2021 17th International Conference on Mobility, Sensing and Networking (MSN) | 978-1-6654-0668-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/MSN53354.2021.00030

Blockchain-based Access Control Model to Preserve Privacy for Students' Credit Information

Quanwen He
College of Computer
and Cyber Security,
Fujian Normal University,
Fuzhou, Fujian, China,
Engineering Research Center
of Cyber Security
and Education Informatization,
Fujian Province University,
Fuzhou, Fujian, China,
e-mail: heqw15890514263@163.com

Hui Lin
College of Computer
and Cyber Security,
Fujian Normal University,
Fuzhou, Fujian, China,
Engineering Research Center
of Cyber Security
and Education Informatization,
Fujian Province University,
Fuzhou, Fujian, China,
e-mail: linhui@fjnu.edu.cn

Fu Xiao
School of Computer,
Nanjing University of
Posts and Telecommunications,
Nanjing, China,
e-mail: xiaof@njupt.edu.cn

Jia Hu
University of Exeter
Exeter, UK
e-mail: j.hu@exeter.ac.uk

Xiaoding Wang
College of Computer
and Cyber Security,
Fujian Normal University,
Fuzhou, Fujian, China,
e-mail: wangdin1982@fjnu.edu.cn

Abstract—In the process of sharing students' credit information across schools and departments, there are some problems such as tampering and leaking of students' credit information.In this paper, combined with the characteristics of blockchain traceability and difficult to tamper, a credit information access control method based on blockchain is proposed, which not only protects students' privacy, but also realizes the cross school access control of students' credit information.This paper designs a multi blockchain architecture that combines consortium blockchain and private blockchain of colleges and universities. It stores credit information summary on the blockchain and original records off the blockchain to relieve the storage pressure of blockchain; Then, the multi authorization attribute encryption technology is used to set the access policy for fine-grained access control.Finally, the simulation results show that the scheme can achieve fine-grained access control of students' credit information while protecting students' privacy.

Index Terms—Blockchain, Access Control, Privacy preserving

I. Introduction

Students' credit information records all kinds of data information such as course selection, examination and evaluation, academic achievements, awards and certificates of college students during their study in school, which completely and truly reflects the learning track of students.With the development of the Internet, universities use information technology to improve the efficiency of credit storage and processing.While the existing educational administration system brings convenience to the management of students' learning records, there are still the following main problems:(1)The course scores, credits and certificates generated in the process of students' learning are easy to be modified and forged in the process of storage, transmission and processing;(2)Every university is the "isolated island" of students' learning data information, and there is a lack of safe and effective channels for students' credit information sharing between universities;(3)Most of the existing credit record systems do not realize encryption function, which is easy to cause the leakage of students' privacy.

Blockchain technology can build trust and transfer value. Through the use of blockchain technology, students' learning records can be stored digitally, students' information privacy can be protected, and cross regional students' credit information can be shared reliably.This paper proposes the following solutions based on blockchain and multi authorization attribute encryption algorithm.

(1)The original data of students' credit information is encrypted by the existing storage server, and the summary information and server storage address of students' credit information are stored with the smart contract on the chain, so as to ensure that the records of students' credit information are true and reliable and can not be forged and tampered with. All institutions in Colleges and universities form a private chain, and all node units in Colleges and universities share information, A complete and traceable record chain of student credit information is established. While ensuring the data security, it reduces the cost of data protection. Colleges and universities form an consortium blockchain to realize the credible sharing of students' credit information across regions;

978-1-6654-0668-0/21/$31.00 ©2021 IEEE
DOI 10.1109/MSN53354.2021.00030

(2)By storing the modification records of students' learning situation on the smart contract, the responsibility of the person in charge of the modification operation of students' learning data is realized;

(3)Based on the method of credit certification and sharing proposed in this paper, a credit certification and sharing system is developed. The system is connected with the traditional educational administration system in the form of interface to reduce the budget cost of building application system and database.

We organize the rest of this paper as follows. The related work is given in section II. Section III introduces some preliminary knowledge. The Proposed Scheme is presented in section IV. The security of the scheme is proved in section V. The performance evaluation of this scheme is given in section VI. Section VII concludes this paper.

