Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 9857063, 1 page
https://doi.org/10.1155/2023/9857063

Retraction

Retracted: Privacy Protection of Medical Service Data Based on Blockchain and Artificial Intelligence in the Era of Smart Medical Care

Wireless Communications and Mobile Computing

Received 19 September 2023; Accepted 19 September 2023; Published 20 September 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] B. Wu, Y. Pi, and J. Chen, "Privacy Protection of Medical Service Data Based on Blockchain and Artificial Intelligence in the Era of Smart Medical Care," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 5295801, 10 pages, 2022.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5295801, 10 pages
https://doi.org/10.1155/2022/5295801

Research Article

Privacy Protection of Medical Service Data Based on Blockchain and Artificial Intelligence in the Era of Smart Medical Care

Bo Wu,[1] Yong Pi,[2] and Jinhong Chen[3]

[1] *Law School, Wuhan University, Wuhan City, Hubei Province, China 430072*
[2] *Shanghai International College of Intellectual Property, Tongji University, Shanghai, China 200433*
[3] *Beijing Jingdong Century Trading Co., Ltd., Beijing, China 100176*

Correspondence should be addressed to Bo Wu; fxywubo@whu.edu.cn

Received 23 March 2022; Revised 22 April 2022; Accepted 28 April 2022; Published 7 June 2022

Academic Editor: Kuruva Lakshmanna

Smart medical care will realize the self-management, selection, and optimization of related things with more thorough induction, more comprehensive interconnection, and more intelligent insight, so that people can get an increasingly personalized medical and health service experience. 5G-enabled Internet of Things and AI (artificial intelligence) will continue to drive innovative applications in the medical industry. Access control and sharing of medical data is of great significance to the development of smart medical care, but the security problems in medical data sharing cannot be ignored. In this paper, a privacy protection scheme of medical service data based on blockchain and AI is proposed. The user chain is constructed as a public chain. In the user chain, the data privacy of users is protected, and users can safely transmit data to doctors and realize the management of session keys. CNN (convolutional neural network) privacy protection protocol based on homomorphic encryption can protect users' privacy input, server model parameters, and calculated intermediate values. Experimental analysis and comparison with other schemes show that the scheme in this model is safer and more practical.

1. Introduction

In recent years, combining with other fields, the medical and health industry has continuously integrated 5G technology, Internet of Things, AI (Artificial Intelligence), big data, blockchain, and other high-tech applications across borders, which has made medical services intelligent and ushered in a brand-new development opportunity [1, 2]. 5G network realizes the connection between people, people and things, and things and things. In the process of mobile medical diagnosis, electronic medical records such as doctors' electronic prescriptions and electronic medical records usually record all sensitive and private data of medical users from the time of medical treatment to the end of diagnosis and treatment, such as illness change, examination report, and treatment process [3]. If these private data are obtained illegally, it is very likely that the personal privacy of medical users will have unpredictable consequences. Only by avoiding the transmission and release of private data can we truly protect the privacy of patients, and the intercepting signature technology is the most suitable solution [4, 5]. Especially in the medical and biomedical fields, blockchain technology has been deeply studied and applied. But so far, there is no blockchain-based application in monitoring medical sensitive information.

This series of advantages of blockchain make it have a very good development prospect and a wide range of application scenarios [6], which is regarded as the key technology to guide the transformation of information Internet to value Internet. The nodes in the block chain jointly maintain the system, and the block data is updated through consensus mechanism, which ensures the consistency and synchronization of data information in each node and prevents hackers from single-point attack. The connection will generate data, and the data system and AI system will receive and process massive data information in real time and feedback relevant analysis and decision-making to the data center to complete the ecological closed loop of smart medical care [7, 8]. Javed et al. proposed an effective access control strategy to support effective decryption and attribute revocation for the medical cloud storage system with multiple authorization centers [9]. Fan et al. used the solution of attribute encryption on mobile devices to protect the privacy of electronic medical information [10]. The system enables users to share information through fine-grained access control policies. Wang et al. designed a lightweight backup and effective recovery model [11] for the key of health data blockchain with body sensor network, which can effectively protect the privacy information of health data blockchain and improve the application of health blockchain. Abou-Nassar et al. put forward a new keyword search mechanism, which realizes the function of automatically revoking the delegation authorization at regular time by combining the designation of testers and the proxy reencryption technology [12]. The hierarchical homomorphic encryption scheme proposed by Tang et al. realizes the privacy protection in the prediction stage of CNN (convective neural network) [13]. The first privacy protection scheme for neural networks with more than two nonlinear layers is designed. They use low-order polynomial functions to approximate the activation function. Li et al. put forward a revocable attribute-based encryption scheme without key escrow in cloud storage environment. In this scheme, attribute authority and central control build a key distribution protocol without key escrow through secure two-party computing technology, which solves the problem of key escrow, but the computational cost of the scheme is still large [14]. Pires et al. proposed a medical data sharing scheme based on blockchain, in which the participants agreed on the rules in advance. Although this scheme realized the sharing of medical data, it lacked a general access control strategy [15, 16].

