A Review of Blockchain-Based Access Control for the Industrial IoT

Peng Zhai[1,2], Liping Zhang[3], Jingsha He[1*]

[1]*Faculty of Information Technology, Beijing University of Technology, Beijing, China*

[2]*School of Mathematics and Computer Application Technology, Jining University, Jining, Shandong, China*

[3]*Department of Theoretical Information Engineering, Shandong Yankuang Technician Institute, Jining, Shandong, China*

**Corresponding Author.*

Abstract

The rapid development and wide application of industrial Internet of things (IoT) have made network security issues such as identity authentication, access control, and data privacy more and more important in the distributed network environment, while blockchain technology benefiting from the advantages of decentralization, high confidence, and difficulty tampering are able to solve the trust problem existing in traditional access control technology. In this paper, firstly the basic concepts of access control and blockchain are explained, and the existing access control model and method based on blockchain in the industrial IoT scenario are summarized. Next, according to different implementation methods of blockchain, two technical routes are innovatively divided, i.e., the blockchain acts as a trusted entity (combination blockchain mode) in combination with the traditional access control technology, and the access control model constructed by completely utilizing the brand-new mode (full blockchain mode) of the distributed and non-tampering characteristics of the blockchain. From the angle of these two technical routes, the unique advantages of applying the blockchain to the IoT access control field are analyzed. Then, according to the key issues in the application of blockchain, the current research progress is summarized from the aspects of dynamic access control, space optimization on the chain, privacy data protection, etc. Finally, the further research direction is provided combined with the current challenges of access control mechanism based on industrial IoT.

Keywords*: Access control, industrial industry, IoT, Blockchain, smart contract*

I. Introduction

Since the concept of Internet of Things (IoT) was put forward in 1999, IoT has attracted great interest from academics, researchers and entrepreneurs with its rich cross-border applications and innovative service capabilities, because it can seamlessly connect heterogeneous devices and network entities [1]. With the emergence of intelligent application scenarios such as intelligent manufacturing and smart cities, the IoT has become a field with great influence, opportunities and development prospects. Figure 1 shows a wide range of application scenarios of the IoT. In 2020, 50 billion IoT devices have been deployed globally, and it is predicted that by 2024, the total data volume of IoT worldwide is expected to reach 71.3 ZB. The diversity of applications of the IoT has changed the industrial manufacturing and intelligent life, but also brought potential safety hazards, because the IoT has produced huge amounts of data, including a large amount of industrial production and private data, which will bring huge losses to users once leaked. Identity authentication and access control to resources and services are the main means to protect the security of the IoT.

Access control determines the communication permissions of authorized subjects to objects according to specific security models and policies. As the basic mechanism to realize security in network system, an effective access control mechanism can meet the information security requirements such as confidentiality, integrity and

availability of the system. At first, in order to solve the problem of authorized access to shared data on mainframe, Discretionary Access Control (DAC) and Mandatory Access Control (MAC) models were proposed. With the development and popularization of computer and network technology, the access control technology in the IoT environment has been developing continuously, which has spawned the mainstream AC methods: Role-based Access Control (RBAC) [2], Attributes-based Access Control, (ABAC) [3], Usage Control (UCON) [4] and Capability-based access control (CapBAC) , etc.

Most of the above-mentioned traditional access control models have a centralized authorization decision entity that make AC decisions based on access control policies and other attribute contents, which makes them vulnerable to various attacks including single point of failure and denial of service. Even though CapBAC model can implement distributed access control decisions, it is also suitable for resource-limited devices, but it cannot solve the access control problem in the untrusted network environment of the IoT. The blockchain is a decentralized, peer-to-peer distributed ledger technology based on cryptographic algorithms, and its tamper-resistant, forgery-resistant, and auditable features can well solve the access control problems of this heterogeneous, multi-source, and dynamic untrusted IoT environment.

