Hindawi
Security and Communication Networks
Volume 2018, Article ID 7817614, 11 pages
https://doi.org/10.1155/2018/7817614

Research Article

Blockchain Based Credibility Verification Method for IoT Entities

Chao Qu, Ming Tao, Jie Zhang, Xiaoyu Hong, and Ruifen Yuan

School of Computer Science and Network Security, Dongguan University of Technology, Dongguan 523808, China

Correspondence should be addressed to Ming Tao; ming.tao@mail.scut.edu.cn

Received 1 April 2018; Revised 28 May 2018; Accepted 4 June 2018; Published 27 June 2018

Academic Editor: Wei Wang

With the fast development of mobile Internet, Internet of Things (IoT) has been found in many important applications recently. However, it still faces many challenges in security and privacy. Blockchain (BC) technology, which underpins the cryptocurrency Bitcoin, has played an important role in the development of decentralized and data intensive applications running on millions of devices. In this paper, to establish the relationship between IoT and BC for device credibility verification, we propose a framework with layers, intersect, and self-organization Blockchain Structures (BCS). In this new framework, each BCS is organized by Blockchain technology. We describe the credibility verification method and show how it provide the verification. The efficiency and security analysis are also given in this paper, including its response time, storage efficiency, and verification. The conducted experiments have been shown to demonstrate the validity of the proposed method in satisfying the credible requirement achieved by Blockchain technology and certain advantages in storage space and response time.

1. Introduction

The Internet of things (IoT) is a worldwide network of interconnected objects and humans, which through unique address schemes are able to interact with each other and cooperate with their neighbours to reach common goals [1]. The primary purpose of the IoT is to share information gained by objects, which reflects the manufacture, transportation, consumption, and other details of people's lives [2, 3]. The development of the IoT makes a large number of devices, such as sensors, interconnection, and interoperability for data collection and exchange. Using information gained from the IoT could make the environment around us be better cognized [4]. On the other hand, the IoT consists of devices that generate, process, and exchange vast amounts of critical security and safety data as well as privacy-sensitive information and hence are appealing targets for cyberattacks [5–8]. The task of affordably supporting security and privacy is quite challenging because many new networkable devices, which constitute the IoT, require less energy, are lightweight and have less memory [9]. These devices must devote most of their available energy and computation to executing core application functions [10]. A lot of researchers have worked on them. The security research includes transmission field [11, 12], cloud storage field [13, 14], digital signature field [15, 16], and permission identification [17, 18].

The Blockchain (BC) technology allows all members to keep a ledger containing all transaction data and to update their ledgers to maintain integrity when there is a new transaction. Since the advancement of the Internet and encryption technology has made it possible for all members to verify the reliability of a transaction, the single point of failure arising from the dependency on an authorized third party has been solved. The Blockchain has broker-free (P2P-based) characteristics, thereby doing away with unnecessary fees through p2p transactions without authorization by a third party. Since ownership of the transaction information by many people makes hacking difficult, security expense is saved, transactions are automatically approved and recorded by mass participation, and promptness is assured. Moreover, the system can be easily implemented, connected and expanded using an open source and transaction records can be openly accessed to make the transactions public and reduce regulatory costs. Since the hash values stored in each

peer in the block are affected by the values of the previous blocks, it is very difficult to falsify and alter the registered data. Although data alteration is possible if 51% of peers are hacked at the same time, the attack scenario is realistically very difficult [19].

2. Related Works

The Blockchain technology first came to prominence in early 2009, through the cryptocurrency Bitcoin (BTC). Bitcoin users that are known by a changeable Public Key (PK) generate and broadcast transactions to the network to transfer money. These transactions are pushed into a block by users. Once a block is full, the block is appended to the Blockchain by performing a mining process. To mine a block, some specific nodes known as miners try to solve a resource consuming cryptographic puzzle named Proof of Work (POW) [20], and the node which solves the puzzle first mines the new block for the Blockchain. Since BTC has flourished, Blockchain, the technology that underpins BTC, could, according to Swan, have far-ranging consequences for all aspects of modern society. Based on the characteristics of Blockchain, many researchers have carried out research on its application in the IoT environment [21], such as applying BC to the smart home system to ensure the security and privacy of information [22], applying smart contract in IoT [23], using the BC platform to manage IoT devices [24], and made security transmission for IoT [25]. The reason for this explosion of interest is that, with the Blockchain technology in place, applications that could previously run only through a trusted intermediary can now operate in a decentralized fashion. The essence of Blockchain technology is a decentralized database for peer-to-peer networks, providing an effective trust mechanism. In the IoT environment, devices form a kind of peer-to-peer network, which is a decentralized application scenario. Therefore, the working conditions required by the Blockchain technology are meted. On the other hand, IoT requires an effective solution for security problems, but the number of devices and their growth rate also make centralized authentication difficult to achieve. For these reasons the Blockchain technology should work well for an IoT environment.

In our previous work [26, 27], we proposed a model of transactions on the Semantic Web of Things (SWoT) to satisfy the needs of intelligent IoT. We described the framework and working mechanism of the model. The framework uses the ontology as the logical reasoning basis and is divided into several parts: the entity link layer, the semantic annotation layer, the service registry center, the transaction construction layer, and the transaction execution control layer. Semantic technology is used to describe the IoT entity as a dynamic Web service. In the model, the technologies of service discovery and service composition are used to build IoT transactions that meet users' requirements and control the transaction processes. Also, it acted as a manager during the execution of a transaction and made effective management and control to the entities. And a use case of traffic accident rescue has been described in the previous paper. The proposed model extends the IoT from sensor networks to real interconnections and provides the underlying structural support for the interaction of entities in IoT. As our research has developed, we have found that although the proposed model satisfies the intelligent construction and execution of IoT transactions, it still has security risks and needs a method to protect the usability and credibility of the devices. Blockchain technology happens to be able to meet our needs and provide IoT devices with privacy and protection through a distributed, decentralized verification approach.