Using blockchain technology in the medical field can not only complete the functions of information management, monitoring, tracking, and updating of medical data but also be expected to break the situation of “information island” in the medical industry, solve the problems such as lack of medical funds and difficult data sharing in the medical field, and build a medical system with information interconnection and intercommunication, so as to realize the beautiful vision of continuous improvement of medical service quality and efficient and accurate remote consultation [17]. At present, the medical and health data storage is too centralized, the versions of different hospitals are not uniform, and there are some problems, such as the difficulty of data sharing, the inability of effective identification and verification in data sharing, and the untraceable data operation records, which threaten the privacy of users. This brings many difficulties to the privacy protection of medical service data. Therefore, this paper proposes an anonymous proxy traceable privacy protection scheme, designs the data structure of transactions in three chains, and provides telemedicine diagnosis services for users while ensuring data security. When the user revokes the doctor’s access right, the doctor is allowed to access his own historical diagnosis record, and the hospital is allowed to supervise the doctor’s diagnosis. Help solve the problems that medical and health data are easy to be monopolized, tampered with, difficult to share and untrustworthy by third parties, so as to truly realize distributed, decentralized, traceable, and unalterable medical and health data storage and sharing.

2. Research Method

2.1. Characteristics of Smart Medical Application Technology. There are similarities between smart medical care and the concepts of “mobile medical care,” “digital medical care,” and “regional health informatization,” which all reflect the application of information technology in the medical and health field and represent different stages of medical and health informatization construction. The differences are mainly manifested in the key points of construction, the level of construction, the supporting technology, and the achievement of goals. With the high level of system integration, interconnection, intelligent processing, etc., it is a higher stage of information construction in the medical and health field to ensure that people can get preventive and therapeutic medical services in a timely manner and to encourage individuals to make wiser decisions.

There are many areas involved in the application of smart medical technology, and most of them are concentrated in three aspects: network layer, perception layer, and platform layer. The applied technologies include the following aspects [18].

2.1.1. Information Processing Technology. Information processing technology mainly includes network computer technology and distributed computing technology. In the aspect of smart medical care, the main task of information technology is to comprehensively sort out and analyze some preprocessed data obtained through the original broadcast of sensors. In addition, information processing technology also needs to realize the integration of higher-level information, so that the efficiency of original data can be fully exerted, and it can also lay a good foundation for the smooth development of nursing work.

2.1.2. Information Intercommunication Technology. Information intercommunication technology mainly includes electromagnetic interference technology and high-efficiency transmission technology. Through the application of this technology, it can help users to achieve effective network cooperation with medical institutions, and it also has certain positive significance for sharing health information [19]. The mode of understanding and analyzing the above data can help nurses have a clear understanding of patient information, which is also of positive significance to the treatment of patients.

The information development trend of internet of things, interconnection, and intelligence has brought new challenges to medical and health information security. The construction of the information security system focusing on ensuring the stability of the information system and strengthening the protection of information data has become one of the key factors to realize the goal of smart medical construction. In order to fully realize the strategic concept of smart medical care, it is necessary to integrate the advantages of government agencies, cooperative operators, research institutes, universities, and consulting institutions in different fields and realize multiresource pooling, integration, and collaborative innovation, with complementary advantages and coordinated advancement.

In the process of construction and approval of existing smart medical projects, it is mainly carried out according to existing policies, which has caused great difficulties for the application of medical institutions. Through the relevant medical service information recommended by the system, we can make a reasonable choice of the medical service we want, which can also play a good role in solving the problem of unequal information between doctors and patients and nurses in traditional medical work, and promote the further development of China's medical industry. Relevant departments should seize the opportunity, give full play to the industrial radiation role of smart medical care construction, promote the optimization and upgrading of related industrial structures, and take this opportunity to establish a market-oriented technological innovation system combining government, enterprise, and research and cultivate new economic growth points.

2.2. Blockchain-Based Privacy Protection Scheme for Medical Service Data. Smart hospitals originate from smart medical care, which has been expanded on the basis of medical health concept. With people's medical health as the basic core and people's life health as the main goal, the hospital information and intelligent construction based on medical Internet of Things can solve the bottleneck problems encountered in the construction of smart hospitals by learning from the scientific advanced 5G technology, Internet of Things technology, and AI technology and fully integrate computer technology and medical care [20].

Privacy issues in the process of data aggregation mainly refer to concerns about direct invasion of privacy. We should also consider another situation; that is, a lot of privacy is leaked without the knowledge of the parties. For example, some companies deliberately collect personal privacy information on the Internet or illegally invade the databases of some medical institutions to steal data, even if these leaked data are not directly used, bring losses to the parties, or even the records have been deleted. However, this situation should also be a medical data security problem, which may be potentially harmful and should be taken seriously.

Privacy violation in AI prediction results may not directly bring serious consequences, but fear of privacy violation may make people nervous, irritable, and even mentally ill. For example, a kind of problems found in the process of automatic comparison of gene pool may lead to thinking about what others will do when they see it, thus leading to some anxiety.

Blockchain technology uses block chain data structure to verify and store data, uses consistency algorithm to generate and update data among distributed nodes, and uses encryption algorithm to ensure the safe transmission and operation of data [20]. Blockchain is not only an innovative technology but also a method of integrating existing technologies to record, store, and express data. From the chain structure of blockchain in Figure 1, blockchain is a data block chain that can be traced from the latest block to the creation block (that is, the first block), which is formed by the generated block according to the timestamp and through the link to the hash value of its parent block [21].

The chain structure of the block chain ensures that the stored transaction data in the block is tamper-proof. Because the Merkle root in the block header is the unique hash value that gathers all transaction summaries in the block from bottom to top, any transaction change in the block will cause the Merkle root to change, and the block hash value will naturally change [22].

