2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)

Unified Authentication Scheme for IoT Blockchain Based on PUF

Dawei Li[1], Yingxian Song[1], Lixin Zhang[1], Di Liu[1], Baoquan Ma[2,3], Zhenyu Guan[1] ✉
[1]School of Cyber Science and Technology, Beihang University, Beijing, China
[2]National Engineering Laboratory for Industry Control System Information Security Technology, Beijing, China
[3]National Computer System Enginering Research Institute of China, Beijing, China
lidawei@buaa.edu.cn, songyingxian@buaa.edu.cn, zhanglixin0319@buaa.edu.cn,
liudi2020@buaa.edu.cn, mabq@ncse.com.cn, guanzhenyu@buaa.edu.cn

***Abstract*—The number of global Internet of Things devices has increased rapidly and has a wide range of application markets. Access authentication methods for massive heterogeneous IoT devices are complicated, and central servers and trusted platforms cannot take effective measures against tampered devices. Analyzing the problems and challenges faced by IoT devices, this paper proposes a unified authentication scheme for IoT blockchain devices based on PUF. The PUF model is used to authenticate IoT devices, and the model parameters are decomposed into various parts and stored in each node in the blockchain. The homomorphic hash function is used to aggregate the partial authentication response values generated by the distribution in the invisible case to complete the authentication of the device information. It solves the complex and diverse problems of device authentication schemes and realizes the credibility and security of devices data sources and devices information storage stability. Finally, the functional analysis confirmed that the scheme is practical and executable.**

***Index Terms*—IoT, Blockchain, PUF, Device authentication, Data Security**

I. Introduction

A large number of different devices and terminals are connected to form the Internet of Things. IoT devices collect adequate information such as sound, light, biology, and location through information sensing and gathering devices to access the Internet through various networks to achieve efficient management and intelligent sensing of devices with minimal human intervention [8, 31]. From 2015 to 2025, the number of global IoT device connections will increase to 25 billion, while IoT revenue will reach nearly $1.1 trillion [11]. Large-scale device manufacturers help keep the number of IoT devices growing but also bring related problems. The production standards of devices vary considerably, resulting in differences in performance and construction between devices; lack of security measures for initial manufacturing [16]. Compromise on performance and computing resources due to the portability and convenience required by some devices and the lack of authenticity of the device can be certified [25], making the device easy to be counterfeited by attackers [27].

Different IoT device structures and central servers of various manufacturers and devices access to the network authentication methods naturally vary. So, the security of other authentication methods is difficult to be effectively guaranteed, leading to the manufacturers trying to ensure the security of the device and consume unnecessary resources, resulting in a waste of social resources [21, 29]. The central server stores authentication information and device information of trusted devices as long as the computing performance of the device and the interaction time allows, which relies heavily on the security of the central server. Once the central server is breached, a large amount of device information will be leaked, and the risk of direct or indirect security incidents will surge [16, 27].

In addition to the risks at the device authentication interaction level, there are also risks of tampering and forgery in the hardware facilities of IoT devices. However, the tampering of IoT devices from the hardware cannot be identified by the central server or trusted platform. Certificate Authority (CA) of Public Key Infrastructure (PKI) [26] is used to issue certificates to IoT devices, but CA cannot take adequate measures against tampering with the IoT devices, so the issuance of certificates may lead to false trust.

The emergence of blockchain provides an idea to solve the hidden problem of device information center storage [24]. Still, it cannot guarantee real reliability on the physical hardware of the device. Blockchain alone cannot detect whether the IoT device has been tampered with. Nor can blockchain take the necessary corresponding measures for the device after being maliciously tampered with, which will lead to the blockchain nodes trusting the hardware device that has been tampered with from the physical level. The trustworthiness and security of device data information sources are not guaranteed, threatening the ecological security of the whole IoT with blockchain as distributed storage.

Physical Unclonable Function(PUF) is a physical entity

Zhenyu Guan is the corresponding author of this paper.

This paper is supported by the National Key R&D Program of China through project 2020YFB10056, 2019QY(Y)0602, the Natural Science Foundation of China through projects 62002006, 61932011, 61932014, 61972018, 61972019, 61772538, and 91646203.

