IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 7, 2021, accepted March 24, 2021, date of publication April 8, 2021, date of current version April 14, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3071031

Secure ABE Scheme for Access Management in Blockchain-Based IoT

JIANSHENG ZHANG[1], YANG XIN[1,2], YULONG GAO[3,4], XIAOHUI LEI[5], AND YIXIAN YANG[1,2]

[1]National Engineering Laboratory for Disaster Backup and Recovery, Information Security Center, School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]Guizhou Provincial Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China
[3]State Key Laboratory of Media Convergence and Communication, Communication University of China, Beijing, China
[4]School of Computer and Cyber Sciences, Communication University of China, Beijing 100024, China
[5]Beijing Everyone Crowdsourcing Technology Company Ltd., Beijing 100018, China

Corresponding author: Yang Xin (yangxin@bupt.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB0802300 and Grant 2018YFB0803700, in part by the Major Scientific and Technological Special Project of Guizhou Province under Grant 20183001, in part by the Foundation of Guizhou Provincial Key Laboratory of Public Big Data under Grant 2018BDKFJJ021 and Grant 2017BDKFJJ015, and in part by the Fundamental Research Funds for the Central Universities.

ABSTRACT Internet of Things (IoT) has been widely used in various fields of our daily life in the past years. Obviously, in the future, the significance of its security will be more evident and enormous. However, there are still many security issues in the IoT, which makes it vulnerable to be attacked easily by some potential factors. Targeting at these issue, in this paper, we propose a secure access management scheme in IoT based on blockchain. Firstly, in our work, by using the Decisional Learning with Error (DLWE) problem, we propose a secure Key-policy Attribute-based Encryption (KP-ABE) scheme, it can implement fine-grained access control in IoT. Secondly, we use blockchain to solve the authentication and access management challenges. In addition, the smart contract in blockchain can process transactions automatically, which greatly reduces the management cost and running time for this scheme. Last but not the least, we further analyze the security of our proposed scheme. The result shows that our scheme can resist some common attacks in IoT, and it is more secure and efficient.

INDEX TERMS IoT, blockchain, Attribute-based Encryption, security, authentication.

I. INTRODUCTION

MIT's Automatic Identification Center proposed the concept of the Internet of Things(IoT) in 1999 for the first time. Subsequently, IoT has already been used in many practical applications in past years. Kevin described the IoT as a global standard system consisting of Radio Frequency Identification (RFID) and other sensors [1]. In 2005, ITU published a report and expanded the meaning of Internet of Things. IoT is interpreted as an extension of the Internet, which includes RFID [2], sensor network technology [3], smart devices, etc. Through IoT technology, data is collected by devices that can be processed in real time. In this way, it can improve the whole system's efficiency and reduce costs [4]. Because it is closely related to people's life and even industrial production, IoT has received more and more research and attention. In particular, with the development of hardware technology, the related devices of IoT have been well optimized and improved. Especially wireless sensor networks (WSN) [5], machine-to-machine(M2M) [6] and cyber-physical systems(CPS)[7], [8] have now become part of Internet of Things [9]. The potential application space of IoT has been greatly expanded in these past few years.

However, with the IoT's development, its security challenges can not be ignored. IP protocol is the main standard of connection, some security issues related to WSN, M2M and CPS also continue to emerge in some IoT applications. Therefore, the entire deployment architecture needs to be protected from attacks by anyone. And it also needs to be avoided which some threats to the privacy, integrity or confidentiality of data [10], [11]. In addition, because the IoT model combines the Internet with heterogeneous devices, it also has traditional security problems related to computer networks.

The device distribution in IoT is scattered, and manufacturers lack security awareness, which makes many devices lack security measures such as encryption, authentication, access control and so on. In many cases, linking device does not even require password for authentication. In addition, some early IoT devices still use very outdated software versions and cannot achieve remote upgrades [12]. These software weak-

The associate editor coordinating the review of this manuscript and approving it for publication was Junaid Arshad.

nesses make IoT devices become very vulnerable when they are attacked. Therefore, through illegal access or Distributed Denial of Service (DDoS) attack, attackers can invade our IoT system and control our intelligent devices. In the past year, the IoT system has been attacked in a number of major network security incidents all around the world. In another paper, Komninos concluded that any security design for IoT needs to satisfy three major security requirements, which are confidentiality, integrity and availability, respectively [13].

In 2008, blockchain technology was presented by Nakamoto for the first time [14]. In general, blockchain is a novel de-centralized, de-trusted, transparent and distributed ledger technology [15]. This technology mainly lets a large number of nodes participate this system and communicate with each other in a certain period of time. A series of data blocks are linked by cryptographic association, and signature is generated to verify the validity of transaction information [16]. At last, though consensus mechanism [17], all nodes share and store a same public database in their own local storage. As mentioned above, combining Elliptic Curve Digital Signature Algorithm (ECDSA) [18], distributed storage, and consensus mechanisms, blockchain technology enables these participants who do not fully trust each other to form and maintain consensus in a distributed network [19], [20].

In recent years, there are more and more researches on the combination of IoT and blockchain and blockchain [21]. In 2017, by introducing blockchain technology, Li *et al.* proposed a multi-layer secure IoT network model [22]. This model can reduce the difficulty of actual deployment and provide a wide-area networking solution of IoT. Unfortunately, it adopts centralized access management. When access control queries and updates frequently, a single centralized access control server will increase the load of the system. Meanwhile, Huh *et al.* provided a scheme to manage IoT devices by using Ethereum [23]. However, there is no detailed security analysis in his scheme.

Different from other previous works, we take attribute based encryption scheme as a technical breakthrough. In this paper, we design a secure Key-policy Attribute-based Encryption (KP-ABE) scheme and introduces it into the access control of the IoT based on blockchain. It can realize fine-grained access control and improve the efficiency and security for accessing IoT system.

The main contributions of this paper are summarized as follows.

- By using the Decisional Learning with Error (DLWE) problem, we first propose a secure lattice-based KP-ABE scheme in this paper. It can support flexible access policies and provides privacy protection for user. More importantly, it implements fine-grained access control in IoT.
- Combining the lattice-based ABE scheme and blockchain, we propose a secure access management scheme with ABE in IoT. In this new scheme, we use blockchain for authentication and access management. Through the signature verification of blockchain, it can realize the safe and reliable identity verification for IoT device and its communication data, and ensure the security of the IoT.
- At last, we provide the security analysis of our new scheme in terms of data security, identity authentication, resistance to attacks. Through our analysis, this novel scheme can not only provide a large number of addresses for the large-scale application of IoT, but also solve the problem of ownership transfer for smart devices. More importantly, it also can resist some common attacks in IoT, such as DDoS attack, illegal access.

