A Biometric-Based IoT Device Identity Authentication Scheme

Qingshui Xue[1(✉)], Xingzhong Ju[1], Haozhi Zhu[1], Haojin Zhu[2], Fengying Li[2], and Xiangwei Zheng[3,4]

[1] School of Computer Science and Information Engineering, Shanghai Institute of Technology, Shanghai 201418, China
xue-qsh@sit.edu.cn
[2] Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[3] School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China
[4] Shandong Provincial Key Laboratory for Distributed Computer Software Novel Technology, Jinan 250014, China

Abstract. IoT is an important part of the new generation of information technologies and the next big thing in the IT industry after the computer and the internet. The IoT has great development potential and a wide range of possible applications, especially commercial applications. And information security of the IoT is the key to the long-term development of the whole industry. Currently, the two most significant factors in the development of the IoT are user identity authentication and privacy protection. This paper contains an analysis on the current picture of inter-device user identity authentication in the IoT and proposes an inter-device biometric authentication solution for the IoT that's designed to work with larger devices, addressing the shortcomings of the traditional user identity authentication technologies including security and efficiency problems. A strategy for further solution optimization is also included. This paper elaborates on the specific process of user identity authentication carried out by users on devices and between devices making use of fingerprints. We'll demonstrate the security of this solution against existing attack methods and in the last part, we enumerate various possible applications of this solution in smart homes.

Keywords: IoT technologies · User identity authentication · Biometrics · Fingerprint recognition · Information security

1 Introduction

IoT is an important part of the new generation of information technologies and the next big thing in the IT industry after the computer and the internet. The definition of the IoT is simply an Internet network connected to objects. It refers to the connection with devices, users, systems, information resources and intelligent services, and information exchange and communication through the Internet to achieve intelligent identification, control, and intelligent services that are managed or monitored. The IoT can be

S. Han et al. (Eds.): AICON 2019, LNICST 287, pp. 139–149, 2019.
https://doi.org/10.1007/978-3-030-22971-9_12

integrated with the Internet through various wired and wireless networks, integrating a large number of sensors, intelligent processing terminals, global positioning systems, etc., to achieve inter-devices and human-and-devices connectivity anytime, anywhere, to achieve intelligent management and control [1].

The IoT technology is widely used in all aspects of our lives, from smart home, smart medical to intelligent transportation, smart city, the IoT is everywhere [20]. At present, the IoT technology is in the stage of rapid development, and it will have a wider impact and change our lives in the future. It is worth noting that while we enjoy the convenience of IoT technology for our lives, the development of the IoT is also faced with various challenges such as market fragmentation, lacking uniform access standards and inadequate equipment security [15]. Especially in terms of safety, this can directly harm the user's personal safety when a security problem occurs [8]. Therefore, reliable and effective security is the prerequisite for the continuous and stable operation of the IoT system [9]. User identity authentication and data privacy disclosure of IoT devices are the two main factors that constrain the rapid development of the IoT [19].

In smart home scenarios, smart door locks, smart cameras, and other devices all have strong user identity authentication security requirements, involving users in the life cycle of binding devices, using devices, and unbinding devices [7]. Currently, various authentication operations for these devices are usually based on account system services provided by the device manufacturer (for example, access to log in the mobile APP, the operating authority is obtained after the cloud user identity authentication). Due to the limitations of the username/password authentication method, the diversity of smart home device manufacturers, and the security of the produced devices, there are some security risks in the process of user identity authentication in some scenarios.

The hierarchical structure of the IoT system can be divided into three layers from bottom to top, namely the sensing layer, the network layer, and the application layer. The sensing layer is mainly composed of sensors, cameras, and other devices. Its main task is to collect and to identify static and dynamic information of objects by means of different types of sensors. The network layer mainly plays the role of transmitting and processing information about the IoT. The application layer is mainly responsible for the intelligent management and control of devices in the IoT.