978-0-7381-2646-3/21/$31.00 ©2021 IEEE
DOI 10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00113

that could produce unavoidable process differences in manufacturing [22]. It can input a challenge C to PUF and output an unpredictable response R using its inevitable random differences in intrinsic physical structure to authenticate IoT devices. Thus, tampering with the device in hardware will inevitably change the correspondence of Challenge-Response Pair(CRP), making the device no longer trusted. PUF ensures the security and reliability of IoT devices and does not overly consume computing resources. Tampering with the device in hardware will inevitably change the correspondence CRP [14], effectively preventing the device from being counterfeited and tampered with to ensure the confirmed availability of the message source.

However, for IoT devices embedded with PUF, the authentication information of the device will be stored on the central server, which significantly increases the uncertainty of device information leakage. Keeping the authentication information of IoT devices embedded with PUF on the blockchain realizes the reliability and distributed storage of device information sources. The remaining problem is that the essential data information of the device PUF will be accessed by a single node on the blockchain network. If the node is evil, there is a certain way for the node to process the device PUF information to counterfeiting the device.

This paper combines blockchain and PUF, proposes a unified authentication scheme of IoT devices based on blockchain and PUF. The scheme makes full use of the advantages of blockchain and PUF and optimizes the existing problems after the combination, gives a complete unified authentication scheme for IoT devices. After security analysis, the scheme is proven to be safe and practical. The main contributions of this paper are as follows:

(1) We propose a perfect and trustworthy unified authentication scheme for IoT blockchain devices based on PUF. The scheme eliminates the complex and diverse authentication methods of massive heterogeneous IoT devices and realizes the unified authentication management of all IoT devices, saving social resources to a certain extent.

(2) We propose to use the model of PUF to do authentication of IoT devices and store the ideal machine learning model parameters obtained into each node of the blockchain network separately to reach distributed trust and realize that each node has only the most minor secret information.

(3) When the IoT devices authentication data are uploaded to the blockchain, we use the homomorphic hash function and hash lock to ensure the invisibility of the original authentication data and data integrity. The property of the homomorphic hash function is used to aggregate part of the authentication response values generated by the distribution without visibility to complete the authentication of the device information without knowing the message's original content.

II. RELATED WORK

With the development of computer and Internet technology [12, 23, 33], big data [13, 32, 20], cloud computing [34], and algorithm design [40, 39, 30], the demand for connections of different devices becomes stronger and stronger. In recent years, a new class of blockchain technology has been used for data storage of IoT devices based on its traceability and audibility features. The large scale of IoT connections and heterogeneous resources pose security issues, including the need for centralized security solutions to be built by third-party identity providers and the problem of single points of failure. Angin [2] designed a blockchain-based framework for IoT data security that leverages the transparency and tamper-proof features of blockchain to accurately verify devices in the network in a decentralized manner and prevent modification of the stored data.Shafaghr [38] proposes the use of blockchain to manage the IoT data flow for fine-grained access control and secure sharing of IoT data, but it consumes more resources and has a higher overhead.

Qiu[25] proposed a novel dynamic scalable blockchain based communication architecture for IoT and a secure digital evidence framework using blockchain [41]. Gai and Qiu[10] proposed a differential privacy-based blockchain for industrial IoT. Li[18] combines blockchain technology with edge computing and certificate-free cryptography to manage data storage and computational execution of tiny IoT devices using edge computing and uses certificate-free cryptography to establish a referencing system for blockchain-based IoT applications. However, the system lacks an identity verification scheme.

PUF can be used for IoT device authentication due to the properties of physical unclonable functions, such as unlovability and tamper resistance. In the authentication phase, the authenticator picks a random CRP from the database and provides it to the current system to motivate the PUF, and if the response of the PUF is close enough to the response stored in the database, then the authentication succeeds, otherwise it fails. Chatterjee [4] used the PUF to generate the public identity of the device and designed a lightweight identity-based based cryptosystem. However, the system is less robust and vulnerable to man-in-the-middle attacks and replay attacks. Braeken [3] addresses the problems that arise in the protocol of paper [4] and designs a more efficient alternative scheme for key negotiation that provides identity denial along with authentication.

In the IoT environment, the use of blockchain technology can effectively solve the traditional shortcomings of centralized data storage services but can not guarantee the authenticity and validity of the identity of the uploaded data devices. PUF provides a unique hardware fingerprint that can effectively authenticate IoT devices, thus compensating for these drawbacks. Javaid [15] combined PUF and blockchain technology to design the BlockPro system to provide a safe and secure data source and guarantee data integrity for the IoT environment. However, IoT device authentication messages may be captured by malicious single-server nodes in the blockchain network to counterfeit the device [43, 19].

