2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)



# Multi-layer Access Control Mechanism based on Blockchain for Mobile Edge Computing

1st YiChen Hou
*School of Mathematics and Information*
*Fujian Normal University*
FuZhou, China
Email:Linvh_11@163.com

2nd WenXin Liu
*School of Mathematics and Information*
*Fujian Normal University*
FuZhou, China
Email:sixwenxin@163.com

3*rd Hui Lin
*School of Mathematics and Information*
*Fujian Normal University*
FuZhou, China
Email:linhui@fjnu.edu.cn

4*th XiaoDing Wang
*School of Mathematics and Information*
*Fujian Normal University*
FuZhou, China
Email:wangdin1982@163.com

***Abstract*—Massive data generated by mobile terminals in edge computing brings new data security threats to data access control. However, previous access control strategies have deficiencies, i.e., coarse-graininess and poor flexibility, which cannot meet the requirements of secure data access to support various mobile edge computing applications. To overcome these shortcomings, in this paper, a Blockchain based Multi-layer Access Control mechanism, named BMAC, is proposed. Specifically, each resource data is assigned a security level. Then, an InfoMap based algorithm is developed to achieve credibility based users grouping. Next, a multi-blockchain is designed, based on which a flexible and fine-grained trusted data access control mechanism is established. The experiment results show that the BMAC scheme has better performance in terms of processing efficiency, throughput, CPU utilization, and latency.**

***Index Terms*—Mobile edge computing, Access control, Blockchain**

## I. Introduction

As an extension of mobile cloud computing [1], Mobile Edge Computing (MEC) [2], [3] has advantages in location awareness, mobile support, low latency, and decentralized computation, which makes it more applicable for complex network infrastructures rather than traditional ones supported by cloud computing [4]. Due to above reasons, MEC can be applied to a variety of fields such as intelligent transportation, smart cities, augmented reality/virtual reality, and real-time big data analysis [5]–[7].

With the rapid development of MEC technologies, the massive data generated by mobile terminals [8] in MEC has brought new security threats to data access such as data leakage, unauthorized access, and so on. However, the existing access control strategies suffer from both coarse-graininess and poor flexibility, for which they cannot meet the requirements of secure data access in mobile edge computing [9].

This work was supported in part by the National Natural Science Foundation of China under Grant No. 61702103 and No. U1905211, and in part by the Fujian Provincial Natural Science Foundation of China under Grant (No. 2020J01167, No. 2020J01169).

To solve the data security problem during the data access process to enhance the confidentiality and integrity of data in MEC, a Blockchain based Multi-layer Access Control mechanism (BMAC) is proposed. The main contributions of this work include:

- To realize fine-grained data security protection, the security level based data classification scheme is proposed according to the sensitivity, importance, and change impact of the data.
- To accomplish the credibility based users grouping, the InfoMap algorithm is employed for grouping accuracy improvement.
- To achieve flexible and fine-grained data access control, a blockchain based multi-layer access control mechanism is developed.
- Experimental results show that the BMAC scheme has better performance in terms of processing efficiency, throughput, CPU utilization, and latency.

## II. Related Work

The majority of traditional access control strategies are centralized ones, which cannot meet the requirements of data security in distributed manner. To realize a flexible, efficient, and secure data access control, researchers combine blockchain technologies with existing access control mechanisms, and propose plenty of excellent strategies.

Maesa et al. [10] apply blockchain technology to an access control system for the first time. They deployed the access control strategy to the Bitcoin blockchain to realize the transfer of permissions between users. Ouaddah et al. [11] proposed a new anonymous and privacy-protected access control framework (FairAccess) to prevent user privacy from leaking and use the consistency of blockchain technology to manage access control. Ding et al. [12] combines traditional attribute-based access control with blockchain technology to prevent data from being tampered with and ensure data security in the

978-1-6654-1485-2/20/$31.00 ©2020 IEEE
DOI 10.1109/ISPA-BDCloud-SocialCom-SustainCom51426.2020.00061