Common consensus mechanisms for blockchain include POW (Proof of Work), and the consensus algorithm that is most used in public chain is POW, because the probability of success of attackers using computing power to attack this algorithm is extremely low. Only when the length of FB exceeds MB can it replace the main chain and become the new main chain. The probability of doing so is as follows:

$$q_m = \left\{ \begin{array}{ll} 1, & p \leq q \\ q/p, & p > q \end{array} \right\}, \tag{1}$$

where p is the probability of honest nodes making new blocks, q is the probability that malicious nodes make new blocks, and q_m is the probability that FB produces m blocks that exceed MB.

If MB generates a new block followed by m blocks, the probability that FB wants to surpass MB is

$$p_m = 1 - \sum_{k=0}^{m} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \left(1 - \left(\frac{q}{p}\right)^{m-k}\right), \tag{2}$$

where p_m is the probability that FB can exceed MB after falling behind by m blocks, and λ is the Poisson distribution expectation of FB.

Through experiments, it is found that FB will not replace the main chain if the number of malicious nodes is less than half of the whole network and m blocks behind. In the bitcoin system, m is usually 6, which means that a new block needs to be followed by 6 blocks before the data in this new block is considered safe.

Medical institutions and regulatory authorities at the same level belong to the same chain. Based on this chain, data sharing among different institutions is realized. The regulatory authorities and all other institutions at the same level jointly maintain the security of data on the chain and ensure the consistency of access records of each node. As shown in Figure 2, medical institutions and regulatory authorities at the same level belong to the same chain, and edge nodes are elected at different levels. These edge nodes belong to the same chain to realize data sharing among different levels.

In the scheme model in Figure 2, the internal system of an institution is composed of several nodes, which belong to the internal blockchain of a medical institution and jointly maintain the data on the chain to ensure the consistency of

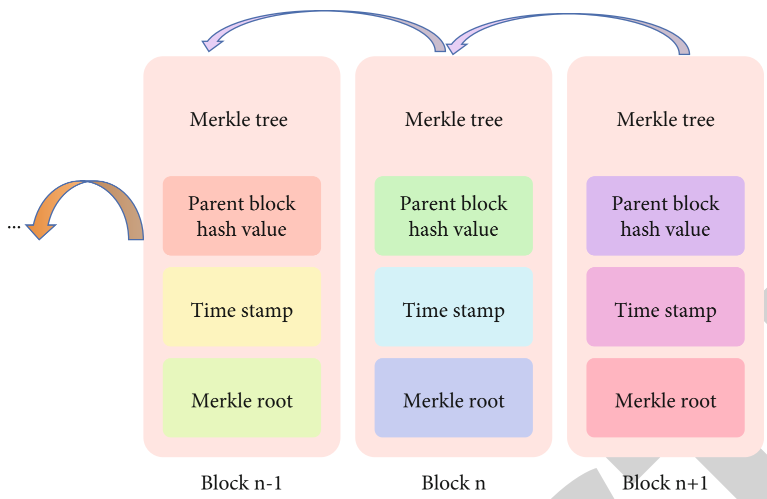

Figure 1: Blockchain chain structure.

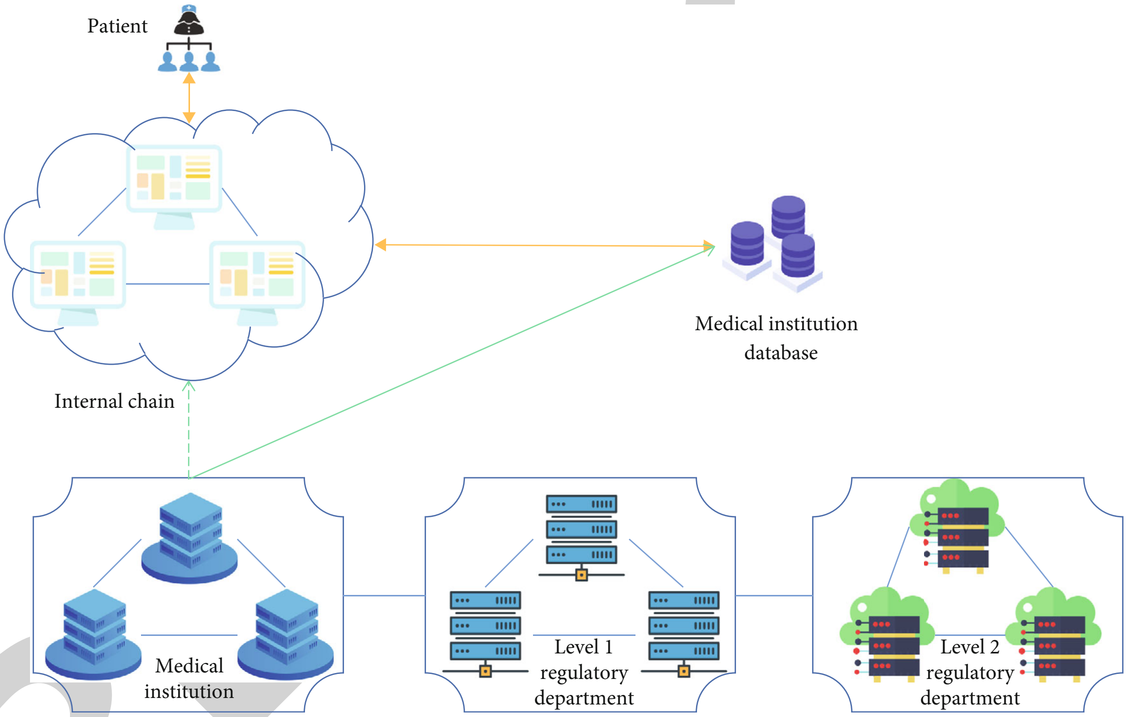
Patient
Internal chain
Medical institution database
Medical institution
Level 1 regulatory department
Level 2 regulatory department

Figure 2: Scheme model.

information stored by all nodes. The internal node of the organization first interacts with the patient to obtain the patient's medical record information, and then the internal node encrypts the patient's medical data symmetrically and stores it in the bottom database of the organization. The encrypted address, Merkle root hash value, and symmetric encryption key are encrypted by the attribute-based encryption algorithm and stored in the internal chain of the organization.