II. Related Work

At present, the use of blockchain for data access control to solve the problem of data island has been well applied in many fields, but with the continuous increase of data, the storage space of blockchain has become its limiting condition, and data privacy is also the key problem of data sharing. Li et al. [3] propose a lightweight dual-blockchain privacy protection and sharing solution for smart grid intelligent pricing systems, in which blockchain,identity-based proxy re-encryption strategies and bilinear pair-based signature scheme is combine to provide the confidentiality, privacy and integrity of electricity data. Guo et al. [4] proposed a hybrid blockchain-edge architecture.The scheme combines the technology of blockchain and edge node to realize the access control management of electronic health records.Identity management, access control policy management and access log storage are implemented based on blockchain technology.Off-chain edge nodes store the electronic health records. Song et al. [5] design an attribute-based access control using smart contracts scheme for IoT.This scheme solves the dynamic, distributed and reliable access control problems in the open IoT environment. Bera et al. [6] design a blockchain access control scheme in an IoT-enabled IoD environment. IoD.The scheme solves the security and privacy problems in the process of UAV Communication. Sultana et al. [7] proposed a data sharing and access control system based on blockchain, which is used for communication between devices in the IoT. The system provides effective access control management through access control contract, registration contract and judgment contract, and realizes the trust, authorization and authentication of data sharing in the IoT. Esposito et al. [8] develop a generic solution of blockchain-based authentication and authorization for smart city applications.This shceme can be coupled to any possible platform.

CP-ABE means that the ciphertext corresponds to an access structure and the key corresponds to an attribute set. If and only if the attributes in the user's attribute set can satisfy the access structure, the user can decrypt the ciphertext and obtain the key. Bethencourt et al [9] proposed CP-ABE for the first time.Lewko et al. [10] proposed an attribute encryption scheme with multiple authorization centers, in which any authorization center can become the central authority, and each attribute authorization center is independent.Banerjee et al. [11] proposed a multi privilege attribute encryption scheme based on CP-ABE for data use in the IoT environment, which has a constant size key and ciphertext.Yang et al[12] design an attributed-based access control for multi-authority systems in cloud storage.The scheme does not need global permission and can support any LSSS access structure.It also solves the problem of attribute revocation.In order to solve the security problem of data trading platform, Zhang et al[13] design a data security sharing method based on CP-ABE and blockchain.

III. Preliminaries

The parameters and their descriptions are given in Table I.

TABLE I

Parameter	Descriptions
UID	User identity
UK_{UID}	User key
SK_{UID}	User private key
S	User attribute set
$\boldsymbol{A}_i$	Access the i-th line of matrix $\boldsymbol{A}(l \times n)$
ASK	Private key of attribute authority
APK	Public key of attribute authority
s	Secret sharing key
$\vec{v}$	Random vector selection in encryption algorithm
M	Data plaintext
CT	Data ciphertext
TK	Transform key
T	Transform cipertext

A. Bilinear Map

Let G_1, G_2 and G_T be multiplicative cyclic groups of prime order P. If $e : G_1 \times G_2 \longrightarrow G_t$ is a bilinear mapping, it has the following three properties:

1) Bilinearity:$\forall g \in G_1$,$\forall h \in G_2$, $\forall x, y \in Z_p$ $e\left(g^x, h^y\right) = e\left(g, h\right)^{xy}$.
2) Non-degeneracy:$\exists g \in G_1, \exists h \in G_2$, such that $e\left(g, h\right) \neq 1$.
3) Computability:For $\forall g \in G_1$,$\forall h \in G_2$,there is an efficient algorithm to calculate $e\left(g, h\right)$.

B. Decisional Bilinear Diffie-Hellman Assumption

Let a bilinear mapping on a group G be $e : G \times G \longrightarrow G_t$,$g$ is the generator of group G, P is the prime order of group G. $a, b, c, Z \in Z_p^*$ is selected randomly, then given the tuple (g, g^a, g^b, g^c, Z), $Z = e(g, g)^z$ and $e(g, g)^{abc}$ must be distinguished. The advantage of attackers to solve the DBDH problem in G_T is ϵ That is to meet the conditions:

$$\begin{aligned} &\left|P[A(g, g^a, g^b, g^c, e(g, g)^{abc}) = 0]\right| - \\ &\left|P[A(g, g^a, g^b, g^c, Z) = 0]\right| \geq \epsilon \end{aligned} \tag{1}$$

IV. Proposed Scheme

A. System Model

This system model combines the blockchain with the local storage server to store the data summary on the blockchain and the original data off the blockchain. At the same time, it combines the multi-attribute central attribute encryption mechanism to realize the fine-grained access control of the data. The model consists of the following seven entities: certificate authority, attribute authorities, data owner, users, consortium blockchain, private blockchain and local storage server, as shown in Figure 1.