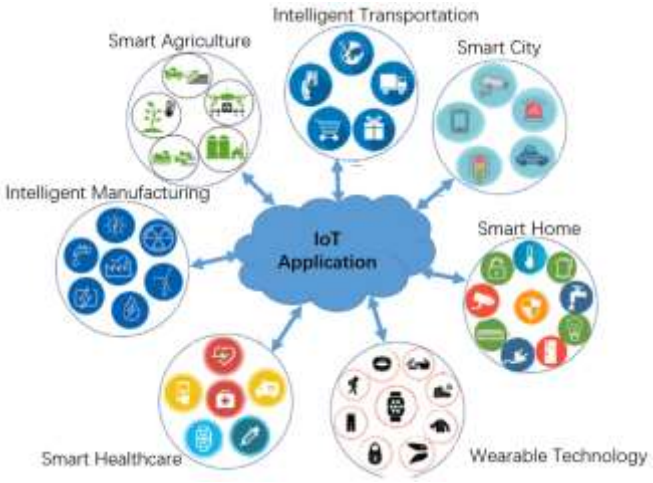

Fig 1: Wide application of the IoT

The rest of this paper is organized as follows: In the second section, the traditional access control technologies RBAC, ABAC, UCON and CapBAC are mainly explained, and they are compared from the perspective of technical realization and function. In the third section, the blockchain technology related to access control is introduced. In the fourth section, the access control models mentioned in the mainstream literature are divided into two types: the blockchain which combines with the traditional access control technology and acts as a trusted entity (combination blockchain mode) and a brand new mode (full blockchain mode) which fully utilizes the distributed and tamper-proof characteristics of the blockchain. From the perspective of these two technical routes, the unique advantages of the combination of blockchain technology and AC technology for IoT terminal devices are analyzed. In the fifth section, the whole paper is summarized and the further challenges and research directions of AC in the IoT environment based on blockchain is discussed.

II. Traditional IoT access control technology

2.1 Basic process of access control

The role of access control is to restrict access of access subjects to the access objects so that information resources can be accessed within a legally controlled scope. The access control model consists of three elements: subject, object and access control policy. The subject is the active entity that initiates the visit request and is the initiator of the visit action operation. An object is the recipient of an access operation because it is a passive entity that

receives access to other entities. An access control policy is a set of access rules that control the behavior of access objects. Figure 2 shows the key elements and processes involved in access control approval decisions.

Fig 2: Access control elements and basic process

2.2 Common access control models in the IoT

With the continuous development of IoT, access control models based on the IoT emerge endlessly, and the more popular access control models are compared and analyzed.

2.2.1 RBAC model

Which is an important model of access control, was first proposed by Ferraiolo and Kuhn [2]. It associates roles with a set of privileges, which enable users to access service resources based on the pre-assigned roles of the computer system. Roles are an essential part of the RBAC model and are categorized based on different attributes of users. RBAC models generally contain five sets of data elements, $Users(U), Roles(R), Objects(OBJ), Operations(OPT), Permissions(P)$.