IoT environment. Xu et al. [13] Xu proposed a blockchain-based distributed access control system (BlendCAC) to provide distributed, fine-grained, and lightweight access control management for IoT systems. Wang et al. [14] combines attribute-based encryption technology with decentralized storage and uses the distributed nature of the Ethereum blockchain to solve the problem of traditional cloud storage failures and achieve fine-grained access control to data. Literature [15] proposes a completely distributed dynamic access control based on blockchain, which uses machine learning algorithms to dynamically adjust and optimize access security policies to meet the security and privacy requirements in the IoT environment. Literature [16] proposes a secure access control system based on blockchain, which uses matching to achieve hierarchical access so that users in ICN can share secure data. Ma et al. [17] proposed a distributed key management mechanism based on blockchain, running multiple blockchains in the cloud to achieve cross-domain access, and introducing multiple permission distribution and group access modes to enhance scalability.

Although existing research results can provide a certain degree of security for resource data, these solutions lack flexibility and cannot meet the multiple security needs of users for resource data access in different service scenarios in mobile edge computing. Therefore, it is necessary to design a dynamic, accurate, and fine-grained security access control mechanism to enhance the security of user data under mobile edge computing.

## III. System Model

In this article, by applying blockchain technology to the access control mechanism under mobile edge computing, a hierarchical access control mechanism based on blockchain is proposed. The system model is shown in Figure 1, including three parts: edge area, edge gateway, and blockchain. In general, because of the characteristics of multiple edge regions in mobile edge computing, the blockchain is built into a distributed server, and the data resources and users of each region are stored on the blockchain in layers to realize the domain availability. Simple resource access between trust and domain. In this article, we use Fabric to build a multi-layer blockchain. The edge area includes user and resource data in the domain and is managed by the edge gateway.

1) Edge area layer: There are multiple edge areas distributed in the mobile edge computing architecture. Each edge area serves as a single trust domain, and there are corresponding user and resource data in the domain. For each edge area, we group and classify users and resource data in the domain, and combine blockchain technology to maintain a blockchain in each area. Users in the domain send access requests through the blockchain to obtain resources, which is convenient for users in the domain share data resources.
2) Edge gateway layer: First of all, as a bridge between users and the blockchain, it can group users and resource data in the domain into the blockchain after grouping or hierarchical processing for subsequent access by users. In this paper, we assume that all edge gateways are trusted. It mainly implements the following two functions: hierarchical processing of resource data in the domain and group users in the domain.
The edge gateway provides a data-sharing platform for users in the domain, where users in the domain can register on the platform according to their attributes so that they can subsequently access resource data in the domain. After the user is registered, the edge gateway mainly implements two functions. One is to sort and upload resource data to the corresponding level chain; the other is to group registered users and join the corresponding level chain.
For the access request of a user outside the domain, when the user registers, first determine whether the user's area is recognized by itself. If it is, then judge whether it meets the requirements of the data to be accessed according to the user's attributes. If it is, add the user outside the domain to the level chain where the corresponding resource is located, and set the effective access time.
3) Blockchain layer: For the resource data and users that have been classified and grouped, the edge gateway deploys the resource data and users to the corresponding level of the blockchain according to the level. At the same time, the access strategy is deployed on the blockchain in the form of smart contracts to perform relevant Access control. The blockchain mainly implements the following functions: hierarchical storage of resource data, hierarchical management of users, and user access management based on attributes.

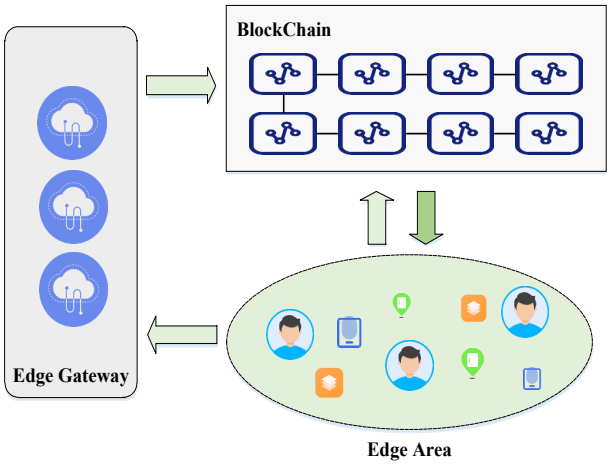


Fig. 1. System model.