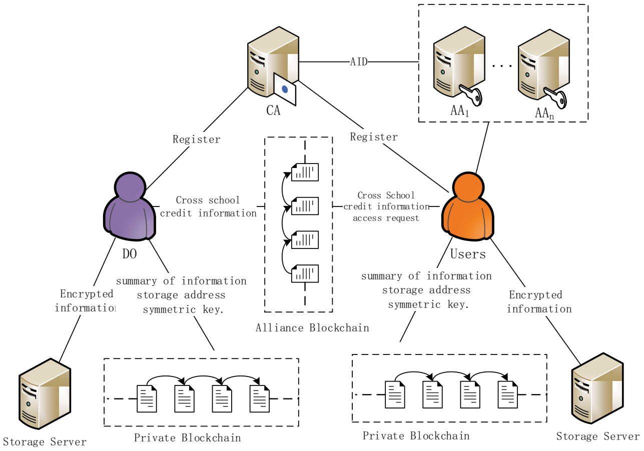

Fig. 1. System Model.

- Certificate Authority(CA): CA is mainly responsible for generating system public parameters. When the system user applies for registration, it generates a unique ID uid for the user, generates an identity key for the user according to the uid, and assigns a unique aid to each attribute center AA.
- Attribute Authorities(AAs): The AA is responsible for generating its own private and public key pairs, and generating attribute private keys for users according to the system public parameters, data user's identity key and attribute set.
- Data owner(DO): The owner of students' credit information can symmetrically encrypt the students' credit information and store it in the local storage server. At the same time, the access control policy can be set to encrypt the summary of credit information, the storage address of credit information and the encrypted symmetric key, and store it in the private blockchain of the university.
- Users: When the user attributes meet the set access control policy, the storage address of the access credit information and the encrypted symmetric key can be obtained, and then the obtained ciphertext data can be decrypted to obtain the plaintext credit information.
- Consortium Blockchain(CB):Store the information of credit information access of cross school users. When the ownership of credit information is in doubt, we can trace the historical information to realize the confirmation of credit information.
- Private Blockchain(PB):It stores the summary of students' credit information, storage address and symmetric key.
- Local Storage Server(LSS):The data owner uses symmetric encryption technology to encrypt the credit information and store it in the local storage server to relieve the storage pressure of blockchain.

B. Blockchain Architecture

This paper intends to use the form of private blockchain and consortium blockchain to build a private chain in colleges and universities. The secondary colleges and other departments of colleges and universities are the nodes of the private blockchain to protect the credit information of students in Colleges and universities. Each university forms an consortium blockchain through the consensus mechanism, and the data is shared among universities through the consortium blockchain. The blockchain architecture is shown in Figure 2. In this paper, the data can not be directly accessed between colleges and universities in the blockchain architecture. The data interaction between colleges and universities is through the sharing node and consortium blockchain. When college students have the problems of postgraduate entrance examination or doctoral degree, the universities that need to cross the university can apply to the consortium blockchain to join the consortium blockchain system. The consortium blockchain stores the information of each university and the sharing node with the University. When university a wants to access the credit information of University B students, it needs to submit the request of Cross University data access, The sharing node of university a sends the access request to the consortium blockchain node and waits for the verification operation of the consortium blockchain. Then the consortium blockchain node calls the blockchain code to access the corresponding student data of University B. the sharing node of University B receives the access request and collects the relevant data from the user. Then the data is returned to the consortium blockchain node, and the consortium blockchain node returns the data to the sharing node of University a, Then the shared node of university a saves the data to the private blockchain of University a. When the cross school data access is successful, the consortium blockchain stores the information of Cross School data access, and realizes the data traceability and data right confirmation in the process of Cross School.

