Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8832341, 9 pages
https://doi.org/10.1155/2020/8832341

Research Article

A Homomorphic Encryption and Privacy Protection Method Based on Blockchain and Edge Computing

Xiaoyan Yan, Qilin Wu, and Youming Sun

School of Information Engineering, ChaoHu College, Chaohu 238000, China

Correspondence should be addressed to Youming Sun; symtnt@163.com

Received 23 May 2020; Revised 13 July 2020; Accepted 25 July 2020; Published 18 August 2020

Academic Editor: Hongju Cheng

With its decentralization, reliable database, security, and quasi anonymity, blockchain provides a new solution for data storage and sharing as well as privacy protection. This paper combines the advantages of blockchain and edge computing and constructs the key technology solutions of edge computing based on blockchain. On one hand, it achieves the security protection and integrity check of cloud data; and on the other hand, it also realizes more extensive secure multiparty computation. In order to assure the operating efficiency of blockchain and alleviate the computational burden of client, it also introduces the Paillier cryptosystem which supports additive homomorphism. The task execution side encrypts all data, while the edge node can process the ciphertext of the data received, acquire and return the ciphertext of the final result to the client. The simulation experiment proves that the proposed algorithm is effective and feasible.

1. Introduction

Network data will be encrypted before they are sent to the server, but the client will face some problems because the service provider needs to perform computation on the data to respond to the requests of the client; so the client must provide the server with the key to decrypt data before implementing necessary computation, which may affect data confidentiality in the cloud. Blockchain is a group of inalterable and well-organized blocks (data blocks), and it records the logs of all transactions. The data blocks in blockchain are saved in every node in the form of file system. Every block includes the data of several transactions, the number of which included in different blocks may vary [1, 2]. Blocks are connected with Hashed-link, and every header includes the Hash of all transactions in this block and the pre-Hash of the last header. Such a chained architecture can ensure that the data in each block are unalterable and so is the sequential relationship between blocks. This characteristic has decided that the blocks can only be added to the tail. But the rigid and single organizational form of data in blockchain has impeded blockchain's applications in relevant fields with demanding data security requirements [3]. Edge computing is now gradually being given more and more attention in academic circles, organizations for standardization, and open-source platforms, and it has been developed rapidly in many aspects. Related enterprises have initiated relevant industry organizations, industry alliances, and organizations for standardization in specific application fields, deployed edge computing, and proposed some suggestions on architecture [4]. Besides, the open-source projects related to edge computing have also developed gradually. Homomorphic encryption is a method that computes on encrypted data. It gets the same result from the computation of the original data, and it uses proxy reencryption technology to protect the selected ciphertext from being attacked. To sum up, in order to protect the security of network environment, the use of blockchain and edge computing technology can reinforce the privacy protection and provide corresponding protection to the user information, transaction activities, and information communication [5, 6].

The special contributions of this paper are as follows:

(i) This paper has analyzed and studied in blockchain and edge computing network, the data blocks, application nodes, edge computing nodes, and terminal,

and it has combined all data blocks into a blockchain, which is maintained by all edge computing nodes

(ii) It has introduced the edge computing model and designed the blockchain-based distributed privacy protection architecture. In order to guarantee the operating efficiency of blockchain and ease the computing burden of the client, it allows some edge nodes which have certain computing, storage and communications ability to write data into the chain, and maintain and update the entire blockchain

(iii) In order to solve the data security problems in escrow, it has presented a homomorphic encryption technique based on the Paillier and RSA cryptosystems, in which the execution encrypts all data received and the edge nodes operate on the ciphertext of the data received, get the ciphertext of the final result, and return it back to the client

(iv) Through the simulation experiment, it has shown the effectiveness and operating time efficiency against hostile attacks of the proposed algorithm, and it has also analyzed the impact different values of parameters play on the update of target value

The rest of this paper is organized as follows. Section 2 discusses related work, followed by the basic framework of blockchain, and its data structure is introduced in Section 3. The edge computing architecture is discussed in Section 4. Section 5 is the homomorphic encryption and privacy protection. Section 6 shows the simulation experimental results, and Section 7 concludes the paper with summary and future research directions.

2. Related Work

After integrating P2P transmission, on-chain consensus algorithm, digital signature, and encryption algorithm, blockchain in recent years has become a focal point in the research and discussion of many international organizations and national governments that have increased their input in research. As the focus of blockchain does not lie in zone boundary but the participants, blockchain is highly sensitive to malicious adversaries, so in the internet operating environment, blockchain has strong adaptability [7]. Homomorphic encryption is extensively applied to support simple aggregation, numerical computation of encrypted data, and retrieval of private information. The breakthrough in homomorphic encryption theory has led to fully homomorphic encryption, which can compute arbitrary functions of encrypted data [8]. Homomorphic encryption is generally considered as a key approach to solve database query problems on the basis of encrypted data. The requirements of privacy for the digital data and algorithms used to process more complex structures have increased exponentially, which just parallels to the growth of communications network and equipment and their capacities [9]. Whether the decentralized network architecture or the constructed distributed architecture, they can directly establish a trust relationship between system architecture and nodes through mathematical methods, without operating the third-party trust platform. The applications of mathematical algorithms in building security mechanism can improve the transparency of information; so they will not suffer from the influence of any factors. Blockchain is not strongly dependent on cipher; as a matter of fact, it can operate safely without cipher, and it does not need the trust mechanism. With no cipher, blockchain without any doubt does not need encryption key. The protection for blockchain can be ensured through mathematical algorithms, and the security function obtained is permanent and all information in the block can be safeguarded permanently. The chain-block structure in blockchain has provided trusted timestamp in information storage, enabling the data information recorded to have a time dimension, and the data to be traceable and validated and making it very difficult to tamper all information in the blocks [10, 11].

