# IoT Security Access Authentication Method Based on Blockchain

Yang Cheng(✉), Min Lei, Shiyou Chen, Zigang Fang, and Shuaipeng Yang

Information Security Center,
Beijing University of Posts and Telecommunications, Beijing, China
chengyangmc@bupt.edu.cn

**Abstract.** With the rapid development of Internet of Things (IoT), The IoT terminal are diversified, and the attack points available to attackers are also diversified, and most IoT terminal are more vulnerable to attacks because they are less secure. In order to achieve secure access of IoT terminal, ensure the legality of IoT terminal accessing the network, improve the security of terminal entering the network and reduce the security risks that IoT terminal may be exposed to when accessing the platform. This paper proposes a secure method to access to the IoT, which is to use the blockchain to store and verify the fingerprint information of the terminal, thereby improving the security of the IoT terminal accessing the cloud. And this paper also proposes a method to store the fingerprint blockchain of the terminal in the IoT terminal, and then verify the collected fingerprint information through the data in the blockchain to ensure the credibility of the fingerprint information.

**Keywords:** IoT · Access authentication · Blockchain

## 1 Introduction

The rapid development of IoT technology has brought society into the era of interconnection of all things. Under the background of full connection of people and things, the number of IoT terminal has grown rapidly. However, while the IoT is booming, it also exposes many security problems. Traditional security protection technology can not adapt to the new security situation of the IoT. The effective security defense system and security ecology between the IoT server, IoT terminal and communication network have not yet been established. In addition, with the IoT terminal joining the Internet, attackers can use a wider range of attacks, the terminal itself is less secure, more vulnerable to attacks. Security risk has become the biggest hidden danger in the application of the IoT. Attacks, hijackings and data embezzlement against IoT terminal are increasing day by day.

Security mechanism is one of the key technologies that determines the success of network convergence. In particular, access authentication mechanism is the first step to implement security protection. Since the implementation of the access authentication mechanism adopted by different networks is quite different, it is difficult to design an access authentication mechanism in the IoT environment enables the terminal to roam


G. Gui and L. Yun (Eds.): ADHIP 2019, LNICST 302, pp. 229–238, 2019.
https://doi.org/10.1007/978-3-030-36405-2_24

and enjoy services seamlessly among various wireless networks. And it has become a major technical challenge when converging networks. The existing technology combines IoT and blockchain are mostly used in networking and asset management, there is almost no involvement in IoT security access authentication. And many existing study on the technology of IoT access authentication are mostly innovative in the identity authentication and ignore the security of terminal information. This paper proposes a method to store the fingerprint blockchain in the IoT terminal, and then verify the collected fingerprint information through the data in the blockchain to ensure the credibility of the fingerprint information. The fingerprint information mentioned in this paper refers to the identity information of IoT terminal. In order to allow access to the cloud and send authentication requests, this will greatly reduce the possibility of an attacker simulating a legitimate terminal for cloud intrusion. At the same time, this paper uses the two-way HTTPS protocol and HMAC authentication technology, which effectively prevents man-in-the-middle attacks and ensures data integrity and confidentiality.

## 2 Related Work

### 2.1 Blockchain

Blockchain is a distributed database system in which nodes participate [1]. It is a supporting technology in Bitcoin applications. In 2008, Nakamoto put forward the concept of "blockchain" in Bitcoin White Paper, and created the Bitcoin social network and developed the first block called "Creation Block" in 2009. The blockchain contains a list of blocks that are constantly growing and neatly arranged. Each block contains a timestamp and a link to the previous block, so that the data in blockchain is designed to be unchangeable [2]. Once recorded, the data in one block will be irreversible. Therefore, it is unchangeable and unforgeable. Bitcoin records every transaction in the application on the blockchain ledger to ensure it can't be changed and can be traced back [3]. Since the successful application of Bitcoin, blockchain technology has begun to receive attention, it has been separated from bitcoin applications and played an important role in the fields of finance, education, and medical care. Blockchain can be divided into "data blocks" and "links". Its data block is a block generated by a blockchain network at intervals [4]. All data in the database is stored in each data block. The block information is encrypted with a password and hashed to ensure the integrity and correctness of the data in the block [5]. The information written on the blockchain will be verified by all nodes on the network to ensure that the information safety and efficiency. Once the information is written, it is difficult to modify or delete.