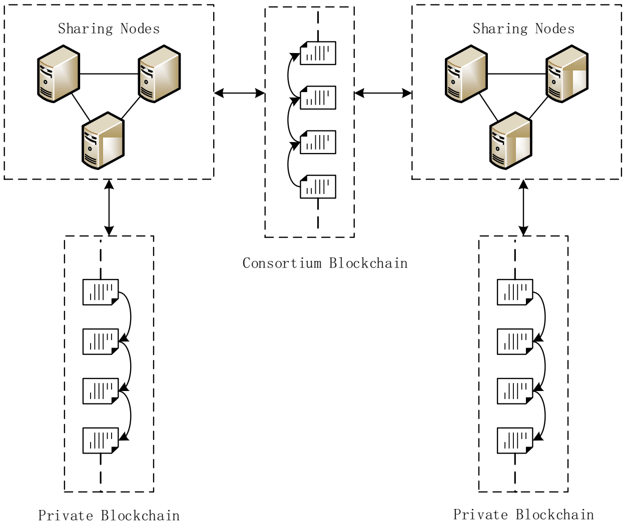

Fig. 2. Blockchain Architecture

C. Access control scheme of credit information

1) In the user registration stage, the user sends a registration application to the CA. the CA verifies the user's identity and generates the UK_{UID} for the user according to its UID. Then the AA generates the corresponding SK_{UID} for the user according to the UK_{UID} and attribute set S submitted by the users;
2) In the credit information authorization stage, the DO uses SM4 encryption algorithm to encrypt the students' credit information and store it in the local storage server, and sets the access policy $(\boldsymbol{A},\rho)$,using the set access policy $(\boldsymbol{A},\rho)$ to encrypt the data storage address and symmetric encryption key to get the ciphertext, and the encrypted data and data digest are stored on the private blockchain;
3) In the credit data link stage, the consensus node verifies and agrees the data information, generates new blocks and joins the blockchain. The student credit information summary, storage address and symmetric encryption key are stored in the private blockchain of the university
4) In the stage of authorized access to student credit information,(1)When users in colleges and universities apply to access the students' credit information according to the data digest, the authorized users can successfully obtain the storage address of the students' credit information and SM4 symmetric key according to their own attribute private key. Before decryption, the encrypted data on the blockchain can be converted to ciphertext by the nodes on the private blockchain of colleges and universities, and the authorized users can decrypt the converted ciphertext, Then the encrypted credit information is obtained according to the storage address request, and the plaintext data is obtained by using symmetric key decryption;For the unauthorized users, they can't get the storage address of credit information and can't access the data, which realizes the controllable data access.(2)In the Cross-School Credit Information authorization access stage, data users send data request information and their own attribute private key to the supervision chain node, and the consortium blockchain node calls the chain code to apply for the data storage address and symmetric key to the private chain in the corresponding University, and the consortium blockchain node obtains the encrypted data, Then, the encrypted data storage address and symmetric key are decrypted, and the converted ciphertext is returned to the data user. The data user can decrypt the data storage address and symmetric key by using the attribute private key, Then, the symmetric encrypted ciphertext data is obtained according to the storage address request data, and the symmetric key is used to decrypt the ciphertext to obtain plaintext.

D. Multi authority attribute encryption scheme

We propose a multi authorization attribute encryption scheme as follows:

1) CA Setup.CA through security parameters λ, two multiplicative cyclic groups G and G_T with prime P are generated, g is the generator of G and bilinear mapping $e: G \times G \longrightarrow G_T$, select a hash function $H: \{0,1\}^* \longrightarrow G$.When the system receives the user's registration request, the system assigns UID to the user, randomly selects $u \in Z_p^*$, and generates an identity key for it. The $PK_{UID} = g^u$. When an AA joins the system, the CA needs to authenticate the identity of the AA. If the attribute authorization mechanism is legal, it assigns a unique AID to the AA;
2) AA Setup.Each AA takes a random number $t_{i,v} \in Z_p^*$ for each attribute $i \in S_n$ according to its own attribute set S_n, and calculates $h_{i,v} = g^{t_{i,v}}$, where v is the version number, and randomly selects parameters $\alpha, \beta \in Z_p^*$ The initialization algorithm is run,then the AA output public key $APK_{i,AID} = \left(g, e(g,g)^\alpha, g^\beta, h_{i,v}\right)$ and private key $ASK_{i,AID} = (\alpha, \beta, t_{i,v})$;
3) Key generation input user's UID, user attribute set S and private key of related attribute center. AA_{AID} runs key generation algorithm to generate user's private key SK_{UID},user's secret parameter SP_{UID} and user's transform key TK_{UID}.Randomly select $t, z \in Z_p$,users' private key $SK_{UID} = t$, transform key $TK_{UID} = \left(K = g^{\alpha/t} g^{\beta z/t}, L = g^{z/t}, \forall i \in S, K_i = (h_{i,v})^{z/t}\right)$;
4) Encry data.Executed by the DO, input the plaintext M and the set LSSS type access policy $(\boldsymbol{A},\rho)$,function ρ map each row of matrix $\boldsymbol{A}$ to an attribute, where $\boldsymbol{A}$