Combined with the architecture of the IoT, scholars have proposed dynamic cryptography and static cryptography in authentication technology. Ke [2] proposed to solve the user identity authentication problem by using USB cryptography in the literature; Lin proposed to use the static cryptography to achieve Internet authentication in the literature [3]. However, the use of static passwords in the IoT environment can easily lead to low security of the system. In addition, as the main authentication method, digital certificates will increase the delay and reduce efficiency [4]. In order to solve the above problems, we propose a fingerprint-based inter-device biometric authentication solution for the IoT. At present, the fingerprint-based biometric authentication solution has been widely used for user identity authentication by users on devices [11], but it is rarely used in user identity authentication between devices. This article will focus on the research and application of fingerprint recognition in user identity authentication between devices.

2 Two Fingerprint-Based Inter-device Biometric Authentication Systems for the IoT

2.1 The Proposed Basic System

When we study the fingerprint-based inter-device biometric authentication solution for the IoT, we assume that all IoT devices have fingerprint information collection modules and the communication links are secure and reliable. Simultaneously, it is assumed that the communication key M1 between devices is secure and can't be stolen. Based on the schematic diagram of the IoT device user identity authentication process shown in Fig. 1, we develop a method based on fingerprint identification with IoT device identity authentication.

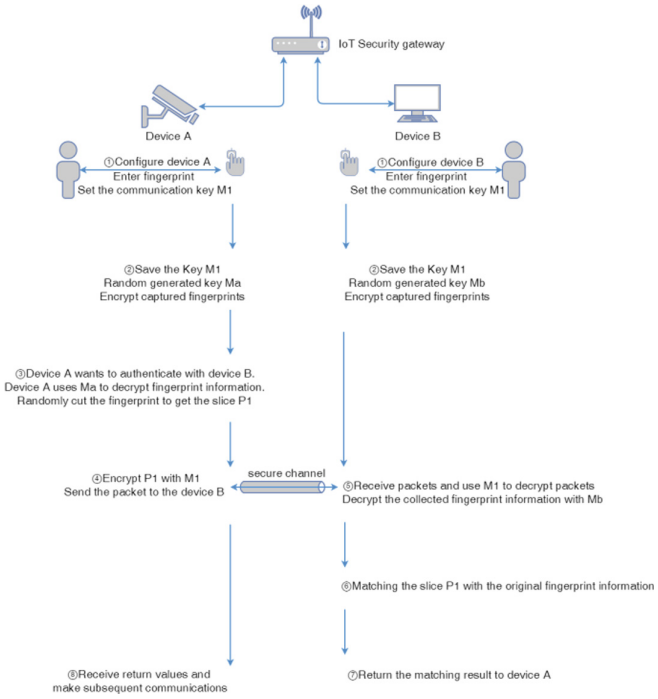

Fig. 1. IoT device identity authentication process map

Step1. The user logs in to the device configuration interface through the initial configuration account password of Device A and modifies the device management password. The device-related information is configured to enable the device to connect to the IoT security gateway. The fingerprint collection module enters fingerprint information and sets the device-to-device communication key M1 (Device B operates as above).

Step2. After Device A collects the fingerprint information of the user, Device A randomly generates a key Ma and uses a symmetric encryption algorithm to encrypt

and store the fingerprint information to ensure the security of the collected fingerprint information. At the same time, the device communication key M1 and the key is saved. Communication key M1 acts as a public key to encryption and decryption between devices (Device B operates as above).

Step3. Device A decrypts the stored fingerprint information with the secret key Ma firstly, When Device A wants to authenticate with Device B. After the fingerprint information is decrypted, Device A randomly cuts the fingerprint image to get a fingerprint slice P1 and ensures that the area of the slice P1 is not less than α % of the original fingerprint area.

Step4. Device A uses a symmetric encryption algorithm, uses the communication key M1 as an encryption key, encrypts slice P1, and transmits the encrypted data packet to Device B through trusted network channels.