III. PRELIMINARIES

A. Blockchain

As a key technology of Bitcoin, Blockchain was formally proposed in 2008 as a decentralized, distributed chain structure database that uses cryptography to ensure information transmission and access security and stores according to time sequence. In the blockchain system, each participating node stores information together in blocks using consensus protocols, and the blocks are in chronological order with cryptographic algorithms to form a chain data structure, which can achieve consistent storage and tamper-proof data. According to whether the system has a node access mechanism, blockchain can be classified as permissioned chain and permissionless chain. Permissioned chains require permission from the blockchain system to join and exit the nodes, while permissionless chains are entirely open, and nodes can join and exit at any time [6]. In this paper, the currently used Fabric permission chain is chosen based on the characteristics of the proposed protocol. The Fabric platform is also permissioned, meaning that, unlike a public permissionless network, the participants should be authenticated when getting access to the blockchian, rather than anonymous and therefore fully untrusted. Fabric utilizes a consensus protocol that does not require native cryptocurrency to incentivize expensive mining or drive smart contract execution. Meaning that the platform can be deployed using roughly the exact operating costs as any other distributed system [1].

B. PUF

PUF is a physical entity for which a challenge C is input and an unpredictable response R is output using the random differences in its intrinsic physical configuration. The input is generally called a challenge, the output is called a response, and a challenge and its measured response are called a Challenge-Response Pair (CRP) [35].

$$R = PUF(C)$$

Unclonability is a fundamental property of PUF, where different devices are given the same challenge as input, and the responses obtained are different, i.e., different CRPs are obtained. At the same time, PUF is robust, i.e., it always return the same response when the same PUF initiates the same challenge multiple times [4]. In addition, PUF is also well tamper-proof. When the physical entity embedded in the PUF changes, it will inevitably change CRP of the PUF, and a tampering attack on the PUF will create an indelible trace of the CRP. In this paper, we obtain the ideal machine learning model called PUFModel by training the correlation of a large number of CRP for the same IoT device PUF in the deployment phase, i.e., for the same challenge value, the response value output by PUFModel is the same as the response value output by the device PUF in the ideal case. If the attacker can not obtain a large number of CRPs, it will not be possible to model PUF of the device . This scheme decomposes the model's key parameters into several parts, and partial response values can be obtained from some of the model parameters. After aggregation, the response values are the same as those generated by the original complete model, making the key information of the same device stored in multiple points and achieving distributed trust.

C. Homomorphic hash function

A hash function is a function that maps data information of arbitrary length into the data of fixed length, satisfying unidirectionality, weak collision resistance, and strong collision resistance[36]. Given the information M, we can compute the hash value $Hash(M)$. The homomorphic hash function [9, 7] is a homomorphic property on the basis of satisfying the properties of the hash function, that is, given messages x and y, $\mathrm{Hash}_H(x+y) = \mathrm{Hash}_H(x) + \mathrm{Hash}_H(y)$[17]. Hash_H is used to denote the homomorphic hash function in this paper.

IV. SYSTEM MODEL

A. System architecture

Fig. 1 shows the system model of this scheme, consisting of CA, IoT devices, and blockchain.

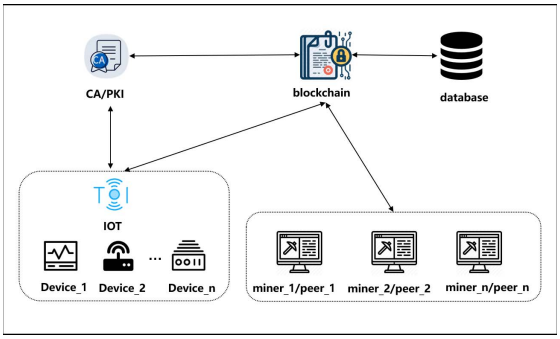

Fig. 1. System architecture .

- **CA**: a component of PKI, which records the identity information ID and issues the public key for the IoT device. CA sends a large number of challenge values to the IoT device embedded with PUF and generates a large number of corresponding response values through PUF to form a large number of CRPs, which are trained by machine learning modeling. Machine learning modeling[42] is used to train and predict the large number of CRPs to generate a PUFModel with the ideal prediction accuracy[37], i.e., if a certain challenge value is an input to the PUFModel, the output challenge value has the same probability of reaching the ideal value as the response value generated by the corresponding IoT device.
- **IoT device**: IoT device with limited computing resources and performance, embedded PUF that can accept challenge values from outside to generate response values that only this device can generate.
- **Blockchain**: Blockchain, transparent and decentralized distributed ledger, maintained by many miner nodes through consensus protocol, reaches the consistency of

each miner node's ledger and achieves the function of blockchain's non-tamperability and traceability. Miner nodes provide computing power and data storage to maintain the stable operation of the blockchain.

