WEP Warwick Evans Publishing

International Journal of Computer Science and Information Technology

ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 4, Number 1, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v4n1.37
Journal homepage: https://wepub.org/index.php/IJCSIT/index

A Combination of Attribute-Based Encryption and Blockchain Access Control Scheme in Smart Home Environment

Xintao Zhang *, Xiaofeng Xie

Computer Science and Technology, Qingdao University, Qingdao, China
*Corresponding Author: 626788676@qq.com

ABSTRACT

In response to the problems of excessive decryption computation burden on users, inability to protect users' privacy information, and the inability of traditional cloud storage methods to meet users' faster file upload and download speed requirements and track malicious users, this paper proposes an attribute-based encryption and blockchain-based trusted data access control scheme for smart home environments. The scheme combines symmetric encryption algorithms and attribute-based encryption algorithms to achieve fine-grained access control of data. At the same time, it leverages edge computing technology to outsource most of the decryption and computation operations to edge computing nodes, reducing the user's decryption and computation burden. Furthermore, the introduction of blockchain technology enables the monitoring and auditing of users within the system, achieving full traceability of access control. Finally, the proposed scheme was analyzed and validated through simulation experiments, which showed that the scheme is safe and effective, protecting users' security and privacy, and enabling secure data sharing.

KEYWORDS

Smart home; Attribute-based encryption; Access control; Blockchain

1. INTRODUCTION

In light of the swift advancements in technology, smart home systems [1] are progressively becoming prominent in public awareness and rapidly assimilating into daily life. Smart home systems are a new living environment that allows people to easily enjoy life and make life smart and convenient [2]. Since the inception of smart home technology, it has rapidly dominated the residential market, establishing the inevitability of intelligent homes in the future.

The ultimate goal of smart home is to make the home more comfortable, convenient, and secure. With the continuous development of human consumption needs and the intelligentization of residential buildings, today's smart home systems have a wealth of content and increasingly complex system configurations. In simple terms, a smart home system is a networked and intelligent home control system that integrates automation control systems, computer network systems, network communication technology, and intelligent cloud control [3]. People will input their lifestyle information into the intelligent cloud [4] end of the smart home system in order to make it more compatible with their lives. The smart home system will also record people's life data in the intelligent cloud end. When people suddenly fall ill or there is a criminal case or other emergencies at home, these data may play an important role in the diagnosis of the disease or the progress of the case. On the other hand, if these information is leaked, it will pose a great threat to people's personal safety and property safety. Therefore, the security of this information is of paramount importance [5]. Cloud platforms, as semi-trustworthy and curious third-party data storage institutions, may try to obtain

sensitive information from smart homes. Therefore, it is particularly important to ensure the secure storage and sharing of this data. To address this issue, it is essential to ensure the integrity and confidentiality of data, and only authorized users should have access rights. Attribute-based encryption (ABE) is an effective solution that allows for flexible creation of access policies for different ciphertexts, providing fine-grained access control for private data based on attributes. Blockchain [6] is a decentralized, tamper-proof, traceable, and multi-party maintained distributed database [7], providing a reliable solution for secure data sharing.

In 2005, Sahai and Waters [8] first introduced the concept of attribute-based encryption, and then KP-ABE (Key Policy Attribute-Based Encryption) [9] and CP-ABE (Ciphertext Policy Attribute-Based Encryption) [10] were subsequently proposed by scholars. For CP-ABE, the user's access policy and ciphertext are bound, the user's attributes and key are bound, and when the user's attributes satisfy the access policy, the user can decrypt the ciphertext using the key. The CP-ABE has a wide range of applications, and it has been used by scholars in many fields to achieve data security sharing, such as access control for medical data [11], access control for cloud storage [12]. With the appropriate access policy set, it can manage data very flexibly. The paper [13] proposes a solution to the privacy and security problems that may arise in centralized IoT by combining blockchain and IoT and proposes a decentralized secure mechanism based on blockchain technology to store critical data generated in IoT on the blockchain. However, there are still many vulnerabilities and defects in current blockchain technology, and storage problems are one of the most important issues.