### 2.2 IoT Access Authentication

The IoT terminal access authentication technology is mainly used to check the identity of the terminal identity when access to the net. There is an authentication module in the terminal, which stores the digital certificate issued by the authority in a hardware encryption authentication card having a security encryption function and an identity authentication function [6]. Before the terminal accesses to the internal network, the terminal must pass the identity verification performed by the hardware encryption

authentication card and the authentication server, so that it can ensure only the terminal that passes the network authentication can access to the intranet [7]. If not, the terminal will be refused to get the service.

IoT terminal device access authentication is a popular technology in the intranet security system, and preform several trends as follows [8]:

1. The terminal access authentication technology based on multiple technologies. At present, among the three commonly used access authentication technologies, NAC and NAP have become alliances, in another word, the network access device uses Cisco's NAC technology, and the host client uses Microsoft's NAP technology to achieve a complementary situation.
2. Access authentication mechanism based on multi-layered protection. Terminal access authentication is the portal of the internal network of the enterprise. To ensure the secure access of the terminal, it is necessary to authenticate and check the legitimacy and security of the access terminal from multiple levels.
3. Standardization of access authentication technology.

At present, although the technical principles of the access control schemes of various vendors are basically the same, the implementation methods of the various vendors are different, and the main difference is represented by the protocol [9]. For example, Cisco and Huawei chose to implement access control by adopting EAP protocol, RADIUS protocol and 802.1x protocol [10]. Microsoft chose to adopt DHCP and RADIUS protocol, while other vendors are still launching their own network standards. Entry and control standards [11]. Standards and norms are the footstone of the long-term development of technology. Therefore, standardization is the inevitable trend of access authentication technology development [12].

## 3 Algorithm Process

The architecture of the IoT is usually divided into three layers: "terminal", "pipe", "cloud", also the architecture representation of "end-pipe-cloud", where "end" means the terminal, "pipe" means the network transport layer, and "cloud" means the IoT cloud. IoT terminal generally has limited by its function, the level of security protection is not enough, and the number is widely distributed. Once a certain type of terminal has serious security problems, the scope of impact will be unimaginable. The terminal fingerprint refers to the terminal characteristics that can identify the terminal. The terminal fingerprint can be generated by the terminal's explicit identifier, which is an inherent identifier of the terminal can uniquely identify the terminal, such as the terminal's hard ID. Simultaneously, terminal fingerprints can be generated from the feature set of terminal implicit identifiers as well, such as terminal name, model, function and so on. The security access scheme of terminal on the perception layer makes use of the unique identification feature of terminal fingerprints to authenticate the identity of terminal in the IoT as a criterion for judging whether they are allowed to access the IoT. And the communication layer is protected by the two-way HTTPS protocol and HMAC technology at the transport layer at the same time. However, in the process of collecting fingerprint information, there is no security mechanism to

improve the unforgeability of fingerprint information. This is an urgent problem to be solved for the secure access of IoT terminal. The access authentication method proposed in this paper mainly covers three parts: the collection of fingerprint information of the IoT terminal, the verification of fingerprint information and the access to the cloud. The overall architecture of the method is shown in Fig. 1.

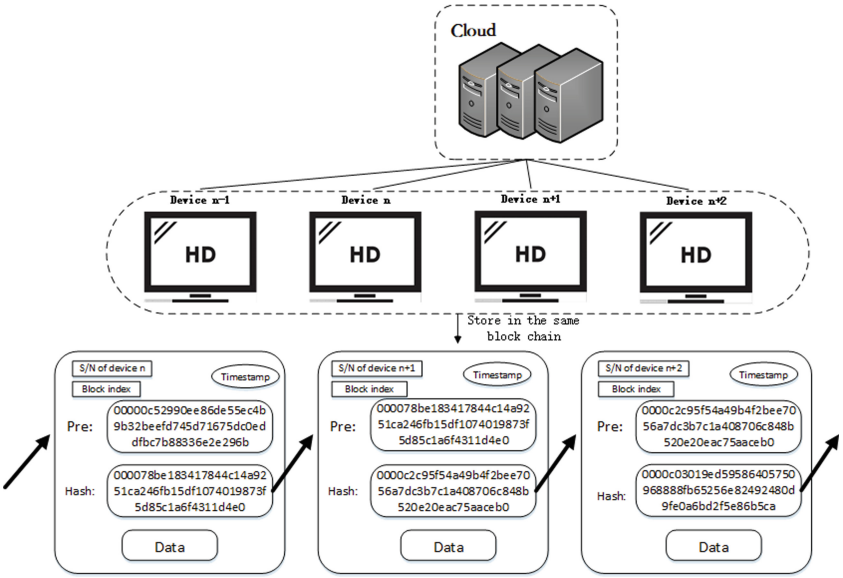


**Fig. 1.** Overall architecture.

### 3.1 Terminal Fingerprint Collection

In this paper, the terminal needs to collect its relevant information itself by its API interface as fingerprint P. before accessing to the IoT cloud.

