Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.028330

ARTICLE

Research on Multi-Blockchain Electronic Archives Sharing Model

Fang Yu[1], Wenbin Bi[2], Ning Cao[3,*], Jun Luo[4], Diantang An[5], Liqiang Ding[4] and Russell Higgs[6]

[1]School of Information Engineering, Qingdao Binhai University, Qingdao, 266555, China

[2]School of Computer and Software, Dalian Neusoft University of Information, Dalian, 116023, China

[3]School of Internet of Things and Software Technology, Wuxi Vocational College of Science and Technology, Wuxi, 214028, China

[4]Archives Management Department, Qingdao West Coast New Area Archives, Qingdao, 266427, China

[5]Editorial Research Department, Qingdao West Coast New Area Archives, Qingdao, 266427, China

[6]School of Mathematics and Statistics, University College Dublin, Dublin, Ireland

*Corresponding Author: Ning Cao. Email: ning.cao2008@hotmail.com

Received: 08 February 2022 Accepted: 13 May 2022 Published: 08 October 2023

ABSTRACT

The purpose of introducing blockchain into electronic archives sharing and utilization is to break the information barrier between electronic archives sharing departments by relying on technologies such as smart contract and asymmetric encryption. Aiming at the problem of dynamic permission management in common access control methods, a new access control method based on smart contract under blockchain is proposed, which improves the intelligence level under blockchain technology. Firstly, the Internet attribute access control model based on smart contract is established. For the dynamic access of heterogeneous devices, the management contract, permission judgment contract and access control contract are designed; Secondly, the access object credit evaluation algorithm based on particle swarm optimization radial basis function (PSO-RBF) neural network is used to dynamically generate the access node credit threshold combined with the access policy, so as to realize the intelligent access right management method. Finally, combined with the above models and algorithms, the workflow of electronic archives sharing and utilization model of multi blockchain is constructed. The experimental results show that the time-consuming of the process increases linearly with the number of continuous access to electronic archives blocks, and the secure access control of sharing and utilization is feasible, secure and effective.

KEYWORDS

Sharing and utilization of electronic archives; dynamic permission management; PSO-RBF; neural network; credit evaluation

1 Introduction

The development of modern electronic archives sharing service platform based on archives information resource sharing and data driving and the construction of electronic archives information security management system with multi blockchain structure based on big data analysis can provide guarantee from three aspects: information security, entity security and carrier security, and effectively

solve the problem of users' distrust of electronic carriers. As a cutting-edge distributed data storage structure, blockchain has unique technical rules such as distributed ledger, asymmetric encryption and consensus mechanism, which can break the information barrier between electronic archives sharing departments, realize the tamperability, privacy protection and data tracking of shared information, and effectively ensure the data ownership, security and confidentiality of shared information. Fundamentally solve the conflict of interest and lack of trust between electronic archives sharing departments, and provide strong technical support for the safe storage, rapid response and cross departmental collaborative sharing of massive electronic archives information [1,2].

The smart contract introduced in blockchain version 3.0 makes it possible to solve the access control problem through blockchain technology [3]. At present, blockchain is used to solve the security problems of the Internet under integrated edge computing, mostly in terms of privacy protection [4,5] and data security [6,7]. There are few studies on the access control of Internet edge nodes. They ignore the potential risks of edge nodes, and the default edge nodes are safe and reliable [8,9]. Edge nodes should be confirmed through trusted mechanism when accessing the Internet. At the same time, the current edge computing has brought strong computing power. Under the new paradigm of Internet system integrating edge computing, the role of edge nodes in the process of electronic archives access control needs to be fully considered. Combined with the principles and characteristics of blockchain, this paper proposes an Internet electronic archives sharing access control model for multi blockchain with edge computing, which provides a new theoretical framework and effective technical support for realizing efficient, secure and reliable electronic archives information sharing.

On February 25, 2019, the National Archives and Records Administration (NARA) released a blockchain white paper, which showed the research of blockchain technology on archives management and other related aspects as of July 2018, such as the true and complete transmission and archiving of electronic data and electronic archives on the blockchain to the National Archives [10]. In 2017, the National Archives of the UK, together with the University of Surrey and the open data research center, carried out the blockchain application and demonstration project-ARCHANGEL project, which uses blockchain to record and verify electronic archives metadata and is permanently preserved through point-to-point distribution and consistency check [11]. Intan Permatasari and others in Indonesia proposed an electronic archives management system called Cilegon E-Archive (CEA) to improve information security in electronic archives management [12]. Thomas Renner and others in Germany proposed an audit framework called Endolith to prevent electronic files from being tampered with. The framework uses the blockchain based on smart contract to verify the integrity of electronic files and track the file history. It uses the alliance chain in a single blockchain to manage electronic files, and all institutions in the alliance jointly manage and maintain the security of electronic files [13].