This paper proposes an intelligent home environment-based attribute-based encryption and blockchain-combined trusted data access control scheme to address the problem of secure sharing of privacy data for users. A combination of symmetric encryption algorithms and attribute-based encryption algorithms will be used to achieve fine-grained access control. Only authorized users who meet the access control policy can successfully access the data. Due to the low storage capacity of blockchain, this solution encrypts the data using a symmetric encryption algorithm first, and then stores the encrypted data in the cloud. This solution introduces edge computing nodes to assist in decryption, effectively reducing the computing load for users during decryption. However, to ensure data security, edge nodes only participate in partial decryption, while the relatively simple final decryption is completed by the visitor.

2. RELATED WORK

2.1. Attribute-based Encryption

In 2005, Sahai and Waters [8] first introduced the concept of attribute-based encryption, which brought attribute-based encryption into people's sight and has been applied by many domestic and foreign scholars. In 2011, Waters first proposed the Linear Secret Sharing Scheme (LSSS) based on linear secret sharing technology [14]. LSSS is an improvement of the CP-ABE scheme, which has better secret sharing performance and flexibility. The schemes proposed in [15, 16] both use the LSSS structure to achieve fine-grained access control, but their efficiency is low. Paper [17] proposed a secure outsourced decryption scheme, but the ciphertext policy was fully disclosed, which may lead to the leakage of users' privacy. The scheme proposed in [18] introduces the idea of linear secret sharing into the CP-ABE scheme, and achieves the hiding of access policies by hiding the attribute values. Paper [19] proposes a secure data sharing scheme for resource-constrained users in cloud computing to solve the problems of high computational overhead and poor big data security in existing ABE schemes by moving part of the encryption offline. Paper [20] proposes a verifiable outsourced encryption keyword search scheme, which outsources the complex search operation to the cloud and verifies whether the cloud has faithfully executed the search operation. Paper [21] proposes a CP-ABE scheme that avoids collusion attacks by users. Paper [22] proposes a new

encryption primitive, namely, attribute-based outsourced key generation and decryption, to solve the problem of inefficient query due to the large number of encrypted files stored in the cloud.

2.2. Edge Computing

Due to the limited computing power of personal computers, it is difficult to quickly and efficiently decrypt data. However, edge computing, as an extension of cloud computing, can greatly improve the efficiency of data decryption and at a lower cost. However, edge computing is vulnerable to malicious attacks and data leakage may occur during data sharing. Some scholars have designed data encryption and decryption schemes for secure data sharing. Paper [23] proposes an attribute-based encryption-based access control scheme that can shift part of the computation and storage overhead from the end-user to selected edge nodes. Paper [24] proposes a system for edge node device data sharing that simultaneously provides data confidentiality and data source identification. Paper [25] proposes a more secure attribute-based encryption scheme with the property of outsourced decryption, which can safely share data between edge nodes and resist chosen-ciphertext attack (CCA).

2.3. Blockchain

The essence of blockchain is a distributed database. Blockchain has two core features: data is difficult to tamper with, and it is decentralized. Based on these two features, the information recorded on the blockchain is more authentic and reliable, greatly reducing the cost of trust. Paper [26] proposes an electronic health record system based on attribute-based encryption and blockchain technology, combining blockchain and attribute-based encryption to ensure the integrity and traceability of medical data using blockchain technology. Paper [27] proposes a property-based access control framework that describes devices using a set of properties, records the distribution of properties on a blockchain, and simplifies access control protocols using hash calculations and digital signatures. Paper [28] proposes a blockchain sharding storage model based on threshold secret sharing, which can effectively reduce the storage capacity of each node. Paper [29] proposes a blockchain-based multi-authorization secure attribute-based signature scheme, formally proving the scheme secure in the random oracle model under the computational bilinear Diffie-Hellman assumption from the perspectives of unforgeability and perfect privacy of the attribute-based signer. Paper [30] proposes a decentralized, multi-authority, traceable attribute-based cryptographic system.