In order to realize fine-grained access control of medical data and data sharing among different institutions, this paper designs three different blockchains for medical institutions and different levels of medical institutions with the help of internal gateway protocol and external gateway protocol, which are called internal chain, peer sharing chain, and hierarchical chain, respectively, and realizes data sharing among medical institutions through three-chain interconnection [23].

While uploading data information, the internal chain of medical institutions also brings the attributes of other medical institutions into the access control tree. As shown in Figure 3, the left branch of the attribute-based encryption policy tree represents the attribute requirements of other medical institutions, and the right branch is the permission requirements of internal nodes of medical institutions. Only the internal nodes of medical institutions that meet the attribute requirements can successfully decrypt the data information.

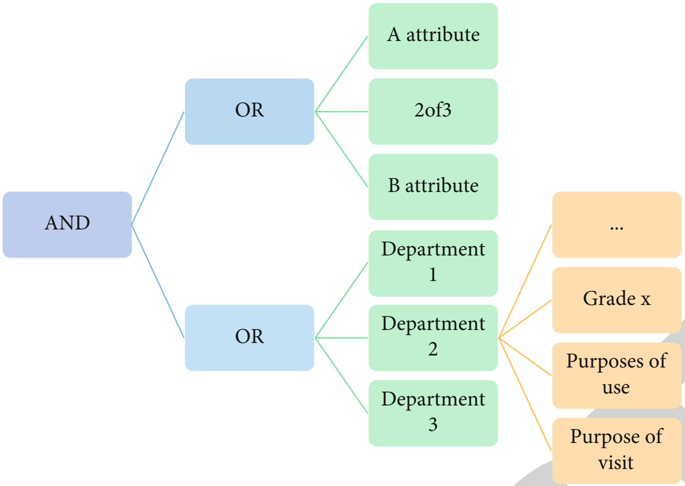

Figure 3: Access policy tree.

When visitors access data, they first send the information keywords they need to access together with their own attribute sets to the edge nodes located in the peer-to-peer sharing chain in their affiliated institutions. All the edge nodes in the peer-to-peer sharing chain jointly verify whether they have access rights. If the verification passes, visitors can successfully decrypt the ciphertext address index information and symmetric encryption key and then successfully decrypt the required medical data [24]. After the visit, all edge nodes will store the visit record together.

Data sharing among medical institutions involves not only the access rights of medical institutions but also the access rights of internal departments or individuals. It is necessary for the attributes owned by the edge nodes in the institutions to intersect with the attribute sets owned by the internal nodes to get access policies:

$$S_A \cap S_B = S'_u, \tag{3}$$

$$\mathrm{StrGen}\left(S'_u\right) \longrightarrow \Gamma'_{\mathrm{com}}. \tag{4}$$

In the above formula, S_A, S_B is the authorization center and the system master and private key, respectively, S'_u is the attribute set corresponding to user u, $\mathrm{StrGen}(S'_u)$ is to formulate access policy (the attribute of visitor u), and Γ'_{com} is the access policy.

When the medical user receives the treatment plan from the proxy doctor, the medical user will first verify the validity of the signature. According to the public key $Y_0, Y_1, \cdots, Y_n$ of the proxy signer and the given anonymous proxy signature σ, the verifier verifies whether it is valid or not:

$$e\left(nR' + V\sum_{i=1}^{n}(Y_0 + Y_1), \sigma\right) = e(P, H(m_w))e\left((n-1)R' + H_0(m_w, R)\widehat{Y}, \sigma_s\right). \tag{5}$$

If the equation is true, the verifier accepts the treatment plan; otherwise, it is considered that the plan is not credible and can refuse to believe the treatment plan.

2.3. Research on Privacy Protection Based on AI. With the continuous development of AI research, neural network has been widely used in computer vision, voice recognition, medical diagnosis, and other fields, attracting more and more attention. As we all know, the training and prediction of neural network need the support of data. However, data always inevitably contains sensitive and confidential information [25]. Therefore, while neural network brings convenience to our life, it also brings hidden dangers of privacy disclosure. How to use neural network without revealing privacy information has become an important research field.

CNN is a special neural network, which is good at analyzing visual images and widely used in image and video recognition, classification, and natural language processing. CNN mainly includes convolution layer, pooling layer, activation layer, and full connection layer. At each position, convolution kernel and input do dot product operation. Generally, the more convolution kernels, the more information will be extracted, and the higher the accuracy rate will be. However, the greater the amount of calculation, the lower the efficiency will be.

The structure of CNN is shown in Figure 4:

CNN has the characteristics of sharing parameters and local connection. Compared with fully connected neural networks, CNN has the advantages of being good at capturing position deviation and having fewer parameters, which effectively reduces the overfitting phenomenon in fully connected neural networks. In this chapter, aiming at the problem of CNN prediction, a CNN privacy protection prediction protocol based on homomorphism only is proposed, which can effectively ensure that the input features, model parameters, and intermediate values are not leaked during the prediction process.

In this scheme, all participants are semihonest; that is to say, all participants are honest in implementing the agreement, but they will collect and infer private information from the agreement (Figure 5).

