Hindawi
Computational Intelligence and Neuroscience
Volume 2022, Article ID 4410075, 8 pages
https://doi.org/10.1155/2022/4410075

Research Article

Multimedia Automation Access Control of Big Data Open Resources Based on Blockchain

Nan Zhao,[1] **Hui Su**,[2] **QingSheng Han**,[1] **and Yan Zhao**[1]

[1] *Beijing Institute of Economics and Management, Beijing 100102, China*
[2] *Unit 78111 of PLA, Chengdu 610011, China*

Correspondence should be addressed to Nan Zhao; 2016214241@smail.jsut.edu.cn

Received 12 February 2022; Revised 31 March 2022; Accepted 15 April 2022; Published 23 May 2022

Academic Editor: Huihua Chen

In order to better mine the value of data, the author proposes a research on the automatic access control of big data open resources multimedia based on blockchain and introduces big data access control BBAC-BD (blockchain-based access control mechanism for big data environment). The author designed a strategy management contract based on the Bloom filter, as a probabilistic data structure with extremely high space utilization efficiency and proposed the strategic management contract (PAP CONTRACT) and the strategic decision contract (PDP CONTRACT). In this way, the nontampering, auditability, and verifiability of the access control information are guaranteed; then, the access control method based on smart contracts is adopted to realize the user-driven, whole-process transparent, and dynamic and automatic access control of big data resources. The simulation results show that the greater the ratio of n/k, the better the optimization effect, and the greater the ratio, the lower the corresponding misjudgment rate, but it will also take up more space costs. At the same time, the true value of the false positive rate is generally less than the theoretical value of the false positive rate. When the performance of Hash (strategy to retrieve) is better, the result of Hash distribution is more uniform. Under the condition of $m = 3$, the misjudgment rate acceptable for the expected use can be achieved, and the increase in the number of Hashes will not bring a significant increase in revenue. Freed from the traditional model of providing access control services based on third parties, solve the problem of transparency of authority judgments; at the same time, through smart contracts, based on the strategy published by the resource owner on the blockchain, realize automatic access control to big data resources; and make the judicial process more flexible and the judgment result more credible. The BBAC-BD mechanism realizes a safe, reliable, and transparent new access control architecture, and it can effectively promote the safe circulation and sharing of big data.

1. Introduction

Human society is accompanied by social networks, e-commerce, and mobile communications, and the rise of the Internet of Things, which has entered the era of big data with data volume, big data analysis, and prediction based on distributed computing. This can make decisions more precise of what people are seeing is just the tip of the iceberg of the true value of big data [1]. Smartphones and wearable devices make every change of our behavior, position, and even physiological information become data that can be recorded and analyzed, but these big data are stored and controlled by various government agencies, business alliances, scientific research institutions, and even individuals, and the phenomenon of "data islands" is formed [2]. Interconnect and sharing of these scattered big data, in order to obtain products and services of great value, is an urgent need coexisting in business, scientific research, public services, and other fields [3]. In order to realize big data sharing, it is first necessary to connect separate and decentralized data sources [4]. However, due to the lack of detailed and transparent institutional standards, open policies, and pricing mechanisms between enterprises, scientific research institutions, and government departments, it is difficult to achieve fairness and equality between sharing parties [5]. Data diversification, storage structure, and interaction standards are not uniform, and the lack of a transparent communication environment is also hindering data interaction; the technical architecture of big data access control is shown in Figure 1 [6]. These problems together

r cause data connection difficulties. Therefore, a transparent and open data connection method is urgently needed to record data information, access conditions, standards, and other related information to achieve interconnection. Fundamentally speaking, the issue of "data islands" is mainly related to interest and security issues. The data are kept by a large data platform or other intermediary organization. Once the data are uploaded, the owner loses the right to control the data. Regardless of whether it is a government agency or an Internet company, it is very sensitive to data, and once it is leaked, it will have a great social impact.