The terminal fingerprint information P is a combination of a plurality of identifiers of the terminal, and includes two types of identifiers: an explicit identifier and an implicit identifier. The explicit identifier can uniquely identify the terminal, including the terminal serial number, terminal MAC address, user ID number, etc. In this paper, the terminal serial number and the terminal MAC address are used as the explicit identifier of the terminal, which can be obtained through a built-in shell script. The implicit identifier does not have the ability to uniquely identify. A single implicit identifier cannot uniquely identify the terminal. However, if multiple invisible identifiers are combined, the identification capability can be effectively improved. The implicit identifier can be invoked by the terminal. The interface is obtained by taking a smart camera as an example, including screen resolution, audio coding type, and terminal running frequency. In actual operation, for a certain terminal, the self-information l(x) amount and information entropy H(x) of the implicit identifier are calculated as the basis for selecting the implicit identifier. The self-information amount of the identifier is the variation of the terminal information. when tampering, the

amount of the self-information is inversely proportional to the probability of passing the next verification, the information entropy contained in the identifier represents the weight of the terminal fingerprint as a whole.

$$1(x) = \log_2(1/p(x)) \tag{1}$$

$$H(x) = E[l(x_i)] = E[\log_2(1/p(x_i))] = -\sum p(x_i)\log_2 p(x_i) \tag{2}$$

### 3.2 Fingerprint Verification

In the built-in blockchain of the terminal, it extracts the data of the latest block B related to the terminal, and compare the terminal fingerprint P and the terminal account and password with the fingerprint recorded in the block B. Then it will determine whether it is allowed to access to the cloud and update information (the blockchain needs to be updated at the same time when updating the information).

The blockchain is distributed and stored in each terminal of the same type, that is, the blockchain contains fingerprint information of all terminal of the type. At the initial shipment of terminal, the initial blockchain is stored in the terminal, and each block in the initial blockchain stores relevant fingerprint information of the terminal according to the factory specific serial number of the terminal. Each block data is as shown in Fig. 2, and includes three parts, part 1 is explicit identifier dictionary which includes device S/N and MAC address, part 2 is recessive identifier dictionary and part 3 is the account and a key encrypted by the terminal initial public key, and the encryption algorithm is SM2.

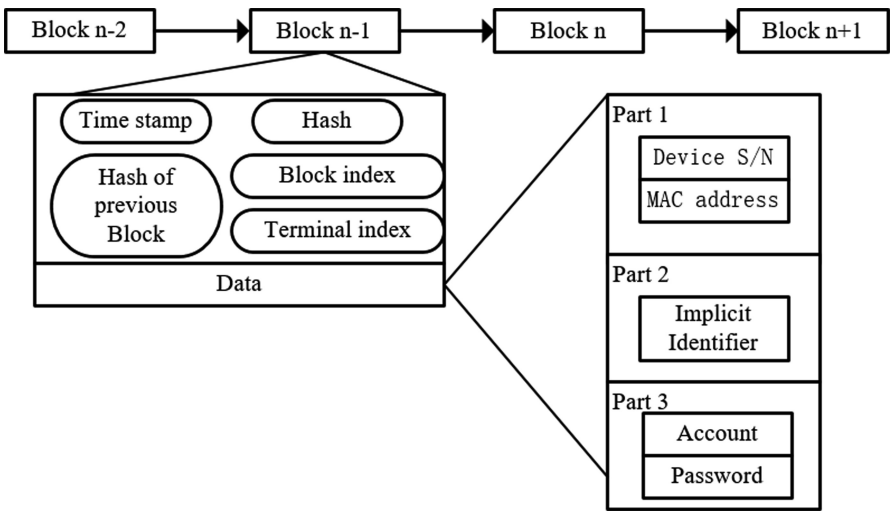


**Fig. 2.** Data in each block.

The whole system is a weakly centralized structure. The blockchain is a coinless blockchain, and the cloud is responsible for generating new blocks. Whenever a new

block is generated, the cloud will also send blockchain update data to each terminal to ensure that the blockchain information of each terminal is consistent. When a blockchain of a terminal is maliciously tampered, then the authentication will fail in HMAC authentication.