Shi et al. proposed to use the digital summary of electronic documents to ensure the authenticity of the whole life cycle of electronic documents, and establish the conceptual model of blockchain technology for the authenticity assurance system of digital archives management, so as to ensure the authenticity and security of the electronic document management process [14]. Referring to the open archive information system (OAIS) model, Wang Ping encapsulates the electronic document information on the block, and provides credible protection for the handover and receiving stage, storage and management stage, utilization and destruction stage of electronic document management [15].

2 Related Work

2.1 Internet Attribute Access Control Model Based on Smart Contract

In the Internet environment, attributes are inherent in each subject, object, operation and environment. By associating the attributes of each device and resource with access rights, attribute based access control (ABAC) model is suitable for managing devices and a wide range of data on the Internet. However, for the dynamic access management of heterogeneous devices, ABAC adopts the attribute discovery mechanism, which can not accurately and appropriately allocate the permissions of the receiving devices according to {attributes, permissions}. This will limit the normal access and real-time processing of data by heterogeneous devices, and bring challenges to the scene with edge nodes. Aiming at the dynamic access of heterogeneous devices, this paper combines smart contract with ABAC [16], and designs management contract (MC), authority judge contract (AJC) and access control contract (ACC).

2.1.1 Manager Contract

MC is used to manage relevant policies. The main body is the access initiator, which is replaced by the corresponding media access control (MAC) address. The attribute is the inherent characteristic of the object. The permission is an operable behavior described by numerical value. The permissions are read, write, management, etc. The custom functions are shown below:

ManageAdd (): used to add permission information of an object.

ManageUpdate (): used to update the permission information of an object.

ManageDelete (): used to delete the permission information of an object.

QueryData (hash): used to obtain the information of an object through hash.

2.1.2 Authority Judge Contract

AJC is used to judge when an object applies for an operation on a resource. The structure is obtained by comparing the subject permission and resource permission, including allowing all operations, read-write, readable and illegal access.

JudgeFromMC () is used to obtain the permission information of the object from MC.

JudgeToACC () is used to send judgment results to personal computer (PC).

JudgeAccess () is used to judge whether the sensor device has access exceptions, and the generated exception report is sent to ACC.

AddAccessIssue () is used to add access exception events.

DeleteAccessIssue () is used to delete access exception events.

PSO-RBFNeualNetworks () calls the trained PSO-RBF neural network model to calculate the threshold of sensor access credit (0∼1).

Feedback () is used to feed back the access credit threshold of the access object.

2.1.3 Access Control Contract

ACC is used to realize the final access control of devices and resources, and return the judgment result to the subject through the AJC result.

ACCAnswer () returns the AJC result to the principal to complete the access control of the resource

ACCSetMC () calls the function in MC to modify the object permission through the result of AJC.

AddPolicy () is used to add a new access policy and receive the new access policy to the policy list.

UpdatePolicy () is used to update the access policy.

DeletePolicy () is used to delete the access policy.

AccessControl () is used for access decision-making. It combines the predefined access policy with the access credit threshold fed back in the AJC contract to make permission decision.

PublishToACC () is used to send penalty results to ACC.

2.2 Credit Evaluation Method of Access Object Based on Particle Swarm Optimization-Radial Basis Function (PSO-RBF) Neural Network

Design a three-layer neural network credit evaluation model [17], see Fig. 1 below.