Wang and others have created effective storage engine, ForkBase, for blockchain and fork applications, while Xu and others have studied verifiable query processing of blockchain database and presented the verification system Vchain that supports blockchain data inquiring the scope of Boolean. Helmer and others have developed a system, EthernityDB, which can integrate the function of a database into the Ethereum blockchain [12]. It has kept all data in the chain and guaranteed the consistency, invariability, and security of data. In 2015, some supports for edge computing have established the OpenFog Consortium (OGC) and released the Edge Computing Reference Architecture 2.0 in 2017. In 2016, some firms have set up the Edge Computing Consortium (ECC) and published many versions of edge computing reference architecture, in order to promote the digital innovation and applications of edge computing [13]. In 2014, the European Telecommunications Standards Institute (ETSI) has proposed Mobile Edge Computing (MEC) as an important part of 5G. In 2018, the Industrial Internet Consortium (IIC) has also issued the Edge Computing Architecture used in Industrial Internet of Things. The Open Source Project–EdgeX has constructed an open-source edge computing architecture and described the criteria to use this architecture in its open-source page. Yao has come up with the first secure two-party computing problem in as early as 1982, i.e., the Millionaire Problem [14]. Afterwards, the secure multiparty computation (SMC) emerged. The Paillier system is a semantically secure homomorphic public key cryptosystem; so it is generally used to construct fundamental protocols for secure multiparty computation, including Millionaire Protocol, scalar product protocol, and OT protocol. Sander and Tschudin have defined the additive and multiplicative homomorphic encryption scheme in the ring of integers. The additive and multiplicative homomorphism has made sure that the computation result of two encrypted variables is the same as that of the original variables. Currently, the management of blockchain data has come across the following difficulties. The organization form of the current blockchain data is coarse-grained so it supports a single way of query, and it cannot meet the requirements of the current data analysis and information digging. The present

data privacy protection scheme in blockchain technology cannot satisfy the needs of secure storage and retrieval of sensitive data. This paper has mainly studied the security of the application of blockchain-based homomorphic encryption to edge computing, including the probability to implement encrypted data computation under various malicious attacks.

3. Basic Framework of Blockchain and Its Data Structure

Blockchain is mainly composed of data layer, network layer, consensus layer, and application layer. Among them, data layer includes the underlying data block and its chain structure, and as it is supported by the relevant techniques such as the Hash algorithm, timestamp, Merkle tree, and asymmetric encryption, it protects the integrity and traceability of bock data. Network layer consists of data transmission mechanism and transaction verification mechanism and supported by P2P network technology; it accomplishes the data transmission and verification between distributed nodes. Consensus layer is mainly the consensus mechanism, and it realizes the consistency between distributed nodes and the authenticity of data through various consensus algorithms. Some blockchain systems, e.g., the consensus layer of Bitcoin, also contain issuing mechanism and incentive mechanism which integrates economic factors. It enters blockchain technology to achieve the stable consensus between nodes. Application layer can realize various top-level application scenarios, relevant systems, and smart contracts supported by a wide range of on-chain script algorithms and blockchains, laying a foundation for the programmable functions of blockchain. In this framework, blockchain incorporates the timestamp-based chain structure, the data transmission mechanism based on P2P network, the consensus mechanism of distributed nodes, and the flexible programmable on-chain script, and blockchain is also the most representative technical innovation [15, 16]. The basic architecture of blockchain is shown as Figure 1.

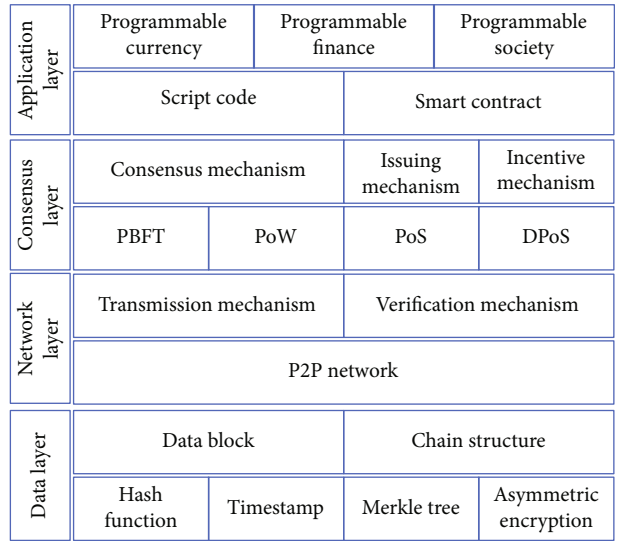

Figure 1: Basic framework of blockchain.