## IV. Blockchain Based Multi-Layer Access Control Mechanism (BMAC)

By using blockchain technology, a layered access control mechanism based on blockchain is proposed. In this mecha-

nism, first, the edge gateway divides the resource data in the domain into different levels in terms of sensitivity, importance, and change impact according to the data classification strategy. Secondly, the edge gateway divides users in the domain into groups with different credibility according to the user grouping strategy based on the InfoMap algorithm. Third, based on the Fabric blockchain, a multi-level blockchain structure is designed, and combined with data classification and user grouping, different levels of resource data and different groups of users are put into different levels of blockchain. Finally, based on the above scheme, a fine-grained access control scheme based on user attributes is proposed, and the user's access request is further evaluated according to the user attributes to realize a dynamic and credible access control mechanism.

### A. Data classification strategy

According to the data's attributes, the data owner classifies the data in the same edge area from three indicators: sensitivity, importance, and change.

1) *Sensitivity*(*S*): Divided into non-sensitive data (*S1*), ordinary sensitive data (*S2*), confidential data (*S3*), and restrict access to the user's identity level based on sensitivity. For example, in a university environment, confidential data (*S3*) can only be accessed by professors and associate professors.
2) *Importance*(*I*): It is divided into unimportant (*I1*), generally important (*I2*), and very important (*I3*). Importance represents the impact of data leakage on the data owner. For example, generally important (*I2*) indicates that the data may contain data that cannot independently identify the data owner, while very important (*I3*) indicates that the data may contain data that can be precisely defined to the data owner. Once the data is leaked, the individual will be leaked. privacy.
3) *Change*(*C*): It is divided into no impact(*C1*), general (*C2*), and important (*C3*). The impact of change determines the impact of unexpected changes to the data owner. For example, if a malicious user updates or deletes a certain piece of data, this will cause confusion to the data owner and other users. The more important the data, the more important it is to prevent malicious users from changing the data.

According to the above three indicators, we divide the data level ($DL$) from low to high into level 0, level 1, and level 2.

### B. User grouping strategy based on InfoMap algorithm

The idea of InfoMap is, from the perspective of information theory, by constructing node occurrence probability and group jump probability, a random walk on the graph is performed to generate the sequence, and then the sequence is coded hierarchically to minimize the length of the code to complete the aggregation class. Assuming that there are any two nodes $t_i$,$t_j$ in an undirected weight graph G, the weight of the edge between the two nodes is expressed as $w_{t_i \to t_j}$ (the weight in this article represents the similarity of the access data

**Algorithm 1** Data classification algorithm

**Input:** Data $data\_1$ = $\{S, I, C\}$
**Output:** Data level $DL$

```
if (S = S3&&I = I3)||(S = S3&&C = C3)||(I = I3&&C = C3) then
    DL=2;
else if S = S1&&I = I1)||(S = S1&&C = C1)||(I = I1&&C = C1) then
    DL=0;
elseDL=1;
end if
```

preference between users), but $T_{i\to}$ is connected to node $t_i$ the set of all nodes, then the transition probability of node $t_i$ arrival $t_j$ is $p_{t_i \to t_j} = \frac{w_{t_i \to t_j}}{\sum\limits_{t \in T_{i\to}} w_{t_j \to t}}$ and the occurrence probability of node $t_i$ is $p_{t_i} = \sum\limits_{t \in T_{i\to}} p_t p_{t \to t_i}$. If the graph G is divided into Z groups, the group jump probability is $q_{F(n)} = \sum\limits_{t_i \in F(n), t_j \notin F(n)} p_{t_i} p_{t_i \to t_j}$.Combined with the information entropy theory, the average bit $L(Z)$ can be calculated as follows:

$$L(Z) = q_{F\searrow} H(Q) + \sum_{n=1}^{r} p_{F(n)\rightleftarrows} H(p_{F(n)}) \tag{1}$$