2. Literature Review

In response to this research question, the author of [7]aimed at third-party collection and control of personal data security vulnerabilities, leading to the problem of user privacy leakage; a distributed personal data management system based on blockchain is proposed to ensure users own and control their private data. For all blockchain transactions, Ansart et al. are transparently embodied in the public network that leads to the leakage of transaction privacy, and they proposed the use of the Hawk protocol based on smart contracts; the agreement encrypts the communication between the parties to the contract to ensure the absolute security of information [8]. Liu et al. addressed the issue of data security and privacy in the Internet of Things, proposed a lightweight blockchain application suitable for IoT devices, and in the smart home scene, they practiced and verified its security, confidentiality, integrity, and availability [9]. Yin et al. adopted an encrypted smart contract, protected public privacy files through public and private keys, and provided auditing and tracking [10]. In terms of data storage and authenticity verification, Xu, J. et al. made an in-depth discussion on the future impact of the audit industry based on big data analysis and blockchain technology, and studied how to incorporate blockchain into future audit procedures based on the existing theoretical framework [11]. Yu et al. proposed using blockchain to build a secure global named storage system, including the three-tier architecture of the blockchain-based naming system. The naming system is divided into three layers: data layer, routing layer, and blockchain layer [12]. Zhang et al. proposed a method for ensuring the authenticity of microbial sampling robot data based on the bitcoin blockchain, which makes the robot not be interfered by human factors in the process of collecting data, especially the malicious tampering behavior of third-party regulatory agencies [13]. Fan et al. aimed at the three types of credibility problems existing in the current Internet of Things data sharing management and proposed blockchain-based solutions, including a decentralized Internet of Things data sharing architecture and smart contract collection [14]. Ling et al. built an access control architecture for the Internet of Things to provide a more flexible management plan [15]. Bera et al. proposed a resource access control method based on blockchain technology and combined XACML with bitcoin to realize the reliable authority control mechanism based on rules [16]. On the basis of the current research, the author proposes a research on the automatic access control of big data open resources multimedia based on blockchain, using the big data access control BBAC-BD mechanism based on blockchain; it also elaborated and analyzed the basic framework and process of access control in detail. At the same time, for access control strategies based on blockchain transactions and entity attribute information management methods, with the increase of policy rules, the success rate of strategic judgments has decreased, and the BBAC-BD mechanism has realized a safe, reliable, and transparent new access control architecture, and it can effectively promote the safe circulation and sharing of big data.

3. Methods

3.1. Big Data Access Control Architecture. Big data access control involves the collection, aggregation, management, and control of big data resources. The big data access control architecture is mainly composed of 6 parts: data layer, resource aggregation layer, infrastructure layer, transaction layer, consensus layer, and access control contract layer. Each layer structure cooperates with each other and performs its own duties to form a complete big data access control architecture [17].

(1) Data layer: real big data resources, including structured data, unstructured data, and semistructured data distributedly stored in different locations and logically managed by the resource aggregation layer [18];

(2) Resource convergence layer: resource management of big data resources based on blockchain technology to realize the convergence of big data resources from different sources. Although real big data resources are in fact distributed and stored by different data owners, but through blockchain technology, it logically forms a unified management of big data resources. The author's research focuses on the access control mechanism, and the resource aggregation layer will not elaborate [19].

(3) Infrastructure layer: the blockchain platform provides infrastructure for big data access control. It is the foundation of the whole architecture, and the nodes and minors of the entire network are required to maintain the normal operation of the system. It is the carrier of big data access control platform transactions and smart contracts. The transaction layer, contract layer, and resource aggregation layer are all upper-layer applications based on blockchain.

(4) Transaction layer: it includes 4 types of access control transactions: data transaction, strategy transactions, attribute transactions, and contract transactions. Data transactions are used to manage big data resources, which serve at the resource convergence layer. Policy transactions are used to manage access control policies, including the release, update, and sale of strategies to provide data support for PAP

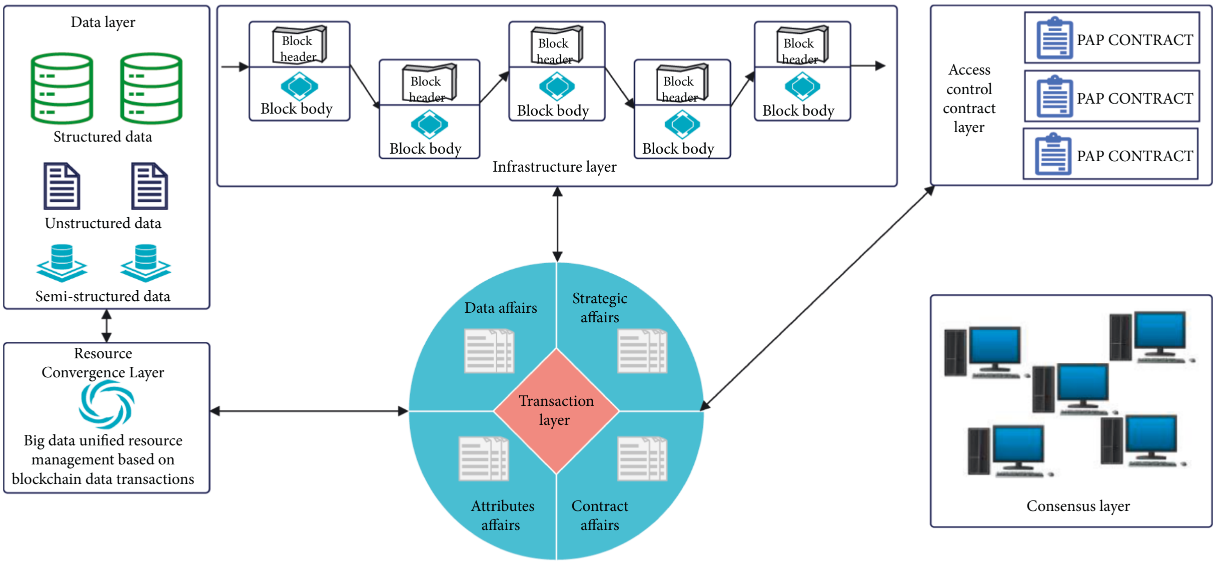

Figure 1: Data access control technology architecture.