The core structure of the data information management system based on blockchain technology is decentralization, which has effectively changed the data risk brought by conventional central authority. Thanks to its nontemperability and traceability, blockchain technology can be widely applied in information data management and meanwhile ensures the accuracy and authenticity of data information. Generally speaking, it is necessary to integrate blockchain technology with external database and separate the data from the corresponding authority, in order to assure the normal use in the decentralized system. When the relative programs need an access to the data information of users, user consent must be obtained. Understandably, when an application program needs an access to the information, blockchain will receive its request. To confirm whether the program can access the information, the record in the blockchain needs to be checked. If the system check is undergone, blockchain will record the implemented operation and feed-back to the application. It is because blockchain has certain recording function that the operations in the entire process are transparent, which is good for the traceability of the follow-up data and makes sure the security of network information. Besides, attention must be paid to the integrity of network information data [17].

Blockchain stores data through data blocks and chain structure. Every data block includes two parts: header and body, and each block has the only Hash value corresponding to the block address. The current block is connected to the previous one by saving the Hash value of the previous block and forming a chain structure, as shown in Figure 2. The header encapsulates the Hash value of the previous block as well as timestamp, Merkle tree root value, and other information. The body stores information, i.e., the data information recorded by the blockchain. All data are generated based upon the Hash processing of Merkle tree so as to generate the only Merkle tree root value and save it in the header. Such a storage structure of Merkle tree has greatly improved the efficiency of inquiring and verifying information as well as the scalability. Meanwhile, when a block is generated, there will be a timestamp to mark and indicate the time of generating a block [18]. As the enhancement of timestamp, this block is continuously extended to form a chain with a time dimension so that the data are traceable and the data traceability is guaranteed.

The secure Hash algorithm refers to the technology to develop information encryption and others. When computing the relevant data, the difficulty of the entire computation is generally determined by the plus-minus of the Hash value computed. If the Hash value is positive, it indicates that the entire computation process is easy to operate; otherwise, the computation is relatively difficult. Blockchain network mainly constructs tree structure of data information by using the Hash tree computing method. In this structure, the node is the abovementioned Hash values in order to check abundant information data to ensure its authenticity and integrity [19]. The data model of the internal structure of blockchain is shown in Figure 3.

As shown in this blockchain architecture, it is clear that when there is a change in the information of a certain block,

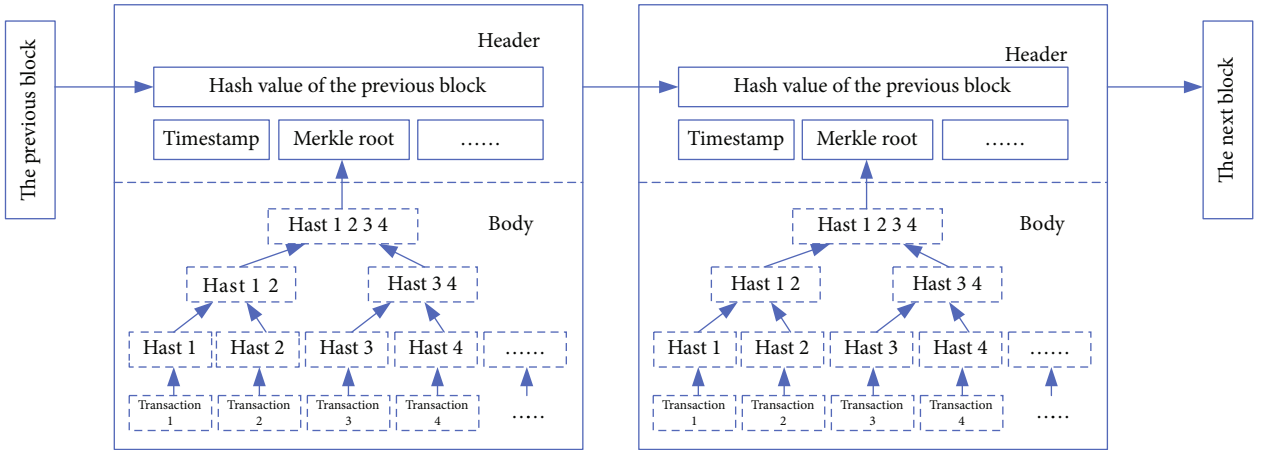

Figure 2: Data structure of blockchain.