B. Security model

The objectives of the system security model mentioned in this paper are as follows.

(1) Every IoT device is embedded with a PUF.

(2) There is no situation in the blockchain where all nodes are complicit.

The attackers' objectives for the scheme proposed in this paper are as follows.

(1) Tampering or impersonating IoT devices to complete authentication.

(2) Intercept and modify the device authentication-related information uploaded to the blockchain.

In the case of meeting the security goals proposed in this article, an attacker attempts to tamper with the registered device and imitates the device for authentication [28, 5]. There may be two situations for the tampered device. One is that the device PUF cannot generate a response value to the challenge value after being tampered with, and the result is that the authentication will inevitably fail; the other is that the structure of the device PUF changes and the correspondence of CRP is very different from before.

When an attacker tries to intercept the information about to be uploaded to the blockchain, he obtains the information after hashing and cannot know the relevant sensitive information. If the information is still maliciously modified and uploaded to the blockchain, the device's authentication will fail. Therefore, under the above attack methods, this scheme is safe and credible.

V. Proposed Scheme

This section describes the scheme design to ensure the trustworthiness of message sources of IoT devices and the decentralized storage of authentication information, including the registration phase and the authentication phase of IoT devices.

A. Registration phase

The registration phase of the IoT device involves CA, IOT device, blockchain. The certificate issuance of CA is simplified in this paper, assuming that each IoT device is embedded with PUF. Two methods can only obtain the response value of a specific challenge value of an IoT device: the PUF of this IoT device, and the other is CA to obtain a large number of CRPs generated by this device PUF. Machine learning modeling of these CRPs generates the ideal PUFModel of the device, i.e., the input challenge value can get the same response value as the device PUF. The parameters $M_1, M_2, M_3, \ldots, M_n$ of the PUFModel are distributed to each node of the blockchain networks. The response values $R_1, R_2, R_3, \ldots, R_n$ are calculated by the critical parameters of the PUFModel model on each node in the blockchain network in the subsequent device authentication phase. The response values corresponding to the specific challenge values are finally aggregated. The specific steps of registration are shown in Fig. 2.

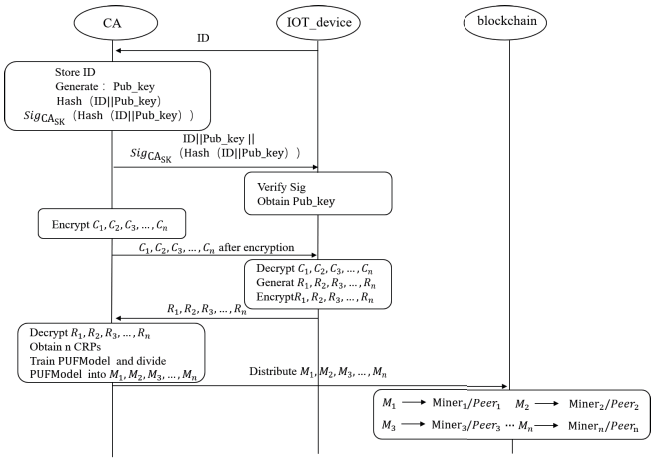

Fig. 2. Registration Phase Flow

Step 1:IoT device sends the identity information ID to CA, which acknowledges and stores the recorded device identity information ID.

Step 2: CA generates the public key Pub_key for IOT device and does hash $Hash(ID||Pub\_key)$ on the public key Pub_key and the device identity information ID, and then signs with CA's private key $\mathrm{CA_{SK}}$. The signed information is combined with the device identity information ID and the public key Pub_key

$$ID||Pub\_key||\,\mathrm{Sig}_{CA_{\mathrm{SK}}}\,(Hash(ID||Pub\_key))$$

together with the IoT device.

Step 3: The IoT device uses CA's public key $\mathrm{CA_{PK}}$ to verify the signature and obtain the public key Pub_key.