CONTRACT at the contract layer. Attribute transactions are used to manage the attributes of entities, including the release, update, and sale of properties to provide data support for the contract layer AA CONTRACT, and contract transactions are used to provide an operating environment for smart contracts, which serve at the contract layer [20];

(5) Consensus layer: it mainly includes consensus mechanism, through various consensus algorithms, in order to ensure the consistency and authenticity of access control data among distributed nodes, so as to reach a stable consensus among nodes [21];

(6) Access control contract layer: it includes three types of contracts: PAP CONTRACT, PDP CONTRACT, and AA CONTRACT; PAP CONTRACT is used for access control strategy management, PDP CONTRACT is used for access control request judgment, and AA CONTRACT is used for entity attribute management.

In order to obtain the initial judgment matrix $EQ = (eqij)_{m\times m}$, there are m matrices $E = (e1, e2, \ldots, em)$, and the matrix is concentrated in the importance of ei and ej for binary comparison, which is shown in the following formula:

$$eqij = \begin{cases} 0, & ei < ej, \\ 0.5, & ei = ej, \\ 1, & ei > ej. \end{cases} \tag{1}$$

Convert the initial judgment matrix into a fuzzy consistent matrix, which is shown in the following formula:

$$\begin{cases} qij = \dfrac{qi - qj}{2m} + 0.5, \\ \\ qi = \displaystyle\sum_{k}^{m} = 1eq_{ik}. \end{cases} \tag{2}$$

Calculate the weight vector $W = (w_1, w_2, \ldots, w_m)^T$ of each evidence of a certain m characteristic, which is shown in the following formula:

$$w_i = \frac{\sum_k^m = 1qik - 0.5}{m(m-1)/2}. \tag{3}$$

Next, the evaluation value matrix of the user behavior characteristic is calculated, and the value on the diagonal of the matrix obtained from the evidence matrix $E = (eij)_{m\times n}$ and the weight matrix $W = (w_{ij})m \times n$ according to $E \times W^T$ is the characteristic evaluation value matrix $F = (f1, f2, \ldots fn)$. The behavioral credit of the final user is shown in the following formula:

$$\text{current\_}T(u) = 1 - F \times W_f^T = 1 - \sum_{i=1}^{n} fiwi. \tag{4}$$

current_$T(u)$ represents the user's current credit rating, and $W_f = (W_{f1}, W_{f2}, \ldots, W_{fn})$ represents the weight of the user's behavioral characteristics. When the user logs in for the first time to perform access control, the system will generate the first historical credit according to the user's software and hardware operations: History_$T_1(u)$ = Current_$T_1(u)$. As the number of visits increases gradually, the user's historical credit needs to be gradually changed according to the passage of time as shown in the following formula:

$$\text{History\_}T(u) = \begin{cases} 0, & n = 0, \\ \displaystyle\sum_{i=1}^{n} (Final\_Ti(u) \times ti), & n > 0, \\ \displaystyle\sum_{i=1}^{n} ti. & \end{cases} \tag{5}$$

Final_$T_i(u)$ corresponds to the user's final credit at the end of each visit and t_i records the access time. This parameter calculates the total time from the user's login to the end of the user's exit from the system. When $n = 0$, it means that the user has logged into the system for the first time and has no corresponding historical credit value. When a user visits for the first time, there is no historical credit, and the recommended credit will have a certain reference value. The user's recommended credit is calculated based on the credit between the user and other service organizations. Assuming that there are n credible access organizations $s = (s_1, s_2, \ldots, s_n)$, T and N representing the historical credit value and the number of successful visits of users of service organizations s_i and u_i, respectively, then the expression of the recommended credit is shown in the following formula:

$$\text{Recommend\_}T(u) = \begin{cases} 0, & n = 0, \\ \dfrac{\sum_{j=1}^{n} \left(Nj \times T_{ui}^{si}\right)}{\sum_{j=1}^{n} Nj}, & n > 0. \end{cases} \tag{6}$$