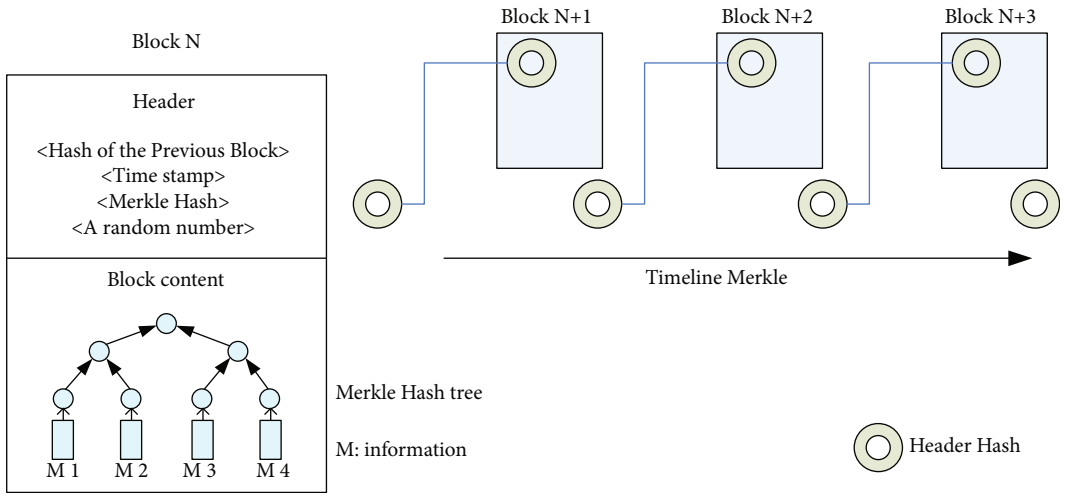

Figure 3: Data model of internal structure of blockchain.

the Hash value of the corresponding Merkle changes correspondingly, followed by a change in the information contained in the block. If a bad intruder tampers the information, the computing power will not generate support for fake data block. If the speed of fake block exceeds the growth rate of blockchain, it will be abandoned. In every block, the information is data information, and the content it covers not just includes text information, but also nonlinear information, e.g., video information, image information, and various structured information. It can permanently protect the information stored in all blocks to prevent malicious alteration. Therefore, the information in blockchain is secure [9].

4. Edge Computing Architecture

Edge computing refers to the new-type computation model which implements computation in the network edge, which includes any computation and network resources along the path from the data source to cloud computing center. Edge computing model is to transfer part or all of computational tasks of the original cloud computing center to near the data source for implementation. Edge computing model and cloud computing model complement with each other. In the environment of Internet of everything, computing efficiency cannot meet real-time requirements due to the increase of data amount and the mass data generated by users. The conventional cloud computing model can no longer effectively satisfy the needs of the current application program; instead, it needs to transfer the computing tasks of the original cloud center to the network edge device, improve data transmission performance by using the computing ability of edge device, assure real-time processing, and reduce computing load and energy consumption [20].

In edge computing, the downstream data of the edge represents cloud service and the upstream data the service of Internet of everything, while the edge in edge computing refers to any computation and network resources along the path from the data source to the cloud computing center. Cloud computing center collects data not only from database but also from such edge devices as sensors and smartphones. These devices have taken into consideration both data

generator and consumer. Therefore, the request transmission from terminal device to cloud center is two-way. Network edge devices not only ask for content and services from the cloud center but also implement some computing tasks, including data storage, processing, caching, device management, and privacy protection. Therefore, it is necessary to better design the hardware platform for edge devices as well as the key software technology so as to meet the demands of reliability and data security of edge computing model [21, 22]. In Figure 4, data generator sends the source data to the cloud center, and the final user sends the use request to the cloud center, which feedbacks the usage result to the final user.

5. Homomorphic Encryption and Privacy Protection

Each blockchain node in the blockchain network stores the same blockchain [23, 24]. The blockchain is composed of multiple blocks [25, 26]. The origination block includes the block head and the block body [27, 28]. The block head stores the input information characteristic value, version number, timestamp, and difficulty value, and the block body stores the input information. The next block of the origination block is the parent block, and the next block also includes the block head and the block body, so that each block is in the blockchain. The block data stored in the block is associated with the block data stored in the parent block, which ensures the security of the input information in the block. The steps of this algorithm are as follows.

Step 1 (generate the key). Initialize random primes p and q and meet the condition of

$$\gcd(pq, (p-1)(q-1)) = 1. \tag{1}$$

Calculate modulus

$$n = pq. \quad \lambda = 1\mathrm{cm}(p-1, q-1), \tag{2}$$

where lcm is to seek the least common multiple of $p-1$ and $q-1$.

Select the random number $g(g \in Z_{n2}^*)$ and meet

$$\mu = \left(L\left(g^{\lambda} \bmod n^2\right)\right)^{-1} \bmod n. \tag{3}$$

Seek the greatest common divisor of $L(g^{\lambda} \bmod n^2)$ and n. Z_{n2}^* represents the set of integers coprime to n^2 in Z_{n2}. The encrypted public key of function $L(x) = x - 1/n$ is (n, g), and the private key is (λ, ω).

In the encryption and decryption process, select the integer $r(r \in Z^*{}_{n2})$, and the plaintext is $m(m \in Z_n)$ and $m < n$.

Step 2 (encryption⟶Enc (m, pk)). Let m be the information to be encrypted and $m \in Z_n$.