Among them, $q_{F\searrow} = \sum\limits_{n=1}^{r} q_{F(n)}$ represents the total probability of entering the group, and $H(Q)$ represents the shortest average code length of entering the group, which can be calculated as follows:

$$H(Q) = -\sum_{n=1}^{r} (q_{F(n)} / q_{F\searrow}) \log(q_{F(n)} / q_{F\searrow}) \tag{2}$$

$p_{F(n)\rightleftarrows} = q_{F(n)\searrow} + \sum\limits_{t \in F(n)} p_t$ represents the probability of a random worker in group $F(n)$ and $H(p_{F(n)})$ represents the shortest average code length of the node in the corresponding group $F(n)$, Both can be calculated as follows:

$$\begin{aligned} H(p_{F(n)}) = &-\left(q_{F(n)} \Big/ p_{F(n)\rightleftarrows}\right) \log\left(q_{F(n)} \Big/ p_{F(n)\rightleftarrows}\right) \\ &- \sum_{t \in F(n)} \left(p_t \Big/ p_{F(n)\rightleftarrows}\right) \log\left(p_t \Big/ p_{F(n)\rightleftarrows}\right) \end{aligned} \tag{3}$$

*Model definition*: We construct a network topology map based on the similarity of access data preferences between users and group users under the constraints of using credit. The user's access data preference attribute set includes the level of access data, access frequency, etc. the access preference similarity $APS(a,b)$ between user a and user b can be calculated as follows:

$$APS(a,b) = \frac{1}{m} * \sum_{i=1}^{m} \frac{\left|AF_a^i \cap AF_b^i\right|}{|AF^i|} \tag{4}$$

Among them, $AF_a^i$ and $AF_b^i$ are the attributes sets corresponding to user a and user b when the data level is i, and $AF_b^i$ is the attribute union set between user a and user b when the data level is i. m is the total number of categories of the data level.

Map users into nodes and all users form a node-set $v$. If the similarity of access preferences between two nodes is greater than the set threshold, an edge is established between the corresponding nodes, and all edges constitute an edge set. All nodes and edges constitute an unauthorized network topology graph. The similarity of nodes is represented by the different weights of edges in the network topology. The lower the similarity, the smaller the edge weight.

In a weighted network topology graph constructed according to the similarity of user access preferences, nodes represent users, and the weight on each edge is expressed as the similarity of access preferences between two users. To improve the credibility of user groups, we consider user credit as a constraint condition and further adjust the division of user groups. When user node a is assigned to the group $F(n)$.

1) When there is currently only one user node b in the group, the constraint conditions are defined as follows:

$$|R_a^{sum} - R_b^{sum}| \geq \lambda_1 \tag{5}$$

where $R_a^{sum}$ and $R_b^{sum}$ are the credit values of user a and user b, respectively, and $\lambda$ is the threshold value of the credit difference between the two user nodes.

2) There are currently multiple user nodes in the group $F(n)$, then the constraint conditions are defined as follows:

$$\lambda_2 = \frac{1}{k}\sum_{j}^{k} R_j^{sum} \tag{6}$$

where $R_j^{sum}$ is the credit value of the jth user node in group $F(n)$ and $k$ is the total number of user nodes in group $F(n)$.