By introducing the blockchain, IoT becomes more intelligent and the operations of smart devices are more easy and efficient. The remainder of this paper is organized as follows. In section II, we introduce the main security threats of IoT. In section III, a secure lattice-based ABE scheme is proposed. In section IV, we provide our secure access management scheme and we analyze its security in section V. Some concluding remarks are given in section VI.

II. RELATE WORKS

A. SECURITY THREATS OF IoT

The IoT is regard as an extension of the Internet, the relationship between them is inseparable and complementary. On the contrary, they also have many differences in organizational forms, network functions and performance requirements. IoT has the following security threats in access control.

1) DATA SECURITY

As a heterogeneous multi-network convergent network, IoT not only has the same security problems as sensor networks, mobile communication networks or the Internet, but also has its particularities, such as equipment management, privacy protection, data storage and management, etc. Many IoT devices are more vulnerable to be attacked without safety protection technology. In many cases, linking devices even do not require password for authentication. In addition, some early Internet of Things devices still use very outdated software versions, which can not achieve remote upgrades. These vulnerabilities and weaknesses make the IoT's data become very vulnerable to attack and ring breaking in storage and transmission easily.

2) CENTRALIZED RISK

At present, the main access control methods in the IoT are role-based access control (RBAC) [24], attribute-based access control (ABAC) [25], usage control (UCON) [26], [27]. These above three access control models, RBAC, ABAC and UCON, are all made by a centralized authorized decision-making entity based on access control strategy and other attribute information. That is to say, the above methods are constructed by introducing the concept of central trusted entity. With the in-depth application of the IoT in our daily life, users put forward higher requirements for the protection of data privacy and personal privacy information. However, each access request points to the same central trusted entity.

TABLE 1. Protocols and attacks for three layers in IoT.

Layer	Protocol	Attack
Perceptual layer	ZigBee, 3G/4G/5G, WiFi, Bluetooth, Weightless, etc.	Physical security, Terminal forgery, Illegal access, DDoS attack, etc.
Network layer	IPv4/IPv6, 6LoWPAN, RoLL TCP/UDP, TLS, DTLS, RPL, etc.	Network eavesdropping, Network service interruption, Unauthorized access, DDoS attack, etc.
Application layer	MQTT, CoAP, HTTP, XMPP, SoAP, etc.	Single points of failure, DDoS attack, Virus attack, etc.

The central trusted entity stores all the information and completes all the decisions based on the stored information. This in itself is the technical level of insecurity, need to rely on the legal level outside technology to ensure security.

3) IDENTITY AUTHENTICATION

Identity authentication is very important in the security of access control for IoT. In terms of technology architecture, the IoT can be divided into three layers as follows, perceptual layer, network layer and application layer. According to its layers, in summary, corresponding protocols and attacks for three layers in the IoT are respectively shown in Table 1. We can see that in order to implement the authentication process in the Internet of things system, it needs to be completed through a variety of protocols, which are often subject to a variety of attacks. For example, the attacker uses the security vulnerability of the Internet of things terminal to obtain the identity and password information of the node, fake identity to communicate with other nodes, and carry out illegal behaviors or malicious attacks, such as publishing false information, replacing devices, launching DDoS attacks, etc.

B. IoT AND BLOCKCHAIN

In 2018, Jason *et al.* proposed a multi-functional infrastructure based on RBAC and smart contract [28]. It can represent the essential trust and recognition relationship in RBAC and implement the challenge response authentication protocol to verify the user's role ownership. In 2018, Dukkipati *et al.* designed a decentralized RBAC access control framework based on blockchain for heterogeneous IoT [29]. In 2019, Guo *et al.* proposed access control based on permission attribute and production permission token [30]. Then, Ren *et al.* designed an identity management combination access control based on blockchain [31], and realized the registration and authentication of network entities by using cryptographic algorithm.

The above research results provide new inspiration for the combination of the IoT and blockchain, and show that the IoT has considerable security requirements for security access control. However, they ignore the problem of overhead redundancy caused by the increase of the size of IoT devices and users. Through the above research, it can be seen that the research on IoT security based on blockchain has become a new trend. With the diversification of IoT devices, how to achieve fine-grained control of user access and improve access efficiency has become a new research difficulty and an urgent problem to be solved, and the relevant research is still insufficient.

C. DEFINITIONS AND LEMMAS

Definition 1 (Lattice [21]): Lattice L is a linear combination of all integral coefficients of n linearly independent vector groups $b_1, b_2, \cdots, b_n$ in m-dimensional Euclidean space R^m, it is shown as follows,

$$L(b_1, b_2, \cdots, b_n) = \{\sum_{i=1}^{n} x_i b_i : x_i \in Z, i = 1, \ldots, n\}. \quad (1)$$

Definition 2 (DLWE Problem): Let q be a prime, $n \in Z^*$, given a specific distribution φ over Z_α. Thus, $(Z_\alpha, n, \varphi) - DLWE$ problem is: for $s \in Z_q^n$, determine whether a unknown model O is a random oracle machine O_r or a pseudo-random oracle machine O_{pr}. OS and OS' have the following characteristics

Lemma 1: TrapGen (q, n). Given a prime $q \geq 2$, $\{n, m\} \in Z, m \geq 5n \log q$. Run *TrapGen* (q, n) algorithm can output $A \in Z_q^{n\times m}$ and $S_A \in Z_q^{m\times m}$, where S_A is a basis for $L_q^{\perp}(A)$ satisfying $\left\|\tilde{S}_A\right\| \leq O(\sqrt{n \log q})$and $\|S_A\| \leq O(n \log q)$.

Lemma 2: SampleLeft (A, B, S_A, u, σ). Input $A \in Z_q^{n\times m}, B \in Z_q^{n\times m_1}, S_A \in Z_q^{m\times m}$, a vector $u \in Z_q^n$ and a Gaussian parameter $\sigma \geq \|S_A\| \omega(\sqrt{\log(m + m_1)})$, run *SampleLeft* (A, B, S_A, u, σ) algorithm can output a vector $e \in L_q^u(F)$ and $F = (A \,|B) \in Z_q^{n\times(m+m_1)}$ satisfying $Fe = u \bmod q$.

III. ATTRIBUTE-BASED ENCRYPTION SCHEME

A. FORMAL DEFINITION AND SECURITY MODEL

1) FORMAL DEFINITION

KP-ABE scheme consists of four probabilistic polynomial time (PPT) algorithms, such as Setup, KeyGen, Encrypt, Decrypt, as follows.