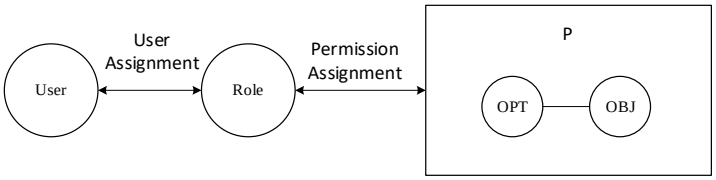

Fig 3: Composition of RBAC access control model

With the rapid development of the IoT, scholars have applied RBAC model to access control in the IoT, which can support distributed scalability, lightweight, cross-domain access control and heterogeneous devices in the IoT environment [6]. Since the operation of RBAC model depends on the association relationship among users, roles and permissions, the system needs to maintain a large amount of associated information of {users, roles}, {roles, permissions}, and their storage and processing, coupled with the limited resources of IoT equipment, cannot meet the access control requirements of massive nodes and data in the IoT. [6] The computing and storage capabilities of the access control are increased through the IoT gateway or a third-party server, and the complexity of the access control list can be reduced by separating the user and the permission, thereby compressing the storage space and reducing the system computation overhead. The related research to solve this kind of problem is that an RBAC access control model was proposed for Manufacturing Internet of Things (MIOT) in reference [7], which mainly solves the problem of permission allocation for specific users and roles in multi-domain systems, and uses the best authorization route for permission diffusion management. In reference [6], a method to obtain information of human wearable IoT sensors through RBAC model in the field of smart medical care was put forward. In reference [5], an access control model which combines RBAC and trust evaluation (TE) algorithm was put forward, which is suitable for the IoT environment. In reference[8], a new access control model of RBAC based on priority authentication mechanism was designed and put forward, which encapsulates different users' access permissions to

resources, improves access control efficiency based on different scheduling of priority authentication and ensures the consistency of individual users' access control policies. In reference [6], a highly scalable and lightweight data fuzzy technology for RBAC access control was proposed, and digital watermarking technology was used for sensitive data access control in health-care scenario.

2.2.2 ABAC model

ABAC model, which controls access to objects by policy according to attributes of entities (subjects, objects), operations and environments related to requests. Both subject and object are identified by attributes related to features. When users initiate access requests, they will be granted the permissions according to related subject and object attributes. ABAC consists of a quaternion {S, O, A, E}, in which S, O, A and E represent the attribute sets of related subject, object, action and environment respectively.

ABAC is widely used in the IoT because of its convenience and fine-grained access control. In reference [9], an effective access control framework was proposed for IoT, which adopted the authorization method based on ABAC as the access control policy and established simple and effective mutual authentication based on ECC security key. The described protocol provides lower storage and communication overhead to solve the resource constraint problem of IoT perception layer. In view of the characteristics of low power consumption and large number of devices in the IoT, an improved ABAC access control model in the IoT environment was proposed in reference [3], and a lightweight trust-ABAC access control and privacy protection method for the IoT was proposed by combining ABAC with trust concept in reference [3].

2.2.3 UCON model

Compared with the traditional RBAC and ABAC access control models, UCON pays more attention to the processing of dynamic problems, and can detect the continuity and variability factors in the access control process, monitor the whole process of subject accessing object resources in real time, and adjust its resource access permission in real time if the attributes of an entity (subject or object) change dynamically with the environment and context . UCON includes six main elements: subject, object, permission, authorization rules, obligations and conditions.

UCON well solves the problem of dynamic access of terminal nodes under the environment of the IoT, and can also immediately deal with the problem of node attribute change in the access control process. In reference [4], UCON was used in the IoT scenarios, and an IoT access control model based on fuzzy theory is proposed. UCON was used for vehicle networking in reference [4], which provides powerful expression ability and flexible authorization strategy.

2.2.4 CapBAC model

CapBAC model is an implementation of access control matrix model, in which each subject is associated with the corresponding capability matrix list, which records the access permissions corresponding to the subject. In CapBAC, the permission can be verified by the IoT entity itself instead of a third party.

The lightweight and distributed access control can be realized by introducing the CapBAC model in the IoT, which can well support the dynamic nature and scalability of the IoT, because CapBAC can grant the access control permission of a subject to others who can further authorize all or part of the permission, with all the permissions controlled. CapBAC model based on distributed implementation can easily realize fine-grained access control decision-making on the IoT devices with limited resources, large number and various kinds.

III. Blockchain Technology Related to Access Control

3.1 Concept and development of Blockchain

Blockchain is a P2P distributed ledger technology based on cryptography, which uses cryptographic algorithm to

ensure the safe transfer of data and value, hash function and timestamp mechanism to ensure the traceability and non-tampering of data, and consensus algorithm to ensure the consistency of data between nodes.