There is a competitive relationship between the chain generated by the honest node and the chain generated by the attacker. When the honest node is ahead, the chain of the honest node is extended by one block; otherwise, the chain of the attacker is extended by one block. The attacker successfully fills the gap behind z blocks, which is similar to the gambler bankruptcy problem, and then the attacker fills the gap and catches up with the honest chain. The probability is shown in the following formula:

$$q_z = \begin{cases} 1, & p \leq q, \\ \left(\dfrac{q}{p}\right)^{z}, & p > q, \end{cases} \tag{7}$$

where p represents the probability of an honest node gaining ownership of the next node, q represents the probability of an attacker gaining ownership of the next node, and qz represents the attacker filling the gap z blocks behind. When $p > q$, the probability of the attacker successfully attacking the next block decreases with the increase of z. Assuming that honest blocks take the average expected time to generate a block, the potential progress of the attacker is calculated according to the Poisson distribution, and the expected value is shown in the following formula:

$$\lambda = z\frac{q}{p}. \tag{8}$$

In order to calculate the probability that the attacker will generate nodes and catch up with the honest nodes in the chain when the attacker is behind, the probability is pz. We compare the Poisson distribution of blocks obtained by the attacker with the potential attack speed and the probability that the attacker can catch up with the honest nodes. The probabilities are multiplied to obtain the following formula:

$$p_z = \sum_{k=0}^{\infty} \frac{\lambda^k e - \lambda}{k} \cdot \begin{cases} \left(\dfrac{q}{p}\right)^{(z-k)}, & k \leq z, \\ 1, & k > z. \end{cases} \tag{9}$$

After simplification, the formula is

$$\begin{aligned} p_z &= 1 - \sum_{k=0}^{z} \frac{\lambda k_e - \lambda}{k} \cdot \left(1 - \left(\frac{q}{p}\right)^{(z-k)}\right) \\ &= 1 - \sum_{k=0}^{z} \frac{(zq/p)^k e - zq/p}{k} \cdot \left(1 - \left(\frac{q}{p}\right)^{(z-k)}\right). \end{aligned} \tag{10}$$

3.2. BBAC-BD Workflow. In the BBAC-BD (blockchain-based access control mechanism for big data environment) proposed by the author, the access control workflow is an extension of the standard ABAC model workflow. The access control workflow can be divided into two phases: the preparation phase and the execution phase. The preparation phase is mainly for the management of access control strategies and attributes, including the release, update, and withdrawal of policies and attributes and the response to the results of the policy and attribute query, and the execution phase is mainly for the judgment, response, and execution of the access request [22].

(1) Preparation stage: from the property release direction to the blockchain, release property, and property relationship information, AA (attribute authority) CONTRACT collects and integrates attribute information in blockchain transactions in advance, for PEP (policy enforcement point) CLIENT and PAP (point administration point) CONTRACT, from the policy release direction, the access control policy is released in the blockchain. PAP CONTRACT combines attribute information to describe, collect, and integrate access control strategies in blockchain transactions, for PDP (policy decision point) CONTRACT to make an access request decision.

(2) Execution stage: when PEPCLIENT receives a request from a user to perform a certain operation on a certain resource, PEPCLIENT analyzes the subject, object, and operational semantics of the original access request, generates an attribute-based access request AAR based on the attribute information obtained from AACONTRACT, sends AAR to PDP CONTRACT, PDP CONTRACT queries PAP CONTRACT for the access control policy set related to the requested big data resource, makes an access control decision, and sends the judgment result response back to PEP CLIENT. According to the response result by PEP CLIENT, authorize access to big data resources, since the access control policy is stored in the blockchain, policy information is verifiable, traceable, and nontamperable to anyone. The access control of big data resources gets rid of the traditional centralized access control management, possible single points of failure, and transparency of access control decisions. It realizes the distributed management of the access control strategy and effectively improves the robustness and credibility of the system. In addition, the decision process of the

access control strategy is realized through the form of smart contract, with no need for the involvement of a third-party central agency, and avoids the possible ultravires behavior of the third-party center, based on the blockchain system to realize the automatic judgment of access control under consensus. It is a truly decentralized access control mechanism, which meets the access control management requirements of big data resources [23].

3.3. Transaction Storage in the Blockchain. In the blockchain, data are stored in the blockchain in the form of transactions, we use the form of transactions in the blockchain to manage access control policies, the transaction data in the block are stored in the data structure of the Merkle tree based on the HashHash algorithm, and the transaction data of inconsistent size are mapped into a fixed-size character string through a HashHash algorithm, stored on the leaf nodes of the Merkle tree. The nonleaf nodes of the Merkle tree store the HashHash values of its child nodes. The blockchain includes physical accounts, data blocks, transaction set data, and configuration data. The data view relationship between them is shown in Figure 2.