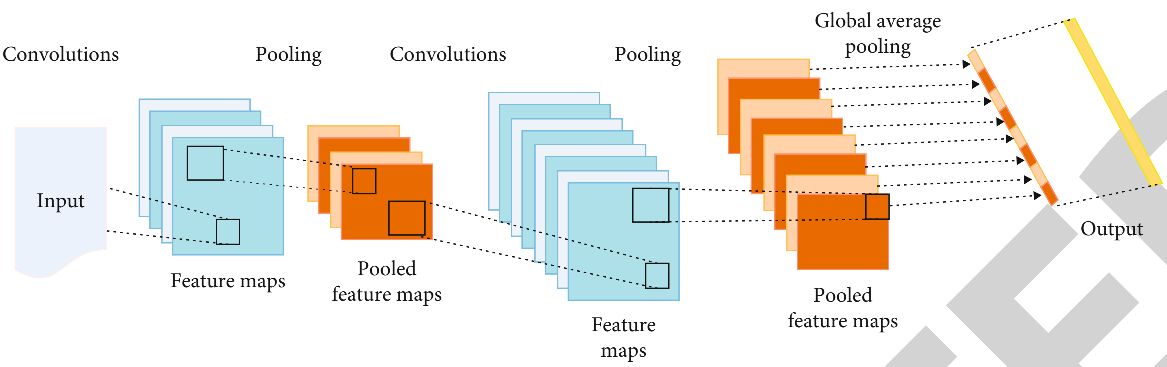

Figure 4: CNN structure.

In our protocol, users encrypt their own feature matrix $\vec{x}$ with their own public key PK and send $[\vec{x}]$ to the server for prediction. The server has a trained model parameter, $\overrightarrow{w^{\text{conv}}}, \overrightarrow{b^{\text{conv}}}$. In CNN, convolution layer and fully connected layer are the processes of calculating dot product; so, the server can use privacy protection dot product protocol and homomorphism to complete the calculation of convolution layer and fully connected layer [26].

Details of the privacy protection CNN agreement in this chapter are as follows.

User's input: private key SK, public key PK, and feature matrix $\vec{x}$

Server's input: the public key PK and the trained model parameter $\vec{w}$, $\vec{b}$

User's output: $m^* = \arg\max_{0\le j\le k-1} o_j^{fc}$

Our privacy protection max protocol needs the interaction between users and servers as the cost to realize the privacy protection calculation of activation function. The activation layer is generally used after convolution layer and full connection layer to make nonlinear mapping to the output result of the previous layer [27].

In the protocol, if the activation layer is located behind the fully connected layer, the server generates a 0 matrix with the same size as the output of the fully connected layer of the previous layer and encrypts it to obtain $[\vec{0}]$. For each neuron, the server acts as participant B with ciphertext $[\overrightarrow{o^{fc}}]$, $[a_2](a_2 = 0)$ as input, and the user acts as participant A with private key SK and public key PK as input, and the server can finally obtain ciphertext $[\overrightarrow{h^{act}}] \longleftarrow \max([\overrightarrow{o^{fc}}], [\vec{0}])$ of the activation result.

3. Results Analysis and Discussion

New AI technology is constantly emerging, and some privacy data cannot take into account its application scenarios and application scope when it is accumulated; so, we cannot ask for the opinions of the collected data in advance, and when it is necessary to use its data, it is difficult to ask for opinions one by one in many cases, especially when seemingly harmless data is used. Therefore, many contradictions can be avoided by using the new AI technology, that is, doing a good job of identifying and predicting the data usage rights in the process of data aggregation and seeking the opinions of the parties in advance.

In this section, the calculation time of several kinds of encryption is tested separately. This scheme uses the 128-bit AES (Advanced Encryption Standard) algorithm to encrypt file data symmetrically. At the same time, the 1024-bit RSA algorithm is used to encrypt the session key.

In addition, encryption tests were carried out on data of different sizes from 1 KB to 40 KB, each experiment was repeated 1000 times, and the minimum time, average time, and maximum time for encryption of data of different sizes were compared, as shown in Figure 6.

Through observation, it can be seen that the encryption time is almost the same when the data amount is 1 KB to 19 KB. Because the user's body data is large, the data from 28 KB to 55 KB are used for simulation. Through observation, it can be seen that the curve increases linearly after 10 KB. Therefore, users can transmit data of any size according to their needs.

The RSA algorithm was used to encrypt and decrypt 128 bit session key for 8 times, with an average encryption time of 17 ms and an average decryption time of 98 ms. The encryption and decryption time test of the RSA algorithm is shown in Figure 7.

The PBFT (Practical Byzantine Fault Tolerance) system is not completely open, because PBFT algorithm needs to enable nodes to verify each other's messages and accurately grasp the number of nodes. Even the most practical PBFT algorithm cannot be extended to more than 1,000 nodes. In addition, the PBFT algorithm uses message verification code, which requires each node to verify the message once every vote. A large number of signatures and verifications are another potential bottleneck.

In the transaction, the PBFT algorithm is used to calculate the hash value, and the elliptic curve digital signature algorithm is used to sign. The generation time of five kinds of transactions was tested separately, and each experiment was conducted 1000 times, as shown in Figure 8.

