that the obtained vectors are also different for different directions in the same distances. In summary, location signature of different locations for the same loudspeaker and microphone pair are completely difference.

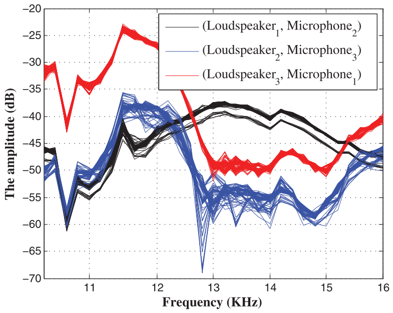


Figure 2: Hardware signature

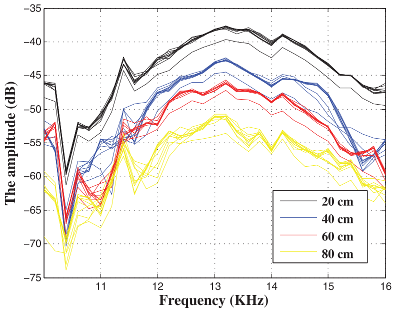


Figure 3: Distance signature

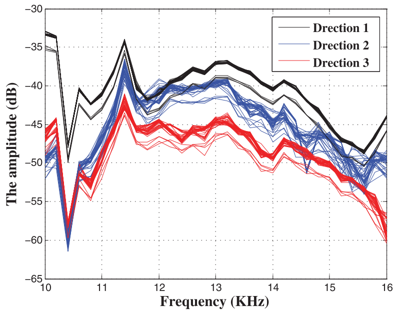


Figure 4: Direction signature

4.2 Audio-Based Location Distinction Scheme

Based on the discussion above, a novel location distinction scheme are proposed by using the AFR. Besides being able to determine whether a node is moving with location signature, the proposed scheme can also resist node impersonation attacks with the audio hardware signature. The details of the proposed scheme is shown as follows:

Audio Signal Generation. When Dev_i is moved from $room_i$ to $room_j$, Dev_i selects a sequence $(\alpha_1, \alpha_2, \ldots, \alpha_N)$ from [0, 1] uniformly at random. And then, Dev_i generates an audio signal

$$AudSig = \sum_{n=0}^{N} \frac{\alpha_n}{\sum_{s=0}^{N} \alpha_s} \sin\left(2\pi(\varphi_0 + nf_\Delta)t\right) \tag{9}$$

for $t \in (0, T]$, where φ_0 is the initial frequency, and f_Δ is the length of step. Here $\{f_0, f_1, \ldots, f_N\}$ is the set of selected frequencies, in which $f_n = \varphi_0 + nf_\Delta$ for $n = 0, 1, \ldots, N$.

Hybrid Signature Extraction. After completing the location report phase, Dev_i transmits audio signals

$AudSig \| Chirp \| AudSig \| Chirp \| AudSig$

with its loudspeaker to AP_j, where $Chirp$ is a chirp signal. Note that, a chirp is a signal in which the frequency increases (called up-chirp) or decreases (called down-chirp) with time. When receiving the audio signals

$\widehat{AudSig}_0 \| \widehat{Chirp}_0 \| \widehat{AudSig}_1 \| \widehat{Chirp}_1 \| \widehat{AudSig}_2$

with the microphone, AP_j first extract $\widehat{AudSig}_0$, $\widehat{AudSig}_1$, and $\widehat{AudSig}_2$. Then, AP_j computes

$$\begin{aligned}\Phi_i &= 20 \log \left(FFT(\widehat{AudSig}_i) \right) \\ &=< 20 \log P_r(d, f_{1i}), \ldots, 20 \log P_r(d, f_{ni}) > \end{aligned} \tag{10}$$

for $i = 0, 1, 2$, where $FFT(\cdot)$ is fast discrete Fourier transform algorithm, which transforms the signals from time-domain to frequency domain. Finally, AP_j obtains the hybrid signature as follows:

$$\Phi = \frac{1}{3} \sum_i \Phi_i =< \phi_1, \ldots, \phi_n >$$

Movement Detection. When Dev_i sends the same audio signal $AudSig \| Chirp \| AudSig \| Chirp \| AudSig$ to AP_j, AP_j first extracts the corresponding hybrid signature

$$\Phi' = \frac{1}{3} \sum_i \Phi'_i =< \phi'_1, \ldots, \phi'_n >$$

where Φ'_i is the FFT result from $\widehat{AudSig}_i$ $(i = 0, 1, 2)$. Then AP_j compares the current signature Φ' with the previous signatures Φ' with Euclidean distance:

$$d(\Phi, \Phi') = \sqrt{\sum_{i=1}^{n} (\phi_i - \phi'_i)^2} \tag{11}$$

If $d(\Phi, \Phi')$ is less than a threshold Δ, then Dev_i is considered to be static; otherwise, Dev_i is considered to be moved.

4.3 Evaluation Methodology

Hypothesis testing is used to decide two hypotheses H_0 or H_1 is true when the outcome of the measurements is given [47]. Here, a kind of evaluation methodology based on hypothesis testing is discussed to analyse the accuracy of the proposed algorithm. We conduct an experiment to show the distribution of statistics of the Euclidean distance between signature Φ_0 of Dev_i at time slot t_0 and Φ_ν at time slot t_ν in the same location, where $\nu = 1, \ldots, 300$, and the distance between Dev_i and AP_j is 60 cm. From Fig. 5, we can see that the result of this frequency statistic is approximately conforming to Gaussian distribution.