(1) Physical account: it is the initiator of various transaction requests and the owner of related data in the blockchain. It is the actual owner of the data resources in the access control mechanism and has a pair of public and private keys generated by the PKI system. In the system, the account is uniquely identified by the public key, and the transaction data published by the resource owner need to be signed by the entity account with a private key for other users to verify the authenticity of transactions in the block [24];

(2) Data block: it is the underlying data in the blockchain network, and multiple blocks together form a chain structure, persist the transaction processing results within a certain period of time in an immutable form.

(3) Transaction set data: it is based on the access control mechanism of the blockchain and stores data for performing actual business activities, including access control transactions and smart contract transactions. Access control transactions are used for the management of access control policies; it mainly covers the release, update, and cancellation of policy information in policy management. Smart contract transactions are used in the decision process of access control, in response to access requests and generating access control responses. Issuing transactions on the blockchain requires tokens that consume a certain amount of data, as the user's expenses for using blockchain services.

(4) Configuration data: it is the configuration information required for the normal operation of the blockchain system, including configuration information such as protocol version number and communication node information.

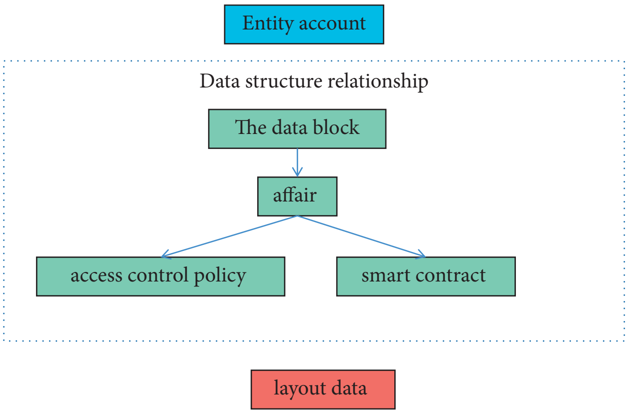

Figure 2: The relationship between data view entities in the block.

3.4. Smart Contract for BBAC-BD. (1) Strategic management contract (PAP CONTRACT).

The flow of the PAP CONTRACT is shown in Algorithm 1.

PAP CONTRACT algorithm flow description.

Analyze the AAR to obtain the requested resource attribute information rttrTuple; traverse the strategic transaction data blocks in each block of the blockchain; obtain the attribute Bloom filter (BF) corresponding to the strategy transaction data block. According to the Hash function corresponding to the BF, calculate the Hash value corresponding to rttrTuple. If the Hash value obtained by calculating rAttrTuple and the corresponding bit in BF are all 1, then add the strategy in the data block in RELEVANT_POLICY_SET; otherwise, there is no rttrTuple related strategy in the data block. When the traversal of strategy transactions in all blocks is completed, return resource-related policy set RELEVANT_POLICY_SET to PDP for permission judgment.

(2) The strategy decision process is carried out by the strategy decision contract (PDP CONTRACT), and the contract flow is shown in Algorithm 2.

PDP CONTRACT algorithm flow description.

Put all pending decisions into UNKNOWN_SET, as a predecision strategy set; traverse the predecision strategy; and get 4 strategy decision result sets:

PERMINT_RESULT_SET DENY_RESULT_SET UNSA TISFY_RESULT_SET UNKNOWN_RESULT_SET. Accor ding to the judgment result set, the final judgment result of the AAR request is obtained: if there is a conflicting judgment result, the final judgment result is obtained after the conflict is processed, and conflict handling can be based on the principle of affirmative priority or negative priority for conflict resolution.

4. Results and Analysis

4.1. Strategy Retrieval Efficiency Test. This experiment is aimed at the management method based on the Bloom filter strategy and performed testing on the optimization effect of strategy retrieval efficiency. In the experiment, matching query tests were performed on test sets of different query

(i) Input: attribute access request AAR and blockchain blocks
(ii) Output: resource-related policy set RELEVANT_POLICY_SET

Algorithm 1: Strategy management contract (PAP CONTRACT).

(i) Input: attribute access request AAR, access control policy set POLICY_SET;
(ii) Output: strategy decision result PERMIT, DENY, UNKNOWN, and UNSATISFY.

Algorithm 2: PDP CONTRACT.

Table 1: Strategy retrieval test results 1.

Serial number	n/k	m test value	M optimal value	Query size	True false positive rate	Theoretical misjudgment rate	Total delay	Single time delay
1	20	3	14	4000	0.1975	0.2721	432	0.118
2	20	3	14	8000	0.1869	0.2721	798	0.079
3	20	6	14	4000	0.0321	0.0331	762	0.198
4	20	6	14	8000	0.0298	0.0331	1484	0.187
5	20	14	14	4000	0.0074	0.0076	985	0.257
6	20	14	14	8000	0.0095	0.0076	2062	0.255
7	20	20	14	4000	0.0029	0.0141	1247	0.332

Table 2: Strategy retrieval test results 2.