*Implementation process*: Next, the user grouping process based on the InfoMap algorithm is introduced. The algorithm can automatically determine the number of user groups by analyzing the weighted network topology. The steps are as follows:

1) Initialize user nodes and treat each user node as an independent group;
2) Randomly sample a sequence of user nodes in the graph;
3) Try to assign each user node to the group of the neighboring user node in order, calculate the average bit value $L(Z)$, and assign the group with the largest decrease in $L(Z)$ value to the user node; if the value of $L(Z)$ is greater than the current value, then the group of the user node remains unchanged;
4) Determine whether the credit constraints of the group are met, if the constraints are met, update the grouping of the group, otherwise keep the original grouping unchanged;
5) Repeat steps 2, 3, and 4 until the value of $L(Z)$ no longer decreases and the grouping result no longer changes.

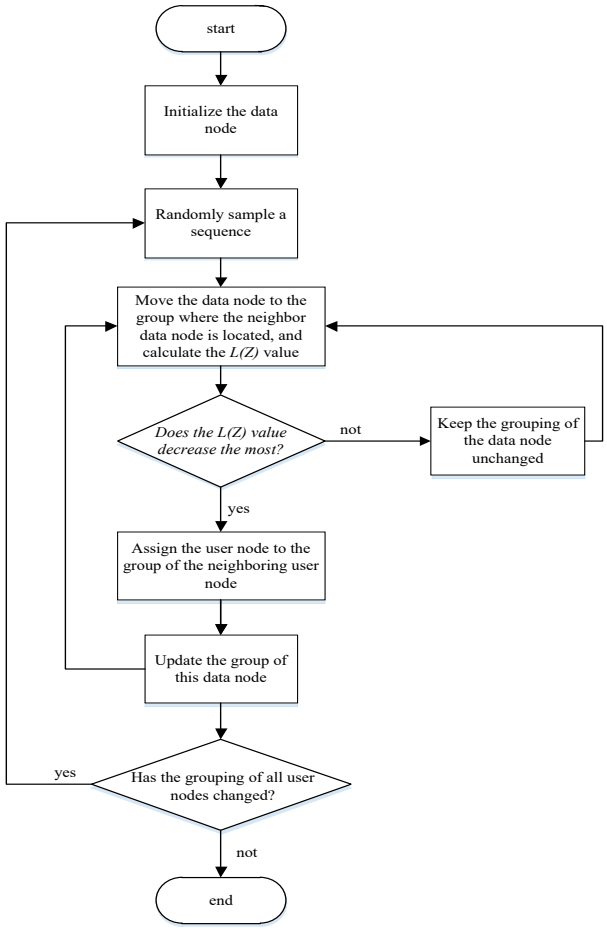


Fig. 2. Implementation process of user grouping.

The implementation process of this process is shown in Figure 2.

### C. Multi-layer blockchain structure based on Fabric

*1) Multi-layer blockchain:* For the resource data of users in the same area, according to the results of the data classification strategy and the user grouping strategy, we use the multi-channel feature of Fabric to design different levels of channels as the corresponding ”0”, ”1”, and ”2” Level chain and store the user group and resource data of the corresponding level in the blockchain for subsequent resource access.

The first is data classification. To ensure data security and effectively isolate different levels of data, the edge gateway will only store different levels of data in the domain in the chain of the corresponding level, and users in the chain can access resources.

Then there are the users. Figure 3 is a user architecture based on a multi-layer blockchain. The edge gateway divides the multi-organization users in the domain into user groups with three security levels: L0, L1, and L2 according to the user grouping strategy. Each security level has multiple user groups. Then add users to the corresponding level chain according

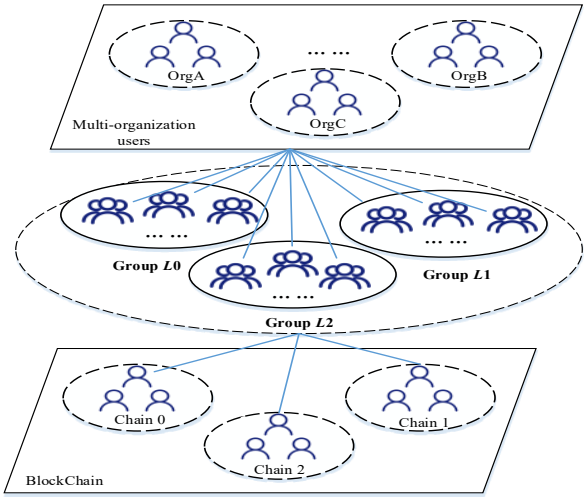


Fig. 3. User architecture based on multi-layer blockchain.