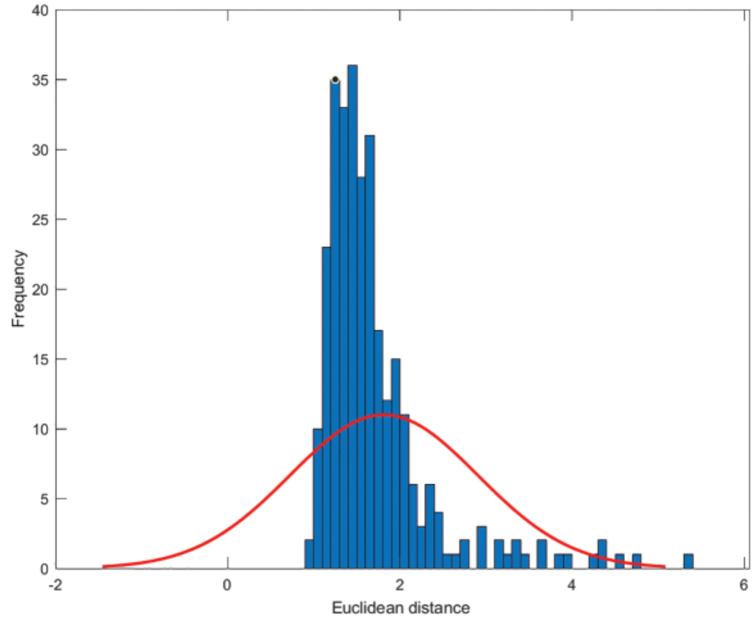


Figure 5: The distribution of statistics of the Euclidean distance between two signatures at the same position

Supposed that $G(\mu_1, \delta_0^2)$ is the distribution of probability of the distance $d(\Phi_{loc_0}(0), \Phi_{loc_0}(\nu))$ between the signature at time slot t_0 in location loc_0 and the signature at other time slot t_ν in location loc_0, and $G(\mu_1, \delta_1^2)$ is the distribution of probability of the distance $d(\Phi_{loc_0}(0), \Phi_{loc_1}(\nu))$ between the signature at time slot t_0 in location loc_0 and the signature at other time slot t_ν in location loc_1. Note that, the signature of Dev_i at location loc_0 is different from the signature of Dev_i at location loc_0 and location loc_1, where $loc_0 \neq loc_1$. Accordingly, we have $\mu_1 > \mu_0$. The location change detection test can be viewed then as a choice between two events H_0 and H_1.

$$\begin{aligned} &H_0 : d(\Phi_{loc_0}(0), \Phi_{loc_0}(\nu)) \geq \Delta \\ &H_1 : d(\Phi_{loc_0}(0), \Phi_{loc_1}(\nu)) < \Delta \end{aligned} \tag{12}$$

Then, the false negative probability P_{FN} and false positive probability P_{FP} can be expressed as

$$\begin{aligned} &P_{FN} = \int_{-\infty}^{x=\Delta} \frac{1}{\sqrt{2\pi}} e^{-(x-\mu_1)^2/2\sigma_1^2} dx \\ &P_{FP} = \int_{x=\Delta}^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-(x-\mu_0)^2/2\sigma_0^2} dx \end{aligned} \tag{13}$$

In order to evaluate the performance of the proposed scheme, we design an evaluation methodology as follows:

$$F_1 = 2/(1/Recall + 1/Precision) \tag{14}$$

where $Precision = TP/(TP + FP)$, $Recall = TP/(TP + FN)$, TP means the number of accurate detection with no movement, and FP and FN are the number of false positive error and false negative error, respectively. Specifically, when F_1 is calculated to be 1, it means there is no false negative alarm.

5 Experimental Verification

In this section, extensive experiments are conducted to verify the performance of the proposed scheme.

5.1 Experimental Environment

In our experiments, several mobile phones (i.e., HUAWEI Mate 40, HUAWEI nova 9pro, and HUAWEI nova 9SE) are used as devices and APs. Note that, due to the limitation of hardware, the maximum frequency of sound produced by a mobile phone is about 16 KHz. Therefore, it selected 31 frequency points ranging from 10 to 16 KHz with steps length of 0.2 KHz in our experiments.

The position change diagram of the device in the experiments is shown in the Fig. 6. We consider the changing of starting position of the device from the 20 to 100 cm with step-length 20 cm in four different directions, where the AP is on the central position. In other words, there are five points for each direction, and each point is 20, 40, 60, 80, and 100 cm away from the central position. The AP records the sound signal from the device to get the 31 results after FFT transformation for each period of time, and then, calculates the Euclidean distance of link signature according to the obtained value. Moreover, we found that the fading of high frequency band is too fast. In order to average the granularity of each frequency, we refer to the experimental test and influence factors of acoustic attenuation model, and change the frequency weight to exponential growth from low frequency to high frequency.