It is generally believed that the development of the blockchain has gone through three stages: the use of digital currency represented by Bitcoin in the blockchain 1.0 stage, which mainly includes the application of data currency issuance, payment, and circulation; the introduction of smart contracts in the blockchain 2.0 stage, which optimized the process of digital asset management and provided a broader application of the blockchain in the financial field; and the provision of a decentralized solution for all walks of life across digital currency and the financial field in the blockchain 3.0 stage.

Blockchain can be divided into private, public and consortium blockchain according to the characteristics of access control mechanism and authentication methods. Table 1 gives the mainstream blockchain platforms used in the IoT platforms, which are compared from the platform release time, ledger type, consensus algorithm, TPS, hashing algorithm, smart contracts, E-currency type, etc.

Table 1 Comparison of Blockchain Systems

	Bitcoin	ETH	Multichain	R3 Corda	IOTA	Fabric	EOS	Libra
Release Year	2009	2015	2015	2016	2016	2017	2018	2020
Ledger Type	Permissionless	Permissionless	Permissioned	Permissioned	Permissionless	Permissioned	Permissioned	Permissioned
Consensus Algorithm	PoW	PoW PoS	PoW	Notary	PoW Tangle	PBFT Kafka	DPos	LibraBFT
TPS	7	15-20	200-1000	-	500-800	3000	4000	1000
Hashing Algorithm	SHA256	KECCAK256	SHA256	SHA256	CurlP27	SHAKE256 SHA3	SHA256	SHA3 HKDF Ed25519
Smart Contracts	Bitcoin Script	Smart Contract	Smart Filters	FLOW	Smart Contract	Chain Code	Smart Contract	
Ecurrency	Bitcoin	Ether	-	-	IOTA	-	EOS	Libra

3.2 Main characteristics of Blockchain

Blockchain technology has many advanced concepts and characteristics, such as well-known decentralization, anti-tampering and traceability, which provides convenience for the wide application of the IoT. Moreover, its distributed, decentralized technology without third-party participation realizes data and entity access control in an untrusted network environment.

Decentralization: In the blockchain, trusted third-party entities are removed to store data in a plurality of nodes of a point-to-point network, and the system has strong resistance to technical failures or malicious attacks, so that even if some nodes are interrupted offline, the availability and security of the whole network are not affected, and the technical bottleneck and the single-point failure are well solved. The decentralized point-to-point network architecture gives all network entities the right to participate fairly and can verify the correctness of the IoT data at any time.

Anti-tampering: Hash function is used in blockchain to ensure that data is not tampered with. The data in the Blockchain is time-stamped after being checked by the relevant network entity, and then inserted into a Block data

block, which is encrypted and protected by a hash function. The blockchain links all the encrypted blocks together through a data structure to form a sequence chain. The new block header holds the hash value of the previous block, and so on, which prevents the data in the block from being updated, modified and deleted.

Safety, transparency and traceability: Blockchain is a decentralized data storage system which combines distributed data storage, P2P transmission, consensus mechanism and encryption algorithm. The data must be verified by a plurality of verification nodes in the blockchain, and can be written into the blockchain only after a consensus algorithm is formed on the authenticity. The write mechanism of that blockchain can realize the real traceability of the information on the premise that the verification node has enough credibility and the verification nodes do not mutually seek profit. Because blockchain is highly transparent and secure, which makes the credit in the data system conductive and traceable, and enhances the credit between entities and users.

3.3 Consensus mechanism

The blockchain technology needs to enable untrusted nodes to verify the reliability of the blocks in a decentralized network without the participation of third-party trusted entities, which requires the nodes in the blockchain to adopt a consensus mechanism to solve the consistency problem generated by the block distributed storage, namely the Byzantine general problem. The blockchain is divided into three types according to different access and management methods: public blockchain, consortium blockchain and private blockchain. Due to different environments and requirements of each type, different consensus mechanisms are required.