3. METHODOLOGY

3.1. System Model

The architecture of the trusted data access control scheme system combining attribute-based encryption and blockchain in smart home environment is shown in Figure 1. It mainly includes six entities: Data Owner (DO), Data User (DU), Trusted Authority (TA), Cloud Storage Provider (CSP), Blockchain (BC) and Edge Computing Provider (ECP).

(1) DO: The owner of the data can encrypt and customize the access control policies for shared data.

(2) DU: The user of the data can decrypt the ciphertext after obtaining it using the attribute private key generated by the trusted key management center, thereby obtaining the plaintext data.

(3) TA: A trusted key management center is responsible for generating the system master key, system master public key, and user attribute private key.

(4) BC: Blockchain is responsible for recording the hash values of encrypted files returned by CSP, as well as the parameters passed for related transactions.

(5) ECP: Edge computing assists DU in decryption calculations, and is responsible for converting attribute-based encrypted ciphertext.

(6) CSP: A third-party storage is responsible for storing the encrypted data and then returning the hash value of the encrypted data file.

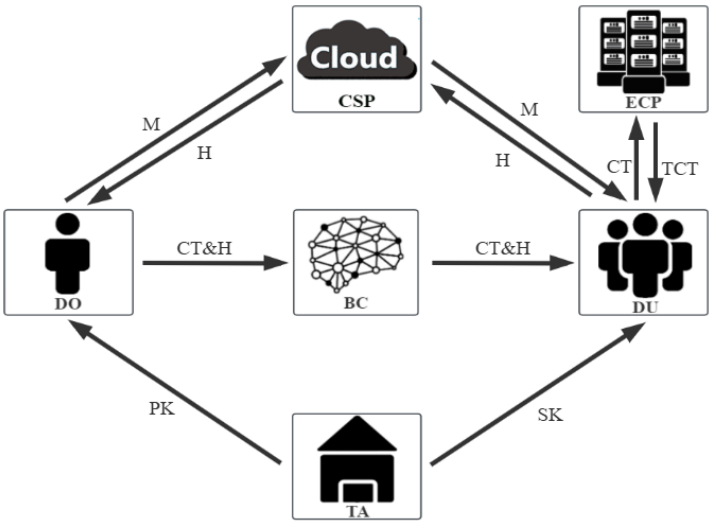

Figure 1. System architecture of proposed scheme

3.2. Implementation

3.2.1. System initialization

During the initialization phase, TA performs the algorithm Setup(U, 1^{λ})→(PK, MSK). First, input the system attributes domain U and the system security parameter λ. Then, output two multiplicative cyclic groups G_1 and G_2 of order p, where p is a prime number, and a computable bilinear map e:$G_1 \times G_1 \rightarrow G_2$, where g is a generator of the group G_1.

The algorithm randomly selects parameters α, a∈Z_p and then, for each attribute U_1, U_2, …, U_i(U_i∈U) in the system attribute domain U, randomly selects a parameter h_1, h_2, …, h_i(h_i∈G) as the attribute value. It then generates the system principal public key PK=(g, e(g, g)$^{\alpha}$, g^a, h_1, h_2, …, h_i) and the system principal secret key MSK=g^{α}. Finally, TA sends the system master key PK to DO and DU, and keeps the system master key MSK confidential.

3.2.2. Data encryption upload

The data encryption stage is performed by the data owner DO, and the encrypted ciphertext is uploaded and shared. In this scheme, the encrypted data is encrypted using a combination of symmetric encryption algorithm AES and attribute-based encryption algorithm, so this stage consists of symmetric encryption algorithm encryption and attribute-based encryption algorithm encryption.