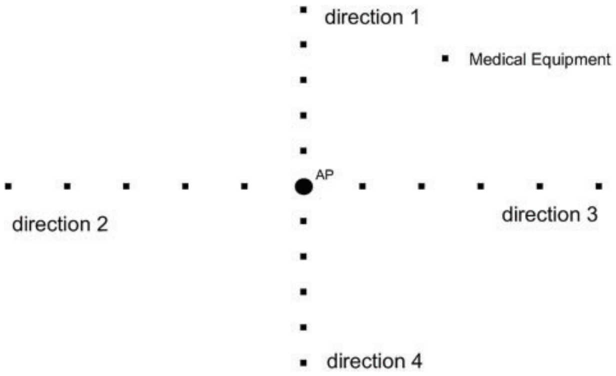


Figure 6: The position change diagram of the device in the experiments

5.2 Threshold Selection

First of all, we discuss how to determine the threshold of the proposed location distinction method. From Figs. 2–4, we have the conclusion that the location signatures have two properties: the aggregation with time difference and the separation with space difference. The conclusion shows that finding a threshold of movement detection is possible.

An experiment is conducted to obtain the Euclidean distance of two signatures under different distance change between device and AP with 20 cm as the step length in each direction. As shown in Fig. 7, the solid black dot means the Euclidean distance of two signatures of the starting position; the red square means the Euclidean distance of two signatures in the starting position and the position at 20 cm, respectively; the red star means the Euclidean distance of two signatures in the starting position and the position at 40 cm, respectively; the blue triangle means the Euclidean distance of two signatures in the starting position and the position at 60 cm, respectively; the green diamond means the

Euclidean distance of two signatures in the starting position and the position at 80 cm, respectively; the black circle means the Euclidean distance of two signatures in the starting position and the position at 100 cm, respectively. From this figure, we can find that the Euclidean distance of two signatures increases as the distance between measured positions increases.

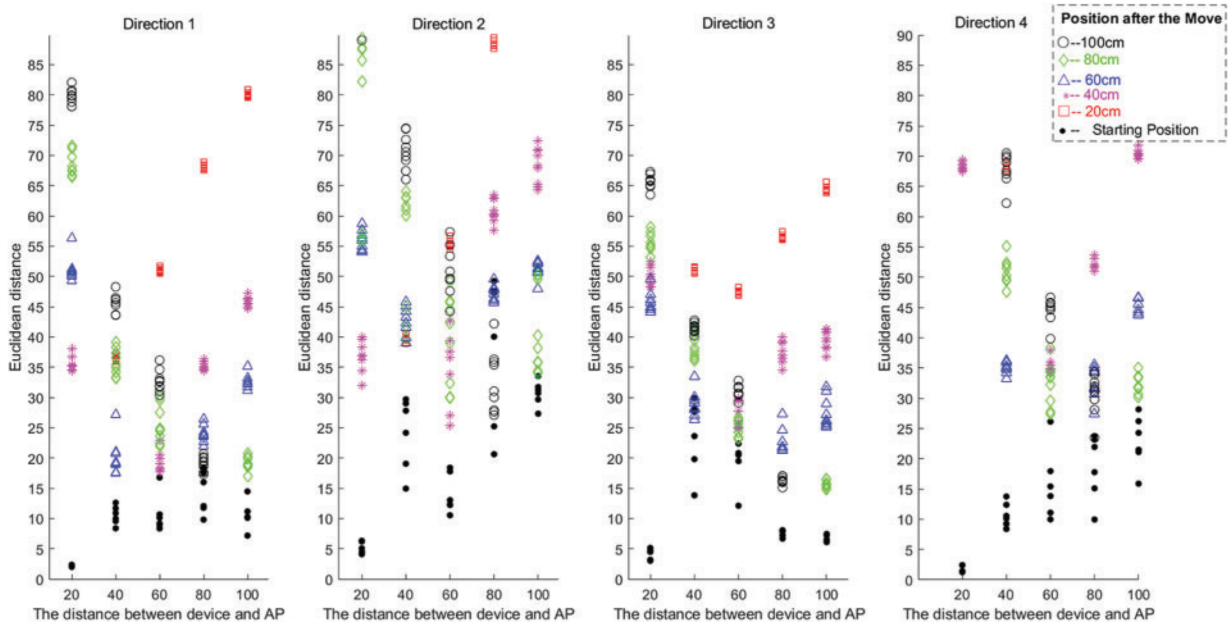


Figure 7: Threshold discussion

In order to obtain a fixed threshold suitable for all distances, the F_1 score is studied over a varying threshold under different starting positions. As shown in Fig. 8, we plot the effect of different threshold increments on F_1 score under different starting positions. From this figure, it can be seen that, when $\Delta = 15$, F_1 scores are 1 for different starting positions. It should be noted that, when $\Delta = 15$, the false positive alarm is likely to happen. If Δ is set to be 30, there is only one false positive alarm in all the tests. However, the proposed scheme will be less sensitive to movement perception. For instance, in case that the starting position is 40 cm in direction 1, the proposed scheme can detect a movement when the movement distance is up to 40 cm.