Consensus mechanism for public blockchain: Public blockchain, also known as unlicensed blockchain, is a completely open blockchain system, in which any entity can freely join and participate in the consensus accounting process, with a huge number of nodes and the lowest trust among nodes. Typical consensus mechanisms include proof-of-work (PoW), proof-of-stake (PoS) and their derivative versions PoC, DPoS, LPoS, Pol, PoA, Casper, PoB, etc.

Consensus mechanism for consortium blockchain: Consortium chain, a kind of licensed blockchain, is semi-open and jointly initiated by several organizations to form a consortium, in which the generation, consensus and maintenance of ledgers are completed by the members designated by the consortium. Typical consensus mechanisms are Byzantine-Fault-Tolerant (BFT) t mechanism, PBFT, dBFT, SCP, Ripple, Tendermint and so on.

Consensus mechanism for private blockchain: Private blockchain is also a kind of licensed blockchain, which is established by the private organizations themselves and has a higher degree of centralization than the consortium blockchain, in which the process of data generation, consensus and maintenance is completely controlled by a single organization. The private blockchain assumes that the participating nodes are not aggressive, which relaxes the assumptions of the consensus mechanism.

IV. IoT AC Model Based on Blockchain

At present, Access control requirements of the IoT include:

1. Lightweight terminal nodes. IoT terminal devices generally do not have very strong computing and storage capacity. Some terminals even have no storage capacity for sensor data collection and transmission, and cannot complete lots of data storage and calculation tasks.
2. A large number of terminal nodes. Generally, the IoT system has a large number of terminal devices, which will generate a large amount of data and require strong computing, storage and data transmission capabilities.
3. Terminal dynamics. Some IoT terminals have the requirement of location movement, which requires access control to meet the mobility and dynamic access problems.
4. Distributed architecture. IoT devices are generally distributed physically and logically, which involves the distributed dynamic access control of devices.

Blockchain is distributed, transparent in transaction, and hard to tamper with, and has a trusted mechanism without endorsement from a third party, which coincides with the access control requirements under the IoT environment. At present, there are two main ways to realize access control technology in the IoT environment based on blockchain: one is to combine blockchain with existing traditional access control such as RBAC, ABAC, UCON, CapBAC, etc., and the other is to build a completely blockchain access control model based on transaction or smart contract based on the characteristics of blockchain.

4.1 Blockchain combined with traditional access control technology (mixed blockchain mode)

Due to its security features such as non-tamper, auditable and traceable, the blockchain itself can act as a trusted third party in the access control of the IoT.

According to the different contents stored on the different blockchain, there are two access control methods:
Access control policies are stored in the blockchain. In reference [10], by using the blockchain storage access control policy and eliminating the concepts of POW and bitcoin, a lightweight example of blockchain especially suitable for IoT is proposed, which is embodied in the smart home environment. In this smart home environment, each scenario has a private blockchain network, which is deployed on a high-performance gateway device, called a "miner", which has high computing, storage, communication capabilities and can handle the operation, control and security of the entire network. In references [11], the access control system is designed by using blockchain technology to ensure the evaluation of AC policy audit, and the attribute-based AC policy is edited into smart contract and stored in blockchain, and the policy evaluation process is transformed into distributed smart contract execution. In addition, a method to publish the right policies for accessing resources is proposed, and these policies can be distributed among users. The exchange of policies and permissions on the blockchain is open and transparent, and any user can know the policy of resource matching at any time.

Access permission is stored in blockchain. an attribute-based AC mechanism is designed, which can provide decentralized, flexible and fine-grained authentication between IoT devices, and provide authentic and reliable authentication credentials by using blockchain. Blockchain is used to store access control permission, and its distributed and unchangeable characteristics ensure the security of permission information.

In addition, some researchers store the data collected, generated and used by IoT devices in the blockchain. However, due to the characteristics that blockchain data can only be added and cannot be deleted, and a large number of IoT devices generate more data, access control data should be stored instead of data generated by IoT when using blockchain storage.