(1) Symmetric encryption algorithms encrypt

First, DO selects the plaintext data file m that is to be shared, then calls a symmetric encryption algorithm to generate a symmetric encryption key key, and finally executes algorithm Encrypt1 (m, key)⟶(M). The algorithm takes in the plaintext data m and the symmetric encryption key key, and outputs the symmetric encrypted ciphertext M. DO will upload the encrypted message M generated by the algorithm to the CSP for storage. After the CSP completes the storage, it will return the hash value H to DO. Finally, DO uploads H to the blockchain BC record.

(2) Attribute-based encryption algorithm encrypts.

In this section, DO formulates access strategy A=(W, ρ) based on matrix W, where W is a matrix of l×n, and ρ is a mapping function that maps each row of the matrix W to the corresponding attribute value. After obtaining the system master public key PK and the symmetric encryption key key obtained through the execution of the symmetric encryption algorithm by the TA, DO performs

algorithm Encrypt2 (key, A, PK)⟶(CT). The algorithm uses an attribute-based encryption algorithm to encrypt the key key. The algorithm performs the following operations on the input plaintext data key, access control policy A, and system master public key PK: it randomly selects a vector $\vec{v}=(s, v_2, \ldots, v_n)\in Z_p$, where s is a randomly chosen and shared secret value, and for each row Wi of the matrix W, it calculates the inner product $\lambda_i=W_i\cdot\vec{v}$. It then randomly selects a parameter $r_1,r_2,\ldots,r_l\in Z_p$. The encrypted CT is as follows:

$$CT=(C=key\cdot e(g,g)^{\alpha s}, C'=g^s, (C_1=g^{a\lambda_1}h_{\rho(1)}^{-r_1}, D_1=g^{r_1}), \ldots, (C_l=g^{a\lambda_l}h_{\rho(l)}^{-r_l}, D_l=g^{r_l})) \quad (1)$$

Finally, DO uploads the encrypted CT to the blockchain BC for record keeping.

3.2.3. Private key generation for attributes

At this stage, TA is responsible for generating the attribute private key. First, the user initiates a request to generate a private key for the attribute, and then sends their attribute set S to the TA. TA receives the user's request and the attribute set S, and then executes algorithm KeyGen (PK, MSK, S)⟶(SK). The algorithm takes in the set of user attributes S, the system master key MSK, and the system master public key PK. First, for each user attribute $\{Ux\}_{x\in S}$, a matching attribute value $\{hx\}_{x\in S}$ is found, and then the algorithm randomly selects a parameter $t\in Z_p$ and constructs the attribute private key $SK=(K=g^{\alpha}g^{at}, L=g^t, \{K_x=h_x^t\}_{x\in S})$. Finally, TA sends the user's private key SK for the attribute.

3.2.4. Key transformation generation

This stage is completed by the data user DU. After obtaining the attribute private key SK generated by the TA, DU ensures the confidentiality of SK and encrypted data during outsourced computation by converting SK into a conversion key TK in this stage. DU implements algorithm TkeyGen (SK)⟶(TK), first inputs the attribute private key SK, then randomly selects $n\in Z^*_p$ and saves it. Finally, the generated conversion key is as follows:

$$K_{tra}=K^{\frac{1}{n}}, L_{tra}=L^{\frac{1}{n}}, K_{trax}=K_x^{\frac{1}{n}}, TK=(K_{tra},L_{tra},K_{trax}) \quad (2)$$

3.2.5. Data decryption

The decryption stage of data access is completed jointly by the data user DU and the edge computing node ECP. First, DU requests to obtain the hash value H and attribute-based encryption ciphertext CT. Then, DU downloads the symmetric encryption file M based on H. Finally, DU sends the ciphertext CT and the conversion key TK to the edge computing node ECP, allowing ECP to assist in the ciphertext conversion, while the final decryption process is completed by DU itself. Therefore, this stage is divided into two parts: the computation of the cipher transformation TCT and the decryption of TCT.