Compute the ciphertext: $c = m \bmod n$. The encryption process is

$$c = E(m) = g^m \cdot r^n \bmod n^2, \tag{4}$$

where c is the ciphertext data corresponding to the plaintext m and $c \in Z^*{}_{n2}$.

Mark the encryption algorithm as $c = E(m, r)$. It can be known that for the same ciphertext m, the value of r, which is randomly selected in the encryption process may be different and so is the corresponding ciphertext data after being encrypted so as to ensure the semantic security of ciphertext data.

Step 3 (proxy reencryption). Compute the public key and private key (R_{sk}, R_{pk}).

The reencryption ciphertext is generated by the RSA algorithm, and the public key (R_{pk}) is sent to the server.

Step 4 (decryption⟶Dec (c, sk)). Ciphertext $c \in Z_n$

$$m = D(c) = L\left(c^{\lambda} \bmod n^2\right) * (\omega \bmod n). \tag{5}$$

After receiving $E(d_i)(i \in p_\tau)$, decrypt it to $\mathrm{get}(d_i)(i \in p_\tau)$, sign it, get and send $Sign_q(d_i)(i \in p_\tau)$ to EN_q.

Step 5 (after EN_q receives $(d_i)(i \in p_\tau)$, divide the degree of dispersion into two kinds). Make the set of users corresponding to the kind with more elements as Q and the set of users corresponding to the degree of dispersion as G. As malicious users take up a small proportion, Q mainly includes normal users with the target value increases after the completion of tasks, while that of G decreases after tasks end. Therefore, it has introduced two parameters μ and ν to control the increase and decrease after the target value is updated, and the target value changes according to the following equation:

$$r_i^{new} = \begin{cases} r_i + (1 - r_i) \cdot \mu & \text{if} \in Q \\ r_i \cdot (1 - \nu) & \text{if} i \in G \end{cases}, \tag{6}$$

where μ and ν are both positive and $\nu < 1$.

When the execution side is transmitting the storage address and key of data file, the asymmetric encryption algorithm RSA is adopted. The data encrypted by RSA public key can only be decrypted by the party which holds the corresponding RSA private key. Therefore, this scheme has ensured the secure transmission of data storage address and decryption key. When acquiring data, it only needs to collect from distributed file system according to the address here data files are saved. Both parties do not make contacts directly, which conceals the identities of both parties and protects their privacy. In the data hand-over process of normal transactions, other people except both parties have no knowledge of the storage address of the data file, and even they can the address through certain means, what they get

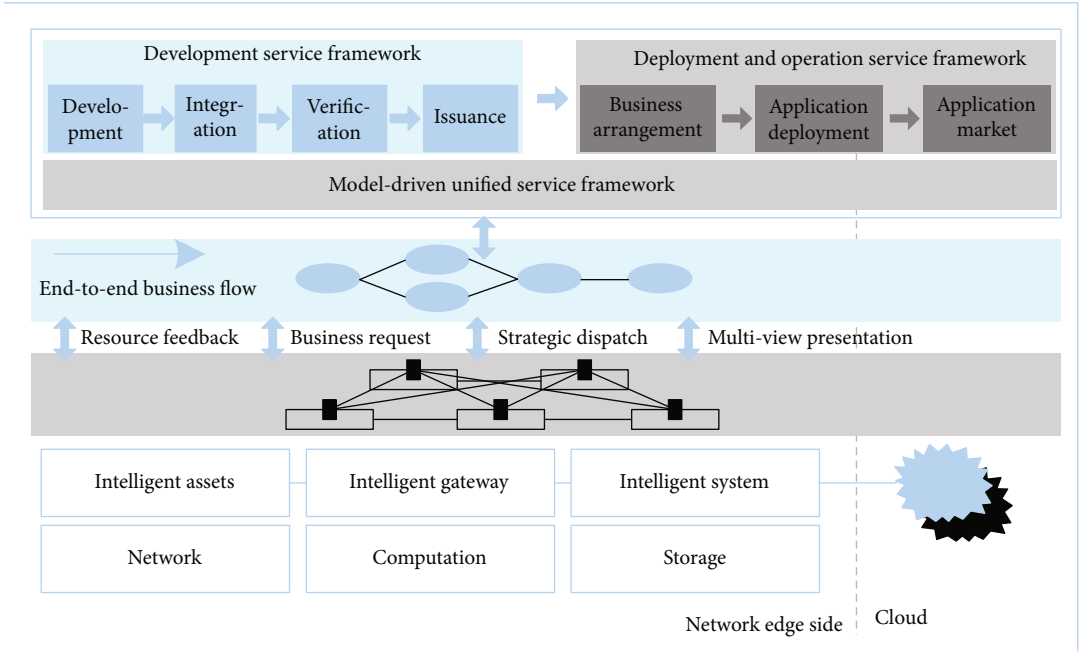

Figure 4: Edge Computing Reference Architecture.