to the user group security level. Among them, a user with a higher user group level can join a chain less than or equal to the group level. For example, if the user group level is "L1", the user will be added to the level chain of "0" and "1". This can effectively distinguish user groups of different security levels, limit the level of data they can access, and achieve the purpose of ensuring data security.

*2) Access strategy:* Access Policy (AP) provides services for user access on the blockchain in the form of smart contracts. Combined with the ABAB model, the access strategy is defined as follows: $AP = \{UA, DA, O_p, TA\}$, $UA = \{ID_u, U_{org}, U^i_{SG(k)}\}$ represents the user's basic attribute set, $ID_u$ is the user identifier, $U_{org}$ represents the organization to which user u belongs, and $U^i_{SG(k)}$ represents user u in the subgroup $SG(k)$ with security level i, $DA = \{ID_d, D_{org}, D_{dl}\}$ represents Is the data attribute set, $ID_d$ is the data identification, $D_{org}$ represents the organization to which the data belongs, $D_{dl}$ represents the level corresponding to the data; $O_p$ is the result of the access request permission, the value "1" indicates that access is allowed, the value "0" Reject the user's access request; $TA$ represents the effective access time, and the $TA$ value determines the effective time for the user to access the resource data. Once the effective access time is exceeded, the user needs to send a resource access request again.

*3) Implementation process:* The whole implementation process mainly includes two parts. Each part is described in detail as follows:

(1) Access strategy formulation

The edge gateway of each edge area develops an access strategy for the resource data in the area and then uploads it to the blockchain. First, the edge gateway formulates access policies based on the data resources and user attributes in the area, and defines them from four aspects: $UA$,$DA$,$O_p$and$TA$; then, the edge gateway uploads the relevant access policies to different levels of blockchain.

(2) Access control enforcement

The implementation process of access control is shown in Figure 5. When a user in the chain wants to access certain resource data on the chain, the user will initiate an attribute-based resource access request. After receiving the access request of the user on the chain, the smart contract for access verification is called. According to user attributes and resource data attributes, evaluate the resource access requests of users on the chain according to the access policy (AP), and verify whether the user attributes to match the access policy. If the user's attributes match the access policy (AP) and the value of $O_p$ is 1, the verification is passed and the user's resource access request is allowed; otherwise, a negative result is returned to the user.

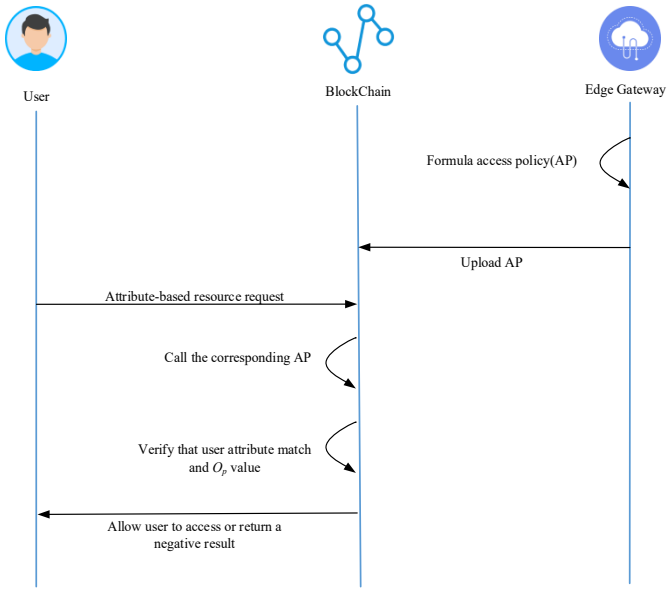


Fig. 4. Implementation process of access control.