(1) Cryptographic transformation calculation

This part is completed by the edge computing node ECP. ECP performs algorithm Transform (TK, CT)⟶(TCT) after obtaining the ciphertext CT and the conversion key TK. Input TK and CT, if TK corresponds to the attribute set $S\notin A$, then the attribute set S does not satisfy the access control policy of the encrypted CT, decryption fails; if TK corresponds to the attribute set $S\in A$, then the attribute set S satisfies the access control policy of the encrypted CT and $\{\lambda_i\}$ is a valid share of the secret value s of the access matrix W, let $I\subset\{1,2,\ldots,l\}$ and define $I=\{i:\rho(i)\in S\}$, where I is a subset of the system attribute domain U, and the algorithm computes $\{w_i\in Z_p\}_{i\in I}$ in polynomial time such that $\sum_{i\in I} w_i\lambda_i=s$. Then the algorithm runs the following formula:

$$TCT=\frac{e(C',K_{tra})}{\prod_{i\in I}(e(C_i,L_{tra})e(D_i,K_{trap(i)}))^{W_i}} \quad (3)$$

$$e(C', K_{tra}) = e\left(g^{s}, g^{\frac{\alpha}{n}} g^{\frac{at}{n}}\right) = e\left(g^{s}, g^{\frac{\alpha}{n}}\right) e\left(g^{s}, g^{\frac{at}{n}}\right) = e(g,g)^{\frac{\alpha s}{n}} e(g,g)^{\frac{sat}{n}} \quad (4)$$

$$\prod_{i\in I}(e(C_i, L_{tra}) e(D_i, K_{tra\rho(i)}))^{w^i} = \prod_{i\in I}(e(g^{a\lambda_i} h_{\rho(i)}^{-r_i}, g^{\frac{t}{n}}) e(g^{r_i}, h_{\rho(i)}^{\frac{t}{n}}))^{w_i} = e(g,g)^{\frac{sat}{n}} \quad (5)$$

$$TCT = \frac{e(C', K_{tra})}{\prod_{i\in I}(e(C_i, L_{tra}) e(D_i, K_{tra\rho(i)}))^{w^i}} = \frac{e(g,g)^{\frac{\alpha s}{n}} e(g,g)^{\frac{sat}{n}}}{e(g,g)^{\frac{sat}{n}}} = e(g,g)^{\frac{\alpha s}{n}} \quad (6)$$

Finally, ECP will convert the ciphertext TCT and send it to the data user DU.

(2) Decrypt ciphertext conversion

This part is completed solely by the data user DU. After receiving the conversion ciphertext TCT from the ECP, the DU performs algorithm Decrypt2 (TCT)⟶(key). By inputting the transformation ciphertext TCT, the key=$\frac{C}{TCT^{n}}$ calculation can be used to directly obtain the symmetric encryption key. Using the key obtained from the above calculation and the ciphertext M downloaded from the CSP, DU applies the algorithm Decrypt1 (M, key)⟶(m) to obtain the desired plaintext file m.

3.2.6. Performance analysis

This section analyzes and verifies the proposed scheme through simulation experiments. The experimental environment of this paper is a Windows 11 computer with a 64-bit operating system, an AMD Ryzen 7 6800H processor, a CPU frequency of 3.2GHz, and 16GB of memory. The virtual machine environment is a 4-core 4GB memory machine with Ubuntu 20.0.4 as the operating system. A local server. The programming language used is Python. The cryptographic library used is pbc-0.5.14. The blockchain network is built using the open-source HyperLedger Fabric framework and Docker container technology.

This proposed scheme will compare the computational overhead with the schemes in [15, 21, 30] in the three stages of key generation, encryption, and decryption.