In view of the problems existing in the PBFT algorithm, combined with the actual situation of blockchain, a set function conversion mechanism is added, and the number of

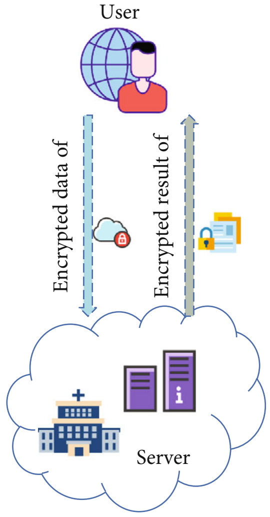

Figure 5: System model.

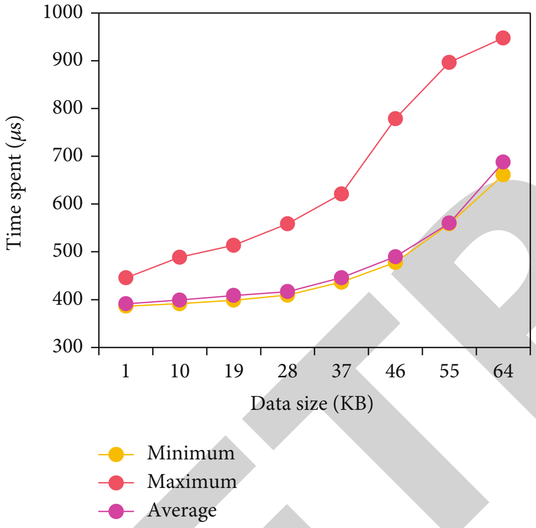

Figure 6: AES algorithm encryption time test.

nodes in two sets is as equal as possible. When one third of the nodes in the consensus node set fail, the candidate node set will take over the consensus task to ensure the consensus work to continue. One broadcast communication in view conversion is reduced, network bandwidth consumption in view conversion is reduced, and view conversion efficiency is improved.

Transaction delay is the time from the client initiating the request to the client confirming the completion of the whole process. In order to ensure the accuracy of the experiment as much as possible, the value of transaction delay is the average of 8 transaction tests. Because the improved algorithm in this chapter divides nodes into consensus nodes and candidate nodes equally, and only consensus nodes participate in consensus, the number of nodes should not be less than 8. Figure 9 compares the transaction delay of the two algorithms.

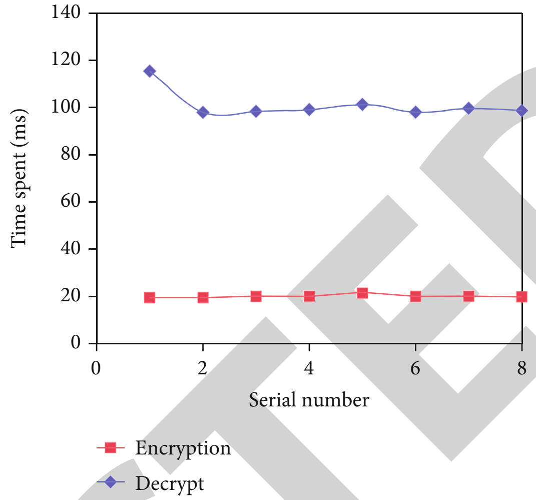

Figure 7: Test of encryption and decryption time of the RSA algorithm.

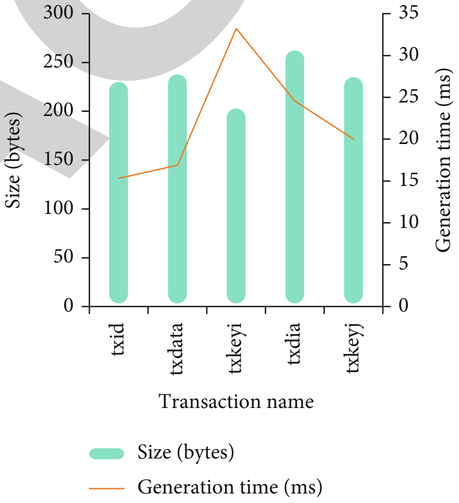

Figure 8: The size and generation time of the transaction.

As can be seen from Figure 9, with the increase of the number of nodes, the transaction delay of PBFT increases almost linearly, but the growth of improved algorithm is not obvious. Overall, the efficiency of improved algorithm is obviously higher than that of PBFT algorithm.

In this experiment, set the number of requests sent by the client to 1000, test the transaction volume per second, and set the number of nodes in the program to different values for the experiment. The throughput comparison results of the two algorithms are shown in Figure 10.

With the increase of the number of nodes, the throughput of the two algorithms is declining, but compared with the two algorithms, the throughput of the improved algorithm is still much higher than that of the PBFT algorithm.

In order to test the feasibility of CNN privacy protection protocol proposed in this chapter, we use MNIST handwritten digital data set to test the accuracy and efficiency of the protocol in this chapter. The MNIST dataset consists of 0-9 handwritten digital pictures and corresponding labels, with

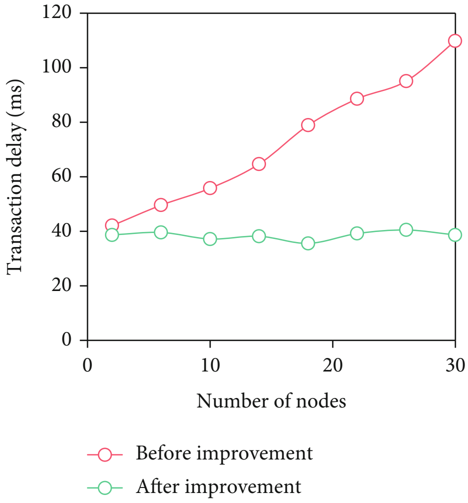

FIGURE 9: The transaction delay of the two algorithms is compared.