5.3 Replay Attack Analysis

Now we discuss the adversary's replay attacks with an experiment. Assumed that a legitimate device is located 20, 40, and 60 cm in direction 1, and an adversary is located at 5 cm before and after these three points. In this experiment, the adversary records and replays the sound of the legitimate device. The experimental result is shown in Fig. 9, in which the threshold is set to 15. The blue line combination is the sum of the signature of the legitimate device. We can see in the figure that its separation from the purple and black lines from the recording playback of the adversary. By comparing the threshold with the Euclidean distance between signatures from the legitimate device and adversary, it is found that the attack inefficiency is 100%. This test verifies the proposed scheme can against recording replay attacks.

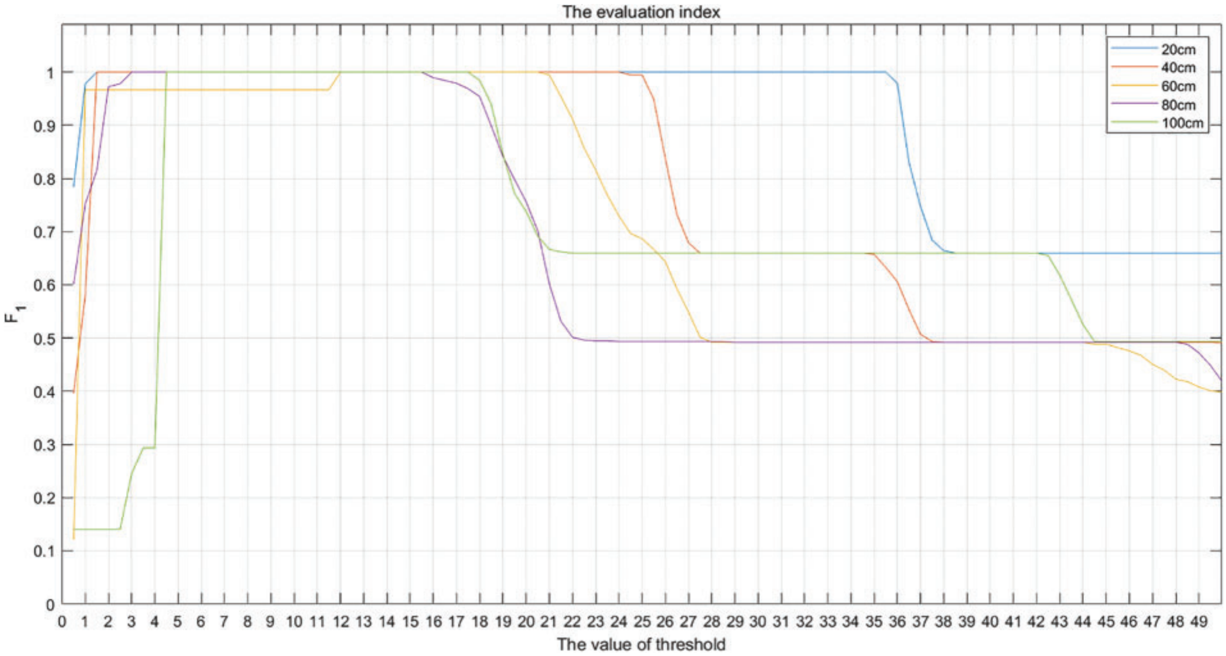
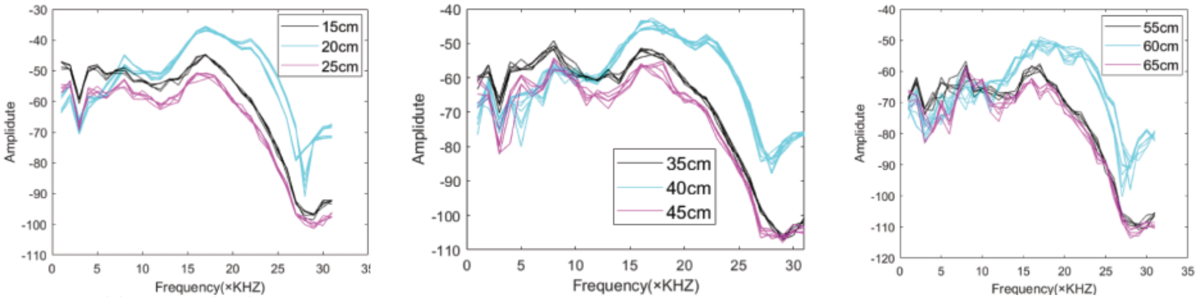


Figure 8: The impact of the value of the threshold on the detection performance



(a) The legitimate device is located at 20cm in direction 1.

(b) The legitimate device is located at 40cm in direction 1.

(c) The legitimate device is located at 60cm in direction 1.

Figure 9: Adversary's replay attacks

Assumed that the adversary can obtain the original position and the original audio from the legitimate device, an experiment is conduct as follows. A mobile phone is used as the legitimate device at the position 20 cm in direction 1, and another mobile phone is used as the adversary at the position 20 and 2 cm before and after, and 2 cm around. Fig. 10 plots the Euclidean distance of the signature of legitimate device and the signature of adversary at different positions in different time slots. In this figure, the middle red line is the threshold. The experimental results show that all attacks failed, although the Euclidean distance between the signature of legitimate device and the signature of adversary at the original position is the closest one to the threshold.