Figure 2 shows the key computation generation time of the proposed scheme compared with the schemes in [15, 21, 30]. From Figure 2, it can be seen that in the attribute key generation stage, compared with the schemes in [15, 21], the proposed scheme has increasingly obvious advantages in key generation computation as the number of user attributes increases, and it is slightly better than the scheme in [30].

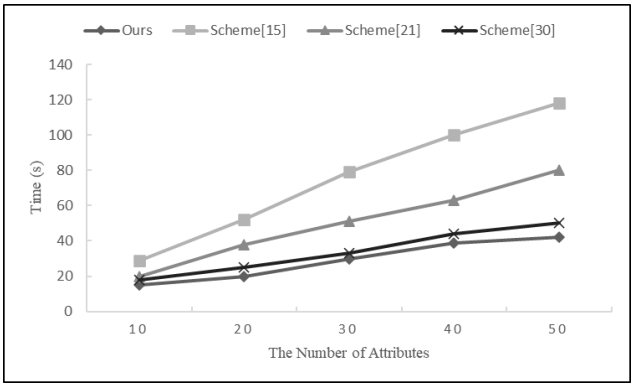

Figure 2. Calculation times of key generation

Figure 3 shows the encryption computation time of the proposed scheme compared with those of the schemes in [15, 21, 30]. From Figure 3, it can be seen that in the encryption computation stage, compared with the schemes in [15, 30], the proposed scheme has increasingly obvious advantages in encryption computation as the number of attributes in the access policy increases, while being basically on par with the scheme in [21].

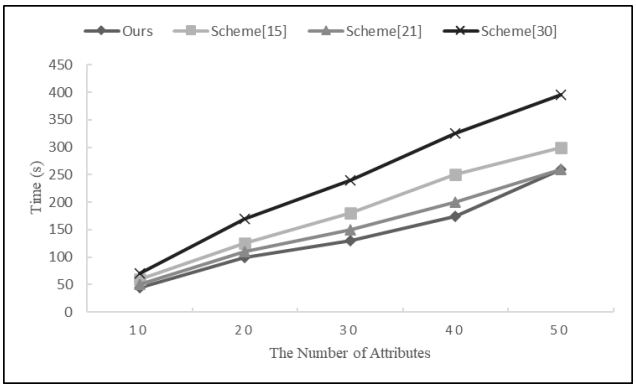

Figure 3. Encryption computation times

Figure 4 shows the decryption computation time of the proposed scheme compared with the schemes in [15, 21, 30]. From Figure 4, it can be seen that in the decryption computation stage, compared with the schemes in [15, 30], the proposed scheme has increasingly obvious advantages in decryption computation as the number of user attributes increases. Compared with the scheme in [21], the scheme in [21] has an advantage.