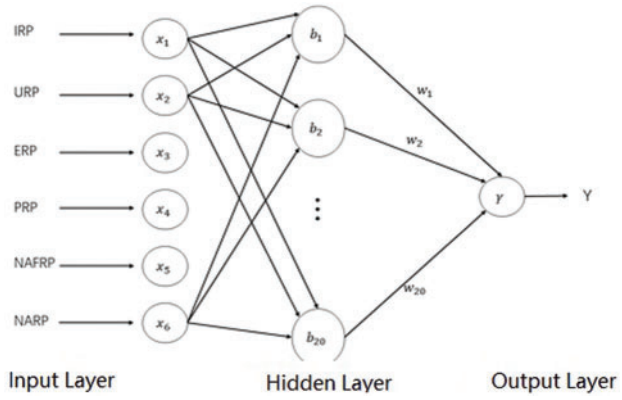

Figure 1: PSO-RBF neural network model for credit evaluation

The number of nodes in the input layer is 6. The access feature vector includes the following six categories, illegal request proportion (IRP), unauthorized request proportion (URP), no access resources proportion (Narp), Exception request proportion (ERP), prohibition request proportion (PrP) and request disallowed proportion (NAFRP). Take the above six types of vectors as the input features, which are recorded as $X = (x_1, x_2, \cdots, x_6)$. The number of hidden layer nodes is 20, which is recorded as $B = (b_1, b_2, \cdots, b_{20})$.The output node is Y, which represents the trust of the access object, expressed as $Y = \gamma, \gamma \in (0, 1)$.

The hidden layer adopts Gaussian kernel function as the basis function.

$$\varphi(x) = \exp\left(-\frac{(x - c_i)^T (x - c_i)}{2\sigma_i^2}\right) \tag{1}$$

The relationship between output $Y(x)$ and input x is as follows:

$$Y(X) = w_0 + \sum_{i=1}^{20} w_i \exp\left(-\frac{(X - C_i)^T (X - C_i)}{2\sigma_i^2}\right) \tag{2}$$

In Eq. (2), w_0 is the offset used to adjust the output. w_i represents the weight between the basis function of the i-th hidden node and the output node. X is the input vector, C_i is the field center of the i-th hidden node, σ_i is the field width of the i-th hidden node.

The parameter update of the model adopts PSO algorithm [18–23]. Suppose the space for searching food is P-dimensional, the total number of particles is n, and the position of the i-th particle in P-dimensional space is $x_i = (x_{i1}, x_{i2}, \cdots, x_{iP})$, flight speed is $\vartheta_i = (\vartheta_{i1}, \vartheta_{i2}, \cdots, \vartheta_{iP})$. The following two factors should be considered when searching:

(1) The particle searches the best position P_b so far.
(2) Search all particles to the best P_g.

The position and velocity equation of PSO algorithm is as follows:

$$\vartheta_{if}^{m+1} = \rho\vartheta_{if}^{m} + x_1\varepsilon\left(P_{if}^{m} - x_{if}^{m}\right) + x_2\varepsilon\left(P_{gf}^{m} - x_{if}^{m}\right) \tag{3}$$

$$x_{if}^{m+1} = x_{if}^{m} + \vartheta_{if}^{m}$$

In Eq. (3), ρ is the inertia weight, ϑ_{if}^{m} is the f-dimensional component of the velocity at the m-th iteration of particle i, x_{if}^{m} is the position f-dimensional component of particle i at the m-th iteration, P_{if}^{m} is the f-dimensional component of particle i at the optimal position, P_{gf}^{m} is the f-dimensional component of the optimal position of all particles, x_1 and x_2 is the weight factor, ε is a random number between [0,1].

$$\rho = \rho_{max}\frac{\rho_{max} - \rho_{min}}{h_{max}} \times h \tag{4}$$

In Eq. (4), ρ_{min} is the minimum, ρ_{max} is the maximum value of inertia weight, respectively. h is the current number of iterations, h_{max} is the maximum number of iterations, respectively.

$$E = (\gamma_i - o_i)^2 \tag{5}$$

E is the square of the difference between the model output and the actual value, γ_i is the model output value, o_i is the actual value. When the error E decreases to a suitable value, the algorithm stops. At the same time, the center C and weight value w of the obtained radial basis function are saved, and the learning process ends.

3 Workflow of Electronic Archives Sharing and Utilization Model Based on Multi Blockchain

This paper designs a multi blockchain electronic archives sharing and utilization model. The model is suitable for the integration of internal information system and archives. At the same time, it has expansibility and supports the integration of cross organizational electronic archives security management. There are two blockchain networks in the whole process of electronic archives management and use: one blockchain network is the electronic archives management chain, and the other blockchain network is the electronic archives use chain. The file management chain uses the alliance chain. Only authorized enterprises and institutions can operate this file management chain. Its main function is to create, modify, delete, approve and other management operations of electronic files. The file use chain uses the public chain, which is mainly used to provide users with electronic file access, electronic file download and verification functions.