5.4 Performance

In order to study the performance of the proposed scheme, an experiment is conducted, in which, the distance between the device and the AP is ±20, ±40 and ±60 cm, the movement distance is

5, 10 and 20 cm, and the threshold is set to 25, where −20, −40 and −60 cm means the opposite direction of distance 20, 40 and 60 cm between the device and the AP, respectively. The experimental results are shown in Fig. 11. It can be seen that, the difference of signatures at the same position over different time slots can be confirmed with 100% accuracy. It can also be seen that the accuracy gradually increases with the increasing movement distance, i.e., a larger movement distance means a more accuracy movement detection. Specifically, it is found that when the movement distance is up to 60 cm, all the device movement can be accurately detected.

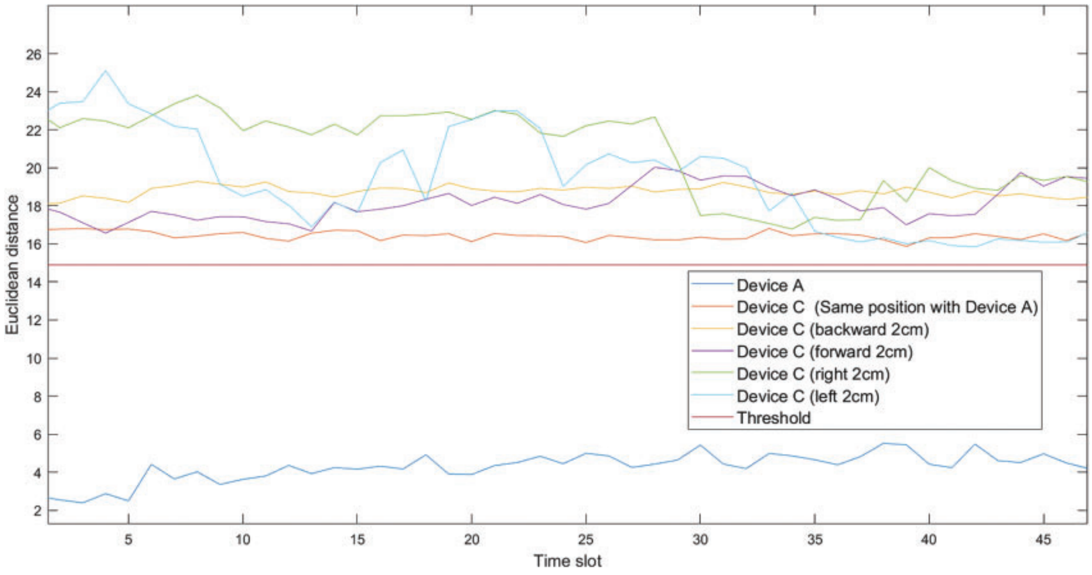


Figure 10: Attacks analysis when the adversary can obtain the original position and the original audio from the legitimate device

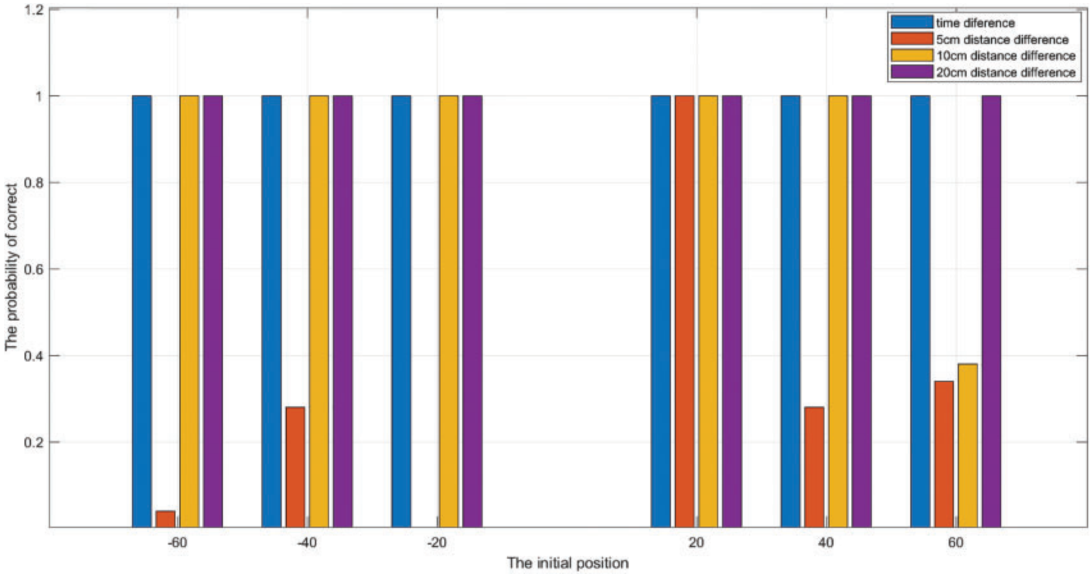


Figure 11: The performance of the proposed scheme

To further discuss the performance, we test the proposed scheme by selecting three places that are very common in daily life, and the noise level ranged from high to low: restaurants, supermarkets and classrooms. In this experiment, the AP is 100 cm away from the device in the direction 1, and 1000 groups of tests are performed for each place, in which the first 500 groups of talking phones do not move and the last 500 groups of talking phones move 30 cm away. The test results are shown in the Fig. 12. It can be seen that, whether in a noisy restaurant or a quiet classroom, the proposed scheme can identify whether a device to move with a 100% probability, which is perfectly in line with the expectation.