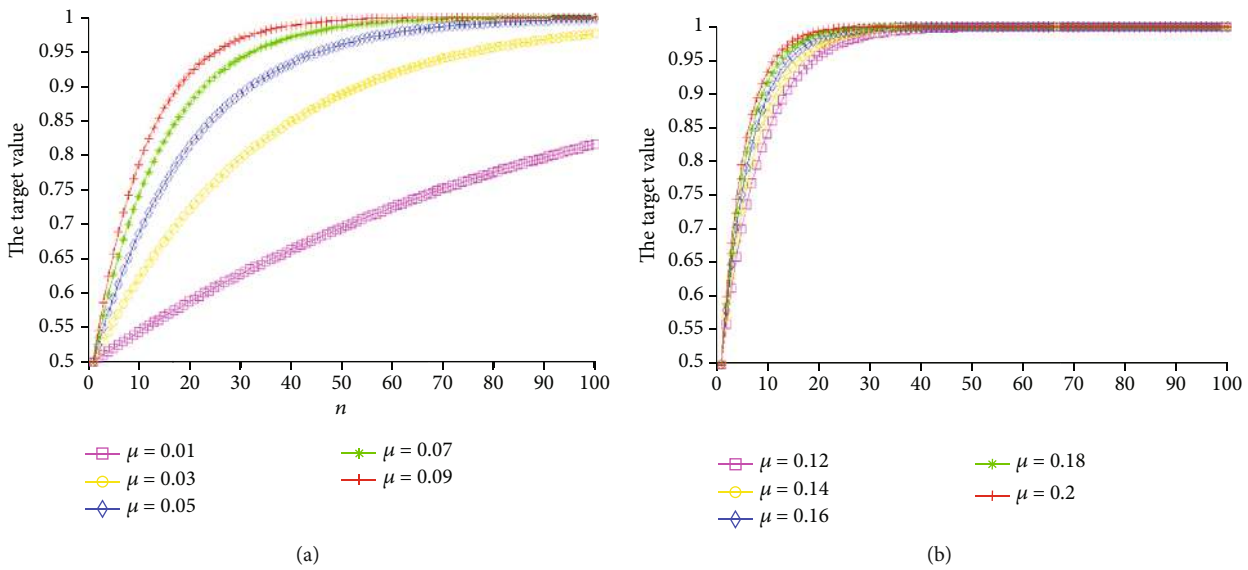

Figure 5: Impact of different μ on target value.

is the ciphertext. So, during the data handover, the security of the data is guaranteed, and the privacy of both parties of the data is protected.

6. Test Experiment and Analysis

The blockchain technology of the algorithm in this paper is implemented based upon Hyperledger Fabric, and probably 120 blocks can be generated every minute. As for the realization of the Paillier cryptosystem, we have used open-source Paillier Library and operated in the virtual machine of Ubuntu 64-bit operating system.

The data in this paper is a 10-dimensional vector. The task executor first gets a 10-dimensional data vector. Then, it encrypts every element in the vector and sends the encrypted result to the edge node of the zone where it is located. According to equation (6), parameter μ determines the growth rate of target value when the task executor provides accurate data, while parameter ν decides the decrease rate of target value when wrong data received is provided. Figure 5 shows the change of target value over the increase of tasks n when the execution side always provides the accurate data received, and the values of μ are 0.01, 0.03, 0.05, 0.07, 0.09, 0.12, 0.14, 0.16, 0.18, and 0.2. μ determines the