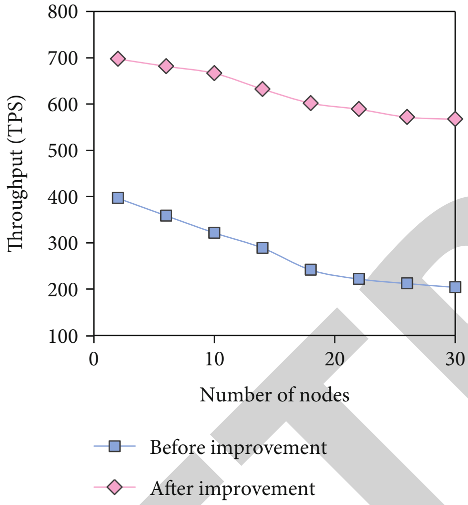

FIGURE 10: Throughput comparison.

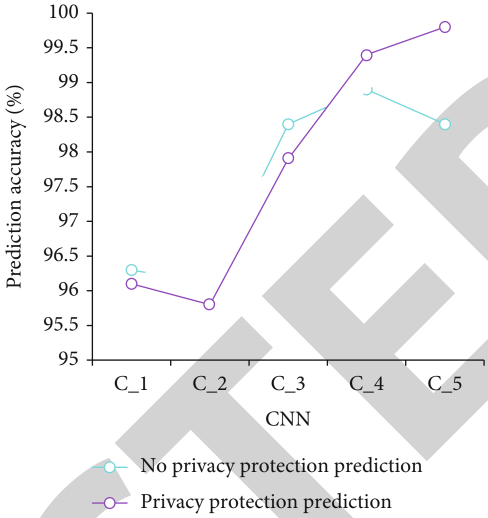

FIGURE 11: Prediction accuracy on data set.

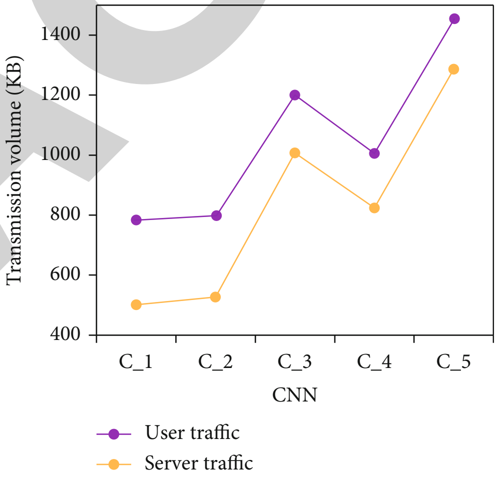

FIGURE 12: Transmission amount of privacy protection protocol.

60,000 training samples and 10,000 test samples. All pictures are composed of 28 × 28 × 1 pixel values, and each pixel value is an integer between 0 and 255.

Our five CNN were trained with 60,000 training samples from MNIST data set and 50,000 training samples from CIFAR-10 data set, named as C_1, C_2, C_3, C_4, and C_ 5, respectively. After the training, 50 test samples of MNIST data set are used to test this protocol on five CNN that have been trained.

By applying the above five C_1, C_2, C_3, C_4, and C_5 predictions, the prediction accuracy on MNIST handwritten data set without privacy protection and with this privacy protection protocol is shown in Figure 11.

It can be seen that the prediction accuracy is closely related to CNN's network structure, and the prediction accuracy can be improved by appropriately increasing the number of CNN's network layers, the number of convolution kernels in convolution layer, and the number of neurons in fully connected layer. Easy, the accuracy of CNN is related to the number of model parameters. Generally speaking, the more model parameters, the higher the accuracy.

The prediction accuracy without privacy protection is the same as that with this privacy protection protocol; that is, this protocol will not affect the prediction accuracy; so, in actual use, the prediction accuracy of CNN can be improved by adjusting the training parameters of the network (iteration times, optimization algorithm, etc.) and adjusting the network structure (convolution kernel number, network layer number, etc.).

The transmission capacity of the privacy protection protocol of this paper applied to five different CNN privacy protection protocols is shown in Figure 12.

It is easy to know that the running time of this protocol is related to the complexity of the network structure, which is determined by the number of network layers, convolution kernels, and the number of neurons in each layer. The most time-consuming operations in the prediction stage are convolution operation and full connection operation, while the running time of pooling operation is short. With the increase of the activation layer, the number of interactions increases, and the transmission volume increases correspondingly. With the increase of the data volume in one interaction, the transmission volume increases correspondingly.

4. Conclusion

As a new medical model, intelligent medical care can actively apply computer technology and provide targeted medical services on the basis of combining people's needs, which has certain positive significance for the modernization and intelligent development of medical care in China. With the continuous development of AI research, neural network has been widely used in computer vision, voice recognition, medical diagnosis, and other fields, attracting more and more attention. This paper completes the design of privacy protection scheme of medical service data based on blockchain. The nodes in the system are divided into consensus node set and candidate node set, and the mechanism of node integral ascending and descending is introduced. The traditional distributed database is used to store the original data, the proxy reencryption is used to complete the encryption of the original data, and the data records are stored in the blockchain, which ensures the data privacy to a certain extent and reduces the pressure of the blockchain. At the same time, a privacy protection training protocol based on homomorphism and a cloud-assisted privacy protection prediction protocol are proposed. The cost of participants can be effectively reduced by using the cloud server for corresponding calculation. Experimental results show that the scheme in this paper is efficient and achieves high accuracy.