Serial number	n/k	m test value	M optimal value	Query size	True false positive rate	Theoretical misjudgment rate	Total delay	Single time delay
8	20	20	14	8000	0.0098	0.0141	2 462	0.328
9	10	3	7	4000	0.9356	1.7451	484	0.124
10	10	7	7	4000	0.792	0.891	I 134	0.285
11	5	3	3	4000	9.12	9.21	837	0.229
12	2	1	1	4000	39.51	39.29	762	0.192
13	2	2	1	4000	39.76	40.12	812	0.203

scales, set different parameters for the Bloom filter to test the error rate and retrieval delay, which were used to evaluate the impact of different parameters of the Bloom filter on retrieval performance. The calculation method of single time delay is total time delay/total number of matches. The optimization effect is mainly through the strategic management contract. The retrieval delay of the strategy is measured. The smaller the delay, the higher the execution efficiency, and the better the search optimization effect. From the test results of Tables 1 and 2, we can see that the larger the ratio of n/k, the better the optimization effect, and the larger the ratio, the lower the corresponding misjudgment rate, but at the same time, it will take up more space and cost. At the same time, the true value of the false positive rate is generally less than the theoretical value of the false positive rate [25].

The results of Figures 3 and 4 show that, when the performance of Hash is better, that is, the result of Hash distribution is more uniform, under the condition of $m = 3$. The misjudgment rate acceptable for the expected use can be achieved, the increase in the number of Hashes will not bring a significant increase in revenue. Therefore, when conditions

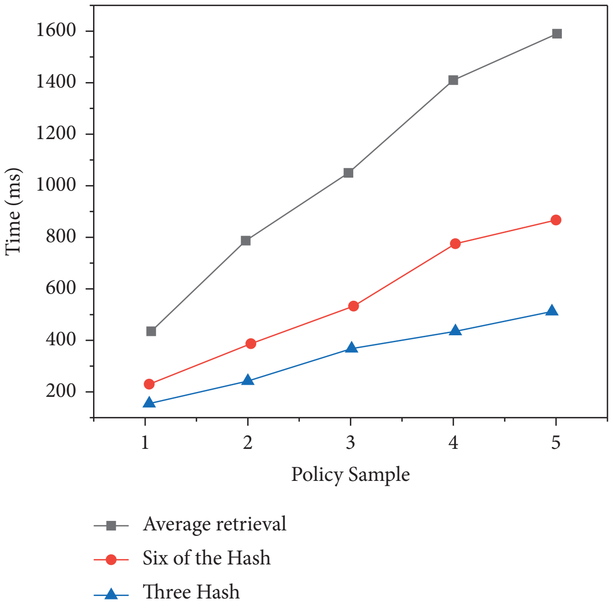

Figure 3: Comparison of strategy retrieval performance.

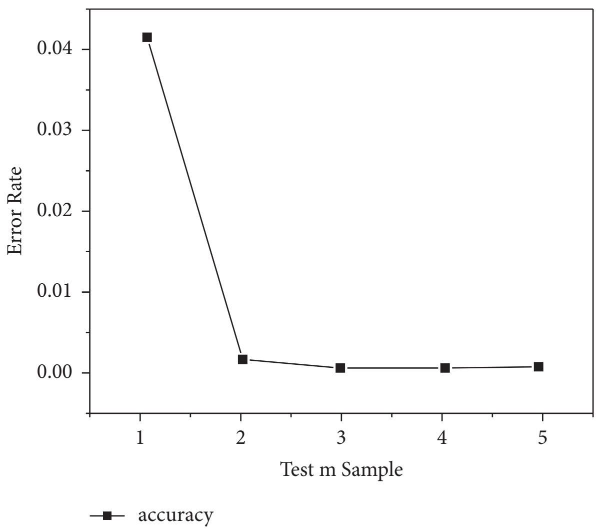

Figure 4: M value affects the accuracy of retrieval results.

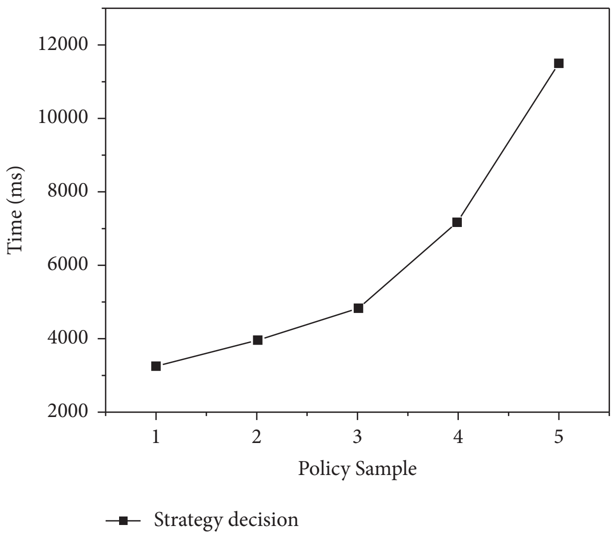

Figure 5: Comparison of strategy decision performance.