## V. Simulation Verification and Analysis

We use the virtual machine VMware Workstation Pro 15 to install the Ubuntu system and build the Hyperledger Fabric 1.4.3 platform in this system. Table 1 shows the relevant parameter configuration of the experiment.

TABLE I
Experiment Related Configuration

| | |
|---|---|
| OS | Ubuntu 16.04 |
| node | v12.13.0 |
| golang | v1.15.1 |
| docker | v19.03.12 |
| docker-compose | v1.26.2 |

In BMAC, we designed a triple-chain structure based on the Hyperledger Fabric blockchain and evaluated the performance of single-chain and multi-chain structures in terms of throughput, CPU utilization, and latency. The experimental results are

shown in Figure 5-7. From the experimental results, it can be found that the multi-chain structure is better than the single-chain structure in terms of throughput, CPU utilization, and latency. For example, in terms of throughput, the multi-chain structure is nearly twice that of the single-chain structure. In terms of utilization, the multi-chain structure is also about 4% higher than the single-chain structure.

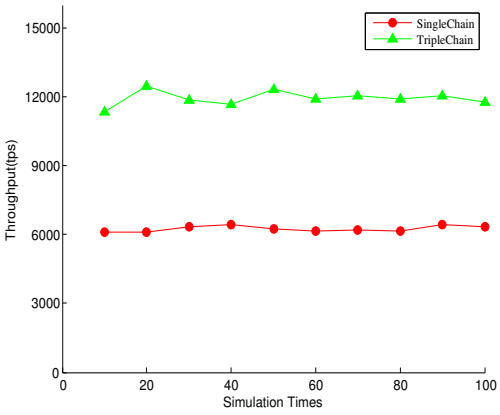


Fig. 5. Throughput.

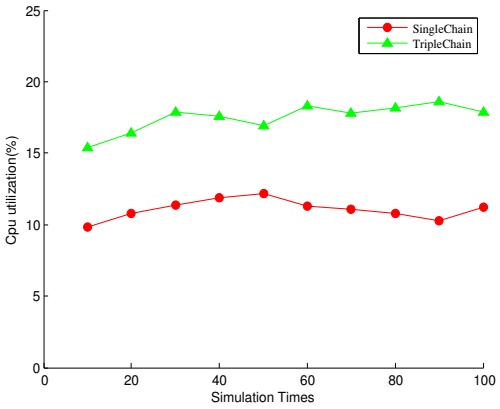


Fig. 6. CPU utilization.

The reasons for the above results are as follows. The multi-chain structure can be regarded as a distributed access control system. Different levels of resource data and users are put into the corresponding level of the blockchain. That is, at the same time, every time all chains can perform data access operations without interfering with each other, thereby improving the throughput and CPU utilization of the blockchain system. Besides, we also compared the time it takes to process different numbers of access requests at the same time. The experimental results are shown in Figure 8. As the number of access requests continues to increase at the same time, the average processing time decreases and stabilizes. , That is, the multi-chain structure can handle different numbers of access requests well.

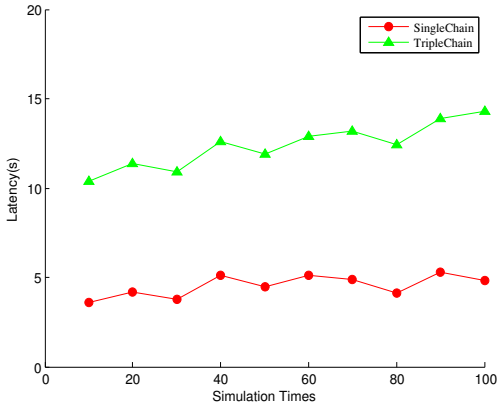


Fig. 7. Latency.