3. Problem Statement

The credibility verification of an IoT device refers to verifying that the target device has the attributes, such as location and function [26], that are known in the service-center and that the data the device transmits and receives has not been tampered with by a network attacker. For example, the monitoring device should verify that the data actually came from the sensor at the specified location rather than being tampered with an attacker [28]. The traditional security and privacy policies based on asymmetric encryption are difficult to implement in an IoT environment, mainly due to the follow reasons:

(i) Asymmetric encryption needs a centralized key management system, which cannot meet the needs of a rapidly growing IoT system. Furthermore, if the key management system is attacked, a large number of IoT devices are likely to be affected.

(ii) Traditional security methods tend to be expensive for the IoT in terms of energy consumption and processing overhead because sensors are lightweight, of slow processing, and of less memory.

Although Blockchain technology can solve these problems, it still faces the following critical challenges for application in an IoT environment.

(1) POW calculation is particularly computationally intensive and time-consuming, but the majority of IoT devices are resource restricted and most IoT applications need low latency.

(2) IoT networks are expected to contain a large number of nodes and have a rapidly increasing rate, so that the Blockchain scales poorly as the number of nodes in the network increases.

(3) The underlying Blockchain protocols create significant network traffic flow, which is a disaster for the communication of IoT devices.

The main contribution of this paper is to propose a novel credibility verification method based on Blockchain technology for IoT entities. We establish a credibility verification framework for IoT devices, and, based on this, we illustrate the process and solve the challenges of applying BC to IoT. The performance of the method is analyzed experimentally.

4. Credibility Verification Method

The existing IoT device access and management modes have many problems of credibility verification to be resolved. Therefore, based on our previous work [29], a new framework

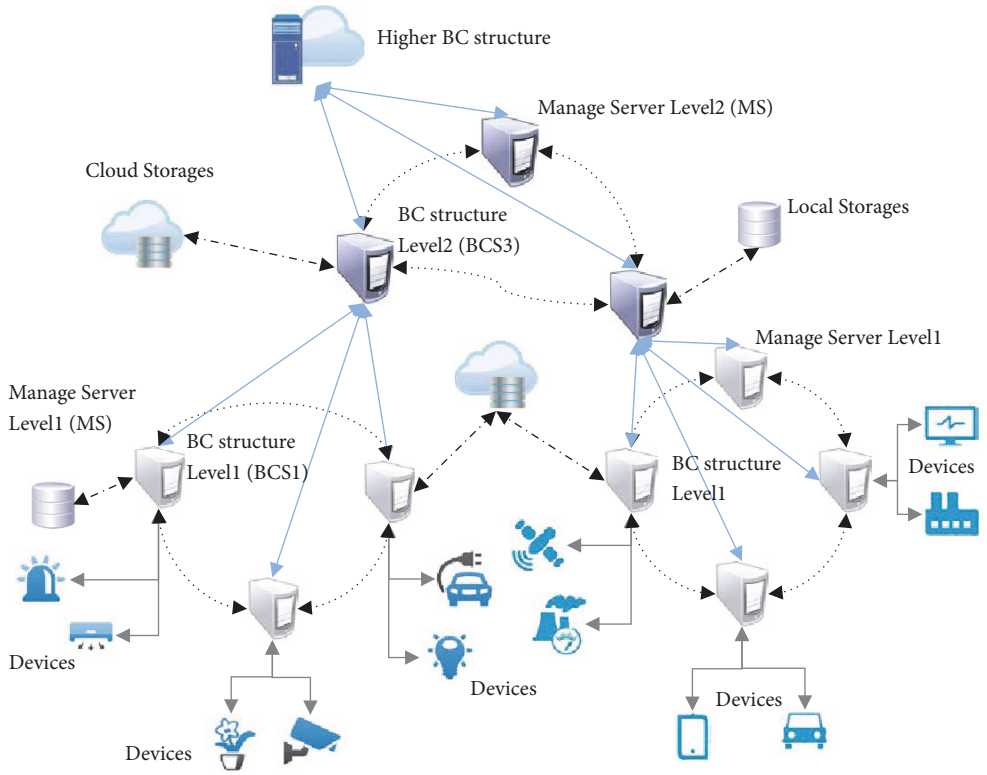


Figure 1: Overview of the credibility verification framework.

needs to be established for the IoT network. First, we define the framework of credibility verification structure. The structure is made of several blockchains with different layer, the Blockchain node in upper layer manage a Blockchain of lower level. Second, we design the data flow under the framework. The register data in the bottom layer is transmitted to the upper Blockchain node sequentially and recorded in each Blockchain in the path. Last, we describe the verify process. The credibility verification process is a verify chain along the source device to the destination device.

4.1. Credibility Verification Network Framework. In the IoT scenarios, every application, such as a smart home, smart healthcare, and shared cycling [30], requires a server that manages the underlying devices, such as a smart home gateway, medical portal server, or shared platform. These servers have better computational ability than bottom IoT devices with limited resources and bandwidth. In addition, these devices often work on cloud computing and cloud storage platforms and thus have good storage capabilities and network communication capabilities. We have divided IoT entities into Devices and Manager Servers to construct a credibility verification network. The overview of the framework is shown in Figure 1. Prior to discussing the details of the proposed framework, we briefly introduce the network framework tiers.

Devices: The smart devices and sensors in the IoT.

Manage Server (MS): Devices for managing and providing calculation and storage. MS is invoked in different BC structures depending on what position they are in.

(1) The bottom MS is directly connected with the device. Their responsibilities were to provide a Private Key and generate the Public Key for the device, store the device information, and published it to the Blockchain network responsible for the devices' credibility verification. Some of the bottom MS constituted a Blockchain network and acted as miners. The technology in [31] can be used.

(2) MSs in other positions were responsible for managing a number of lower-level MSs and were responsible for providing key pairs to the accessed lower-level MSs, storing their information. The MSs were also responsible for publishing the information to the Blockchain network where they were located and verifying the credibility of the lower-level MS that it managed. On the other hand, the MSs managed by the same MS also formed a Blockchain network and each MS served as a Blockchain network node and acted as a miner. MSs published the "add" or "delete" information of entities as records (similar to the transaction records in the BTC) to the Blockchain network where they formed. The information constructed Blockchain-blocks.