permit, try to expand the value of n/k and can effectively improve query performance. This is mainly due to the Bloom filter's attribute keyword filtering process of policy detection, the retrieval time is less affected by the scale of the strategy set, so compared to the traversal retrieval process, strategy retrieval and matching based on the Bloom filter can achieve high performance and strategy retrieval based on the Bloom filter can effectively save cache space, reduce the number of requests to the cache, and improve the efficiency of strategy query and the isolation of strategy management services.

4.2. Strategy Decision Function Test. In order to verify the effectiveness of the BBAC-BD access control mechanism, the author under different scales of strategies, judgment function of access control strategy based on smart contract, performed a functional test; the test content includes the efficiency of the strategy decision and the success rate of the decision result. The PolicySamples of 1 to 5 groups correspond to 1000, 2000, 3000, 4000, and 5000 single strategy test set samples, respectively. The test set sample constructs 800 different access requests for 80 user identities; each logo has an average of 5 attribute values, and each request is sent randomly 5 times. The strategy decision delay is obtained by calculating the average response delay of all requests as shown in Figures 5 and 6.

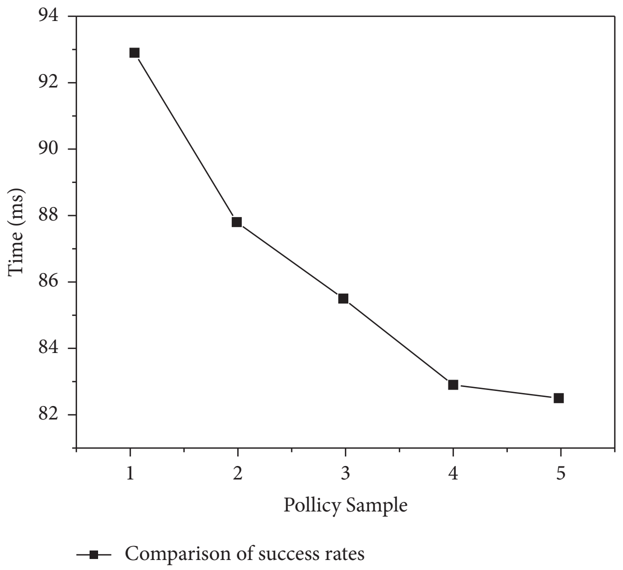

Figure 6: Comparison of the success rate of strategy decision results.

As can be seen from Figure 5, the strategy decision delay is directly related to the strategy scale, with the increase of strategy rules, the delay of access control decision has increased significantly. At the same time, it can be seen from Figure 6 that, as the strategy rules increase, the strategy decision success rate decreases.

5. Conclusion

The author proposes a research study on the automatic access control of big data open resources multimedia based on blockchain. The author uses the big data access control BBAC-BD mechanism based on blockchain. It also elaborated and analyzed the basic framework and process of access control in detail. At the same time, access control strategies based on blockchain transactions and entity attribute information management methods explain that, with the increase of strategy rules, the success rate of strategy decisions decreases. The BBAC-BD mechanism implements a safe, reliable, and transparent new access control architecture, which can effectively promote the safe circulation and sharing of big data. Through smart contracts, based on the strategy released by the resource owner to the blockchain, the automatic access control of big data resources is realized, the judgment process is more flexible, and the judgment results are more credible. The BBAC-BD mechanism is safe, reliable, and transparent. The new access control architecture can effectively promote the safe circulation and sharing of big data. This is because there are some conflicting strategies in the strategy set. For conflicting strategies, the strategic judgment contract cannot get a consistent judgment result, it should be noted that the author has not yet introduced the strategy conflict handling part into the strategy judgment contract, the conflict resolution has not been effectively resolved, and this part of the content will continue to be improved in the follow-up research work.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the Project of Beijing Vocational College of Economics and Management "Research on Blockchain Technology and Application Progress" (project no. 20BSA11).

References

[1] Z. Li, H. Guo, A. V. Barenji, W. M. Wang, and Y. Guan, "A sustainable production capability evaluation mechanism based on blockchain, lstm, analytic hierarchy process for supply chain network," *International Journal of Production Research*, vol. 58, no. 24, pp. 7399–7419, 2020.

[2] B. Huabai and B. Jiaqi, "Research on the improvement of village governance efficiency based on blockchain technology," *Journal of Agricultural Science*, vol. 12, no. 9, 2020.