Step5. After receiving the data packet sent by the Device A, the Device B decrypts the received data packet by using the stored communication key M1, and restores the plaintext information about the slice P1, and simultaneously decrypts the encrypted stored fingerprint information by using the secret key Mb to obtain the plaintext information of the fingerprint.

Step6. Device B matches the slice P1 with the original fingerprint information. When the similarity reaches β, the matching is successful, and the user identity of the sending method is confirmed. When the matching result does not meet the requirement, the user identity authentication fails. At the same time, the decrypted fingerprint is encrypted back.

Step7. When Device B matches successfully, the return value of the successful authentication is sent to Device A. When the match fails, the return value of the authentication failure is sent to Device A.

Step8. After Device A successfully receives the matching value of Device B and confirms the user identity of the sender of the return value, the user identity authentication process is completed, and subsequent operations such as communication, management, control or data sharing between devices can be performed. When device A receives the message of authentication failure, it will return to the step3–8 to restart authentication.

The participants in this system are: user, Device A, and Device B. The functional tasks for each participant are as follows:

Users: (1) Configure the device to connect the IoT security gateway normally and set the communication key of devices. (2) Input the fingerprint.

Device A: (1) Save the user-configured communication key. (2) Randomly generate the key Ma, encrypt and store the collected fingerprint information. (3) Decrypt the fingerprint information and randomly cut the fingerprint picture to obtain the fingerprint slice P1. (4) Encrypt fingerprint slice P1 with communication key M1 and send it to Device B. (5) Receive the return result of Device B for subsequent communication.

Device B: (1) Save the user-configured communication key M1. (2) Randomly generate the secret key Mb to encrypt and store the collected fingerprint information. (3) Receive the encrypted data packet sent by Device A. (4) Decrypt the data packet to obtain the slice P1. (5) Decrypt the original fingerprint information to get the complete fingerprint. (6) The fingerprint slice is matched with the original fingerprint information. (7) The matching result is returned to Device A.

The specific information interaction process is shown in Fig. 2.

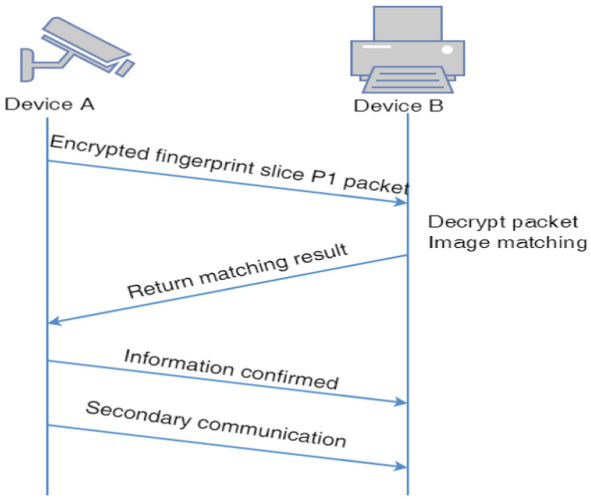

Fig. 2. Information exchange in the basic inter-device biometric authentication system

2.2 The Improved System

In the above solution, the premise of our research is that each IoT device has a module for collecting fingerprint information of the user. Considering the actual situation and equipment production cost, some devices may not have a fingerprint collection module. In order to solve this problem and optimize user experience, we further improved the solution. We also assume that the communication link is secure and trustworthy and that the communication key M1 between the devices is secure and cannot be stolen.

In the improved system, we design the task of fingerprint collection and encryption by the IoT security gateway. The specific steps are as follows:

Step1. The user logs in the device configuration interface through the initial configuration account and password of the IoT security gateway, and modifies the device management password; configures device related information; inputs the fingerprint through the fingerprint collection module, and sets the communication key M1 among devices.

Step2. The IoT security gateway stores the communication key M1 and uses M1 to encrypt the collected fingerprint information. When the user completes the first configuration, the password and fingerprint matching is needed for the second configuration modification to enter the gateway configuration interface and modify the gateway configuration. This will prevent an attacker from a malicious attack on the security gateway device.