BC Structure (BCS): Different from the fact that all the nodes in the BTC network existed in the same Blockchain network and all had peer-to-peer characteristics, the credibility verification network had a plurality of Blockchain networks composed of MSs. Each Blockchain network was managed by one MS. Different Blockchain networks could constitute a hierarchical relationship.

Storage: The information BC-blocks in the credibility verification network can be stored in local storage or cloud storage [32]. The access method can be used as in [33, 34].

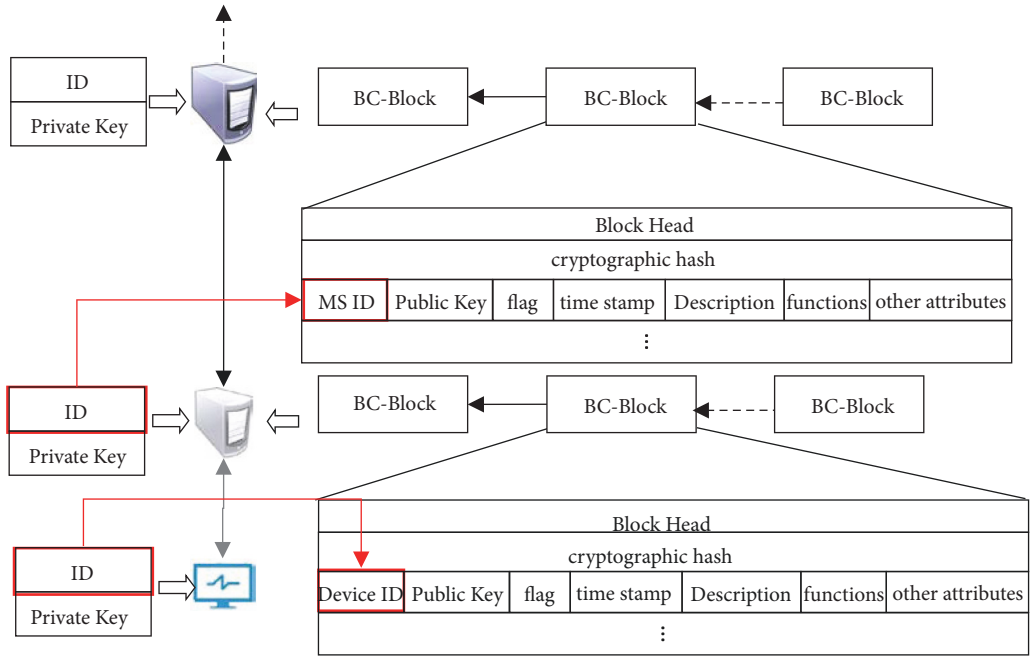


Figure 2: Data model for verification.

4.2. Credibility Verification Data Model. In order to achieve verification, a corresponding data model needed to be established based on the original IoT data communication. Therefore, we designed a data model and applied it to credibility verification, as shown in Figure 2.

For Devices, the added data includes an ID and a Private Key, where the ID was used as a unique identifier of Device to distinguish each other; the Private Key used for asymmetric encryption was used as the verification flag of device credibility. The Private Key is generated and issued by the MS which was responsible for managing the device.

The additional data in the MS included the ID, Private Key, and BC-blocks. Among them, the ID was the unique identifier of the MS. It should be noted that the MS is also a kind of IoT device (except for computing ability and storage capacity, it is the same as the other devices) and should therefore have the same attribute ID as those Devices; that is, the MS and the IDs of the devices should have the same definition. For each BC-block, block head, cryptographic hash, and block records were included according to Blockchain technology. Block head is used to store information such as the BC-block number, archive time, and the hash of the previous block. Cryptographic hash is considered as the POW for each BC-block. As with BC-blocks in Blockchain technology, there were several records in each BC-block. Each record was used to record the "adding" or "deleting" of information of the entities managed by the MS. Of course, additional items may be added according to further requirements. The structure of the BC-block-record included: Device or MS ID, flag of adding or deleting, timestamp, description, and entity functions. The Public Key in one BC-block-record should be generated from the Private Key of the right entity. Description and entity functions used to record device information and its ability, of course, may also need to add other attributes.

The transaction data were recorded in the BCT network. However, in the BCS which we are proposing in this paper, the action information, such as addition or deletion of a device, was recorded. The purpose is to verify the credibility of the entity. Data storage occurred only in the corresponding BCS and did not require synchronization of all network nodes, but synchronization was required in each BCS on the BCS chain.

4.3. Credibility Verification Process. The proposed credibility verification model and its associated data model are primarily used as the basis for the verification process. The primary goal of the credibility verification of a device is to prove that a device is the one that joins the network as originally declared, not the device which tampered with the attacker. Therefore, the verification of credibility has three aspects. One is that the device needs to establish its own certificate when it joins the network. Second, when the device is accessed, it needs to be verified as the original one. Last, the data sent by the device must be proven that it was generated by the original device. The concrete realization method includes the following three parts.