1) **Setup.** The algorithm takes security parameters as input, and system generates public key *PK* and master key *MK*. Among them, the *MK* is kept by system.
2) **KeyGen.**The algorithm takes *PK*, *MK* and user access control policy W as input. The system generates secret key *sk* for users according to attribute policy T.
3) **Encrypt.**The algorithm takes public key *PK*, attribute policy T and message M as input and outputs ciphertext C.
4) **Decrypt.** The algorithm takes the public key *PK*, secret key *sk* and ciphertext *C* as inputs. Only if access control policy W matches the user attribute policy T, the algorithm outputs plaintext M.

2) SECURITY MODEL

In 2012, Agrawal *et al.* proposed the security model of ABE scheme and proved its security [32]. The KP-ABE scheme can prove to be secure which should satisfy key-policy indistinguishability against adaptive chosen-policy attack (IND-CPA). Based on this security model, the specific process is as follows.

(1) **Initialization.** A query-response game is established between Challenger $\mathscr{C}$ and the adversary $\mathscr{A}$. and adversary $\mathscr{A}$ first assigns a challenge attributes s.

(2) **System setup.** Challenger $\mathscr{C}$ creates the system public key PK and master key MK by executing System Setup algorithm. Then, PK will be sent to adversary $\mathscr{A}$ and MK will be kept by himself.

(3) **Phase 1.** The adversary $\mathscr{A}$ performs queries on the KeyGen, Encrypt and Decrypt algorithms with polynomially bound as following: $\mathscr{A}$ asks for a private key which its attribute s. If s satisfies W, according to this query submitted, challenger $\mathscr{C}$ runs the KeyGen algorithm to get the adversary attribute private key and send it to $\mathscr{A}$.

(4) **Challenge.** Adversary $\mathscr{A}$ chooses two plaintexts $M_0, M_1 \in \{0, 1\}$ and sends them to Challenger $\mathscr{C}$. Then, challenger $\mathscr{C}$ randomly chooses a plaintext and calculates ciphertext C. Thus, its ciphertext C is generated and returned to $\mathscr{A}$.

(5) **Phase 2.** Challenger $\mathscr{C}$ and adversary $\mathscr{A}$ repeat phase 1.

(6) **Guess.** $\mathscr{A}$ submits the conjecture e' of ciphertext e. The advantage that adversary $\mathscr{A}$ can win this game can be defined as

$$Adv = \left| \Pr[e' = e] - \frac{1}{2} \right|.$$

B. OUR SCHEME

In this subsection, we propose a KP-ABE scheme based on lattice as follows. Suppose that the plaintext $M = \{m_1, m_2, \cdots, m_x\} \in \{0, 1\}^x$. Our scheme consists of the following four algorithms.

1) SETUP

The algorithm takes security parameters as input, and system generates public key PK and master key MK. The public key PK is very important in the ABE scheme, which is used to generate the secret key sk and ciphertext. In our scheme, the attribute is associated with the ciphertext, and the access structure of the attribute is associated with the secret key sk. If and only if the attribute of the ciphertext meets the access structure of the secret key, the user can decrypt the ciphertext to recover the plaintext.

Algorithm 1 Setup algorithm

Input: Security parameters n, m, q
Output: The public key PK, master key MK
1: Given two primes $n, q \geq 2$, and a integer $m \geq 2n \lg q$
2: Run $(P, S) \leftarrow TrapGen(1^n)$, $P \in Z_q^{n \times m}$
3: Give the user attribute $at_i \in T$, $i = 1, 2, \cdots, m$
4: Choose hash function $H : \{0, 1\}^* \rightarrow \mathbb{Z}_q^{m \times m}$, $H(at) \sim D_{m \times m}$
5: Choose randomly $k_i \in Z_q^n$ with relate to the attribute $at_i = k_i^{\mathrm{T}}$
6: Return the public key $PK = P$, master key $MK = S$

2) KEYGEN

The algorithm takes PK, MK and attribute access control policy W as input. The system generates secret key sk for users.

Algorithm 2 KeyGen Algorithm

Input: Public key P, master key S, attribute access control policy $W = \{k_1, k_2, \cdots, k_n\}$
Output: Secret key sk
1: Choose randomly $b \in Z_q^{n \times m}$
2: Choose $\sigma \geq \|S\| \omega(\mathrm{lbm}) \sqrt{m}$
3: Run $s_i \leftarrow SampleLeft(P, k_i, S, b, \sigma)$
4: Return the secret key $sk = (s_i, b)$

3) ENCRYPT

The algorithm takes PK, user attribute $at_i \in T$ and plaintext M as input and outputs ciphertext C.

Algorithm 3 Encrypt Algorithm

Input: Public key P, plaintext M, attribute at_i
Output: Ciphertext C
1: Choose error parameter $a \leftarrow \chi$, where χ is Gaussian error distribution.
2: Compute $c_1 = a + m_x \lfloor q/2 \rfloor$
3: Choose $x \in Z_q^m \leftarrow \chi$
4: Choose randomly $d \in \{-1, 1\}^{m \times m}$
5: Compute $c_2 = P \left| at_i^{\mathrm{T}} + dx \right.$
6: Return the ciphertext $C = \{c_1, c_2\}$

4) DECRYPT

The algorithm takes the public key, private key sk and ciphertext C as inputs. Only if access control policy W matches the user attribute policy T, the algorithm outputs plaintext M.

Algorithm 4 Decrypt Algorithm

Input: Secret key (s_i, b), ciphertext C, public key PK attribute access control policy k_i
Output: Plaintext M
1: Compute $w = s_i c_2 = s_i (P \left| at_i^{\mathrm{T}} + dx \right.)$
2: Compute $g = c_1 - w + b$
3: If $\left| g - \lfloor q/2 \rfloor \right| < \lfloor q/4 \rfloor$, return $m_x = 1$. Else, return $m_x = 0$
4: Return the plaintext M

C. SECURITY ANALYSIS

1) CORRECTNESS

Theorem 1: Using the encryption algorithm in our ABE scheme to encrypt plaintext M, the decryption algorithm decrypts plaintext M with a probability close to 1.

Proof: In the decryption phase of the scheme, $w = s_i c_2 = s_i (P \left| at_i^{\mathrm{T}} + dx \right.)$, $g = c_1 - w$. And according to the lemma 2,

we have $b = (P|k_i)s_i$. So

$$\begin{aligned} g &= c_1 - w \\ &= a + m_x \lfloor q/2 \rfloor - s_i((P|at_i^{\mathrm{T}}) + dx) + b \\ &= a + m_x \lfloor q/2 \rfloor - s_i dx. \end{aligned} \tag{2}$$

In addition, the parameters a and $s_i dx$ are short vectors, therefore, the result will be in $(-q/4, q/4)$. As the above Eq. (1) holds, we can derive that the decryption algorithm can decrypt ciphertext and obtain plaintext M.