Step 4: CA uses the public key Pub_key of IoT device to encrypt a series of challenge values $C_1, C_2, C_3, \ldots, C_n$, and sends the encrypted result to IoT device; IoT device uses its own private key Pri_key to decrypt the encrypted result and obtain a series of challenge values $C_1, C_2, C_3, \ldots, C_n$ in plaintext, generate a series of corresponding response values $R_1, R_2, R_3, \ldots, R_n$ through PUF. The response values are encrypted with CA's public key $\mathrm{CA_{PK}}$ and sent to CA.

Step 5: CA uses the private key $\mathrm{CA_{SK}}$ to decrypt the received messages to obtain a series of corresponding challenge-response pairs CRPs. The ideal PUFModel of the device is gained by machine learning modeling and the model parameters $M_1, M_2, M_3, \ldots, M_n$ of the corresponding PUFModel of the device are sent to Miner_1/Peer_1, Miner_2 /Peer_2, Miner_3/Peer_3, …, Miner_n /Peer_n in the blockchain network. Now, the device registration is completed.

B. Authentication phase

As shown in Fig. 3, the authentication phase of IoT device involves IOT device , blockchain and various nodes in

the blockchain network Miner_1/Peer_1, Miner_2 /Peer_2, Miner_3/ Peer_3, . . ., Miner_n /Peer_n. The specific steps of authentication phase are as follows.

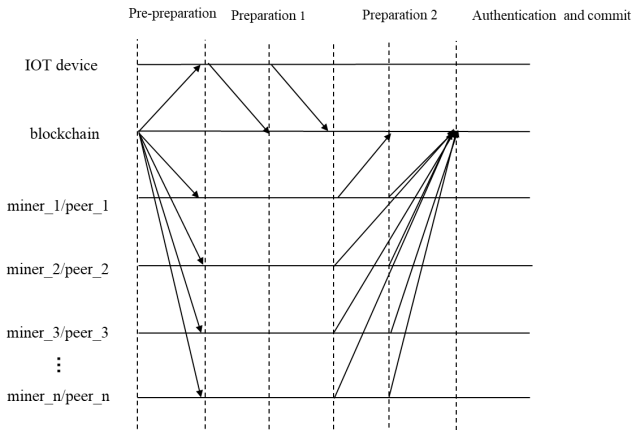

Fig. 3. Authentication Phase Flow

a) ***Pre-preparation****:* The IoT device gets the block header hash of the current block of the blockchain, i.e., the hash of the previous block as the challenge value, i.e., $c = Pre\_hash$. Miner_1/ Peer_1, Miner_2 /Peer_2, Miner_3/Peer_3, . . ., Miner_n /Peer_n in the blockchain network also obtains the challenge value

$$c = Pre\_hash$$

.

b) ***Preparation 1****:* The IoT device uses the device PUF to generate the corresponding response value r, calculates the homomorphic hash value $\mathrm{Hash}_H(r)$ of the response value r and the hash value of that homomorphic hash $Hash(\mathrm{Hash}_H(r))$ and uploads the hash value of the homomorphic hash $Hash(\mathrm{Hash}_H(r))$ to the blockchain first. After the previous message is uploaded to the block acknowledgment, the homomorphic hash value $\mathrm{Hash}_H(r)$ of the response r is then uploaded to the blockchain.

c) ***Preparation 2****:* Miner_1/Peer_1, Miner_2 /Peer_2, Miner_3/Peer_3, . . ., Miner_n /Peer_n in the blockchain network use the challenge value $c = Pre_hash$ and PUFModel with their respective model parameters $M_1, M_2, M_3, \ldots, M_n$.

$$r_i = \mathrm{PUFModel}\left(M_i\right)$$

Calculate the corresponding partial response values $r_1, r_2, r_3, \ldots, r_n$, and then calculate the homomorphic hash values

$$\mathrm{Hash}_H\left(r_1\right), \mathrm{Hash}_H\left(r_2\right), \mathrm{Hash}_H\left(r_3\right), \ldots, \mathrm{Hash}_H\left(r_n\right)$$

. To ensure the data integrity of the homomorphic hash values, each node then calculates the hash values of each homomorphic hash value $\mathrm{Hash}\left(\mathrm{Hash}_H\left(r_1\right)\right), \mathrm{Hash}\left(\mathrm{Hash}_H\left(r_2\right)\right)$, Hash $\left(\mathrm{Hash}_H\left(r_3\right)\right), \ldots$, Hash $\left(\mathrm{Hash}_H\left(r_n\right)\right)$. Each node uploads the hash of homomorphic hash of the respective partial response values $\mathrm{Hash}\left(\mathrm{Hash}_H\left(r_i\right)\right)$ to the blockchain one after another. After the hash value of the homomorphic hash value of each partial response value is recorded by the confirmation of the blockchain, each node then uploads the homomorphic hash value of the partial response value $\mathrm{Hash}_H\left(r_i\right)$ to the subsequent block.