(a) Recording the Addition or Deletion of Entities. In the IoT environment, access to the device needs to be controlled by the MS. When the device accesses the IoT environment, the device sends its description, function, and other attributes to the MS that is responsible for managing it. The MS needs to assign an ID, generate a specific Private Key, and send both to the devices. At the same time, the MS needs to generate the corresponding Public Key according to the

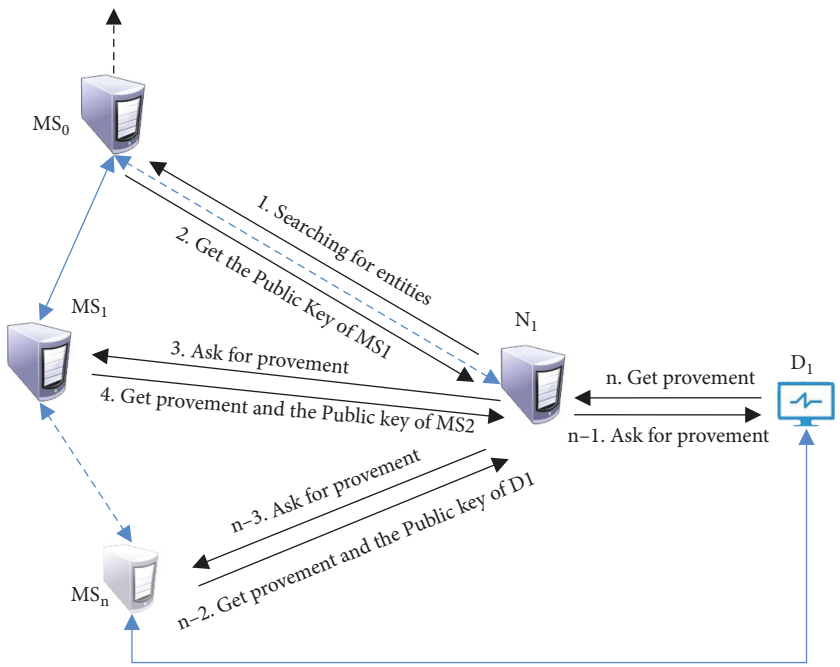


Figure 3: The process of verifying the device credible.

Private Key. When the operation is completed, the MS adds a record to the BC-block and broadcasts it to the BCS it joined. When receiving the broadcast, other MSs also add the record to their BC-block. If the BC-block is full, according to BC technical specifications, the MSs calculate the cryptographic hash as the POW and seal the current BC-block. In the MS, the Device ID in the record is replaced with its own MS ID and the record is sent to the upper-level MS, the manager. The upper-level MS receives the record and uses the same policy to process the record. The process is repeated until the record reaches the top MS. This is similar to accessing a new MS under a MS. The communication process packet aggregated authentication can be protected with cryptography techniques such as [35]. When a device is removed from the network, the responsible MS generates a record for device removal, adds it to the BC-block, and passes the record up as described above.

(b) Credibility Verification Process of the Accessing Entity. According to the IoT model designed in the previous work [26], the credibility of the selected device must be verified when establishing a transaction. The credibility verification of the accessed device is achieved by building a verification chain through the BCSs on the path. Suppose that when a network node N_1 issues an application for the use of a specific function device, the application information will be propagated upwardly along the upper-level MS of N_1. The device records in the BC-blocks in each MS on the path are queried until it is found that the function described in the device record in one MS fulfills the function required by N_1.

Assuming that there is an MS_0 that meets the record and D_1 is the device capable of providing the function, each MS passing from MS_0 to D_1 is named as MS_1 to MS_n in turn. MS_n is the management node of D_1. The subsequent verification process is as follows.

(I) The MS_1's ID and its Public Key are obtained from MS_0's BC-block-record.

(II) A request is sent to MS_1 to ask for the encrypted data by using the Private Key, and the identity is verified with the Public Key of MS_1.

(III) When MS_1 is identified, we can get MS_2's ID and the Public Key from its BC-block-record, using the same method to verify the credibility of MS_2.

(IV) Steps 2–3 are repeated until the Public Key of D_1 is obtained. Then a request is sent to D_1 to ask for encrypted data and the resulting Public Key is used for verification.

(c) Credibility Verification of Data Is Achieved. After verifying the device's credibility and obtaining its Public Key, the Private Key of the device can be used to encrypt the data sent by the device as a digital signature. The receiver can use its Public Key for verification to obtain the trusted data. The whole process is just like a routing [36]. The credibility verification process is shown in Figure 3.

5. Analysis and Discussion

5.1. Validity of Verification. The method presented in this paper is based on several intersecting Blockchain networks, and credibility is transmitted through Blockchain networks. Therefore, this method is reliable only if each Blockchain network can be proven trustworthy. The security of Blockchain technology lies in the sharing mechanism of its distributed

data. The "mining" mechanism is defined so that when a node wants to tamper with certain records, it must recalculate the encryption hash of the entire Blockchain thereafter. The computational workload is so great that cheating nodes can never keep up with the whole network Blockchain generation rate (unless their processing power overtakes 51% of the whole network processing power, which is almost impossible). Therefore, if the entire IoT is regarded as a Blockchain network, its credibility is guaranteed (also impossible). The proposed method of verifying credibility differs from taking the entire IoT as a Blockchain network in that the IoT is divided into several BCs intersecting with each other. Therefore, each Blockchain network is relatively small in size with respect to the entire IoT. As a result, transactions (addition or deletion of entities) are generated too slowly to meet the security requirements at all, resulting in excessive idle time and allowing the cheating node to have enough time to recalculate the entire Blockchain. In this regard, we propose three solutions.

(a) Select the right size of each BCS and let the transaction record generation speed meet "mining" requirements so that the counterfeit records' costs are unacceptable.

(b) Devices should send empty transaction records with a random probability, making the transaction records' generation speed (real or empty) meet the "mining" requirement in each BCS.

(c) When verifying the credibility of a particular MS, several nodes are randomly selected from the BCSs in which it is located, and the records in the selected MSs are compared to the records in the MS (cryptographic hash can be used as well) to determine the credibility of the MS. Given a threshold, if the rate of unequal nodes in the selected nodes is over the threshold we can take the node as a forged one.

Although these three solutions can improve the validity of the verification, there are still some problems. For solution (a), it is difficult to determine the size of each BCS, and the higher the level is, the more the transaction records BCS receives. If there is no proper size control it can lead to inefficient record insertion. For solution (b), the same problem as in (a) exists and storage space can be wasted. For solution (c), credibility can be affected, but the probability of reducing noncredibility can be further improved. In addition, the 51% calculation problem exists in all three methods and this problem is inevitable for the Blockchain network.