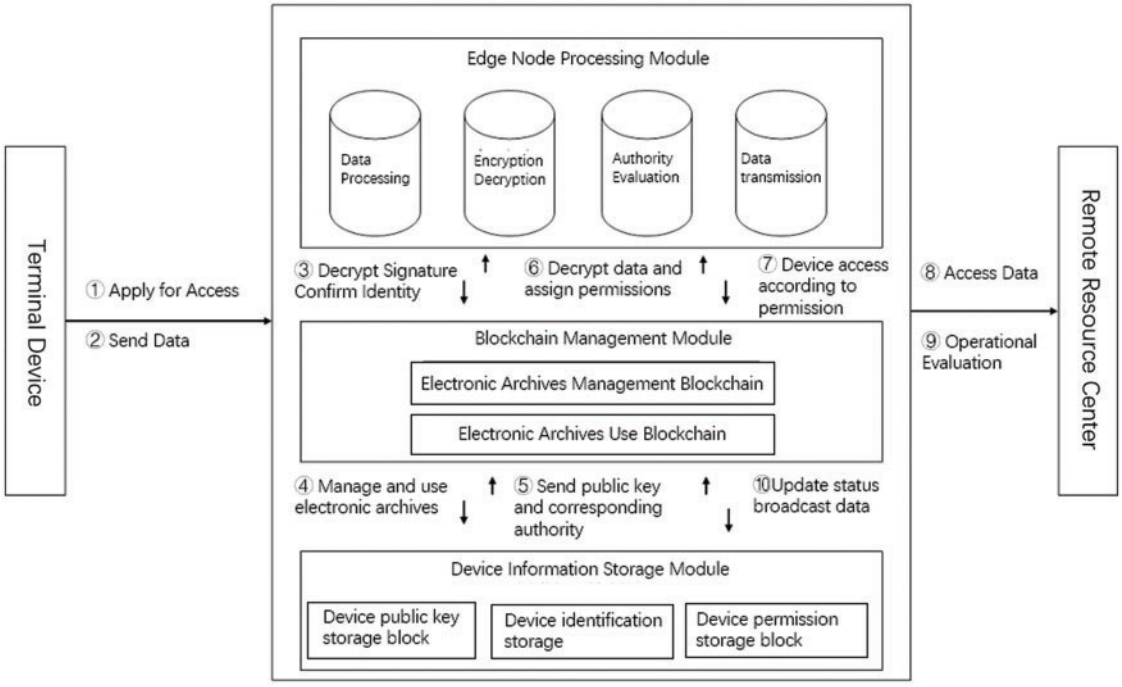

Figure 2: Multi blockchain electronic archives sharing and utilization control process

The sharing and utilization process of multi blockchain electronic archives (Fig. 2) is mainly divided into four stages: Initialization stage, device registration stage, authority dynamic allocation stage and execution stage.

In the initialization phase, the agent node deploys the smart contract. After the MC, AJC and ACC contracts are successfully deployed in the blockchain, the proxy node obtains the addresses of the three contracts and lets all nodes on the blockchain get the addresses through broadcasting.

In the registration phase, the manager sends a registration request to the MC, registers itself and its managed devices, and generates a pair of keys, including public and private keys. The manager sends a request to AJC to add an access policy for device S_1 to access device S_2 resource R_2. The management node encapsulates the access policy as a transaction, broadcasts it in the blockchain with S_1 public key as the transaction output address, and adds the transaction to the AJC contract after being verified by the miner to complete the addition of the access policy.

In the access control phase, the device S_1 accesses the resource R_2 of the target device S_2, and the MC sends an access policy request to ACC after receiving the message. After ACC obtains the request, it inquires from AJC whether there is any access exception event. If it is normal, it will feed back to MC access policy. If it is abnormal, ACC sends a request for obtaining credit value to AJC. AJC generates the access credit threshold by calling PSO-RBF algorithm and feeds it back to ACC, and updates the access history of the access object. ACC calculates the access decision in combination with the credit and access policy, and feeds back the result to MC.