2) ABE CIPHERTEXT SECURITY

Theorem 1: This ABE scheme satisfies ABE ciphertext secure which satisfies indistinguishability under chosen-plaintext attack (IND-CPA) in random oracle model.

Proof: Suppose the game has two sides, the challenger $\mathscr{C}$ and the adversary $\mathscr{A}$. Then, they take the following steps.

Initialization. $\mathscr{A}$ selects the policy W and gives it to $\mathscr{C}$.

System setup. $\mathscr{C}$ does the following.

(1) $\mathscr{C}$ uses LWE sampling oracle O to obtain samples $(u, v_u) \in Z_q^n \times Z_q$ and $(A, v_0) \in Z_q^{n\times m} \times Z_q^m$.
(2) Run $TrapGen(n, q)$ algorithm to output (P, S).
(3) For $R_i \in \{-1, 1\}^{m\times m}$, if attribute $i \in T$, compute $A_i = AR_i - P$, otherwise, $A_i = AR_i$.
(4) $\mathscr{C}$ returns the $PK = \{P, k, \{A_i\}_{i\in T}, u\}$ to $\mathscr{A}$.

Phase 1. $\mathscr{A}$ asks for a private key which its attribute does not satisfy the attribute set T. According to this query submitted, challenger $\mathscr{C}$ runs the KeyGen algorithm to get the adversary attribute private key sk' and send it to $\mathscr{C}$.

Challenge. $\mathscr{A}$ chooses two plaintexts $M_0, M_1 \in \{0, 1\}$ and sends them to $\mathscr{C}$. $\mathscr{C}$ randomly chooses a plaintext and calculates $c_1 = v_u + M_e \lfloor q/2 \rfloor$, $e \in \{0, 1\}$, $c_2 = R_1 v_0$. Thus, its ciphertext $C = \{c_1, c_2\}$ is generated and returned to A.

Phase 2. $\mathscr{C}$ and $\mathscr{A}$ repeat phase 1.

Guess. $\mathscr{A}$ submits the conjecture e' of ciphertext e. According to LWE problem, if $e' = e$, output the $O' = O$, $\mathscr{A}$'s advantage $\Pr[e' = e | O' = O] = 1/2 + \delta$. if $e' \neq e$, output the $O' = O$. Thus, $\mathscr{A}$'s advantage $\Pr[e' \neq e | O' = O] = 1/2$. Therefore, as the Eq. (2) holds, $\mathscr{A}$ can distinguish the uniform random distribution on the $Z_q^n \times Z_q$ and ciphertext e' with a negligible advantage and solve the DLWE problem.

$$\begin{aligned} Adv &= \frac{1}{2}\Pr[e' = e | O' = O] + \frac{1}{2}\Pr[e' \neq e | O' = O] - \frac{1}{2} \\ &= \frac{1}{2} + \frac{1}{2} \times (\frac{1}{2} + \delta) - \frac{1}{2} = \frac{1}{2}\delta \end{aligned} \tag{3}$$

Therefore, in probability polynomial time, no attacker can win this game with an unnegligible advantage, the scheme supports the security of indistinguishability under selective attribute and chosen plaintext attack.

IV. ACCESS MANAGEMENT SCHEME

In this section, we will construct and describe a secure access management scheme in IoT based on blockchain in detailed. Then, we will analyze the efficiency of our scheme and compare it with other schemes.

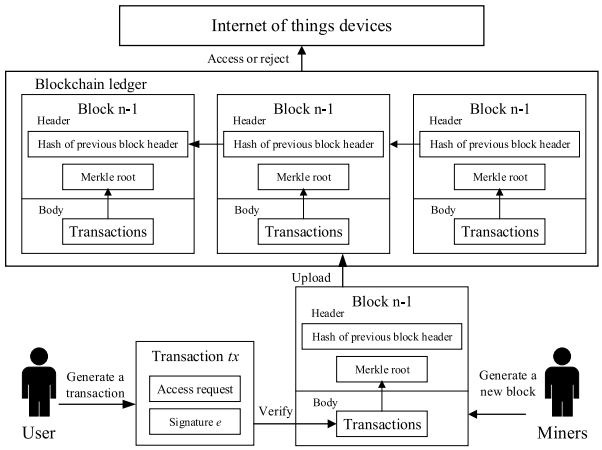

FIGURE 1. The model of access management in blockchain-based IoT.

A. SCHEME MODEL

In this subsection, we will describe our scheme and process in detail. In one case, when the intelligent device is traded, its ownership will change. In another case, through illegal access or DDoS attack, attackers can enter into our IoT system and control our intelligent devices. This constitutes a great threat to our property and information security. Therefore, the identity and access management (IAM) for IoT has a great significance for its security. As the previous section mentioned, blockchain technology provides a method to create consensus networks without trusting other nodes in a distributed network. Based on blockchain, each device can self-manage without manual maintenance. As long as the equipment still exists, the life cycle of the whole network can become very long, and the operation cost can be significantly reduced. For example, all daily household items can spontaneously and automatically carry out financial activities with other objects or the outside world. Smart meters can facilitate more favorable electricity bills by regulating electricity consumption and frequency, and so on. Blockchain is very suitable for authentication and access management.

Combining IoT with blockchain technology, in this study, we design a secure access management with ABE scheme, which is used to solve the identity and access challenges of linking smart devices in IoT system. The scheme model is mainly divided into three parts: user, IoT and blockchain system, as shown in the figure 1. The blockchain network is composed of base stations, which maintain a unified blockchain. And blockchain cannot be tampered with. The smart contract saved in the blockchain specifies the main process of access control for IoT devices. The blockchain plays an important role in the initialization process, which is mainly used for user registration and authentication, blockchain control and management, etc.

The specific implementation steps of IoT with blockchain are described as follows.

Initialization. Users are divided into device owner and ordinary user. By running the elliptic curve digital signature algorithm, we can obtain a set of public-private key pairs Key=$\{(pk_1, sk_1), (pk_2, sk_2), \cdots, (pk_x, sk_x)\}$. Then, the

blockchain system generates a public-private key pair for each user.

Device marking. Users add their own devices to blockchain system. By performing hashing operations on owner's public key, each device is assigned by a unique value $g = hash(pk)$, which is its serial number. In this way, each device can be uniquely identified and represented as (pk, g). The public key pk proves this device's owner, and g represents device.