5.2. Efficiency Analysis

(a) Response Efficiency. In the current IoT environment, credibility verification depends on the management center. Device information is obtained by querying the center. In this case, it is only necessary to get the certification of the management center, which can be considered as time complexity of O(1), which means a higher response rate. If the entire IoT environment is using Blockchain technology to achieve the credibility verification, the processing of synchronizing requires a large network overhead and response time. Because it needs to synchronize all the nodes in the network, the time complexity means O(n).

The proposed method is relatively complex with respect to the management center model (current IoT structure) and relatively simple with the whole network model (the whole IoT environment organized by a big Blockchain).

Suppose the number of nodes in each BCS is K, then, for an IoT environment with n nodes, the depth of the complete K-tree is formed by these nodes, that is, the longest length of certification chain is $\log_K n$, it can be proven that the verification time complexity is $O(\log_K n)$.

(b) Storage Efficiency. The IoT device management adopts a central management-based approach for now, and each device keeps a record in the management center. Therefore, the data storage in the entire network is directly proportional to the total amount of devices. If the entire IoT network implements Blockchain technology completely, records should be recorded on each node, and the total storage capacity is proportional to the square of the network size [37]. In the approach adopted in this paper, the IoT environment for n nodes constitutes a complete K-tree structure, and the information of the device only needs to be stored on the intermediate node from the device to the topmost BCS. Therefore, the total storage capacity is proportional to the sum of the length of each node to the root [38].

Suppose the total path length of each node to the root is S; then we have the following formula.

$$S = \sum_{h=1}^{\log_K n} h \times K^h \tag{1}$$

where h is the height of the K-tree and $h \approx \log_K n$. The overall storage capacity is $K*S$.

(c) Credibility Analysis. For different methods of credibility verification, the management center model has the best response time and the storage capacity, but the credibility is the worst. Once the management center is attacked, all nodes in the entire network are invalid. For the whole network model, the response time and the storage capacity are unacceptable and cannot be achieved, but its credibility is the best. In the method proposed in this paper, if using scheme (a) and scheme (b) in Section 5.1, the response time is the same as that of the whole network model and can significantly reduce the storage capacity. If using scheme (c), the storage capacity can be further reduced, but the security depends on the size of each BCS and the verification sampling rate [39]. The greater the number of BCS nodes and the larger the sampling rate, the greater the credibility.

In summary, the use of a management center for credibility verification used the least amount of storage space, but the center received a large range of attacks. Although credibility verification with the whole network model has the best reliability, its storage capacity, computational ability, and response time of each node are unacceptable. The proposed credibility verification method has a smaller storage requirement without computational ability and storage

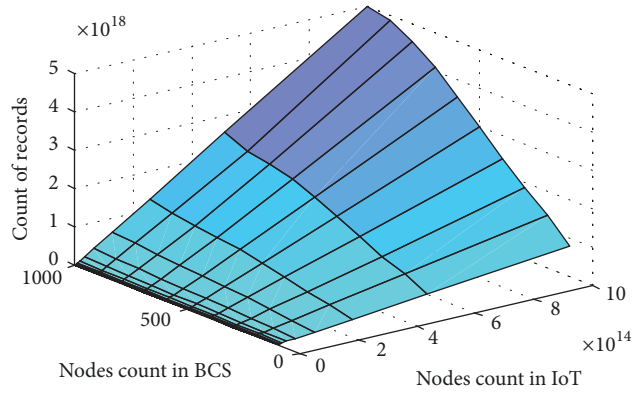


Figure 4: Storage capacity measurement with different K (node count in BCS) and n (node count in IoT).

capacity requirement for the terminal node and also has better advantages in response time.

6. Experiments and Evolution

As discussed in Section 5, response efficiency can be proven directly. In this section our experiments demonstrate the storage and credibility efficiencies. The measurements include the amount of the data to storage, the effect of the tree's degree "K" and nodes forged rate. It is also including the sampling rate and the value of threshold when we verify the data in the selection node.

6.1. Storage Evaluation. For our proposed method, the overall storage capacity is K∗S, for different values of K and n, the storage capacity regular pattern is shown in Figure 4. As can be seen from Figure 4, for the same number of nodes, the greater the value of K, the greater the storage space required. The comparison of the storage efficiency of the three methods is shown in Figure 5.

In Figure 5, the curves prove our analysis of storage efficiency and our method is much better than the full BC model.

6.2. Performance Evaluation. For the proposed method, there has been a lot of research to prove the performance of solution like (a) and (b) in Section 5.1. Thus, we focus on solution (c). There are many factors that affect the performance evaluation, and the most important include the following:

(i) The degree of the tree (*K*)

(ii) The number or probability of forged nodes *(FP)*

(iii) The count of samples for solution (c) in Section 5.1 *(SR)*

(iv) The threshold to determine whether the node is forged *(T)*

The degree of the tree determined the average path length of the node pair. The probability of forged nodes determined the probability of forged node appearing on the path. Hence, these two facts decide the probability of counterfeiting [40]. We simulate the environment with ten million IoT entity

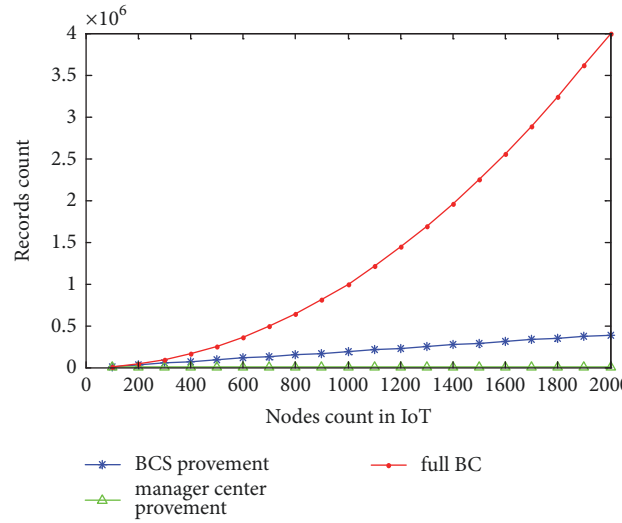


Figure 5: Comparison of storage efficiency.

nodes and select one million times node pair randomly for each parameter combination. The statistical results are shown in Figure 6.