d) ***Authentication****:* Get the information about the device that has been uploaded to the blockchain, including the homomorphic hash of the full response value $\mathrm{Hash}_H(r))$ and the hash of the homomorphic hash $Hash(\mathrm{Hash}_H(r))$, the homomorphic hash of each partial response value $\mathrm{Hash}_H\left(r_i\right)$ and the hash of the homomorphic hash $\mathrm{Hash}\left(\mathrm{Hash}_H\left(r_i\right)\right)$. The obtained homomorphic hash value is hashed and compared with the hash value of the existing homomorphic hash value to verify whether the data has been modified. If the data is modified, it means that it is under attack and the device authentication fails; if the data is not modified, the homomorphic hash of partial response values $r_1, r_2, r_3, \ldots, r_n$ is aggregated to get a new complete homomorphic hash $\mathrm{Hash}'_H(r)$:

$$\mathrm{Hash}'_H(r) = \mathrm{Hash}_H\left(r_1\right) + \mathrm{Hash}_H\left(r_2\right) + \mathrm{Hash}_H\left(r_3\right)$$
$$+ \cdots + \mathrm{Hash}_H\left(r_n\right) == \mathrm{Hash}_H\left(r_1 + r_2 + r_3 + \cdots + r_n\right)$$

e) ***Commit****:* Determine whether $\mathrm{Hash}_H(r)$ and $\mathrm{Hash}'_H(r)$ are equal. If they are not equal, the data source is no longer reliable, and the device authentication fails; if they are equal, the device authentication is successful. The identity information of the device and the information of successful authentication, $ID||"Available"$, are uploaded and broadcasted to the blockchain, which indicates that the device is trusted and the device is successfully authenticated.

VI. Performance Analysis

This section discusses the unified authentication scheme process for IoT devices proposed in this paper, analyzing it in detail regarding theory, feasibility, and security.

1. Unified authentication for IoT devices. All IoT devices with PUFs can interact with the blockchain and CA by generating CRP to reach the registration and authentication process of the device and realize the identification and unified authentication of the device. Before IoT devices are connected to the network, they are authenticated by each identification and authentication method. However, the complex identification and authentication methods are not easy to manage in a unified manner. IoT devices uniformly embedded PUF will not only not increase excessive resource burden but also form the same physical structure form and unified authentication method, which is conducive to the whole IoT ecological security and management.

2. Untamperability of IoT devices. Due to the tamper-evident nature of PUF, once an entity attacks an IoT device at the physical level, i.e., some hardware facilities of the device are maliciously tampered with or replaced, the PUF will be irreversibly damaged, which will seriously affect the correctness and correspondence of CRP. Then, the unified authentication process of the device will definitely fail.

3. Data sources and integrity. IoT devices with PUFs are guaranteed to be absolutely trustworthy and reliable after unified authentication. Trusted devices ensure the trustworthiness of the information sent by the devices, i.e., the data source of the devices is guaranteed. In the process of unified authentication of devices, hash function and homomorphic hash function are used, which also ensure the data integrity of the device during its interaction with CA and blockchain.

4. Distributed Trusted Storage and Data Untamperability. The distributed nature of blockchain enables the unified authentication data of IoT devices to be stored in multiple nodes to avoid a single point of failure. A block cannot be modified or deleted after it is added to the blockchain. The more blocks are added over time, the more difficult it is for the data in the block to be modified. Once a block is modified, it will cause the whole blockchain to break. Thus the data uploaded to the blockchain cannot be modified.

5. Resistant to man-in-the-middle attacks. In the unified authentication process of IoT devices, the interaction process of devices with CA and blockchain is encrypted with a secure public-key cryptosystem to encrypt the interaction information. So, it is tough for intermediaries to obtain CRP to prevent man-in-the-middle attacks effectively.

6. Resistant to replay attacks. The block header hash of the current block of the blockchain, that is, the hash of the previous block, is unpredictable and time-sensitive, so the challenge value $c = Pre\_hash$ used for device authentication is not repeatable. Replay attacks using information about devices that have been authenticated are not effective.