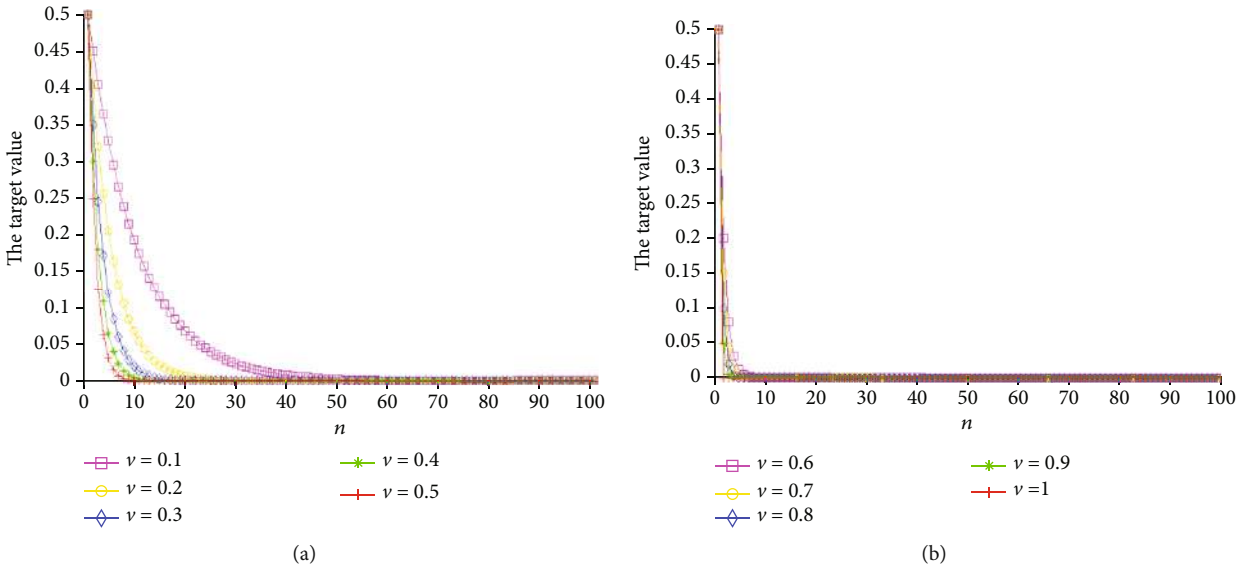

Figure 6: Impact of different ν on target value.

speed at which the target value of users that provide accurate data received is converged to 1. Besides, the bigger the value of μ, the faster its target value is converged to 1. However, when μ is too big, the user only needs to provide very few accurate data received to get a higher target value. In practical applications, μ is usually 0.1~0.2.

Next, analyze the impact of ν on the target value. Figure 6 has shown the change of the target value of users that provide wrong data received over the increase of tasks n. Here, the value of ν is 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, and 1. When the user continuously provides wrong data received, the parameter ν determines the rate of the target value converged to 0. Moreover, the bigger the value of ν, the faster the target value is converged to 0. However, the value of ν cannot be too big. To resist malicious attacks, the value of ν cannot be too small. Practically speaking, the value of ν is generally 0.2~0.5.

In the encryption process, the time consumed is the computation between the fusion of encrypted data and the degree of dispersion of data. So, let t_{ed} and t_{dd} represent the time to encrypt data and the time to calculate the encrypted degree of dispersion, respectively, and n represents the number of tasks to be executed. Figure 7 is the change of t_{ed} over n, and Figure 8 shows the change of t_{dd} over n.

As shown in Figure 7, t_{ed} grows linearly over the increase of n. Obviously, the bigger n, the more data ciphertext to be processed and the bigger t_{ed}. The reason is that when encrypted data, the necessary ciphertext operation is linearly correlated to the number of task executors n. When $n = 5$, the average time needed for the processing result is 2.82 s, and when n is 120, the time becomes 38.26 s. In Figure 8, when n also changes from 5 to 120 at the same step-length, t_{dd} basically remains the same over the increase of n.

This algorithm combines the characteristics of blockchain and edge computing network, and a large number of legitimate edge computing nodes ensure the security of data. On the premise of making full use of edge computing resources, it can achieve a wide range of data collection and

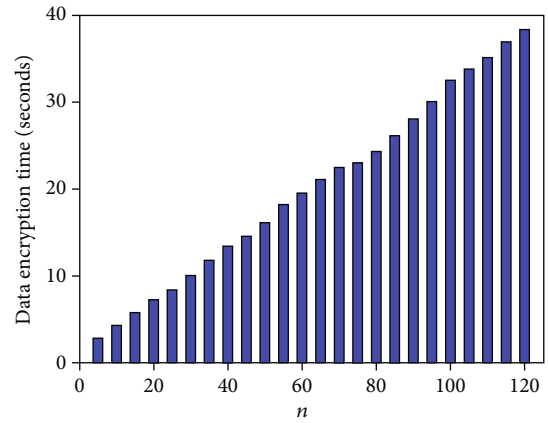

Figure 7: Change of data cipertext processing time t_{ed} over the number of tasks n.

analysis, storing fully and publicly output data resources for any organization, enterprise, and individual to query, and reuse without worrying about data tampering or deletion; and finally, realizing data security, data openness, and data in the process of data resource management source traceability and nontemperability, data utilization has been improved.

7. Conclusion

As an Internet-based new-type computing paradigm, edge computing has always been a hot field which attracts consistent attention from the academia and industry. Blockchain is a decentralized brand-new distributed computing paradigm. It is a promising research topic to apply blockchain technology in edge computing and use the security mechanism of the former to improve the performance of secure storage and computation of the latter. In order to meet the noncorrelation, anonymity, and supervision of identity privacy in blockchain system, this paper has introduced edge computing and

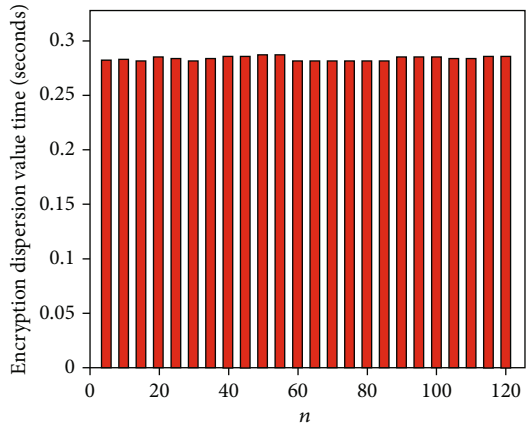

Figure 8: Change of time calculating the degree of dispersion t_{dd} over the number of tasks n.

fully-homomorphic Paillier cryptosystem, designed the blockchain-based distributed privacy protection architecture, and analyzed and verified that the algorithm in this paper can better achieve the goals of encryption and privacy protection through theoretical research and experiment result, laying a foundation for the subsequent 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 there are no conflicts of interest regarding the publication of this study.