Transaction generation. As shown in Fig. 1, the owner, who has ownership of these smart devices, can manage and operate devices through system authentication by his public and private keys. At the same time, he generates a transaction tx, which is an access request to his device. By using his private key sk, he generates a signature e, which is included in this transaction tx. Thus, this access request to this smart device will be uploaded to the distributed network as a transaction tx.

Verification. Miners (mining nodes) in the distributed network get this transaction tx and verify the signature e by corresponding owner's public key. If the signature e is correct, it means that this signature is generated by this device's owner. Otherwise, this transaction is rejected.

Block generation. Miners include an available transaction tx into a new block. Through the consensus mechanism, such as Proof of Stake (PoS), miners compete for the right to add this new block to chain.

Access. Miners agree on a common set of validated transactions to be added to the ledger. Besides, the miner who gets the right to produce a new block will be rewarded. After this block is agreed by all network nodes, transaction tx will be confirmed and this user can access and control this device.

User's account address is generated by his public key for the purpose of privacy protection. Public key and private key are respectively used for information encryption and verification. Firstly, each interaction between entities needs to be signed by the sender's private key, and then verified by the receiver according to the sender's public key to ensure that the message has not been tampered with.

B. ACCESS MANAGEMENT WITH ABE SCHEME IN BLOCKCHAIN-BASED IoT

For some special equipment, when allowing others to use, it is necessary to review the user's qualification, otherwise it will cause danger. For example, if a person wants to use a smart car in the IoT, he needs to verify the user's driving license. For optimizing the access management of IoT devices and realize fine-grained access control of users, we introduce ABE scheme in our scheme.

Suppose that the secret key can be transmitted safely in distribution and transmission. In order to more intuitively illustrate our access control scheme process, without losing generality, we use the following examples to illustrate. Suppose that there are Alice(owner), Bob(user), and IoT device(car). This car belongs to Alice, and Bob wants to use her car. In this subsection, we describe our scheme through

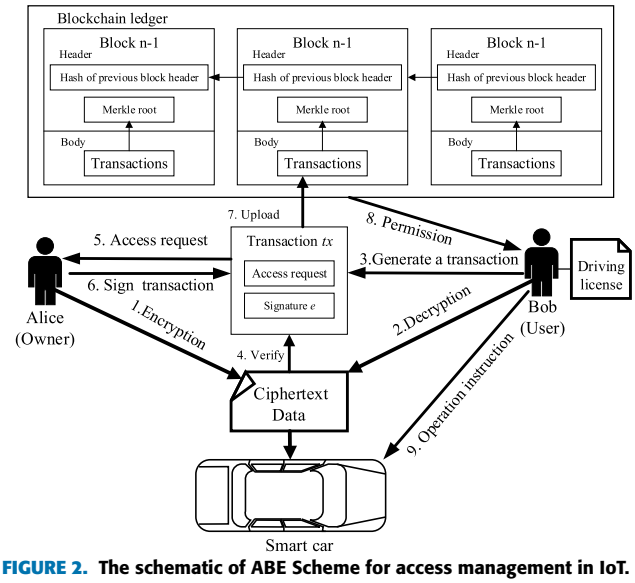

FIGURE 2. The schematic of ABE Scheme for access management in IoT.

the process of Alice and Bob accessing Alice's device respectively. The workflow of our scheme is shown in Figure 2, which is mainly divided into these following steps.

Initialization. As mentioned above, Alice and Bob complete registration in the decentralized blockchain system and obtain account address. Then, by running KeyGen algorithm, the system generates and distributes secret keys to them. At last, Alice add their own devices to blockchain system.

Encryption. According to the access policy in ABE scheme, driving license is used to as user's attribute. Alice use Encrypt algorithm to encrypt the information of the equipment to get the ciphertext information. Only users with the corresponding attributes of driving cars, such as driver's license, can decrypt this ciphertext.

Device status update. Using the device sensing, computing and communication module, the device obtains its current position and other status information. Through the smart contract of blockchain, we can set IoT device to broadcast their status on the blockchain network every five minutes.

Decryption. Bob wants to use Alice's car, he needs to run the Decrypt algorithm to decrypt this ciphertext through his secret key and get the plaintext information. If Bob can successfully decrypt this ciphertext, it means that Bob satisfies the qualification of using the device.

Access request. Bob obtains the status of nearby IoT devices through the terminal. Then, he run access request function with plaintext and send access request to Alice. if the request is accepted, Bob needs to call publish transaction function to complete the transfer money to Alice. therefore, Bob submits a new transaction to the blockchain system. This transaction contains Alice and Bob's signatures. the use time for this device will be added to this transaction.

Block generation. The miner generates a new block and puts the above transactions in the block body.

Consensus. Through the consensus mechanism, such as PoS, miners compete for the right to add this new block to

chain. Then, after the information of this block is reached and confirmed by the whole distributed network, Bob is added in the permission list. Otherwise, the access request is denied.

Access. The blockchain system send a permission to Bob. Then, Bob uses this permission to send operating instruction to the smart car. The car queries Bob's authority and permission through the authority list, and accepts Bob's operation instructions within the specified time range.

State recovery. After the use time, by using mart contract, blockchain system deletes the previously added Bob's permission. Thus, Bob cannot continue to use the car. At last, this car enters the idle state again and broadcasts its status information to the whole network.

C. EFFICIENCY

Because of its security and privacy protection, blockchain has attracted tremendous attention. As is mentioned above, blockchain has great potential for solving the security and privacy challenges, especially in IoT. In this new construction, the advantages of the access management with ABE scheme in Blockchain-based IoT are summarized as follows.

Fine-grained. Different from other previous works, we use ABE scheme to implement a security fine-grained access control in blockchain-based IoT. ABE scheme is a novel public key encryption scheme. It allows users to encrypt and decrypt messages based on attributes. Moreover, it is expressive and can implement fine-grained access control on encrypted data. Only when the key associated with the ciphertext is given an access property of the ciphertext, can the attribute of the associated secret key satisfy the attribute of the ciphertext. Therefore, in our study, we introduce attribute based encryption scheme in our scheme, When the user wants to use the device and send a request, it can check the user's corresponding qualification. Through this verification mechanism, it can realize fine-grained access control for user and protects the security of user and IoT device.