The matching algorithm is shown in Fig. 3. The specific steps are as follows:

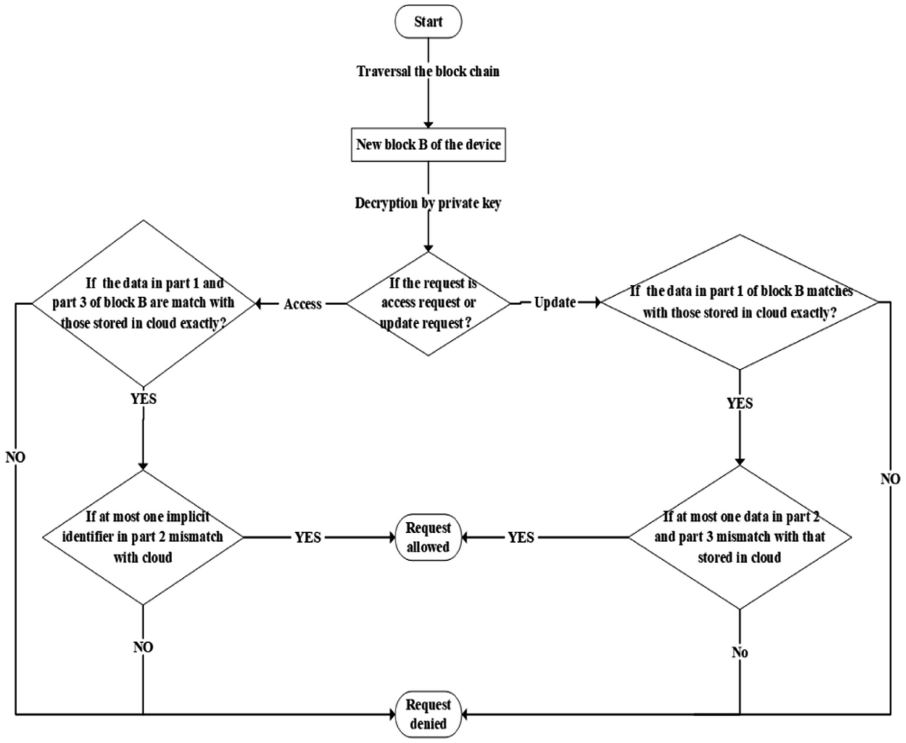


**Fig. 3.** Matching algorithm.

1. Traverses the data information of the latest block B related to the terminal, and decrypts the data of the three parts by using the private key.
2. Determine whether to access the cloud request or update the information request.
3. When the request is for accessing the cloud request, the data information of each part needs to be matched one by one, and if it cannot be matched one by one, the access to the cloud is denied. Since the implicit identifier of the terminal may change due to the small probability of the access environment, If at most one of the invisible identifiers does not match, the part 2 is judged to be matched, when the request is updated, the part 1 information is first, and if the part 1 information is matched, the matching determination of the part 2 and the part 3 is performed. When at most one of them does not match the blockchain information, the request is considered a legitimate update request. Assume that the update request completes the authentication. After the cloud confirms the request for the update information,

the cloud will generate a new block access blockchain based on the update information, and deliver the updated blockchain to each terminal.

### 3.3 Access to the Cloud

After verifying the fingerprint information P through the blockchain, the terminal will send an authentication request to the cloud, where the two-way HTTPS authentication and the adaptation of the blockchain HMAC authentication will be used. Pass through to complete the access operation.