4.2 new model that takes full advantage of the blockchain feature (full blockchain model)

The combination of blockchain and traditional access control technology mainly focuses on the trusted entities in the blockchain and does not give full play to the characteristics of the blockchain. Due to the inefficiency and low performance of using blockchain to store data of the IoT, some researchers store a large amount of data under the chain and only store hash values pointing to the data on the chain. Blockchain provides a trusted platform for access control to execute smart contracts.

According to different blockchain-based platforms, access control can be divided into two types:

1.Access control model based on bitcoin architecture.
A novel system of IoT access control of Bitcoin blockchain technology is proposed. FairAccess is introduced as a completely decentralized management framework for pseudonym and privacy protection authorization, which enables users to own and control the data. A blockchain is used and adapted as a decentralized AC manager. Unlike bitcoin transactions, FairAccess has introduced new transactions for granting, acquiring, delegating and revoking access permissions. Ouaddah proposed a dynamic distributed security policy, and realized the access

control of terminal devices in the Internet of Things environment by using the method of machine learning, which indicates that access control technology will be more combined with artificial intelligence technology in the future.

2. AC model based on ETH architecture

Support for smart contracts is the biggest feature of the ETH platform, which can perform any complex computation with the computing power provided by the smart contracts. In order to solve the problem of massive terminals and dynamic access in the IoT, a lot of research has been done from the dimensions of distributed management, data compression and performance optimization. In reference [12], a blockchain-based AC framework for distributed IoT is proposed, in which the blockchain node account address is used as the identity account to access the IoT management server, and the access control authority of device data is redefined and the blockchain storage is carried out. In this model, the processes of authentication, authentication revocation, access control and audit are also designed. Finally, the privacy of IoT data is protected by using lightweight symmetric encryption algorithm. In reference, three smart contracts, subscription, publication and client, are created by using blockchain technology to manage the access control rules, authentication information and network communication of IoT nodes. The PKI system based on multi-layer framework, which manages token-based access control of records under the chain, assigns token-based access control policies with different roles to users, access control policies that encode smart contracts in the IPFS file system, access permissions that encode data stored in the DHT in the smart contracts. ABAC technology is used to simplify access management, data providers can safely share, audit and revoke access control schemes, access control framework applied to UAV networks, and AC mechanism based on super ledger Fabric.

Generally speaking, the current AC mechanism based on smart contract can be divided into five aspects by utilizing the characteristics of blockchain trusted computing: 1) user information management. Users are bound with their Ethernet address, public key and other information, so that the user information can be traced back without being tampered with. 2) Authority information management. The data in the smart contract management chain is used to realize the management of data including access control policy, entity access permissions, subject and object attribute information, etc. 3) Access control behavior monitoring. By tracing the source by means of timestamp and user signature on the blockchain, the data on the chain can be guaranteed not to be damaged or tampered with. 4) Access control. The smart contract is utilized to judge whether a subject visitor meets an object access control policy or not according to the information such as the identity, the role, the token, the attribute and the like of the subject visitor, and the access control judgment is carried out, so that a trusted environment is constructed for a host-object resource owner and a requester without the intervention and participation of a trusted third party and relying on the execution in the smart contract.

V. Summary and Outlook

In summary, firstly the traditional AC technologies such as RBAC, ABAC, UCON and CapBAC are illustrated and compared from the view of technology implementation and function. Then, the blockchain technology related to access control is introduced, the basic concepts of access control and blockchain are explained, and the existing access control models and methods based on blockchain in the IoT scene are summarized. According to different implementation modes of blockchain, two technical routes, namely, the combination of blockchain and traditional access control technology as a trusted entity (combination blockchain mode) and a brand-new mode (full blockchain mode) that makes full use of blockchain characteristics, are respectively elaborated. From the perspective of these two technical routes, the application of blockchain technology to IoT access is analyzed. Then, according to the key problems in blockchain application, the existing research progress is summarized from the aspects of dynamic access control, space optimization on the chain, and privacy data protection.