is an $l \times n$, l is the number of attributes.Do randomly selects a secret value s for sharing and a random vector $\vec{v} = (s, \vec{v}_2, \vec{v}_3, ..., \vec{v}_n)$,where $s, v_i \in Z_p^*$.Output ciphertext $CT = (C = Me(g,g)^{\alpha s}, C' = g^s, C_i = g^{\beta\lambda_i}(h_{i,v})^{-r_i}, D_i = g^{r_i})$ $1 \leq i \leq l$ $\lambda_i = v\boldsymbol{A}_i$,where $\boldsymbol{A}_i$ is the i line of $\boldsymbol{A}$;

5) Transform CT.Input the ciphertext CT and the transform key TK corresponding to the user's attribute set to judge whether the attributes in the attribute set S meet the access policy set in the CT $(\boldsymbol{A}, \rho)$,If it is satisfied, the CT can be decrypted successfully to obtain the converted ciphertext. If the attribute in attribute set S does not meet the $(\boldsymbol{A}, \rho)$ in the ciphertext,the output is $\perp$.$\rho(i) \in S$,$\omega_i \in Z_p^*$,$\sum_{i=1}^{l} \omega_i \lambda_i = s$,Calculating and converted ciphertext:$E = \prod_{i=1}^{l}(e(C_i, L)e(D_i, K_{\rho(i)}))^{\omega_i}$
$T = \frac{e(C',K)}{E} = e(g,g)^{\alpha s/t}$;
6) In the data decryption stage, the input is the user's private key and the pre decrypted ciphertext, and the calculation is performed:
$M' = \frac{C}{T^{SK_{UID}}} = \frac{Me(g,g)^{\alpha s}}{(e(g,g)^{(\alpha s/t)})^t} = M$

V. Security Analysis

A. Security Model

The security model of this scheme is completed by an indistinguishable game.In the game, challenger B answers the query request of adversary A. the game process is as follows:

(1) Initialization phase,adversary A chooses an access structure to challenge and sends it to challenger B. Challenger B runs initialization algorithm to generate public parameters of the system. Then, the AA executes AA initialization algorithm to generate public-private key pairs;
(2) Inquiry phase,adversary A sends attribute set S_{UID} to challenger B for query, and challenger B runs key generation algorithm to calculate adversary A's private key and transform key;
(3) Challenge phase,adversary A submits two messages $M_0, M_1 (M_0 \neq M_1)$ of the same length to challenger B, After receiving the message,challenger B randomly selects $x \in 0, 1$ to encrypt the message, and sends the ciphertext to adversary A;
(4) Repeat inquiry phase, repeat the operation of inquiry phase;
(5) Guessing phase,adversary A guesses x to get x'. if $x' = x$, adversary A wins the game. Opponent a's advantage is $Adv_A = \left|P(x' = x) - \frac{1}{2}\right|$

B. Security Proof

Theorem 1:If the decisional bilinear Diffie-Hellman problem holds, then there is no nonnegligible advantage of adversary A in polynomial time ϵ Win the challenge game. Otherwise, there is another adversary $\frac{\epsilon}{2}$ to solve the bilinear Diffie-Hellman problem.

Proof:Two multiplicative cyclic groups G and G_T with prime order P are selected.g is the generator of G,and a bilinear mapping $e : G \times G \longrightarrow G_t$. In addition, the Challenger gives an instance (g, g^a, g^b, g^c, Z) and randomly selects $x \in 0, 1$, If $x = 0$, then $Z = e(g,g)^{abc}$; if $x = 1$, then $Z \in G_t$. The game process of challenger B and adversary A is as follows:

1) Initialization phase, challenger B runs the initialization algorithm to generate public parameters and send them to adversary A. Adversary A specifies the destroyed AA to run initialization algorithm to generate public key and private key;
2) Inquiry phase,adversary A submits S_{UID} to challenger B for private key query and transform key query, where S_{UID} does not meet the set access structure (A, ρ),challenger B runs the key generation algorithm to generate the corresponding and transform key for adversary A.Randomly select $t, z \in Z_p$,users' private key $SK_{UID} = t$, transform key $TK_{UID} = \left(K = g^{\alpha/t} g^{\beta z/t}, L = g^{z/t}, \forall i \in S, K_i = (h_{i,v})^{z/t}\right)$;
3) Challenge phase,adversary A submits two messages $M_0, M_1 (M_0 \neq M_1)$ of the same length to challenger B, After receiving the message,challenger B randomly selects $x \in 0, 1$ to encrypt the message, the encrypted message is CT,calcuating parameters $C = Me(g,g)^{\alpha s}, C' = g^s, C_i = g^{\beta\lambda_i}(h_{i,v})^{-r_i}, D_i = g^{r_i}$.Then challenger B sends the $CT = (C, C', C_i, D_i)$ to adversary A;
4) Repeat inquiry phase, repeat the operation of inquiry phase;
5) Guessing phase,adversary A outputs a guess value x',if $x' = x$, challenger B outputs a guess value $x' = 0$; Otherwise, the output result $x' = 1$. If $x = 0$, $Z = e(g,g)^{abc}$, The advantage of adversary A in distinguishing M_0 and M_1 is ϵ,then $P(x'|x = 0) = \frac{1}{2} + \epsilon$;If $x = 1$, then$P(x' \neq x|x = 1) = \frac{1}{2}$.Therefore, the probability of challenger B winning the game is as follows:
$\frac{1}{2}\left(P(x' = x|x = 0) + P(x' \neq x|x = 1)\right) - \frac{1}{2} = \frac{\epsilon}{2}$
The proof is complete.
It can be seen from the above proof that if adversary A breaks the scheme in this paper with an advantage that can not be ignored ϵ,challenger B can alsoe solve the DBDH problem with the same advantage

VI. Performance Evaluation

A. Blockchain Network Experiment

The experimental test environment of blockchain network is shown in Table II. The test blockchain network

TABLE II

Operating environment	Tools and version number
Operating system	Ubuntu20.04.2 LTS
Software	Hyperledger Fabric2.2
Database	LevelDB
Development Language	Go1.16.4

runs on a single host, including a single node belonging to two organizations, two MSPs, and one sorting service using solo consensus, which are located in the same channel. The test method is to send 500-4000 transactions to the blockchain network, and the transaction types are write and query. Observe the changes of duration and TPS of the system under different transaction volumes. The results are shown in Figure 4-5.

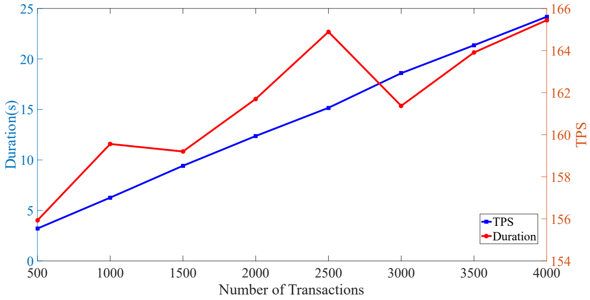

Fig. 3. Write Performance

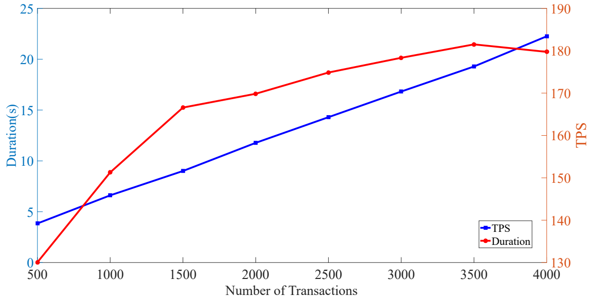

Fig. 4. Query Performance

From the experimental results, we can see that the duration increases linearly with the increase of transaction volume. The TPS reaches the maximum when the transaction type is query and the number of transactions is 3500. The TPS reaches the maximum when the transaction type is write and the number of transactions is 4000.

B. Multi Authorization Attribute Encryption Experiment

The experiment of multi authorization attribute encryption is carried out on the virtual machine of Ubuntu20.04.2 LTS operating system. The hardware configuration is Intel(R) core(TM) i5-7500H CPU, the main frequency is 3.40GHz, and the memory is 2GB. The scheme is implemented by using pairing based PBC cipher library and programming language python.