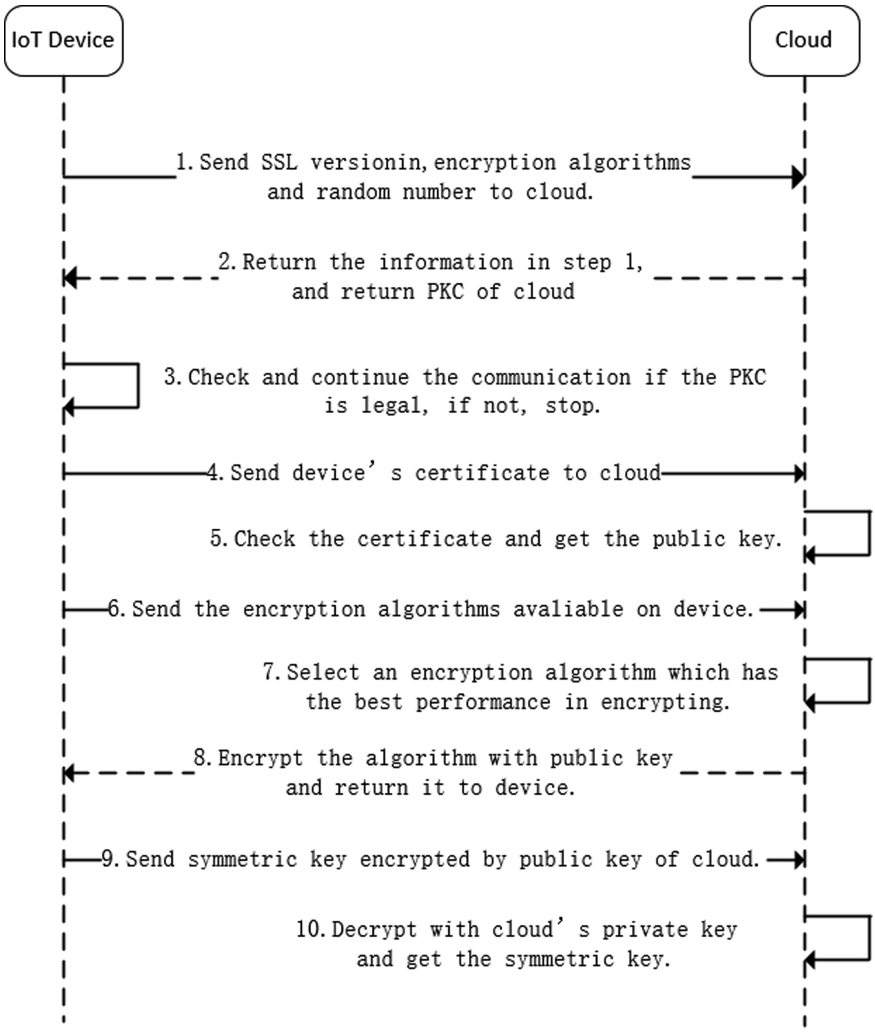


**Fig. 4.** The two-way HTTPS authentication.

The prerequisite for the two-way HTTPS authentication is that there are two or more certificates, one is a cloud certificate, and the other is a terminal certificate. The cloud saves the certificate of the terminal and trusts the certificate, and the terminal stores the certificate of the cloud and trust the certificate. In this way, the request response can be completed if the certificate verification is successful. As shown in Fig. 4.

The principle of the HMAC authentication is that the terminal initiates a request to the cloud, and the request encapsulates the blockchain information of the terminal, and the cloud verifies whether the blockchain information of the terminal is consistent with the blockchain information stored by the terminal. If the verification fails, the access is denied. When the verification succeeds, the cloud generates a random number and sends it to the terminal. After receiving the random number, the terminal hashes it with the private key to get the summary information H, and sends it to the cloud, the cloud hash the terminal's secret key from its own database with random numbers to get abstract message H'. The cloud compares the message H with H', and establish a connection to process the request from the terminal if verification succeeds.

The cloud will preferentially process the normal access authentication request of each terminal, and then process the update information request, and the update information request of each terminal also needs to be controlled by a certain amount in a unit time, thereby controlling the block speed of cloud.

The key used in the HAMC authentication process is agreed by both parties in advance, and it is impossible for a third party to know. As can be seen from the entire process of HAMC authentication in Fig. 5, the attacker can only intercept the random number as a "challenge" and the HMAC result as a "response", and cannot calculate the key based on the two data. Because the key is not known, the attacker cannot forge the correct response. At the same time, since the "challenge" random number obtained by each request is different, the attacker cannot replay the request, so the data security of the IoT device interacting with the cloud during the access authentication process can be ensured.