Device ownership safety transfer. If a person has ownership of a smart device, the confirmation information of this smart device will be uploaded to the public ledger with blockchain. When this smart device is traded or transferred, transaction will be generated. And both sides of this transaction can use their own public/private key pairs to make sure that the right information of the device can be changed safely and effectively with blockchain in public ledger. At the same time, the information will be consensus to other nodes with recording. More importantly, because of the unique characteristics of blockchain, the information on block can not only be tampered with, but also be securely tracked. By introducing blockchain technology, this novel IoT system can solve the problem of ownership transfer for smart devices.

High efficiency. By introducing smart contract into the IoT, we can make full use of the computing power, storage capacity and bandwidth of a large number of IoT devices in different locations. In our scheme, smart contract technology can store and process transactions efficiently, which greatly reduces the cost and time of information management, protection and processing. It makes transaction processing more efficient and greatly reduces the cost of calculation and storage. In practice, the combination of blockchain technology and IoT can eliminate the auditing between nodes, and it can directly build a bridge between the two parties for communication. Especially with the introduction of smart contract, a large number of functions can be called and controlled automatically. At the same time, the signature verification method can ensure the high security of the scheme. By this way, this IoT with blockchain scheme reduces operating costs for enterprises and improves operational efficiency.

D. COMPARISON

In general, IoT needs to have two important characteristics. One is lightweight, so it can be implemented on the IoT nodes with limited resources. The other one is fine-grained, that is, the IoT system can perform measurement at the fine-grained level, not just at the aggregation level. In addition, with in-depth study of IoT, its security problem is becoming more and more important. As mentioned above, under the public key cryptography algorithm and hash algorithm, blockchain technology has strong security which can resist multiple attacks.

On one hand, compared with traditional IoT model, as mentioned earlier, different software vendors adopt different protocols, which make it difficult to be compatible with other devices. Hence, the deployment of IoT devices is often complex. At the same time, as analyzed in section II, there are many security holes and threats in the IoT, especially authentication. In our scheme, blockchain-based IoT scheme can easily provide authentication and secure data transmission for IoT devices, which makes the IoT's deployment simpler and safer. Furthermore, when users control devices, based on the anonymity of blockchain, miners can only verify the public key in the transaction. They can not find out the identity of users, or even the information of devices. It protects the privacy of users and devices. And the data on blockchain cannot be tampered with. That is, blockchain achieves anonymity and community autonomy of each device, and ensures data integrity.

On the other hand, we compare our scheme with other blockchain-based IoT schemes. In the scheme of Ref. [23], the centralized management will enhance the system load and cause the delay of system response. Thus, the centralized management can reduce the efficiency of IoT system. In the scheme of Huh *et al.*(2017), there is no detailed security analysis for this scheme in this paper. In our construction, we introduce a lattice-based KP-ABE scheme in our scheme. It can support flexible access policies and provides privacy protection for user. More importantly, it implements fine-grained access control in IoT. In particular, lattice cryptography can provide the quantum-resist security for our KP-ABE scheme, which protects user's privacy in the future quantum age. Meanwhile, we use blockchain technology to realize distributed management intelligent devices. The comparison between our scheme and other access control schemes is shown in the following Table 2. Through this method, the

TABLE 2. Comparison with other access control schemes.

Scheme	RBAC	ABAC	UCON	Ref.[23]	Our scheme
Decentralization	No	No	No	No	Yes
Lightweight	No	Yes	Yes	No	Yes
De-trusted	Yes	No	No	Yes	Yes
Fine-grained	No	Yes	No	Yes	Yes
Dynamics	Yes	Yes	No	Yes	Yes

TABLE 3. Performance comparison with other ABE schemes.

Scheme	Public key size	Private key size	Ciphertext size
Ref.[33]	$3lmn\log q$	$2nlm$	$(2nml+n)\log q$
Ref.[34]	$(5mn+2n)\log q$	$2nlm\log q$	$(3nml+2)\log q$
Ref.[35]	$(m^2+mn+n)\log q$	$(m^2+2n)\log q$	$(2n^2+2ml+1)\log q$
Our scheme	$mn\log q$	$(n+lm)\log q$	$(nl+1)\log q$

problems of centralized management can be avoided and the operation efficiency of IoT can be improved.

In 2015, Wu *et al.* proposed a fuzzy identity-based encryption scheme[33]. However, the efficiency of the scheme is not high. Afterwards, in 2018, Wang *et al.* designed a ABE scheme with revocation support and flexible access structure on lattice by using binary tree[34]. In 2019, Liu et al proposed a KS-ABE scheme to strength ciphertext-search security for cloud storage[35]. However, due to the high ciphertext expansion rate, the size of the ciphertext is large. As a result, the computational complexity of the two schemes is increased. In terms of system storage overhead, the size of the public and private keys of the proposed scheme is related to the related parameters (q, n, m) on the lattice. l represents the number of user attributes. In addition, this paper compares the related schemes from the following aspects: the sizes of public key, private key and the ciphertext. The specific performance comparison results are shown in Table 3. Compared with these schemes in Ref. [33], Ref. [34] and Ref. [35], the sizes of the public key, private key and ciphertext in our scheme are shorter than that in other schemes. It can decrease computational complexity of our proposed cryptocurrency scheme. Additionally, in the next section, we will provide a detailed security analysis on some attacks in IoT for our scheme. Therefore, our blockchain-based IoT scheme has a better performance in security and efficiency. It shows that our scheme is more secure and effective.

V. SECURITY ANALYSIS

As we described, we discuss the security threats of the IoT. Correspondingly, in this section, we will provide the security analysis of our new scheme in terms of data security, identity authentication, resistance to attacks.

A. DATA SECURITY

1) CREDIBILITY

The centralized model usually belongs to a specific company or organization, and its data storage and program running process are likely to be manipulated. More importantly, the centralized structure in IoT easily leads to performance bottleneck and single point of failure. On the contrary, blockchain can provide a method to run safely in a completely untrusted environment. In our scheme, the blockchain does not belong to a specific unit, but is a distributed network participated by all participants, so as to provide a trusted interaction platform among users and the IoT devices. Furthermore, compared with the centralized structure, our scheme is decentralized. Through consensus mechanism, all nodes in the system keep the same copy of data to maintain the integrity of the data. In this way, each node in the distributed smart contract network can operate relatively independently. Even if a small number of nodes fail, it will not have a fatal impact on the whole system, thus eliminating the single point of failure and other hidden dangers. At the same time, due to the characteristics of the blockchain, the data is saved in each node and cannot be tampered with. Therefore, the IoT's data in our scheme is more secure and reliable.