In Figure 6, we can see that, with the increase of forge probability, paths with forged node increased, but for different K with the same FP the difference is not obvious.

We examine the relationship of SR and T. There are two indicators to be measured:

(i) The rate of forged node to be detected (*DR*)

(ii) The rate of nonforged nodes being detected as forged nodes (*NFR*); it is a negative measurement.

When we simulate a use case, if the different rates of selected nodes are more than the given threshold T, and the observed node is a forged one, we mark it as a detected one. Otherwise, if the different rates of selected nodes are more than the given threshold T but the observed node is not a forged one, we mark it as an error. With the given $K = 300$ and FP=1/1000, the detected rate and the error rate are shown in Figure 7.

From Figure 7(a), we can see that the higher the threshold, the lower the detected rate. That means the higher the

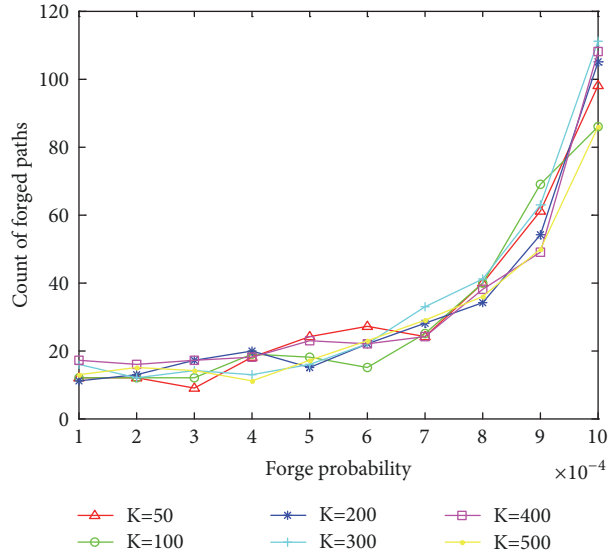
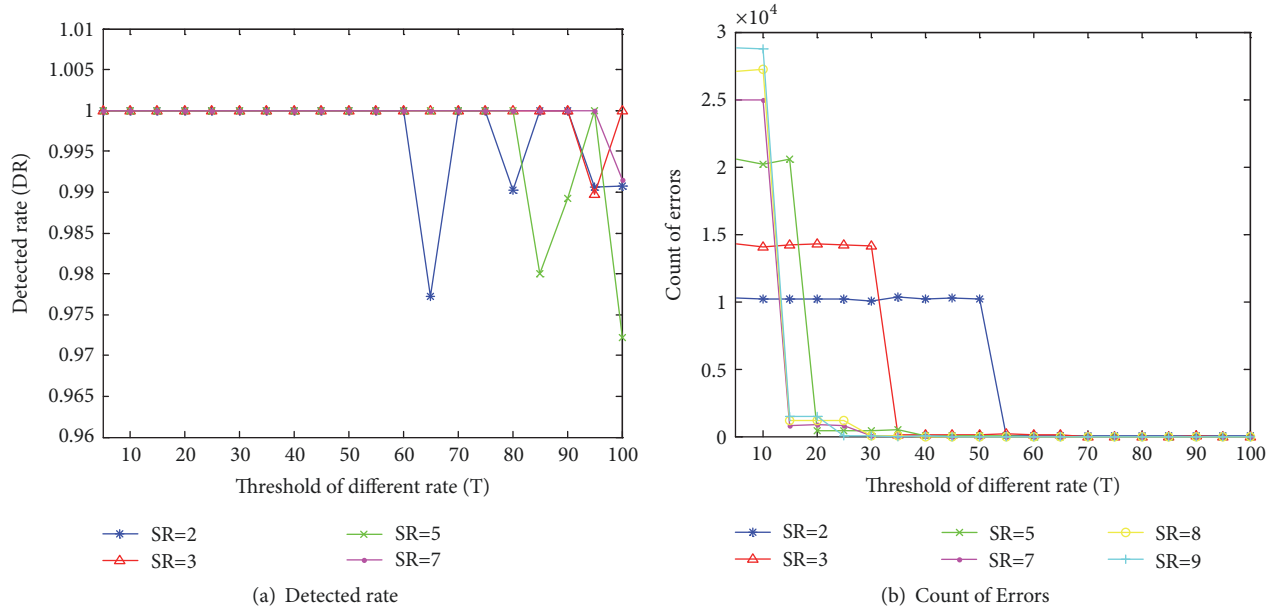


Figure 6: Paths with forged node.



(a) Detected rate

(b) Count of Errors

Figure 7: The experimental results of detected rete and error rate.

requirement of proving a given node is a forged node, the lower its chance of being detected. We can also draw a conclusion that the better threshold is less than 75%.

From Figure 7(b), we can see that the sample count determines the error count and the error convergence speed. The bigger the count of samples is, the more the error occurs, but the faster the convergence rate increases with the increase of the threshold. Also, we can see that, if the threshold is over 65%, there are almost no errors.

Hence, we suggest the threshold of different rate is 65%-75%. However, we want to know whether it is suitable for other parameter combinations. We selected K as 200, 400, 500, and 1000 and then repeated the experiments. The results are shown in Figure 8. It shows that, with different K, the threshold of 65%-75% still worked well and the suggestion is effective.