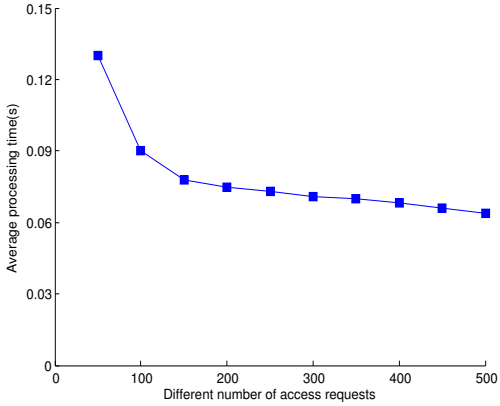


Fig. 8. Average processing time under different numbers of access requests.

## VI. CONCLUSION

To ameliorate the security threats of the data access process for mobile edge computing and solve the shortcomings of the existing access control strategies such as poor flexibility and coarse granularity, we propose a blockchain-based multi-layer access control mechanism (BMAC) in this paper. Specifically, each resource data is assigned a security level. Then, an InfoMap based algorithm is developed to achieve credibility based users grouping. Next, a multi-blockchain is designed, based on which a flexible and fine- grained trusted data access control mechanism is established. The experiment results show that the BMAC scheme has better performance in terms of processing efficiency, throughput, CPU utilization, and latency.

## REFERENCES

[1] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," *Future generation computer systems*, vol. 29, no. 1, pp. 84–106, 2013.

[2] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18 209–18 237, 2018.

[3] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450–465, 2017.

[4] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.
[5] X. Li, S. Liu, F. Wu, S. Kumari, and J. J. Rodrigues, "Privacy preserving data aggregation scheme for mobile edge computing assisted iot applications," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4755–4763, 2018.
[6] J. Wang, J. Hu, G. Min, W. Zhan, Q. Ni, and N. Georgalas, "Computation offloading in multi-access edge computing using a deep sequential model based on reinforcement learning," *IEEE Communications Magazine*, vol. 57, no. 5, pp. 64–69, 2019.
[7] J. Wang, J. Hu, G. Min, A. Y. Zomaya, and N. Georgalas, "Fast adaptive task offloading in edge computing based on meta reinforcement learning," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 1, pp. 242–253, 2020.
[8] S. Weisong, S. Hui, C. Jie, Z. Quan, and L. Wei, "Edge computing an emerging computing model for the internet of everything era," *Journal of Computer Research and Development*, vol. 54, no. 5, p. 907, 2017.
[9] J. Zhang, Y. Zhao, B. Chen, H. Feng, and K. Zhu, "Survey on data security and privacy-preserving for the research of edge computing," *Journal on Communications*, vol. 39, no. 3, pp. 1–21, 2018.
[10] D. D. F. Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in *IFIP international conference on distributed applications and interoperable systems*. Springer, 2017, pp. 206–220.
[11] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "Fairaccess: a new blockchain-based access control framework for the internet of things," *Security and Communication Networks*, vol. 9, no. 18, pp. 5943–5964, 2016.
[12] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for iot," *IEEE Access*, vol. 7, pp. 38 431–38 441, 2019.
[13] R. Xu, Y. Chen, E. Blasch, and G. Chen, "Blendcac: A blockchain-enabled decentralized capability-based access control for iots," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018, pp. 1027–1034.
[14] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *Ieee Access*, vol. 6, pp. 38 437–38 450, 2018.
[15] A. Outchakoucht, E. Hamza, and J. P. Leroy, "Dynamic access control policy based on blockchain and machine learning for the internet of things," *Int. J. Adv. Comput. Sci. Appl*, vol. 8, no. 7, pp. 417–424, 2017.
[16] Q. Lyu, Y. Qi, X. Zhang, H. Liu, Q. Wang, and N. Zheng, "Sbac: A secure blockchain-based access control framework for information-centric networking," *Journal of Network and Computer Applications*, vol. 149, p. 102444, 2020.
[17] M. Ma, G. Shi, and F. Li, "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the iot scenario," *IEEE Access*, vol. 7, pp. 34 045–34 059, 2019.