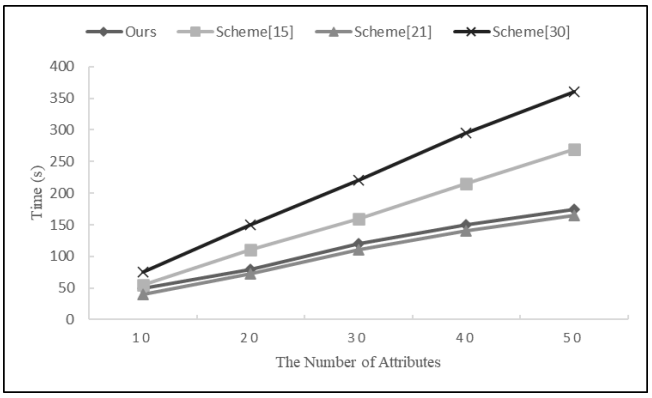

Figure 4. Decryption computation times

4. CONCLUSION

In the context of smart home environments, this paper proposes a trusted data access control scheme combining attribute-based encryption and blockchain to improve the efficiency of shared data, protect users' data privacy and security, and alleviate users' computing pressure. The scheme uses a combination of symmetric encryption algorithms and attribute-based encryption algorithms to encrypt user data in smart homes and upload it to the cloud for storage. The hash value generated by the cloud is stored on the blockchain. When a user initiates an access transaction, the system will send a corresponding proof transaction to the blockchain. This method of associating blockchain technology with cloud storage not only enables the system to monitor and audit users but also greatly reduces the storage burden on the blockchain. To alleviate the decryption calculation pressure on users, the proposed scheme introduces edge computing nodes to assist users in performing decryption calculation operations. To prevent the leakage of users' sensitive information, the encrypted ciphertext is first outsourced to the edge computing node for partial decryption, while the final decryption calculation is performed by the user himself/herself. Finally, the proposed scheme is analyzed and validated through simulation experiments. The experimental results show that the scheme is safe and effective, and is suitable for smart home environments.

ACKNOWLEDGEMENTS

We would like to extend our sincere appreciation to the editors and reviewers of the International Journal of Computer Science and Information Technology, whose expert insights and recommendations have significantly guided our research. Furthermore, we wish to acknowledge all our colleagues and friends who have offered their support and assistance in the preparation of this article.

REFERENCES

[1] RICQUEBOURG V, MENGA D, DURAND D, et al. The Smart Home Concept: Our Immediate Future[C]//IEEE. 2006 1ST IEEE International Conference on E-Learning in Industrial Electronics, December 18-20, 2006, Hammamet, Tunisia. New York: IEEE, 2007: 23-28.

[2] HAN D M, LIM J H, et al. Design and Implementation of Smart Home Energy Management Systems Based on Zigbee [J]. IEEE Transactions on Consumer Electronics, 2010(3): 1417-1425.

[3] STOJKOSKA B L R, TRIVODALIEY K V, et al. A Review of Internet of Things for Smart Home: Challenges and Solutions [J]. Journal of Cleaner Production, 2017, 140(3): 1454-1464.

[4] DORRI A, KANHERE SS, JURDAK R, et al. Blockchain for IoT Security and Privacy: The Case Study of a Smart Home[C]//IEEE. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, March 13-17,2017, Kona, HI, USA. New Yark: IEEE, 2017: 618-623.

[5] FERNANDES E, JUNG J, PRAKASH A, et al. Security Analysis of Emerging Smart Home Applications[C]//IEEE. 2016 IEEE Symposium on Security and Privacy (SP), May 22-26, 2016, San Jose, CA, USA. New Yark: IEEE, 2016: 636-654.

[6] BOTTICELLI M, MORETTI F, PIZZUTI S, et al. Challenges and Opportunities of Blockchain Technology in The Energy Sector[C]//IEEE. 2020 AEIT International Annual Conference (AEIT), September 23-25, 2020, Catania, Italy. New Yark: IEEE, 2020: 1-6.

[7] SHAO Qifeng, JIN Cheqing, ZHANG Shao, et al. Blockchain Technology: Architecture and Progress [J]. Journal of Computer Science, 2018, 41(5): 969-988.

[8] SAHAI A, WATERS B. Fuzzy Identity-Based Encryption[C]//Springer. Proceedings of the 24th annual international conference on Theory and Applications of Cryptographic Techniques, May 22-26, 2005, Aarhus, Denmark. Berlin Heidelberg: Springer, 2005: 457-473.

[9] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//ACM. Proceedings of the 13th ACM Conference on Computer and Communications Security, November 1-3, 2006, Alexandria, VA, USA. New Yark: ACM, 2005: 89-98.

[10] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-Policy Attribute-Based Encryption[C]//IEEE. 2007 IEEE Symposium on Security and Privacy (SP '07), May 20-23, 2007, Berkeley, CA, USA. New Yark: IEEE, 2007: 321-334.

[11] LI Wei, XUE Kaiping, et al. TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage [J]. IEEE, 2016, 27(5): 1484-1496.