Encrypting and storing the access records of each node in the chain are convenient for medical institutions to jointly supervise and manage, but it is also a test for the security and performance of hash algorithm and asymmetric encryption algorithm used for encryption in blockchain. If we can quickly encrypt and decrypt the underlying data without lowering the security, it will be the greatest help for medical data sharing, and it will also be the focus of this research in the future.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no competing interest.

Acknowledgments

This paper is supported by the "research on criminal law guarantee system of network security in China from the perspective of new development concept and overall national security concept" (No. 21AZD082) and the "research on the criminal law guarantee of the safe development of artificial intelligence under the perspective of new development concept" (No. 21YJ820017).

References

[1] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "AuthPrivacyChain: a blockchain-based access control framework with privacy protection in cloud," *IEEE Access*, vol. 8, pp. 70604–70615, 2020.

[2] M. Shen, Y. Deng, L. Zhu, X. du, and N. Guizani, "Privacy-preserving image retrieval for medical IoT systems: a blockchain-based approach," *IEEE Network*, vol. 33, no. 5, pp. 27–33, 2019.

[3] M. Shen, X. Tang, L. Zhu, X. du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7702–7712, 2019.

[4] Y. Qi, M. S. Hossain, J. Nie, and X. Li, "Privacy-preserving blockchain-based federated learning for traffic flow prediction," *Future Generation Computer Systems*, vol. 117, no. 2946, pp. 328–337, 2021.

[5] H. A. Kurdi, S. Alsalamah, A. Alatawi, S. Alfaraj, L. Altoaimy, and S. H. Ahmed, "HealthyBroker: a trustworthy blockchain-based multi-cloud broker for patient-centered eHealth services," *Electronics*, vol. 8, no. 6, p. 602, 2019.

[6] S. Wang, D. Zhang, and Y. Zhang, "Blockchain-based personal health records sharing scheme with data integrity verifiable," *IEEE Access*, vol. 7, pp. 102887–102901, 2019.

[7] B. S. Egala, A. K. Pradhan, V. R. Badarla, and S. P. Mohanty, "Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11717–11731, 2021.

[8] R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang, and Z. Wang, "Flexible and efficient blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system," *Access*, vol. 7, pp. 88012–88025, 2019.

[9] I. T. Javed, F. Alharbi, T. Margaria, N. Crespi, and K. N. Qureshi, "PETchain: a blockchain-based privacy enhancing technology," *Access*, vol. 9, pp. 41129–41143, 2021.

[10] 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.

[11] J. Wang, K. Han, A. Alexandridis et al., "A blockchain-based eHealthcare system interoperating with WBANs," *Future Generation Computer Systems*, vol. 110, pp. 675–685, 2020.

[12] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O. Y. Song, A. K. Bashir, and A. A. Abd El-Latif, "DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems," *Access*, vol. 8, pp. 111223–111238, 2020.

[13] F. Tang, S. Ma, Y. Xiang, and C. Lin, "An efficient authentication scheme for Blockchain-based electronic health records," *IEEE Access*, vol. 7, pp. 41678–41689, 2019.

[14] R. Li and H. Asaeda, "A blockchain-based data life cycle protection framework for information-centric networks," *IEEE Communications Magazine*, vol. 57, no. 6, pp. 20–25, 2019.

[15] T. Nóbrega, C. Pires, and D. C. Nascimento, "Blockchain-based privacy-preserving record linkage: enhancing data privacy in an untrusted environment," *Information Systems*, vol. 102, p. 101826, 2021.

[16] Y. Yin, Y. Li, B. Ye, T. Liang, and Y. Li, "A Blockchain-based incremental update supported data storage system for intelligent vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4880–4893, 2021.

[17] A. Li, G. Tian, M. Miao, and J. Gong, "Blockchain-based cross-user data shared auditing," *Connection Science*, vol. 34, no. 1, pp. 83–103, 2022.

[18] B. Xu, D. Han, P. Liu et al., "Enhanced luminescence property of InGaN/GaN nanorod array light emitting diode," *Optical Engineering*, vol. 58, no. 4, p. 1, 2019.

[19] B. Chen, L. Wu, H. Wang, L. Zhou, and D. He, "A Blockchain-based searchable public-key encryption with forward and backward privacy for cloud-assisted vehicular social networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5813–5825, 2020.

[20] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE Network*, vol. 32, no. 6, pp. 184–192, 2018.

[21] A. A. Abdellatif, A. Z. Al-Marridi, A. Mohamed, A. Erbad, C. F. Chiasserini, and A. Refaey, "ssHealth: toward secure, blockchain-enabled healthcare systems," *IEEE Network*, vol. 34, no. 4, pp. 312–319, 2020.

[22] S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere, and S. P. Mohanty, "Interoperability and synchronization management of blockchain-based decentralized e-health systems," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1363–1376, 2020.

[23] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A secure and efficient blockchain-based data trading approach for internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9110–9121, 2019.

[24] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the internet of things," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 12–18, 2018.

[25] M. Elhoseny, N. N. Thilakarathne, M. I. Alghamdi et al., "Security and privacy issues in medical Internet of Things: overview, countermeasures," *Challenges and Future Directions. Sustainability*, vol. 13, no. 21, p. 11645, 2021.

[26] N. N. Thilakarathne and D. Wickramaaarachchi, "Improved hierarchical role based access control model for cloud computing," 2020, arXiv preprint arXiv:2011.07764.

[27] T. T. Kuo and L. Ohno-Machado, "Modelchain: decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks," 2018, arXiv preprint arXiv:1802.01746.