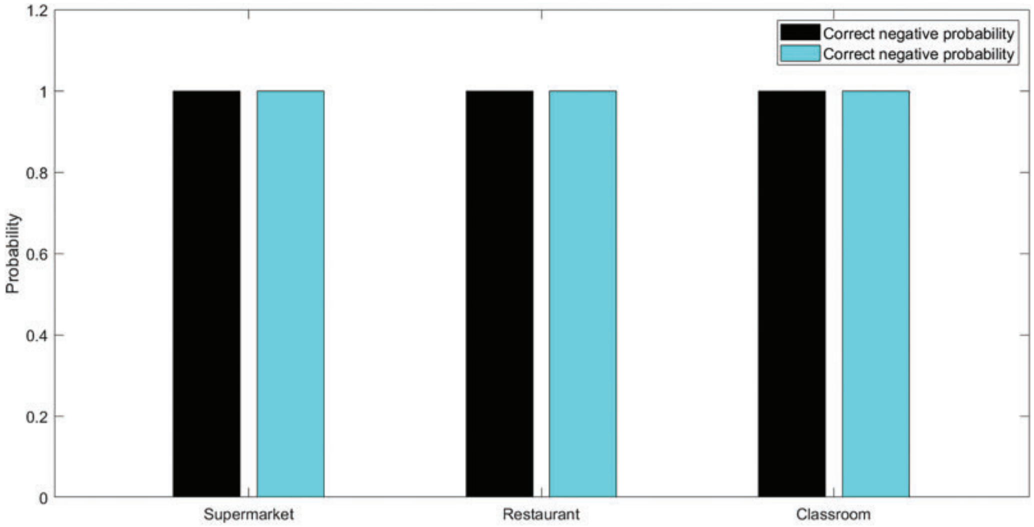


Figure 12: The test of the proposed scheme over restaurants, supermarkets and classrooms

Finally, we conduct an experiment to evaluate the energy consumption compared with several common APPs on mobile phones in the Fig. 13. In this experiment, all applications are turned off except the test software. We measure the power consumption of the proposed scheme and other applications (i.e., NetEases could music, QQ music, QQ, and Microblog) within one hour to verify the efficiency of the software. We can see that the power consumption of the proposed scheme is more than 30 times lower than that of similar music playing software, 18 times lower than that of chat tool software, and 40 times lower than that of video and picture browsing software.

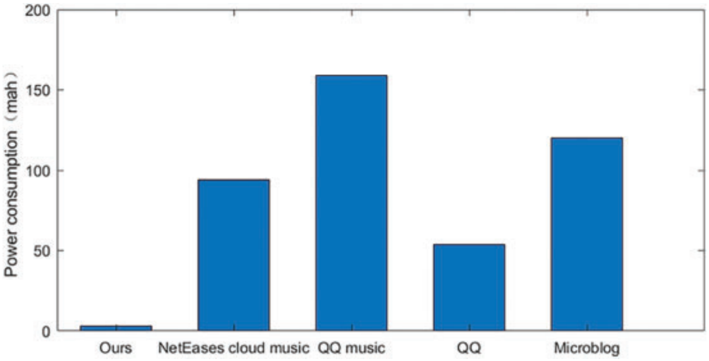


Figure 13: The energy consumption of the proposed scheme compared with several common APPs

Discussion. The disadvantage of the proposed scheme is that the transmission of high-frequency sound waves may disturb nearby people. Possible solutions include replacing mixed sine-wave signals with melodious mid-to-high frequency music or using ultrasonic frequencies to send and receive acoustic signals.

6 Conclusion

In this paper, a secure device management scheme with audio-based location distinction in IoT has been proposed by utilizing traditional cryptographic techniques. In our scheme, the traditional cryptographic techniques are utilized to realize the integrity, authentication, and non-repudiation of information transmitted between devices, APs, and Severs; and the audio-based location distinction method is designed for identifying the devices, as well as detecting the position change of them. The audio frequency response (AFR) at several frequency points is utilized as the signature of a device to identify the devices and detect the movements. To evaluate the performance of the proposed scheme, extensive experiments are conducted. The experimental results show that the proposed scheme has a good performance in security, accuracy and energy consumption. Future research directions include implementing the designed method using ultrasound and verifying the validity of the method in a real IoT scenario, such as the Internet of Medicine (IoM).

Acknowledgement: Authors thank editors and reviewers for helping the enrichment of this article.

Funding Statement: This work is supported by Demonstration of Scientific and Technology Achievements Transform in Sichuan Province under Grant 2022ZHCG0036, National Natural Science Foundation of China (62002047).