7. Resistant to modeling attacks. There are only hash values and homomorphic hash values on the blockchain and no plaintext response values. After the PUFModel of the IoT device is extracted and the authentication is complete, the interface for reading PUF from the outside world is destroyed. The attacker cannot read the CRPs from the device and can not perform modeling attacks.

VII. Conclusion

This paper proposed a unified authentication scheme for IoT devices based on blockchain and PUF. Achieving the unified authentication effect of all IoTs through effective interaction between devices with PUF and blockchain network nodes and CA, the scheme could eliminate complicated authentication methods for massive heterogeneous IoT devices and solve the problem of different authentication methods for each IoT device. Meanwhile, device data source reliability, security, and device authentication information storage were effectively guaranteed. After the security proof analysis, it ensured that the IoT unified authentication scheme was executable, secure, and less resource-consuming, and could be put into market use and widely promoted.

References

[1] Elli Androulaki et al. "Hyperledger fabric: a distributed operating system for permissioned blockchains". In: *Proceedings of the thirteenth EuroSys conference*. 2018, pp. 1–15.

[2] Pelin Angin et al. "A blockchain-based decentralized security architecture for IoT". In: *International Conference on Internet of Things*. Springer. 2018, pp. 3–18.

[3] An Braeken. "PUF based authentication protocol for IoT". In: *Symmetry* 10.8 (2018), p. 352.

[4] Urbi Chatterjee, Rajat Subhra Chakraborty, and Debdeep Mukhopadhyay. "A PUF-based secure communication protocol for IoT". In: *ACM Transactions on Embedded Computing Systems (TECS)* 16.3 (2017), pp. 1–25.

[5] Wenyun Dai et al. "Who moved my data? privacy protection in smartphones". In: *IEEE Communications Magazine* 55.1 (2017), pp. 20–25.

[6] Tien Tuan Anh Dinh et al. "Untangling blockchain: A data processing view of blockchain systems". In: *IEEE transactions on knowledge and data engineering* 30.7 (2018), pp. 1366–1385.

[7] K Gai and M Qiu. "Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers". In: *IEEE Transactions on Industrial Informatics* 14.8 (2017), pp. 3590–3958.

[8] K. Gai and M. Qiu. "Optimal resource allocation using reinforcement learning for IoT content-centric services". In: *Applied Soft Computing* 70 (2018), pp. 12–21.

[9] K. Gai et al. "Advanced fully homomorphic encryption scheme over real numbers". In: *IEEE 4th int'l conf. on cyber security and cloud computing (CSCloud)*. 2017.

[10] K. Gai et al. "Differential privacy-based blockchain for industrial internet-of-things". In: *IEEE Transactions on Industrial Informatics* 16.6 (2019), pp. 4156–4165.

[11] GSMA. *The Mobile Economy 2020*. https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf. Accessed July 9, 2020.

[12] Y. Guo et al. "Data placement and duplication for embedded multicore systems with scratch pad memory". In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits* (2013).

[13] Y. Guo et al. "Optimal data allocation for scratch-pad memory on embedded multi-core systems". In: *IEEE International Conference on Parallel Processing (ICPP)*. 2011, pp. 464–471.

[14] Zhao Huang and Quan Wang. "A PUF-based unified identity verification framework for secure IoT hardware via device authentication". In: *World Wide Web* 23.2 (2020), pp. 1057–1088.

[15] Uzair Javaid, Muhammad Naveed Aman, and Biplab Sikdar. "Blockpro: Blockchain based data provenance and integrity for secure iot environments". In: *Pro-*

ceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems. 2018, pp. 13–18.

[16] H Jiang et al. "AI and machine learning for Industrial Security with a Level Discovery Method". In: *IEEE Internet of Things Journal* (2020).

[17] Maxwell N Krohn, Michael J Freedman, and David Mazieres. "On-the-fly verification of rateless erasure codes for efficient content distribution". In: *IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004*. IEEE. 2004, pp. 226–240.

[18] Ruinian Li et al. "Blockchain for large-scale internet of things data storage and protection". In: *IEEE Transactions on Services Computing* 12.5 (2018), pp. 762–771.

[19] Y. Li et al. "Intelligent Fault Diagnosis by Fusing Domain Adversarial Training and Maximum Mean Discrepancy via Ensemble Learning". In: *IEEE Trans. on Indu. Info.* 17.4 (2021), pp. 2831–2842.

[20] R. Lu et al. "A study on big knowledge and its engineering issues". In: *IEEE Trans. on Knowledge and Data Eng.* 31.9 (2018), pp. 1630–1644.