2) VERIFIABLE

Through the signature algorithm, every data on the blockchain can be verified and traceable. At the same time, using smart contract, the rules made by users are completely open and transparent, and the system can easily execute and check every rule or even every interaction. The detailed content of the review can provide unchangeable evidence for the possible differences between the parties. Firstly, the access control policy is stored, maintained and executed by the miners in the blockchain network to ensure that the data is recognized by multiple nodes in the network, which greatly reduces the probability that the system is controlled by attackers. Secondly, the chain storage structure ensures that the data storage is not tampered with. These provide the safe and reliable evidence for our access management scheme.

B. IDENTITY AUTHENTICATION

As shown in Table 1, there are many protocols being used in IoT application communication, including HTTP, MQTT, CoAP, XMPP. Unfortunately, some of these protocols still have many risks and vulnerabilities in terms of security. For example, SSL/TLS is a transit protocol between HTTP and TCP. Through TLS/SSL protocol, the unencrypted Base64 coded username and password are used for authenticating the service client in HTTP basic authentication. Another example, MQTT is a messaging protocol which only supports the lowest level of security and additional services. Similar to HTTP, MQTT also has minimal authentication which relies on some simple usernames and passwords [36], [37]. As we have seen, in traditional IoT, many protocols are needed to deal with secret key distribution and authentication for service client. Obviously, Centralized management makes some security risks in traditional IoT system. Moreover, some problems are also obvious, for instance, complex secret key management, low system efficiency.

Compared with traditional IoT, we use a decentralized authentication method for authentication in access management. Through the signature verification and consensus mechanism in blockchain, the safe and reliable identity

verification can be realized for IoT device and its communication data to ensure IoT's security. In particular, when the conditions are met and the smart contract is activated, the smart contract can automatically process transactions according to the preset rules. More importantly, the lattice-based KP-ABE scheme in our scheme can support flexible access policies for user, which implements fine-grained access control in IoT. Therefore, our work can greatly improve the authentication security in IoT system.

C. RESISTANCE TO ATTACKS

1) RESIST DDOS ATTACK

In DDoS attack, by controlling distributed servers and computers, the attacker sends a large amount of malicious traffic to the target. It consumes network bandwidth and system resources greatly, thus making normal service requests rejected.

In our scheme, we adopt the asymmetric cryptographic algorithm in blockchain technology to add a verification process for each operation (transaction) of IoT smart devices. More specifically, using operator's private key generates the signature of operation which controls the IoT smart devices, so this corresponding operator cannot deny it. Each transaction which needs to be uploaded to the block will be authenticated and tested by miners. And consensus will be reached in this network. In this way, the requests that constitute the DDoS attack traffic will not be authenticated. Therefore, the requests are blocked from exiting this IoT based on blockchain system. It is shown that this proposed IoT based on blockchain can resist DDoS attack.

2) RESIST ILLEGAL ACCESS ATTACK

In IoT based on blockchain system, the public key represents the identity of the owner (user). Furthermore, each smart device has a unique GUID. There is a one-to-one correspondence between the smart device and the owner's public key, and it is recorded on the blocks. Because of the unique characteristics of blockchain, the information on block is very secure and cannot be tampered with. At the same time, because each owner's identity is bound to his public key, when the user needs to control the system and his own smart device, the IoT based on blockchain system can validate whether the user's identity and the device to be controlled match the recorded information on the blocks. In particular, KP-ABE scheme supports flexible access policies and implements fine-grained access control in IoT. If they match, the user can continue the next operation. That is to say, he can enter into the IoT based on blockchain system and control his smart devices with management authority. Otherwise, he will not be allowed to enter into the system with smart devices. In other words, in this scheme, the attacker cannot obtain the private key corresponding to the owner's public key to verify his forged identity. Blockchain technology provides a more secure and reliable access control method for IoT. Consequently, the attacker cannot illegal access this system and controls the IoT smart devices. And, this system can effectively authenticate operators and resist illegal access attack. Therefore, this system can effectively authenticate operators and resist illegal access attack.

VI. CONCLUSION

IoT has been widely used in various fields of our daily life in these past years. Cisco Inc. predicts that there will be more than 50 billion connected devices by 2020. Obviously, in the future, the significance of its security will be more evident and enormous. However, as mentioned above, there are three major security requirements, confidentiality, integrity, and availability, all of which are important for the security design of IoT. DDoS attack and illegal access often threaten IoT's security. Targeting at these issues, in our study, by using KP-ABE scheme and blockchain technology, we design a secure access management scheme for IoT. In this new scheme, KP-ABE implements fine-grained access control in IoT, and blockchain provides data security. Through the signature verification of blockchain, we realize the secure and reliable authentication of IoT devices, so as to ensure the communication security of devices in IoT. At the same time, we design and add a series of IoT smart contract functions. These functions can store and process transactions efficiently. Through our analysis, our scheme is secure and more efficient. In future research, we will continue to focus on the security issues of access management and data sharing in IoT.

REFERENCES

[1] K. Ashton, "That 'Internet of Things' thing," *RFID J.*, vol. 22, no. 7, pp. 97–114, Jun. 2009.
[2] R. Want, "An introduction to RFID technology," *IEEE Pervasive Comput.*, vol. 5, no. 1, pp. 25–33, Jan./Mar. 2006.
[3] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Comput. Netw.*, vol. 52, no. 12, pp. 2292–2330, 2008.
[4] A. A. Khan, M. H. Rehmani, and A. Rachedi, "Cognitive-radio-based Internet of Things: Applications, architectures, spectrum related functionalities, and future research directions," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 17–25, Jun. 2017.
[5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw.*, vol. 38, no. 4, pp. 393–422, 2002.
[6] S.-Y. Lien, K.-C. Chen, and Y. Lin, "Toward ubiquitous massive accesses in 3GPP machine-to-machine communications," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 66–74, Apr. 2011.
[7] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Proc. 47th Design Autom. Conf. (DAC)*, Anheim, CA, USA, Jun. 2010, pp. 731–736.
[8] D. Ding, Q.-L. Han, Z. Wang, and X. Ge, "A survey on model-based distributed control and filtering for industrial cyber-physical systems," *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 2483–2499, May 2019.
[9] M. Burhanuddin, A. A.-J. Mohammed, R. Ismail, M. E. Hameed, A. N. Kareem, and H. Basiron, "A review on security challenges and features in wireless sensor networks: IoT perspective," *J. Telecommun., Electron. Comput. Eng.*, vol. 10, nos. 1–7, pp. 17–21, 2018.
[10] W. Shi, C. Ma, S. Kulshrestha, R. Bose, and Y. Okada, "A framework for automatically generating IoT security quizzes in a virtual 3D environment based on linked data," in *Proc. Int. Conf. Emerg. Internetw., Data Web Technol.* Cham, Switzerland: Springer, 2019, pp. 103–113.
[11] Y. Kawamoto, H. Nishiyama, N. Kato, Y. Shimizu, A. Takahara, and T. Jiang, "Effectively collecting data for the location-based authentication in Internet of Things," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1403–1411, Sep. 2017.