The access control scheme proposed in this paper is based on blockchain and multi authorization attribute encryption technology, which realizes complete decentralization, solves the problem of single attribute centralized risk and heavy computing load, and increases the ciphertext conversion function to alleviate the decryption cost of users.As shown in Figure 5-7, the number of attribute authority is fixed to two, the generation time of user key, and the time of data encryption and decryption increases with the increase of the number of the attribute.

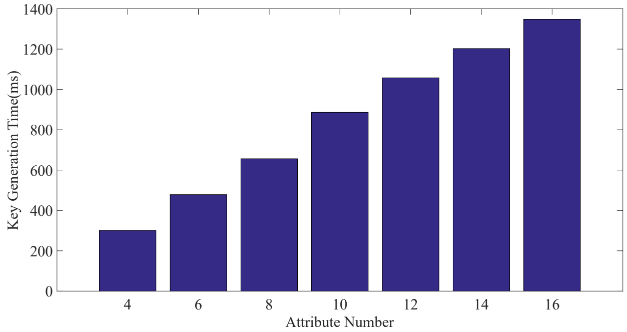

Fig. 5. Key Generation Time

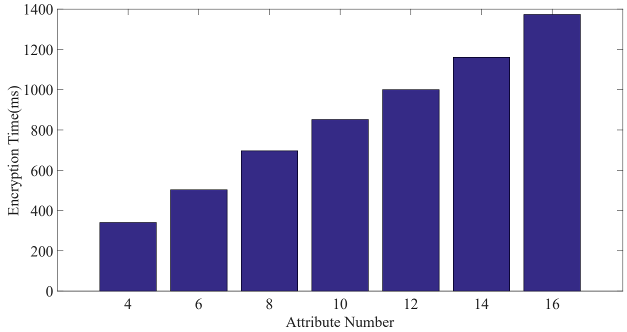

Fig. 6. Encryption Time

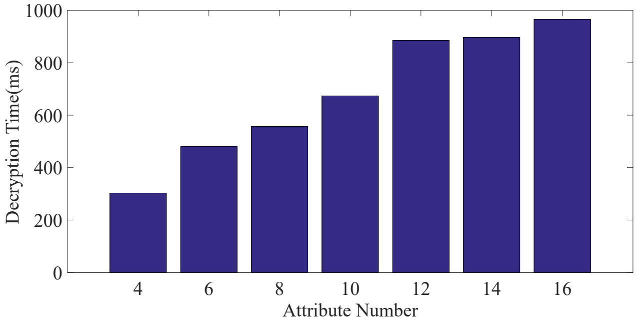

Fig. 7. Decryption Time

As shown in Figures 8 and 9, when the access attributes are fixed to eight, the corresponding encryption and decryption time increases gradually with the increase of the size of the data to be encrypted and decrypted. But the time of decryption changes little.

VII. Conclusion

In order to achieve fine-grained access control between colleges and universities, this paper proposes a credit

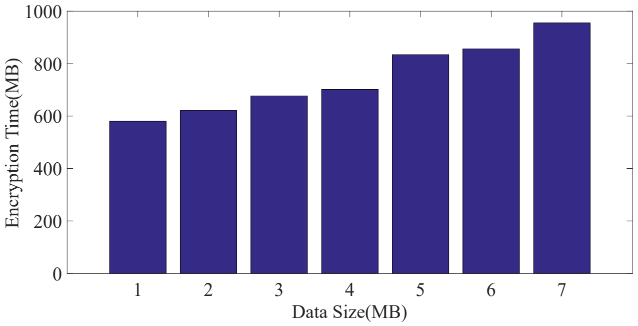

Fig. 8. Encryption Time

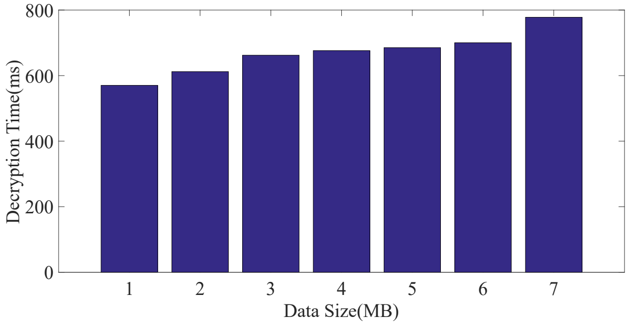

Fig. 9. Decryption Time

information access control method based on blockchain multi chain, multi authorization attribute encryption and other technologies, in which the private blockchain is used to isolate and protect the credit information of college students, and the consortium blockchain is used to realize cross-school Interaction and storage; In the process of credit information access control, to solve the problems of single authority overload and risk concentration and alleviate the problem of data user decryption calculation overhead, multi authorization attribute encryption technology is used to meet the fine-grained access control. Finally, simulation results show that the proposed scheme can achieve fine-grained access control of students' credit information while protecting students' privacy.