Step3. When a new Device A needs to join the network, the user logs in to the device configuration interface through the initial configuration account password of Device A, and modifies the device management password; configures device-related

information to enable the device to connect to the IoT security gateway normally and set the communication key M1 between devices.

Step4. After the gateway detects that the new device is normally connected to the network, the intelligent gateway first encrypts a string of characters with the communication key M1and sends it to the Device A. After Device A receives the data packet of the gateway, it uses the communication key M1 to unlock the data packet. And send the unwrapped string to the intelligent gateway.

Step5. After the smart gateway receives the decrypted information of Device A, it compares with the string sent by the smart gateway. After the comparison is successful, the smart gateway will send the fingerprint information encrypted by the communication key M1 to Device A, so that Device A can receive the encrypted fingerprint information.

Similarly, when Device B needs to join the network, the above steps will also be performed to obtain the encrypted fingerprint information. When Device A and Device B are authenticated, the subsequent authentication process will be the same as that of step3–step8 in the 2.1 basic solutions, except that in step 3 and step 5, the secret key Ma and Mb are no longer needed to decrypt the fingerprint information and only the communication key M1 is needed to decrypt fingerprint information.

Of course, for some devices with fingerprint collection module, we can manually select whether the input of fingerprint information needs to be obtained from the intelligent gateway in the configuration interface. If necessary, the fingerprint collection will be sent from the gateway to the device. If not, the above steps will not be performed.

The participants in this solution are: user, intelligent gateway, Device A and Device B. The tasks that participants need to accomplish are as follows:

User: (1) Configure the device communication key M1. (2) Enter the fingerprint and complete the fingerprint collection.

Intelligent gateway: (1) Save the user-configured communication key M1. (2) Encrypt and store fingerprint information. (3) Use the communication key M1 to encrypt random string to verify Device A. (4) After receiving the correct return value of Device A, send the encrypted fingerprint information to Device A.

Device A: (1) Save the user-configured communication key M1. (2) Receive and decrypt the encrypted data packets sent by the intelligent gateway and result to the intelligent gateway. (3) Receive and store the fingerprint information encrypted data packets sent by the intelligent gateway. (4) Decrypt the fingerprint information and randomly cut fingerprint pictures to get the fingerprint slice P1. (5) Encrypt fingerprint slice P1 with the communication key M1 and send it to Device B (6) receive the return result of Device B for subsequent communication.

Devices B: (1) Save the user-configured communication key. (2) Receive and decrypt the encrypted data packet sent by the intelligent gateway and return the result to the intelligent gateway. (3) Receive and store the encrypted data packets sent by the intelligent gateway. (4) Receive the encrypted data packets from Device A and decrypt the data packets to get slice P1. (5) Decrypt the original fingerprint information and get the complete fingerprint. (6) Match the fingerprint slice with the original fingerprint information. (7) Return the matching result to Device A. The specific information interaction process is shown in Fig. 3.