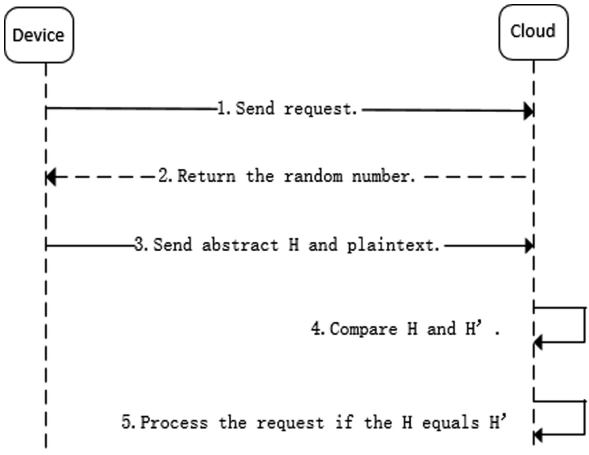


**Fig. 5.** The HAMC authentication.

## 4 Conclusion

With the rapid development of the IoT, more and more smart terminal are connected to the network for our lives. Along with the explosive growth of equipment access, the management and maintenance of centralized management solutions are under great pressure, and the disadvantages are gradually highlighted, accompanied by a single point of trust. In face of the rapid growth of access to IoT terminal, this paper analyzes the access authentication technologies that are available at present and proposes their existing problems: forgery. And then, proposing the research content of the paper, combining with blockchain technology to complete fingerprint information collection, storage and verification. At the same time, this paper considers the security in the process of information transmission, and uses the two-way HTTPS protocol and HMAC technology to protect the communication data.

**Acknowledgments.** This work is supported by the National Key R&D Program of China (2017YFB0802703), National Natural Science Foundation of China grant (U1836205), Major Scientific and Technological Special Project of Guizhou Province (20183001), Open Foundation of Guizhou Provincial Key Laboratory of Public Big Data (2018BDKFJJ014), Open Foundation of Guizhou Provincial Key Laboratory of Public Big Data (2018BDKFJJ019) and Open Foundation of Guizhou Provincial Key Laboratory of Public Big Data (2018BDKFJJ022).

## References

1. Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C.: Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In: 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, pp. 839–858. IEEE (2016)
2. Ouaddah, A., Elkalam, A.A., Ouahman, A.A.: Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In: Rocha, Á., Serrhini, M., Felgueiras, C. (eds.) Europe and MENA Cooperation Advances in Information and Communication Technologies. AISC, vol. 520, pp. 523–533. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-46568-5_53
3. Ouaddah, A., Elkalam, A.A., Ouahman, A.A.: A new blockchain-based access control framework for the internet of things. Secur. Commun. Netw. **9**(18), 5943–5964 (2016)
4. Di Francesco Maesa, D., Mori, P., Ricci, L.: Blockchain based access control. In: Chen, L. Y., Reiser, H.P. (eds.) DAIS 2017. LNCS, vol. 10320, pp. 206–220. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-59665-5_15
5. Le, T., Mutka, M.W: CapChain: a privacy preserving access control framework based on blockchain for pervasive environments. In: 2018 IEEE International Conference on Smart Computing (2018)
6. Pinno, O.J.A., Gregio, A.R.A., De Bona, L.C.E.: ControlChain: blockchain as a central enabler for access control authorizations in the IoT. In: 2017 IEEE Global Communications Conference, GLOBECOM 2017, Singapore, pp. 1–6. IEEE (2017)
7. Dorri, A., Kanhere, S.S., Jurdak, R.: Towards an optimized BlockChain for IoT. In: 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), Pittsburgh, PA, pp. 173–178. IEEE (2017)
8. Novo, O.: Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J. **5**(2), 1184–1195 (2018)

9. Lunardi, R.C., Michelin, R.A., Neu, C.V., Zorzo, A.F.: Distributed access control on IoT ledger-based architecture. In: 2018 IEEE/IFIP Network Operations and Management Symposium, NOMS 2018, Taipei, pp. 1–7. IEEE (2018)
10. Ourad, A.Z., Belgacem, B., Salah, K.: Using blockchain for IOT access control and authentication management. In: Georgakopoulos, D., Zhang, L.-J. (eds.) ICIOT 2018. LNCS, vol. 10972, pp. 150–164. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-94370-1_11
11. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., Wan, J.: Smart contract-based access control for the internet of things. IEEE Internet Things J. **6**(2), 1594–1605 (2019)
12. Bao, Z., Shi, W., He, D., Chood, K.K.R.: A three-tier blockchain-based IoT security architecture (2018)