7. Conclusion

With the continuous development of IoT technology, the problems of security, privacy, and credibility are attracting increasing attention [41]. In this paper, we have presented an IoT device credibility verification method based on Blockchain technology and discussed it in detail. The validity

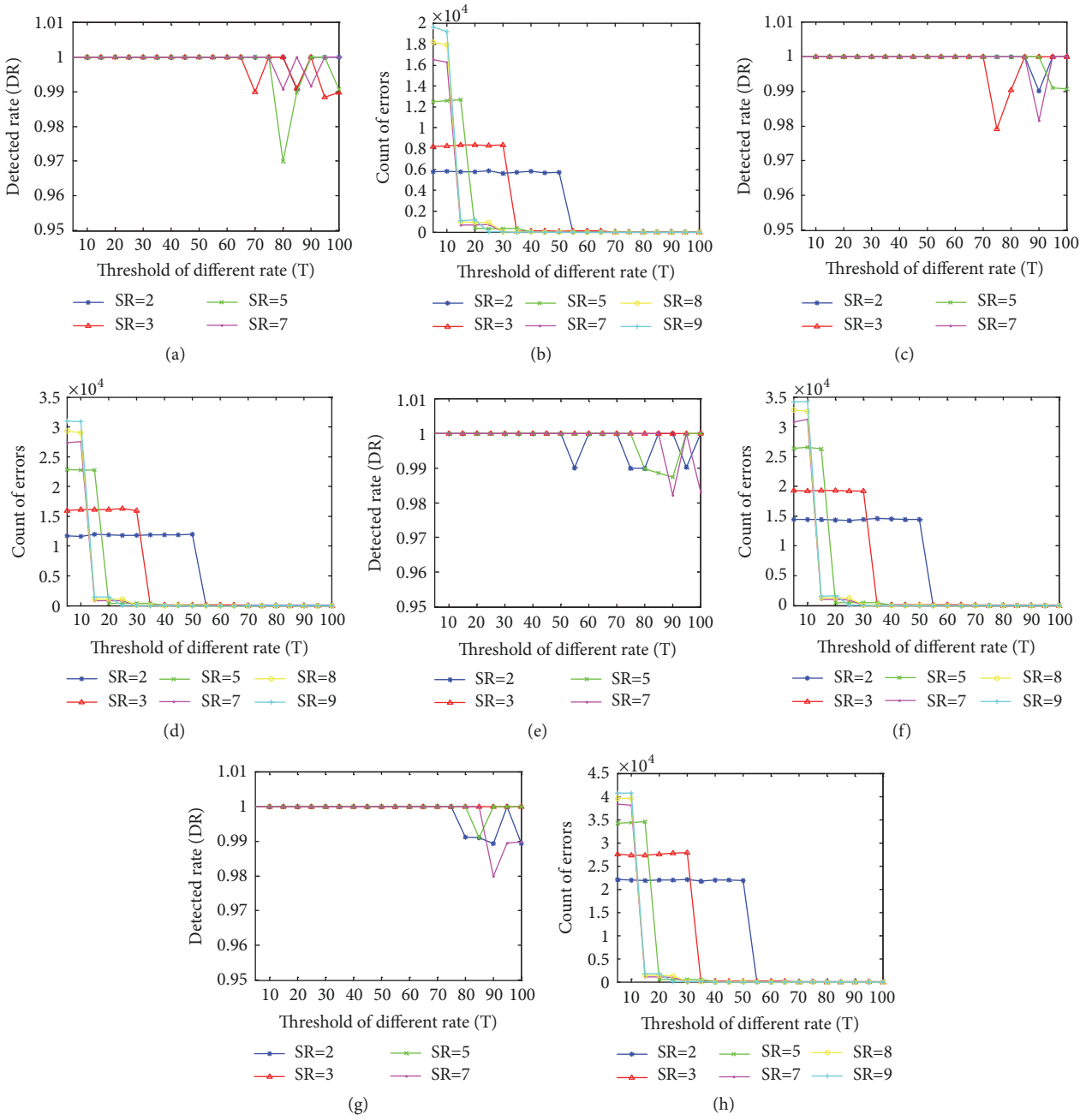


FIGURE 8: Detected rate and count of errors with different K: (a) and (b) $K = 200$; (c) and (d) $K = 400$; (e) and (f) $K = 500$; (g) and (h) $K = 1000$.

of the proposed model and method can reach the credible requirement by Blockchain technology and also has certain advantages in regard to storage space and response time.

Although the proposed method has some advantages, there are still some problems to be resolved. For example, an attack on the MS cannot verify the credibility of all the nodes under it, which does not achieve complete decentralization. The 51% of the computation problem is still not effectively addressed and still threatens the entire network under such an attack. In addition, for a large scale IoT environment, determining how to choose the number of BCS nodes and how to control the height of the tree is still a problem requiring further study.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Key R&D Program of China (Grant no. 2016YFD0400206); the Guangdong University Scientific Innovation Project (Grant no. 2017KTSCX); the Outstanding Young Teacher Training Program of the Education Department of Guangdong Province (Grant no. YQ2015158); Guangdong Provincial Science and Technology Plan Projects (Grant no. 2016A010101035); the National Natural Science Fund, China (Grant no. 61300198).

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Future Generation Computer Systems*, vol. 78, pp. 1040–1051, 2018.

[3] H. Li, Y. Tian, Y. Liu, T. Li, and W. Mao, "UAI-IOT framework: A method of uniform interfaces to acquire information from heterogeneous enterprise information systems," in *Proceedings of the 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, GreenCom-iThings-CPSCom 2013*, pp. 724–730, chn, August 2013.

[4] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 983–994, 2017.

[5] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: the road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[6] C. Gao, Q. Cheng, P. He, W. Susilo, and J. Li, "Privacy-preserving Naive Bayes classifiers secure against the substitution-then-comparison attack," *Information Sciences*, vol. 444, pp. 72–88, 2018.

[7] Z. Huang, S. Liu, X. Mao, K. Chen, and J. Li, "Insight of the protection for data security under selective opening attacks," *Information Sciences*, vol. 412-413, pp. 223–241, 2017.

[8] M. Tao, K. Ota, and M. Dong, "Locating Compromised Data Sources in IoT-Enabled Smart Cities: A Great-Alternative-Region-Based Approach," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2579–2587, 2018.

[9] R. Xie, C. He, D. Xie, C. Gao, and X. Zhang, "A Secure Ciphertext Retrieval Scheme against Insider KGAs for Mobile Devices in Cloud Storage," *Security and Communication Networks*, vol. 2018, pp. 1–7, 2018.