In the execution phase, the proxy node MC generates access control results and initiates transactions in the blockchain. Miner obtains the management of electronic files, writes the transaction information into the new block after using the transaction, triggers the corresponding event of smart

contract, and feeds back the access permission result to the manager. Assuming that the permission is allowed access, the R_2 resource of S_2 allows S_1 access and feeds back the request result to S_1.

4 Experimental Simulation and Security Test

4.1 Simulation and Result Analysis of Credit Model Based on PSO-RBF Neural Network

Select 500 sample data and credit evaluation results. First, initialize the initial data, enlarge it by 100 times as the network input, take 400 node samples as the training data, the number of training rounds is 200, and the remaining 100 node sample data as the test data. As shown in Figs. 3 and 4, the credit model based on PSO-RBF neural network has the characteristics of good convergence, high learning efficiency and high accuracy. Compared with multiple linear regression algorithm, it is more accurate. Compared with back propagation (BP) neural network algorithm, it has the characteristics of fast convergence and stable learning.

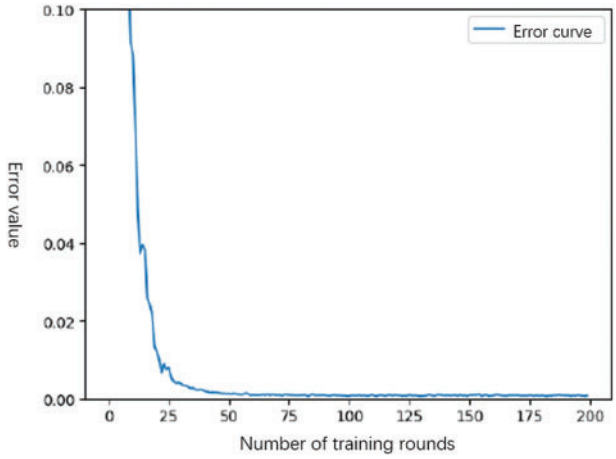

Figure 3: Error variation curve

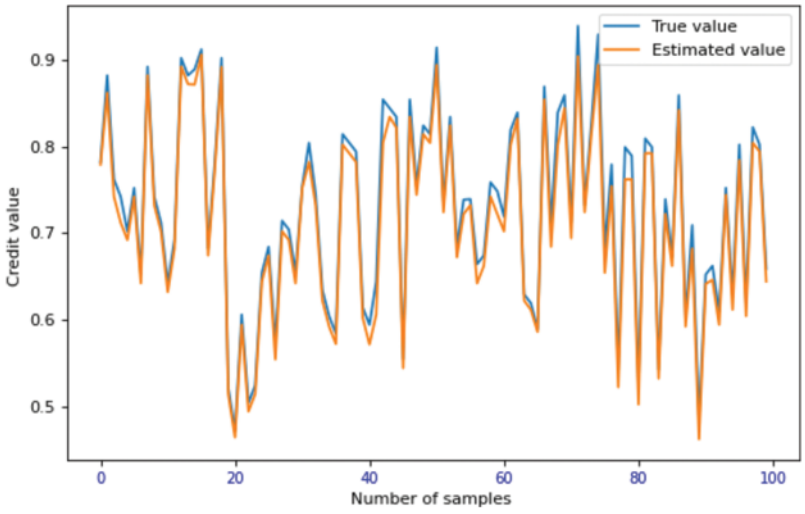

Figure 4: Error variation curve

4.2 Performance Test of Electronic Archives Sharing and Utilization Model Based on Multi Blockchain

Fig. 5 shows the time-consuming of 500 consecutive accesses to different data by different subjects, and the corresponding data is the average time-consuming of every 10 times. With the increase of the number of visits, the time of each visit increases linearly, and the average time of each visit in the 500th time is about 1.3 s. Since the access records are stored in the blockchain after each access process, the query data of each access is increasing, resulting in a linear increase in access time with the increase of access times.