Author Contributions: Study conception and design: Haifeng Lin, Mingsheng Cao; data collection: Xiangfeng Liu, Chen Chen; analysis and interpretation of results: Zhibo Liu, Dexin Zhao; draft manuscript preparation: Yiwen Zhang, Weizhuang Li. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not available.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Shen, X., Gao, J., Wu, W., Li, M., Zhou, C. et al. (2022). Holistic network virtualization and pervasive network intelligence for 6G. *IEEE Communications Surveys & Tutorials, 24(1),* 1–30.
2. Wu, W., Zhou, C., Li, M., Wu, H., Zhou, H. et al. (2022). AI-native network slicing for 6G networks. *IEEE Wireless Communications, 29(1),* 96–103.
3. Zhang, N., Yang, P., Ren, J., Chen, D., Yu, L. et al. (2018). Synergy of big data and 5G wireless networks: Opportunities, approaches, and challenges. *IEEE Wireless Communications, 25(1),* 12–18.
4. James Jose, C., Rajasree, M. (2023). Implicit continuous user authentication for mobile devices based on deep reinforcement learning. *Computer Systems Science and Engineering, 44(2),* 1357–1372.
5. Chen, D., Zhao, Z., Qin, X., Luo, Y., Cao, M. et al. (2022). MAGLeak: A learning-based side-channel attack for password recognition with multiple sensors in IIoT environment. *IEEE Transactions on Industrial Informatics, 18(1),* 467–476.

6. Ale, L., Zhang, N., Wu, H., Chen, D., Han, T. et al. (2019). Online proactive caching in mobile edge computing using bidirectional deep recurrent neural network. *IEEE Internet of Things Journal, 6(3),* 5520–5530.
7. Chen, D., Jiang, S., Zhang, N., Liu, L., Choo, K. K. R. (2022). On message authentication channel capacity over a wiretap channel. *IEEE Transactions on Information Forensics and Security, 17,* 3107–3122.
8. Mei, Q., Xiong, H., Chen, Y., Chen, C. (2022). Blockchain-enabled privacy-preserving authentication mechanism for transportation CPS with cloud-edge computing. *IEEE Transactions on Engineering Management*. https://doi.org/10.1109/TEM.2022.3159311
9. Xiong, H., Zhou, Z., Wang, L., Zhao, Z., Huang, X. et al. (2022). An anonymous authentication protocol with delegation and revocation for content delivery networks. *IEEE Systems Journal, 16(3),* 4118–4129.
10. Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-ALi, A. et al. (2020). Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet of Things Journal, 8(11),* 8707–8718.
11. Bohr, A., Memarzadeh, K. (2020). The rise of artificial intelligence in healthcare applications. In: *Artificial intelligence in healthcare*, pp. 25–60. Cambridge: Academic Press.
12. Gheisari, M., Najafabadi, H., Alzubi, J., Gao, J., Wang, G. et al. (2021). OBPP: An ontology-based framework for privacy-preserving in IoT-based smart city. *Future Generation Computer Systems, 123,* 1–13.
13. Wang, J., Xu, C., Zhang, J., Zhou, R. (2022). Big data analytics for intelligent manufacturing systems: A review. *Journal of Manufacturing Systems, 62,* 738–752.
14. Chen, D., Wang, H., Zhang, N., Nie, X., Dai, H. et al. (2022). Privacy-preserving encrypted traffic inspection with symmetric cryptographic techniques in IoT. *IEEE Internet of Things Journal, 9(18),* 17265–17279.
15. Iadanza, E., Gonnelli, V., Satta, F., Gherardelli, M. (2019). Evidence-based medical equipment management: A convenient implementation. *Medical Biological Engineering & Computing, 57(10),* 2215–2230.
16. Hernǎndez-Lǒpez, L., Pimentel-Aguilar, A., Ortiz-Posadas, M. (2020). An index to prioritize the preventive maintenance of medical equipment. *Health and Technology, 10(2),* 399–403.
17. Lu, L., Pan, J. (2021). Does hospital competition lead to medical equipment expansion? Evidence on the medical arms race. *Health Care Management Science, 24(3),* 582–596.
18. Park, J., Yim, K. (2021). Technical survey on the real time eye-tracking pointing device as a smart medical equipment. *Smart Media Journal, 10(1),* 9–15.
19. Yao, W., Wu, M., Wang, J. (2018). Internet of Things in centralized management of medical equipment. *2018 11th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, pp. 1–5. Piscataway, IEEE.
20. Kai, Y. (2020). Research on intelligent interactive system of medical equipment and sickbed. *2020 IEEE 2nd Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS)*, pp. 89–91. Piscataway, IEEE.
21. Verma, R., Kumari, A., Anand, A. (2022). Revisiting shift cipher technique for amplified data security. *Journal of Computational and Cognitive Engineering*. https://doi.org/10.47852/bonviewJCCE2202261
22. Jang, B., Kim, H. (2018). Indoor positioning technologies without offline fingerprinting map: A survey. *IEEE Communications Surveys & Tutorials, 21(1),* 508–525.
23. Zuo, Z., Liu, L., Zhang, L. (2018). Indoor positioning based on Bluetooth low-energy beacons adopting graph optimization. *Sensors, 18(11),* 3736.
24. Bahreini, R., Doshmangir, L., Imani, A. (2018). Affecting medical equipment maintenance management: A systematic review. *Journal of Clinical & Diagnostic Research, 12(4),* IC01–IC07.
25. Wani, A., Khaliq, R. (2018). SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL). *CAAI Transactions on Intelligence Technology, 6(3),* 281–290.