In the future, the research on access control based on blockchain will focus on the following dimensions: 1) Cross-domain and cross-chain access problems under the organization of few consortium blockchains. As there are multiple trusted domains in the network which are closed respectively under the environment of the IoT, how to use the safe and trusted characteristics of the blocks to realize the interconnection and intercommunication of each

trusted domain, and establish a low-cost trust mechanism to meet users' cross-domain access control requirements. 2) Access control performance optimization. The original purpose of blockchain is to serve the financial application fields such as e-currency as the underlying technology of Bitcoin. Its mining mechanism is not suitable for access control requirements. Moreover, it also faces the problems of large delay, slow block generation and high data computing and storage overhead on ETH platform, which restricts the performance of access control system. How to improve the consensus, bookkeeping, contract mechanism and computing and storage structure of blockchain to meet the access control requirements is also a problem that must be solved in the future. 3) User privacy protection. Blockchain, as an open ledger, needs to consider the privacy protection of sensitive and critical data in its application. How to design a distributed cryptographic protocol suitable for blockchain and solve security and performance problems is also the next research focus. 4) The combination of blockchain and AI. Introducing AI into the access control mechanism based on blockchain can reduce the workload and improve the security of the system through technologies such as machine learning. Furthermore, deep learning algorithm can be used to improve access control policies, optimize authorization scope and solve policy conflicts.

References

[1] D. F. Li, Y. Hu, and M. M. Lan, "IoT device location information storage system based on blockchain," Future Generation Computer Systems-the International Journal of Escience, vol. 109, pp. 95-102, Aug 2020.

[2] D. F. Ferraiolo, and Kuhn, R., "Role-based access controls," presented at the Proceedings of 15th NISTNCSC National Computer Security Conference, Baltimore MD, 1992.

[3] O. H and A. NB, "Trust-ABAC Towards an Access Control System for the Internet of Things," presented at the In: Proc. of the Int'l Conf. on Green, Pervasive, and Cloud Computing. Cham, 2017.

[4] Z. Guoping and G. Wentao, "The Research of Access Control in the Application of VANET Based on UCON," Procedia Engineering, vol. 29, pp. 4091-4095, 2012.

[5] H.-C. Chen, "Collaboration IoT-Based RBAC with Trust Evaluation Algorithm Model for Massive IoT Integrated Application," Mobile Networks and Applications, vol. 24, no. 3, pp. 839-852, 2018.

[6] P. A. Yavari A, G. D, J. PP, and S. RV, "Scalable role-based data disclosure control for the Internet of things," presented at the In: Proc. of the IEEE 37th Int'l Conf. on Distributed Computing Systems., 2017.

[7] Q. Liu, H. Zhang, J. Wan, and X. Chen, "An Access Control Model for Resource Sharing Based on the Role-Based Access Control Intended for Multi-Domain Manufacturing Internet of Things," IEEE Access, vol. 5, pp. 7001-7011, 2017.

[8] A. Thakare, E. Lee, A. Kumar, V. B. Nikam, and Y.-G. Kim, "PARBAC: Priority-Attribute-Based RBAC Model for Azure IoT Cloud," IEEE Internet of Things Journal, vol. 7, no. 4, pp. 2890-2900, 2020.

[9] Y. Z. N. Ye, R.-c. Wang , R. Malekian , L. Qiao-min, "An efficient authentication and access control scheme for perception layer of internet of things," Applied Mathematics & Information Sciences, vol. 1624, no. 4, 2014.

[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 English), 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (Percom Workshops), 2017.

[11] D. Di Francesco Maesa, P. Mori, and L. Ricci, "A blockchain based approach for the definition of auditable Access Control systems," Computers & Security, vol. 84, pp. 93-119, 2019/07/01/ 2019.

[12] N. Shi et al., "BacS: A blockchain-based access control scheme in distributed internet of things," (in English), Peer-to-Peer Networking and Applications, Jun 12, 2020.