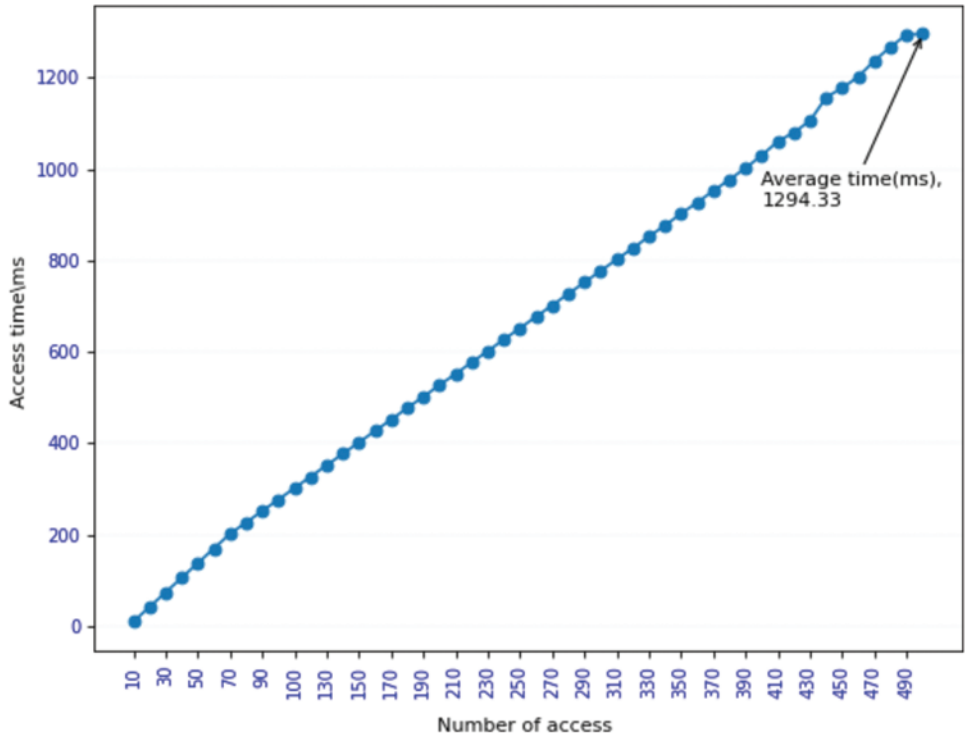

Figure 5: Time-consuming situation under different access times

Test the response time of the model access control request, and the response time of sending request nodes from 0 to 10000 per second. Test the response time comparison after calling PSO-RBF algorithm and not calling the algorithm, as shown in Fig. 6. Due to the large amount of calculation required to call PSO-RBF algorithm, there will be delay, and the response time of 10000 request nodes will increase by about 5 s.

By simulating the concurrent requests of multithreaded clients, test the processing time of ManageAdd(), QueryData() and PublishToACC() under different concurrent requests with proof of work (PoW) difficulty of 0, difficulty of 1 and difficulty of 2, as shown in Fig. 7.

It can be seen that under different concurrent requests, adding and judging contracts will hardly take time, which proves the superiority of edge nodes in the Internet scenario. Based on the need to complete consensus, access record and synchronous query in the blockchain during the query process, the time will increase with the increase of the number of requests. Due to the small difficulty discrimination, the time required for PoW is negligible compared with the query time, but in comparison, the method proposed in this paper still has high application value.