[12] SINGH P, RAMAN B, AGARWAL N, et al. Secure Cloud-Based Image Tampering Detection and Localization Using POB Number System [J]. ACM Transactions on Multimedia Computing Communications and Applications, 2017, 13(3): 1-23.

[13] GE Chunpeng, LIU Zhe, FANG Liming. A blockchain based decentralized data security mechanism for the Internet of Things [J]. Journal of Parallel and Distributed Computing, 2020, 141(7): 1-9.

[14] WATERS B. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization [J]. Springer, 2011: 53-70.

[15] ZHANG Yinghui, ZHENG Dong, DENG R H. Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control [J]. IEEE, 2018, 5(3): 2130-2145.

[16] LIU Zhenhua, XU Jing, LIU Yan, et al. Updatable Ciphertext-Policy Attribute-Based Encryption Scheme with Traceability and Revocability [J]. IEEE Access, 2019, 7: 66832-66844.

[17] LAI Junzuo, DENG R H, GUAN Chaowen, et al. Attribute-Based Encryption with Verifiable Outsourced Decryption [J]. IEEE, 2013, 8(8): 1343-1354.

[18] LAI Junzuo, DENG R H, LI Yingjiu. Expressive CP-ABE with partially hidden access structures[C]// ACM. 7th ACM Symposium on Information, Computer and Communications Security (ASIACCS), May 2-4, 2012, Seoul, Korea. New Yark: ACM, 2012.

[19] LI Jin, ZHANG Yinghui, CHEN Xiaofeng, et al. Secure attribute-based data sharing for resource-limited users in cloud computing [J]. Computers & Security, 2018, 72: 1-12.

[20] ZHENG Qingji, XU Shouhuai, ATENIESE G. VABKS: Verifiable attribute-based keyword search over outsourced encrypted data[C]//IEEE. IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, April 27, 2014-May 2, 2014, Toronto, ON, Canada. New Yark: IEEE, 2014: 522-530.

[21] LI Jiguo, YAO Wei, HAN Jinguang, et al. User Collusion Avoidance CP-ABE With Efficient Attribute Revocation for Cloud Storage [J]. IEEE Systems Journal, 2018, 12(2): 1767-1777.

[22] LI Jiguo, LIN Xiaonan, ZHANG Yichen, et al. KSF-OABE: Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage [J]. IEEE, 2017, 10(5): 715-725.

[23] MIAO Yinbin, MA Jianfeng, Liu Ximeng, et al. Lightweight Fine-Grained Search Over Encrypted Data in Fog Computing [J]. IEEE, 2019, 12(5): 772-785.

[24] XU Shengmin, NING Jianting, LI Yingjiu, et al. Match in My Way: Fine-Grained Bilateral Access Control for Secure Cloud-Fog Computing [J]. IEEE, 2022, 19(2): 1064-1077.

[25] ZUO Cong, SHAO Jun, et al. CCA-secure ABE with outsourced decryption for fog computing [J]. Future Generation Computer Systems-The International Journal of eScience, 2018, 78: 730-738.

[26] WANG Hao, SONG Yujiao. Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain [J]. Journal of Medical Systems, 2018, 42(8): 152.

[27] DING Sheng, CAO Jin, LI Chen, et al. A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT [J]. IEEE Access, 2019, 7: 38431-38441.

[28] ZHANG Guochao, WANG Ruijin. Blockchain shard storage model based on threshold secret sharing [J]. Journal of Computer Applications, 2019, 39(9): 2617-2622.

[29] GUORui, SHI Huixian, ZHAO Qinglan, et al. Secure Attribute-Based Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems [J]. IEEE Access, 2018, 6: 11676-11686.

[30] SETHI K, PRADHAN A, BERA P. PMTER-ABE: a practical multi-authority CP-ABE with traceability, revocation and outsourcing decryption for secure access control in cloud systems [J]. Cluster Computing-The Journal of Networks Software Tools and Applications, 2021, 24(2): 1525-1550.