[3] 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.

[4] E. B. Sifah, Q. Xia, K. O. B. O. Agyekum et al., "Chain-based big data access control infrastructure," *The Journal of Supercomputing*, vol. 74, no. 10, pp. 4945–4964, 2018.

[5] X. Zheng, M. Li, Y. Chen, J. Guo, and W. Hu, "Blockchain-based secure computation offloading in vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, no. 99, pp. 1–15, 2020.

[6] R. Xu, Y. Chen, E. Blasch, and G. Chen, "Exploration of blockchain-enabled decentralized capability-based access control strategy for space situation awareness," *Optical Engineering*, vol. 58, no. 4, p. 1, 2019.

[7] None, "Call and calendar," *Computer*, vol. 48, no. 7, pp. 81–83, 2015.

[8] M. Ansart, S. Epelbaum, G. Gagliardi et al., "Reduction of recruitment costs in preclinical ad trials. validation of automatic pre-screening algorithm for brain amyloidosis," *Statistical Methods in Medical Research*, vol. 29, no. 1, pp. 151–164, 2019.

[9] L. Liu, C. Wang, H. Zhang, Y. Tang, and Z. Zhang, "Automatic monitoring method for surface deformation of coastal area based on time series analysis," *Journal of Coastal Research*, vol. 93, no. sp1, 2019.

[10] Z. Yin, C. Du, J. Liu, X. Sun, and Y. Zhong, "Research on auto-disturbance-rejection control of induction motors based on ant colony optimization algorithm," *IEEE Transactions on Industrial Electronics*, no. 4, p. 1, 2017.

[11] J. Xu, K. Xue, H. Tian, J. Hong, and D. S. L. Wei, "An identity management and authentication scheme based on redactable blockchain for mobile networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6688–6698, 2020.

[12] G. Yu, X. Zha, X. Wang et al., "Enabling attribute revocation for fine-grained access control in blockchain-iot systems," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1213–1230, 2020.

[13] N. Zhang and K. Zheng, "Research and design of the architecture of the marine logistics information platform based on big data," *Journal of Coastal Research*, vol. 106, no. sp1, p. 628, 2020.

[14] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5g," *IET Communications*, vol. 12, no. 5, pp. 527–532, 2018.

[15] X. Ling, Y. Le, J. Wang, and Z. Ding, "Hash access: trustworthy grant-free iot access enabled by blockchain radio access networks," *IEEE Network*, vol. 34, no. 1, pp. 54–61, 2020.

[16] B. Bera, S. Saha, A. K. Das, N. Kumar, and P. Lorenz, "Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9097–9111, 2020.

[17] S. Biswas, K. Sharif, F. Li, and S. Mohanty, "Blockchain for e-health-care systems: easier said than done," *Computer*, vol. 53, no. 7, pp. 57–67, 2020.

[18] X. Wei and C. Qin, "Risk early-warning model of ocean international trade based on svm," *Journal of Coastal Research*, vol. 93, no. sp1, p. 785, 2019.

[19] A. Fioravanti, G. Fico, D. Salvi, R. I. García-Betances, and M. T. Arredondo, "Automatic messaging for improving patients engagement in diabetes management: an exploratory study," *Medical, & Biological Engineering & Computing*, vol. 53, no. 12, pp. 1285–1294, 2015.

[20] M. Hooshyar, D. Wang, S. Kim, S. C. Medeiros, and S. C. Hagen, "Valley and channel networks extraction based on local topographic curvature and k-means clustering of contours," *Water Resources Research*, vol. 52, no. 10, pp. 8081–8102, 2016.

[21] H. Lu, C. Jin, X. Helu, C. Zhu, and Z. Tian, "Autod: intelligent blockchain application unpacking based on jni layer deception call," *IEEE Network*, vol. 35, no. 99, pp. 1–7, 2020.

[22] G. Pin, G. Fenu, V. Casagrande, D. Zorzenon, and T. Parisini, "Robust stabilization of a class of nonlinear systems controlled over communication networks," *IEEE Transactions on Automatic Control*, no. 99, p. 1, 2020.

[23] L. Zhang, "Application research of automatic generation technology for 3d animation based on ue4 engine in marine animation," *Journal of Coastal Research*, vol. 93, no. sp1, p. 652, 2019.

[24] A. Macaranas, A. N. Antle, and B. E. Riecke, "What is intuitive interaction? balancing users' performance and satisfaction with natural user interfaces," *Interacting with Computers*, vol. 27, no. 3, pp. 357–370, 2015.

[25] Y. Dong, S. Xiao, H. Ma, and L. Chen, "Research on quantum authentication methods for the secure access control among three elements of cloud computing," *International Journal of Theoretical Physics*, vol. 55, no. 12, pp. 5106–5117, 2016.