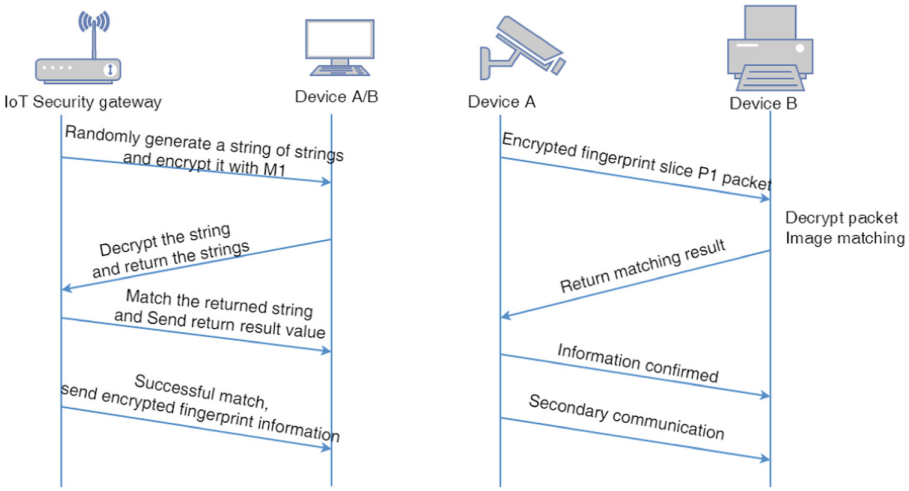

Fig. 3. Information exchange in the improved inter-device biometric authentication system

3 Performance Analysis of the Fingerprint-Based Inter-device Biometric Authentication Solution for the IoT

IoT technology integrates the Internet, mobile Internet, wireless communication network and various wireless sensor network technologies [14]. The complex structure and rich application scenarios make IoT security more serious than traditional network security [16]. Specifically, on the issue of user identity authentication, the challenge of user identity authentication faced by the IoT is far greater than that of traditional networks.

In order to consider the feasibility and security of fingerprint-based inter-device biometric authentication solution for the IoT comprehensively, we will analyze and demonstrate this solution form the following aspects.

3.1 Feasibility Analysis of the Fingerprint-Based Inter-device Biometric Authentication Solution for the IoT

Fingerprints have become a synonym of biometric recognition because of its lifetime invariance, uniqueness and convenience [17]. At present, fingerprint recognition is quite mature as an identification technology and has a solid market backing [13]. Fingerprint recognition technology can extract the feature values extracted from fingerprints by analyzing the global features of fingerprints and local feature points such as ridge, valley and end points, bifurcation points or divergence points, so as to reliably identify a user's identity through fingerprints [18]. On average, each fingerprint has several unique and measurable feature points, each feature point has about seven features, and our ten fingers produce a minimum of 4,900 independently measurable features, which is sufficient to prove that fingerprint recognition is a more reliable identification method [5].

At present, the mainstream of the market is to apply fingerprint identification with the user identity authentication by users on devices. Our solution further promotes fingerprint identification with the user identity authentication between devices. And the reliability of the user identity authentication method can be subjectively controlled by the user, and the user only needs to input more finger fingerprints, which can greatly improve the security of user identity authentication between devices.

3.2 Comparison of Fingerprint-Based Inter-device Biometric Authentication Solution for the IoT and How Current User Identity Authentication on IoT Devices Works

At present, the methods of user identity authentication on IoT devices mainly include: based on user knowledge such as user name and password, dynamic password [12] and other software and hardware devices such as smart cards owned by users [10]. The solution adopts a two-factor authentication method combining password and fingerprint in the user identity authentication between the user and the device, which is more secure than the single-factor or two-factor authentication methods of the traditional password and the dynamic password. Similarly, compared with smart cards and other authentication methods, this solution is more convenient and fast, and the fingerprint recognition is extended to the user identity authentication between devices. Due to the unique and complex characteristics of fingerprints, the security of the solution is guaranteed in user identity authentication between devices.

3.3 Performance Comparisons Between the Basic and Improved Systems

The main difference between the basic system and the improved system is that the basic system requires each device to have a fingerprint collection function, and the improved system only requires the intelligent gateway to have a fingerprint collection function. Compared with the basic system, the improved system has the following advantages: (1) it does not need the fingerprint acquisition module on each device to reduce the cost of equipment production. (2) The user does not need to perform fingerprint collection of each device, thereby reducing user intervention. The operation is more convenient. (3) It is difficult to ensure that the collected information is consistent because each fingerprint is collected, so the success rate is higher when the fingerprint is matched.

3.4 Security Analysis of the Fingerprint-Based Inter-device Biometric Authentication Solution for the IoT

The main security threats currently faced by IoT authentication included user identity-based forgery, eavesdropping-based attacks, user identity-based forgery, and eavesdropping combined attacks, data manipulation-based attacks, and service availability attacks [6].