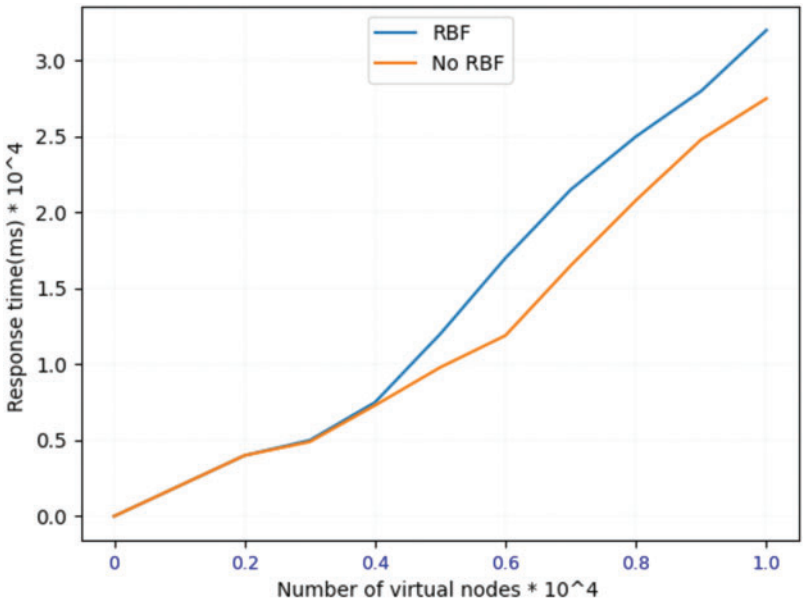

Figure 6: Response times of access control request

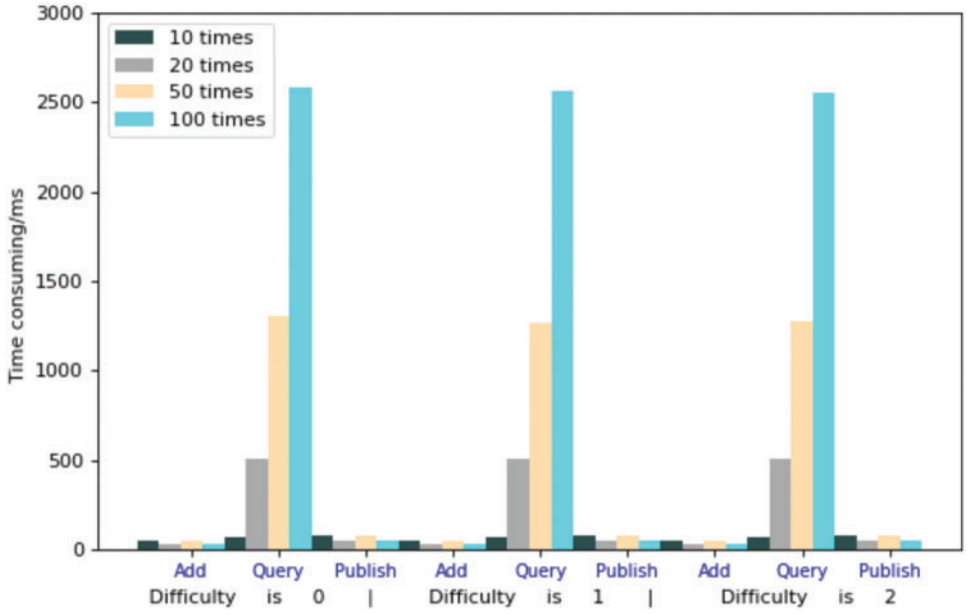

Figure 7: The processing time of ManageAdd (), QueryData () and PublishToACC ()

5 Conclusions and Future Work

The electronic archives sharing and utilization model based on multi blockchain has the following typical characteristics: The public chain and alliance chain adopt distributed ledger technology to make multiple backups of data, which can effectively ensure the integrity of shared data within and among entities. All members in the public chain and alliance chain have been authenticated and have high credibility. The three smart contracts of MC, AJC and ACC are used to realize the functions of

registration management, authority management and access policy management. By introducing PSO-RBF algorithm, the access credit threshold of access nodes is evaluated, the dynamic and intelligent management of access control of massive nodes is realized, and the flexible, intelligent and fine-grained control process is realized. The economy of the model is mainly reflected in cost and operation efficiency. The multi-layer blockchain model is dominated by the alliance chain and supplemented by the public chain. The data is mainly stored in the alliance chain, and only a small amount of data to be shared is uploaded to the public chain, so as to avoid the circulation of too much redundant data in the public chain. Electronic archive data is stored in the form of hash value in the chain, which can reduce the storage burden of the model, effectively improve the throughput and response speed of the model and improve the operation efficiency. For future work, we will try to combine attribute based encryption to build an efficient alliance chain environment. At the same time, because this model introduces PSO-RBF neural network algorithm to learn and record the knowledge of access nodes, it requires large data storage space and high requirements for computing power. However, there are bottlenecks in the storage capacity and computing power of the current blockchain system. In the next step, further research will be carried out in the aspect of model lightweight.

Acknowledgement: None.

Funding Statement: This work was supported by Shandong Social Science Planning and Research Project in 2021 (No. 21CPYJ40).

Author Contributions: Conceptualization, Yu and Cao; methodology, Yu and Bi; software, Yu and Bi; validation, Yu and Luo; formal analysis, An and Ding; investigation, Yu; resources, Yu; writing—original draft preparation, Yu; writing—review and editing, Higgs; All authors have read and agreed to the published version of the manuscript.