[12] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 111, no. 7, pp. 1–6, Feb. 2015.

[13] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, 4th Quart., 2014.

[14] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[15] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, San Jose, CA, USA, May 2015, pp. 180–184, doi: 10.1109/SPW.2015.27.

[16] M. Hamilton, "Blockchain distributed ledger technology: An introduction and focus on smart contracts," *J. Corporate Accounting Finance*, vol. 31, no. 2, pp. 7–12, Apr. 2020.

[17] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3680–3689, Jun. 2019.

[18] A. Abidi, B. Bouallegue, and F. Kahri, "Implementation of elliptic curve digital signature algorithm (ECDSA)," in *Proc. Global Summit Comput. Inf. Technol. (GSCIT)*, Jun. 2014, pp. 1–6.

[19] Z. Li, Z. Yang, and S. Xie, "Computing resource trading for edge-cloud-assisted Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3661–3669, Jun. 2019.

[20] F. Chang, J. Dean, S. Ghemawat, W. C. Hsieh, D. A. Wallach, M. Burrows, T. Chandra, A. Fikes, and R. E. Gruber, "Bigtable: A distributed storage system for structured data," *ACM Trans. Comput. Syst.*, vol. 26, no. 2, pp. 1–26, Jun. 2008.

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

[22] C. Li and L.-J. Zhang, "A blockchain based new secure multi-layer network model for Internet of Things," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Honolulu, HI, USA, Jun. 2017, pp. 33–41, doi: 10.1109/IEEE.ICIOT.2017.34.

[23] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, Bongpyeong, South Korea, 2017, pp. 464–467, doi: 10.23919/ICACT.2017.7890132.

[24] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[25] V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, Feb. 2015.

[26] J. Park and R. Sandhu, "Towards usage control models: Beyond traditional access control," in *Proc. 7th ACM Symp. Access Control Models Technol. (SACMAT)*, Jun. 2002, pp. 57–64.

[27] R. Sandhu and J. Park, "Usage control: A vision for next generation access control," in *Proc. Int. Workshop Math. Methods, Models, Archit. Comput. Netw. Secur.* Berlin, Germany: Springer, 2003, pp. 17–31.

[28] J. P. Cruz, Y. Kaji, and N. Yanai, "RBAC-SC: Role-based access control using smart contract," *IEEE Access*, vol. 6, pp. 12240–12251, 2018.

[29] C. Dukkipati, Y. Zhang, and L. C. Cheng, "Decentralized, BlockChain based access control framework for the heterogeneous Internet of Things," in *Proc. 3rd ACM Workshop Attribute-Based Access Control (ABAC)*. New York, NY, USA: Association for Computing Machinery, Mar. 2018, pp. 61–69, doi: 10.1145/3180457.3180458.

[30] H. Guo, E. Meamari, and C.-C. Shen, "Multi-authority attribute-based access control with smart contract," in *Proc. Int. Conf. Blockchain Technol. (ICBCT)*. New York, NY, USA: Association for Computing Machinery, 2019, pp. 6–11, doi: 10.1145/3320154.3320164.

[31] Y. Ren, F. Zhu, J. Qi, J. Wang, and A. K. Sangaiah, "Identity management and access control based on blockchain under edge computing for the industrial Internet of Things," *Appl. Sci.*, vol. 9, no. 10, p. 2058, May 2019.

[32] S. Agrawal, X. Boyen, V. Vaikuntanathan, P. Voulgaris, and H. Wee, "Functional encryption for threshold functions (or fuzzy IBE) from lattices," in *Proc. 15th Int. Conf. Pract. Theory Public Key Cryptogr.*, Berlin, Germany: Springer, May 2012, pp. 280–297.

[33] L. Q. Wu, X. Y. Yang, and Y. L. Han, "An efficient FIBE scheme based on ideal lattices," *Chin. J. Comput.*, vol. 38, no. 4, pp. 775–782, 2015.

[34] S. Wang, X. Zhang, and Y. Zhang, "Efficient revocable and grantable attribute-based encryption from lattices with fine-grained access control," *IET Inf. Secur.*, vol. 12, no. 2, pp. 141–149, Mar. 2018.

[35] L. Liu, S. Wang, B. He, and D. Zhang, "A keyword-searchable ABE scheme from lattice in cloud storage environment," *IEEE Access*, vol. 7, pp. 109038–109053, 2019.

[36] V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the Internet of Things," *Trans. IoT Cloud Comput.*, vol. 3, no. 1, pp. 11–17, 2015.

[37] N. Naik, "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP," in *Proc. IEEE Int. Syst. Eng. Symp. (ISSE)*, Vienna, Austria, Oct. 2017, pp. 1–7, doi: 10.1109/SysEng.2017.8088251.

JIANSHENG ZHANG is currently pursuing the Ph.D. degree with the Beijing University of Posts and Telecommunications. His research interests include blockchain, information security, and cryptography.

YANG XIN currently holds the position of an Associate Professor with the School of Cyberspace Security, Beijing University of Posts and Telecommunications (BUPT). He is also the Vice Director of the National Engineering Laboratory for Disaster Backup and Recovery, National Engineering Laboratory for Big Data Circulation and Transaction Technology, the Director of the Data Security and Disaster Recovery Research Center, and the Director of the Beijing Engineering Laboratory for Cloud Security. He is also a Professor and a Doctoral Supervisor. His current research interests include cyberspace security, artificial intelligence, storage disaster recovery, and big data technologies.

YULONG GAO received the M.S. degree in computer technology from Henan Polytechnic University, Jiaozuo, China, in 2017. He is currently pursuing the Ph.D. degree with the Beijing University of Posts and Telecommunications. His research interests include cryptography, information security, and digital watermark.

XIAOHUI LEI received the master's degree in artificial intelligence and data sciences from the School of Hebei University of Technology. His research interests include robots and advanced learning acquisition.

YIXIAN YANG received the M.S. degree in applied mathematics and the Ph.D. degree in electronics and communication systems from the Beijing University of Posts and Telecommunications, Beijing, China, in 1986 and 1988, respectively. He is currently the Managing Director of the Information Security Center, Beijing University of Posts and Telecommunications. His research interests include coding and cryptography, information and network security, and signal and information processing. He received the Yangtze River Scholar Program Professor Award, the National Outstanding Youth Fund Award, and the National Teaching Masters.