In order to prevent attackers from illegally registering Device And stealing the communication key M1 and user fingerprinted information between the devices, the solution adopts this method: in the basic system, we assume that each device has a fingerprint collection function, after completing the first configuration, users need to

use double authentication of account password and fingerprint to log in normally in the second time you log in again. When viewing or modifying important parameters (such as communication keys), the current device needs to verify the fingerprint information again and requires the smart gateway to authorize the changes. For the collected fingerprint information, the smart device randomly generates a key for encrypted storage and ensures that the stored fingerprint information is secure again. In the improved system, we do not require each IoT device to have a fingerprint acquisition module. However, in order to ensure the security of the device, you need to log in to other devices to view the configuration information after you log in to the smart gateway for the second time. Also, when viewing or modifying important parameters (such as communication keys), you need to verify the fingerprint information on the smart gateway, and you can view the changes after authorization.

In the solution, we assume that the communication key to devices is not stolen, and the transmission channel is safe and reliable. In order to prevent the attacker from intercepting the intercepted fingerprint information about the transmission, we take the form of fingerprint random cutting (Random cutting means that the shape of the slice is arbitrary, and the ratio of the cut area is larger than the programmed value α %). Only randomly cut fingerprint slices are transmitted during each verification process, and the slices are encrypted using a symmetric encryption algorithm. This ensures that even if the packet is intercepted, the attacker cannot obtain the complete fingerprint information.

4 Application Scenarios of Fingerprint-Based Inter-device Biometric Authentication Solution for the IoT

In the fingerprint-based inter-device biometric authentication solution for the IoT, the device needs to perform image encryption and decryption, image segmentation and image comparison, which have certain requirements on the performance and computing processing capability of the device. At present, we only consider the system to be applied to an inter-device biometric authentication system with a relatively large device size and relatively strong computing processing capability. We will use this program to do application scenario analysis in a smart home.

Suppose Andy ends his busy day's work and prepares to go home. He plans to go home and have a hot bath. Andy opens the IoT device client installed on the mobile phone. After successful login through fingerprint matching, the mobile phone client randomly encrypts the fingerprint information and sends it to the smart water heater at home. The smart water heater decrypts the fingerprint slice sent by the mobile phone to perform fingerprint image matching. After the matching is successful, the device is in a controlled state, and Andy remotely turns on the smart water heater, and the water will be heated to a suitable temperature. At the same time, after the smart gateway communicates with the mobile APP, the APP will obtain the location of Andy, and estimate the time required for Andy to arrive at the smart gateway through the cloud service. When it is calculated that Andy will arrive home after about 20 min, the intelligent gateway will perform device authentication with the air conditioner, encrypt the randomly segmented fingerprint slice and send it to the smart air conditioner. After the

smart air conditioner receives the information and decrypts it successfully, the air conditioner controls the air conditioner according to the temperature sensor. To the temperature data, the automatic opening adjusts the indoor temperature to a comfortable range. After Andy arrives at the door of the house, the door is opened by the fingerprint lock. At the same time, after the fingerprint lock receives the door opening command from Andy, the command to automatically turn on the light is sent to the smart light fixture. The smart light fixture automatically determines whether the light needs to be turned on according to the data of the light sensor. When Andy arrives home, the Bluetooth speaker will play Andy's favorite songs according to Andy's daily hobbies, so Andy can soak in a hot bath in a comfortable room.

5 Conclusions

This paper presents a fingerprint-based authentication solution for IoT devices. This solution not only applies fingerprint recognition by users on devices but also extends it to devices. Through a series of steps such as random cutting of fingerprints, encrypted transmission of slices, decryption and image matching, the process of user identity authentication between devices through fingerprints is completed. And for the possible existence of IoT identity authentication attacks, corresponding solutions are proposed, which greatly improves the security and reliability of user identity authentication between devices as well as users and devices. It is also noteworthy that this solution requires that the device must be able to perform image segmentation, encryption and decryption, image matching and other operations, so it has certain requirements for the operating performance of the device, and is more suitable for the relatively large equipment, relatively strong computing capacity, and relatively centralized equipment distribution scenarios. At the same time, how to continue to optimize the solution so that it can be applied to more relatively small computing capacity of relatively weak equipment is the direction of future research.