References

[1] M. Sookhak, M. Jabbarpour, N. Safa and F. Yu, "Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues", Journal of Network and Computer Applications, vol. 178, p. 102950, 2021, doi: 10.1016/j.jnca.2020.102950.

[2] H. Li and D. Han, "EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme", IEEE Access, vol. 7, pp. 179273-179289, 2019, doi: 10.1109/access.2019.2956157.

[3] K. Li, Y. Yang, S. Wang, R. Shi and J. Li, "A lightweight privacy-preserving and sharing scheme with dual-blockchain for intelligent pricing system of smart grid", Computers & Security, vol. 103, p. 102189, 2021, doi: 10.1016/j.cose.2021.102189.

[4] H. Guo, W. Li, M. Nejad and C. Shen, "Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture", 2019 IEEE International Conference on Blockchain (Blockchain), 2019, doi: 10.1109/blockchain.2019.00015.

[5] L. Song, M. Li, Z. Zhu, P. Yuan and Y. He, "Attribute-Based Access Control Using Smart Contracts for the Internet of Things", Procedia Computer Science, vol. 174, pp. 231-242, 2020, doi: 10.1016/j.procs.2020.06.079.

[6] B. Bera, D. Chattaraj and A. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment", Computer Communications, vol. 153, pp. 229-249, 2020, doi: 10.1016/j.comcom.2020.02.011.

[7] T. Sultana, A. Ghaffar, M. Azeem, Z. Abubaker, M. Gurmani and N. Javaid, "Data Sharing System Integrating Access Control Based on Smart Contracts for IoT", Advances on P2P, Parallel, Grid, Cloud and Internet Computing, pp. 863-874, 2019, doi: 10.1007/978-3-030-33509-0_81.

[8] C. Esposito, M. Ficco and B. Gupta, "Blockchain-based authentication and authorization for smart city applications", Information Processing & Management, vol. 58, no. 2, p. 102468, 2021, doi: 10.1016/j.ipm.2020.102468.

[9] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption", 2007 IEEE Symposium on Security and Privacy (SP '07), 2007, doi: 10.1109/sp.2007.11.

[10] A. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption", Advances in Cryptology – EUROCRYPT 2011, pp. 568-588, 2011, doi: 10.1007/978-3-642-20465-4_31.

[11] S. Banerjee et al., "Multi-Authority CP-ABE-Based user access control scheme with constant-size key and ciphertext for IoT deployment", Journal of Information Security and Applications, vol. 53, p. 102503, 2020, doi: 10.1016/j.jisa.2020.102503.

[12] K. Yang and X. Jia, "Attributed-Based Access Control for Multi-authority Systems in Cloud Storage", 2012 IEEE 32nd International Conference on Distributed Computing Systems, 2012, doi: 10.1109/icdcs.2012.42.

[13] Z. Zhang and X. Ren, "Data security sharing method based on CP-ABE and blockchain", Journal of Intelligent & Fuzzy Systems, vol. 40, no. 2, pp. 2193-2203, 2021. doi: 10.3233/jifs-189318.

[14] S. Gao, G. Piao, J. Zhu, X. Ma and J. Ma, "TrustAccess: A Trustworthy Secure Ciphertext-Policy and Attribute Hiding Access Control Scheme Based on Blockchain", IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5784-5798, 2020, doi: 10.1109/tvt.2020.2967099.

[15] S. Rasool, A. Saleem, M. Iqbal, T. Dagiuklas, S. Mumtaz and Z. u. Qayyum, "Docschain: Blockchain-Based IoT Solution for Verification of Degree Documents," in IEEE Transactions on Computational Social Systems, vol. 7, no. 3, pp. 827-837, June 2020, doi: 10.1109/tcss.2020.2973710.