[21] Z. Lu et al. "IoTDeM: An IoT Big Data-oriented MapReduce performance prediction extended model in multiple edge clouds". In: *Journal of Parallel and Distributed Computing* 118 (2018), pp. 316–327.

[22] Roel Maes, Anthony Van Herrewege, and Ingrid Verbauwhede. "PUFKY: A fully functional PUF-based cryptographic key generator". In: *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer. 2012, pp. 302–319.

[23] J. Niu et al. "Energy efficient task assignment with guaranteed probability satisfying timing constraints for embedded systems". In: *IEEE Transactions on Parallel and Distributed Systems* 25.8 (2013), pp. 2043–2052.

[24] Xiaodong Qi et al. "BFT-Store: Storage partition for permissioned blockchain via erasure coding". In: *2020 IEEE 36th International Conference on Data Engineering (ICDE)*. IEEE. 2020, pp. 1926–1929.

[25] H Qiu et al. "A dynamic scalable blockchain based communication architecture for IoT". In: *Int'l Conf. on Smart Blockchain*. 2018, pp. 159–166.

[26] H. Qiu, M. Qiu, and R. Lu. "Secure V2X communication network based on intelligent PKI and edge computing," in: *IEEE Network* 34.2 (2019), pp. 172–178.

[27] H. Qiu et al. "Adversarial Attacks against Network Intrusion Detection in IoT Systems". In: *IEEE Int. of Things J.* (2021), pp. 1–9.

[28] H. Qiu et al. "All-or-nothing data protection for ubiquitous communication: Challenges and perspectives". In: *Information Sciences* 502 (2019), pp. 434–445.

[29] H. Qiu et al. "Towards secure and efficient deep learning inference in dependable IoT systems". In: *IEEE Internet of Things Journal* (2020).

[30] M. Qiu, Z. Chen, and M. Liu. "Low-power low-latency data allocation for hybrid scratch-pad memory". In: *IEEE Embedded Systems Letters* 6.4 (2014), pp. 69–72.

[31] M. Qiu, K. Zhang, and M. Huang. "An empirical study of web interface design on small display devices". In: *IEEE/WIC/ACM International Conference on Web Intelligence (WI'04)*. 2004, pp. 29–35.

[32] M. Qiu et al. "Data transfer minimization for financial derivative pricing using Monte Carlo simulation with GPU in 5G". In: *IEEE International Journal of Communication Systems* 29.16 (2016), pp. 2364–2374.

[33] M. Qiu et al. "RNA nanotechnology for computer design and in vivo computation". In: *Philosophical Transactions of the Royal Society A* (2013).

[34] Meikang Qiu et al. "Enabling cloud computing in emergency management systems". In: *IEEE Cloud Computing* 1.4 (2014), pp. 60–67.

[35] Mahmood Azhar Qureshi and Arslan Munir. "PUF-IPA: A PUF-based identity preserving protocol for internet of things authentication". In: *2020 IEEE 17th annual consumer communications & networking conference (CCNC)*. IEEE. 2020, pp. 1–7.

[36] Phillip Rogaway and Thomas Shrimpton. "Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance". In: *International workshop on fast software encryption*. Springer. 2004, pp. 371–388.

[37] Ulrich Rührmair and Jan Sölter. "PUF modeling attacks: An introduction and overview". In: *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE. 2014, pp. 1–6.

[38] Hossein Shafagh et al. "Towards blockchain-based auditable storage and sharing of iot data". In: *Proceedings of the 2017 on cloud computing security workshop*. 2017, pp. 45–50.

[39] Z. Shao et al. "Real-time dynamic voltage loop scheduling for multi-core embedded systems". In: *IEEE Transactions on Circuits and Systems II* 54.5 (2007), pp. 445–449.

[40] X. Tang et al. "A hierarchical reliability-driven scheduling algorithm in grid systems". In: *Journal of Parallel and Distributed Computing* 72.4 (2012), pp. 525–535.

[41] Z. Tian et al. "Block-def: A secure digital evidence framework using blockchain". In: *Information Sciences* 491 (2019), pp. 151–165.

[42] Manasi Vartak et al. "ModelDB: a system for machine learning model management". In: *Proceedings of the Workshop on Human-In-the-Loop Data Analytics*. 2016, pp. 1–3.

[43] Z. Zhang et al. "Jamming ACK attack to wireless networks and a mitigation approach". In: *IEEE GLOBECOM*. 2008, pp. 1–5.