[10] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017*, pp. 618–623, IEEE, Kona, HI, USA, March 2017.

[11] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure Multiple Amplify-and-Forward Relaying with Cochannel Interference," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1494–1505, 2016.

[12] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy Cooperative Networks with Outdated Relay Selection over Correlated Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7599–7603, 2017.

[13] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 106, pp. 117–123, 2018.

[14] Z. Wu, L. Tian, P. Li, T. Wu, M. Jiang, and C. Wu, "Generating stable biometric keys for flexible cloud computing authentication using finger vein," *Information Sciences*, vol. 433-434, pp. 431–447, 2018.

[15] Q. Lin, J. Li, Z. Huang, W. Chen, and J. Shen, "A short linearly homomorphism proxy signature scheme," *IEEE Access*, vol. 6, pp. 12966–12972, 2018.

[16] M. Tao, K. Ota, M. Dong, and Z. Qian, "AccessAuth: Capacity-aware security access authentication in federated-IoT-enabled V2G networks," *Journal of Parallel and Distributed Computing*, 2017.

[17] J. Li, L. Sun, Q. Yan, Z. Li, W. Srisa-an, and H. Ye, "Significant Permission Identification for Machine Learning Based Android Malware Detection," *IEEE Transactions on Industrial Informatics*, vol. PP, no. 99, pp. 1-1, 2018.

[18] J. Chen, K. He, Q. Yuan, G. Xue, R. Du, and L. Wang, "Batch Identification Game Model for Invalid Signatures in Wireless Mobile Networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 6, pp. 1530–1543, 2017.

[19] J. Park and J. Park, "Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions," *Symmetry*, vol. 9, no. 8, p. 164, 2017.

[20] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Čapkun, "On the security and performance of Proof of Work blockchains," in *Proceedings of the 23rd ACM Conference on Computer and Communications Security, CCS 2016*, pp. 3–16, aut, October 2016.

[21] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: a new Blockchain-based access control framework for the Internet of Things," *Security and Communication Networks*, vol. 9, no. 18, pp. 5943–5964, 2017.

[22] J. Shen, C. Wang, T. Li, X. Chen, X. Huang, and Z.-H. Zhan, "Secure data uploading scheme for a smart home system," *Information Sciences*, vol. 453, pp. 186–197, 2018.

[23] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[24] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proceedings of the 19th International Conference on Advanced Communications Technology, ICACT 2017*, pp. 464–467, kor, February 2017.

[25] C. Wang, J. Shen, Q. Liu, Y. Ren, and T. Li, "A Novel Security Scheme Based on Instant Encrypted Transmission for Internet of Things," *Security and Communication Networks*, vol. 2018, pp. 1–7, 2018.

[26] C. Qu, F. Liu, and M. Tao, "Ontologies for the transactions on IoT," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 934541, 12 pages, 2015.

[27] M. Tao, K. Ota, and M. Dong, "Ontology-based data semantic management and application in IoT- and cloud-enabled smart homes," *Future Generation Computer Systems*, vol. 76, pp. 528–539, 2017.

[28] P. Li, T. Li, H. Ye, J. Li, X. Chen, and Y. Xiang, "Privacy-preserving machine learning with multiple data providers," *Future Generation Computer Systems*, 2018.

[29] C. Qu, F. Liu, M. Tao, and D. Deng, "An OWL-S based specification model of dynamic entity services for Internet of Things,"

Journal of Ambient Intelligence and Humanized Computing, vol. 7, no. 1, pp. 73–82, 2016.

[30] M. A. Razzaque and S. Clarke, "Smart management of next generation bike sharing systems using Internet of Things," in *Proceedings of the 1st IEEE International Smart Cities Conference, ISC2 2015*, mex, October 2015.

[31] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. PP, no. 99, pp. 1-1, 2018.

[32] Q. Liu, Y. Guo, J. Wu, and G. Wang, "Effective query grouping strategy in clouds," *Journal of Computer Science and Technology*, vol. 32, no. 6, pp. 1231–1249, 2017.

[33] J. Li, X. Chen, S. S. Chow, Q. Huang, D. S. Wong, and Z. Liu, "Multi-authority fine-grained access control with accountability and its application in cloud," *Journal of Network and Computer Applications*, vol. 112, pp. 89–96, 2018.

[34] S. Peng, A. Yang, L. Cao, S. Yu, and D. Xie, "Social influence modeling using information theory in mobile social networks," *Information Sciences*, vol. 379, pp. 146–159, 2017.

[35] W. Chen, H. Lei, and K. Qi, "Lattice-based linearly homomorphic signatures in the standard model," *Theoretical Computer Science*, vol. 634, pp. 47–54, 2016.

[36] J. Chen, K. He, R. Du, M. Zheng, Y. Xiang, and Q. Yuan, "Dominating set and network coding-based routing in wireless mesh networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 2, pp. 423–433, 2015.

[37] R. H. Jhaveri, N. M. Patel, Y. Zhong, and A. K. Sangaiah, "Sensitivity Analysis of an Attack-Pattern Discovery Based Trusted Routing Scheme for Mobile Ad-Hoc Networks in Industrial IoT," *IEEE Access*, vol. 6, pp. 20085–20103, 2018.

[38] K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, "DeyPoS: deduplicatable dynamic proof of storage for multi-user environments," *Institute of Electrical and Electronics Engineers. Transactions on Computers*, vol. 65, no. 12, pp. 3631–3645, 2016.

[39] T. Li, J. Li, Z. Liu, P. Li, and C. Jia, "Differentially private Naive Bayes learning over multiple data sources," *Information Sciences*, vol. 444, pp. 89–104, 2018.

[40] Y. Li, G. Wang, L. Nie, Q. Wang, and W. Tan, "Distance metric optimization driven convolutional neural network for age invariant face recognition," *Pattern Recognition*, vol. 75, pp. 51–62, 2018.

[41] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When Intrusion Detection Meets Blockchain Technology: A Review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018.