26. Wang, Y., Wang, Q., Chen, X., Chen, D., Fang, X. et al. (2020). Containerguard: A real-time attack detection system in container-based big data platform. *IEEE Transactions on Industrial Informatics, 18(5),* 3327–3336.
27. Xiong, H., Hou, Y., Huang, X., Chen, C. (2022). Heterogeneous signcryption scheme from IBC to PKI with equality test for WBANs. *IEEE Systems Journal, 16(2),* 2391–2400.
28. Qin, Z., Sun, J., Chen, D., Xiong, H. (2017). Flexible and lightweight access control for online healthcare social networks in the context of the Internet of Things. *Mobile Information Systems, 2017,* 1–15.
29. Xiong, H., Yang, M., Yao, T., Chen, J., Kumari, S. (2022). Efficient unbounded fully attribute hiding inner product encryption in cloud-aided WBANs. *IEEE Systems Journal, 16(4),* 5424–5432.
30. Ahmed, S., Alhumam, A. (2021). Unified computational modelling for healthcare device security assessment. *Computer Systems Science and Engineering, 37(1),* 1–18. https://doi.org/10.32604/csse.2021.015775
31. Turab, N., Abu Owida, H., Al-Nabulsi, J., Abu-Alhaija, M. (2022). Recent techniques for harvesting energy from the human body. *Computer Systems Science and Engineering, 40(1),* 167–177. https://doi.org/10.32604/csse.2022.017973
32. Tsai, M. H., Pan, C. S., Wang, C. W., Chen, J. M., Kuo, C. B. et al. (2019). RFID medical equipment tracking system based on a location-based service technique. *Journal of Medical and Biological Engineering, 39(1),* 163–169.
33. Yao, L., Shang, D., Zhao, H., Hu, S. (2021). Medical equipment comprehensive management system based on cloud computing and Internet of Things. *Journal of Healthcare Engineering, 2021(4),* 1–12.
34. Ni, M., Deng, H., He, X., Gong, X. (2021). A single pixel tracking system for microfluidic device monitoring without image processing. *Optics and Lasers in Engineering, 151,* 106875.
35. Gladson, S., Purusothaman, T. (2022). Lightweight and secure mutual authentication scheme for iot devices using coap protocol. *Computer Systems Science and Engineering, 41(2),* 767–780. https://doi.org/10.32604/csse.2022.020888
36. Ahmad, M., Al-Amri, J., Subahi, A., Khatri, S., Hussain, A. et al. (2022). Healthcare device security assessment through computational methodology. *Computer Systems Science and Engineering, 41(2),* 811–828. https://doi.org/10.32604/csse.2022.020097
37. Cao, S., Zhang, G., Liu, P., Zhang, X., Ne, F. (2019). Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. *Information Sciences, 485,* 427–440.
38. Zou, J., Ling, F., Shi, X., Xu, K., Wu, H. et al. (2021). An electromagnetic fiber acoustic transducer with dual modes of loudspeaker and microphone. *Small, 17(45),* 2102052.
39. Chen, D., Zhang, N., Qin, Z., Mao, X., Qin, Z. (2017). S2M: A lightweight acoustic fingerprints based wireless device authentication protocol. *IEEE Internet of Things Journal, 4(1),* 88–100.
40. Qin, Z., Zhao, P., Zhuang, T., Deng, F., Ding, Y. et al. (2023). A survey of identity recognition via data fusion and feature learning. *Information Fusion, 91,* 694–712.
41. Chen, D., Mao, X., Qin, Z., Wang, W., Li, X. et al. (2015). Wireless device authentication using acoustic hardware fingerprints. *Proceedings of Bigcom 2015*, pp. 193–204. Hangzhou, China.
42. Akkar, M., Giraud, C. (2001). An implementation of DES and AES, secure against some attacks. *Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 309–318. Berlin, Heidelberg, Springer.
43. Malone-Lee, J., Mao, W. (2003). Two birds one stone: Signcryption using RSA. In: *Topics in cryptology-CT-RSA 2003*, vol. 2612, pp. 211–225. San Francisco, CA, USA, Berlin, Heidelberg: Springer.
44. Chen, D., Zhang, N., Wu, H., Zhang, K., Lu, R. et al. (2022). Security techniques for secure device-to-device (D2D) communications. *IEEE Network, 36(6),* 54–59.
45. Faragallah, O., Farouk, M., El-Sayed, H., El-Bendary, A. M. (2022). Secure audio transmission over wireless uncorrelated rayleigh fading channel. *Computers, Materials & Continua, 70(1),* 1603–1615. https://doi.org/10.32604/cmc.2022.019710

46. Si, H., Cai, Y., Cheng, Z. (2010). An improved RSA signature algorithm based on complex numeric operation function. *IEEE International Conference on Challenges in Environmental Science and Computer Engineering*, pp. 397–400. Wuhan, China.

47. Christ, M., Braun, N., Neuffer, J., Kempa-Liehr, A. W. (2018). Time series feature extraction on basis of scalable hypothesis tests (tsfresh–A python package). *Neurocomputing, 307,* 72–77.