Acknowledgments. This paper is supported by NSFC under Grant No. 61672350 and 61373 149, NSSFC under Grant No. 16BGL003, Ministry of Education Fund under Grant No. 39120 K178038 and 14YJA880033, SIT Collaborative innovation platform under Grant No. 3921NH 166033, and SIT Foundation for Distinguished Scholars under Grant No. 39120K176049. We are also grateful for the support of the National Natural Science Foundation of China (61170227).

References

1. Chuankun, W.: An overview on the security techniques and challenges of the Internet of things. J. Cryptologic Res. **2**(1), 40–53 (2015)
2. Ke, J., Zhou, P., Jing, X.: Mixed parameters of differential and weighted mel cepstrum used in speaker recognition. Microelectronics Comput. **31**(9), 89–91 (2014)
3. Lin, W., Wang, X.: One-time password authentication protocol based on non-homogeneous linear equations. Comput. Eng. **36**(13), 154–155 (2010)
4. Zhang, M., Ma, Z., Zhang, X., Gao, F.: An identity authentication scheme on IoT. Designing Tech. Posts Telecommun. 19–22 (2017)

5. Wang, A., Guo, Y., Wang, X.: An introduction to identification and authentication technology. Comput. Appl. Softw. (2002)
6. Internet Finance Authentication Alliance. https://ifaa.org.cn/whitebook. Accessed Sept 2018
7. IoT Security Guidelines for IoT Endpoint Ecosystem. http://www.gsma.com/connectedliving. Accessed 23 May 2017
8. Chuankun, W.: Security Fundamentals for Internet of Things. Science Press, Beijing (2013)
9. IoT Security Guidelines Overview Document. http://www.gsma.com/connectedliving. Accessed 23 May 2017
10. Lee, S., Ong, I., Lim, H., et al.: Two factor authentication for cloud computing. J. Inf. Commun. Convergence Eng. **8**(4), 427–432 (2010)
11. Yuan, J., Jiang, C.: A biometric-based user authentication for wireless sensor networks. Wuhan Univ. J. Nat. Sci. **15**(3), 272–276 (2010)
12. Das, A.K., Chatterjee, S., Sing, J.K.: Formal security verification of a dynamic password-based user authentication scheme for hierarchical wireless sensor networks. Commun. Comput. Inf. Sci. **2**(1), 78–102 (2013)
13. Periaswamy, S.C.G., Thompson, D.R., Di, J.: Fingerprinting RFID tags. IEEE Trans. Dependable and Secure Comput. **8**(6), 938–943 (2011)
14. Ai, Y.X., Mei, L.X.: Security characteristic and technology in the Internet of Things. Network Secur. Technol. Appl. **30**(4), 20–29 (2013)
15. National Internet Emergency Response Center: China Internet Network Security Report 2016. People's Posts and Telecommunications Publishing House, Beijing (2017)
16. Bertino, E., Islam, N.: Botnets and Internet of Things security. Computer **50**(2), 76–79 (2017)
17. Zhang, N., Zang, Y.-L., Tian, J.: The integration of biometrics and cryptography—a new solution for secure identity authentication. J. Cryptologic Res. **2**, 159–176 (2015)
18. Long, W., Sun, D.: Research on security and user privacy of biometric authentication solution. Secret Sci. Technol. (2014)
19. Li, C., Xin, Y., Niu, X., et al.: Identity authentication scheme based on biometric certificate. Comput. Eng. **33**(20), 165–167 (2007)
20. Xiao, W.U., Jian-Ping, Z., Chu-Hua, L., et al.: Application of Internet of Things in smart home. Internet Things Technol. (2012)