Availability of Data and Materials: The authors do not have permission to share the data.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] B. Roman, "Beyond bitcoin: The rise of blockchain world," *Computer*, vol. 51, no. 2, pp. 54–58, 2018.
[2] I. Eyal, "Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities," *Computer*, vol. 50, no. 9, pp. 38–49, 2017.
[3] D. Maesa and P. Mori, "Blockchain 3.0 applications survey," *Journal of Parallel and Distributed Computing*, vol. 138, no. 1, pp. 99–114, 2020.
[4] A. Dwivedi, G. Srivastava and S. Dhar, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, pp. 326, 2019.
[5] C. Lin, D. He and N. Kumar, "Homechain: A blockchain-based secure mutual authentication system for smart homes," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 818–829, 2020.
[6] S. Tuli and R. Mahmud, "Fogbus: A blockchain-based lightweight framework for edge and fog computing," *Journal of Systems and Software*, vol. 154, no. 8, pp. 22–36, 2019.
[7] Y. Ren and L. Yan, "Secure data storage based on blockchain and coding in edge computing," *Mathematical Biosciences and Engineering*, vol. 16, no. 4, pp. 1874–1892, 2019.
[8] H. Nyamtiga, S. Sicato and Y. Rathore, "Blockchain-based secure storage management with edge computing for IoT," *Electronics*, vol. 8, no. 8, pp. 828, 2019.

[9] Y. Ren, F. Zhu and J. Qi, "Identity management and access control based on blockchain under edge computing for the industrial internet of things," *Applied Sciences*, vol. 9, no. 10, pp. 2058–2074, 2019.
[10] M. A. Rasheed, "White paper: Blockchain for wearable devices," *Research Gate*, vol. 1, no. 1, pp. 1–13, 2017.
[11] C. Nsulea and S. M. Mic, "Using blockchain as a platform for smart cities," *Journal of E-Technology*, vol. 9, no. 2, pp. 37, 2018.
[12] I. Permatasari, M. Essaid and H. Kim, "Blockchain implementation to verify archives integrity on Cilegon E-Archive," *Applied Sciences*, vol. 10, no. 7, pp. 2621, 2020.
[13] T. Renner, J. Müller and O. Kao, "Endolith: A blockchain-based framework to enhance data retention in cloud storages," in *2018 26th Euromicro Int. Conf. on Parallel, Distributed and Network-Based Processing (PDP)*, Cambridge, UK, 2018.
[14] J.Shi, S. X. Xue and X. K. Zhao, "Research on the system model of electronic records authenticity guarantee based on blockchain," *Document, Informaiton & Knowledge*, vol. 192, no. 6, pp. 111–119, 2019.
[15] P. Wang, M. Y. Li and R. W. Ji, "Research on the trusted protection framework for electronic records based on blockchain technology," *Archives Science Study*, vol. 166, no. 1, pp. 101–107, 2019.
[16] Y. Zhang, S. Kasahara and Y. Shen, "Smart contract-based access control for the Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, 2019.
[17] X. H. Jia, Y. M. Han and W. Q. Wang, "Control system design based on RBF neural network for roll-pitch seeker," *Journal of Ordnance Equipment Engineering*, vol. 37, no. 8, pp. 1–5, 2016.
[18] S. F. Wang, K. Y. Du and Y. Meng, "Machine learning-based road terrain recognition for land vehicles," *Acta Armamentarii*, vol. 38, no. 8, pp. 1642–1648, 2017.
[19] Z. Shahbazi and Y. Byun, "Blockchain and machine learning for intelligent multiple factor-based ride-hailing services," *Computers, Materials & Continua*, vol. 70, no. 3, pp. 4429–4446, 2022.
[20] S. R. Khonde and V. Ulagamuthalvi, "Blockchain: Secured solution for signature transfer in distributed intrusion detection system," *Computer Systems Science and Engineering*, vol. 40, no. 1, pp. 37–51, 2022.
[21] F. Baothman, K. Saeedi, K. Aljuhani, S. Alkatheri, M. Almeatani *et al.,* "Computational intelligence approach for municipal council elections using blockchain," *Intelligent Automation & Soft Computing*, vol. 27, no. 3, pp. 625–639, 2021.
[22] J. Liu, X. Sun and K. Song, "A food traceability framework based on permissioned blockchain," *Journal of Cyber Security*, vol. 2, no. 2, pp. 107–113, 2020.
[23] A. I. Khan, A. Saad, F. J. Alsolami, Y. B. Abushark, A. Almalawi *et al.,* "Integrating blockchain technology into healthcare through an intelligent computing technique," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 2835–2860, 2022.