Acknowledgments

The finding is sponsored by the Scientific Research Project of Chaohu College (Grant No. XLZ-201807) and Anhui Key Research and Development Plan (Grant No. 201904a05020091).

References

[1] C. Ye, D. Xu, and X. Liang, "Overview of network security technology based on blockchain," *Telecommunication Science*, vol. 34, no. 3, pp. 10–16, 2018.

[2] S. Moin, A. Karim, Z. Safdar, K. Safdar, and M. Imran, "Securing Iots in distributed blockchain: analysis, requirements and open issues," *Future Generation Computer Systems*, vol. 100, no. 11, pp. 325–343, 2019.

[3] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: a lightweight scalable blockchain for IoT security and anonymity," *Journal of Parallel and Distributed Computing*, vol. 134, no. 12, pp. 180–197, 2019.

[4] S. Weisong, Z. Xingzhou, W. Yifan, and Z. Qingyang, "Edge-computing: the most advanced and future direction of the country," *Journal of Computer Research and Development*, vol. 56, no. 1, pp. 69–89, 2019.

[5] P. P. Ray, D. Dash, and D. De, "Edge computing for internet of things: a survey, E-healthcare case study and future direction," *Journal of Network and Computer Applications*, vol. 14015, no. 8, pp. 1–22, 2019.

[6] C. Li, Y. P. Wang, H. Tang, Y. Zhang, and Y. Luo, "Flexible replica placement for enhancing the availability in edge computing environment," *Computer Communications*, vol. 14615, no. 10, pp. 1–14, 2019.

[7] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: a survey on applications and security privacy challenges," *Internet of Things*, vol. 8, no. 12, pp. 100–107, 2019.

[8] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based Iot systems: integration issues, prospects, challenges, and future research directions," *Future Generation Computer Systems*, vol. 97, no. 8, pp. 512–529, 2019.

[9] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.

[10] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A Survey on Privacy Protection in Blockchain System," *Journal of Network and Computer Applications*, vol. 12615, no. 1, pp. 45–58, 2019.

[11] Y. Chen, H. Xie, K. Lv, S. Wei, and H. Changzhen, "DEPLEST: a blockchain-based privacy-preserving distributed database toward user behaviors in social networks," *Information Sciences*, vol. 501, no. 10, pp. 100–117, 2019.

[12] R. Thakore, R. Vaghashiya, C. Patel, and N. Doshi, "Blockchain - based IoT: a survey," *Procedia Computer Science*, vol. 155, no. 1, pp. 704–709, 2019.

[13] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, and J. P. Jue, "All one needs to know about fog computing and related edge computing paradigms: a complete survey," *Journal of Systems Architecture*, vol. 98, no. 9, pp. 289–330, 2019.

[14] S. Vimal, M. Khari, N. Dey, R. G. Crespo, and Y. Harold Robinson, "Enhanced resource allocation in mobile edge computing using reinforcement learning based MOACO algorithm for IIOT," *Computer Communications*, vol. 1511, no. 2, pp. 355–364, 2020.

[15] S. Tuli, R. Mahmud, S. Tuli, and R. Buyya, "FogBus: a blockchain-based lightweight framework for edge and fog computing," *Journal of Systems and Software*, vol. 154, no. 8, pp. 22–36, 2019.

[16] E. Wang, D. Li, B. Dong, H. Zhou, and M. Zhu, "Flat and hierarchical system deployment for edge computing systems," *Future Generation Computer Systems*, vol. 105, no. 4, pp. 308–317, 2020.

[17] J. Yang, Z. Lu, and W. Jie, "Smart-toy-edge-computing-oriented data exchange based on blockchain," *Journal of Systems Architecture*, vol. 87, no. 6, pp. 36–48, 2018.

[18] Y. Qian, Y. Jiang, J. Chen, Z. Yu, and M. Pustišek, "Towards decentralized IoT security enhancement: a blockchain approach," *Computers & Electrical Engineering*, vol. 72, no. 11, pp. 266–273, 2018.

[19] S. Li, W. Chen, Y. Chen, C. Chen, and Z. Zheng, "Makespan-minimized computation offloading for smart toys in edge-cloud computing," *Electronic Commerce Research and Applications*, vol. 37, no. 9, p. 100884, 2019.

[20] S. Sahmim, H. Gharsellaoui, and S. Bouamama, "Edge computing: smart identity wallet based architecture and user

centric," *Procedia Computer Science*, vol. 159, no. 1, pp. 1246–1257, 2019.

[21] M. Qiu, S.-Y. Kung, and K. Gai, "Intelligent security and optimization in edge/fog computing," *Future Generation Computer Systems*, vol. 107, no. 6, pp. 1140–1142, 2020.

[22] H. Liang, Z. Jialing, Z. Kai, and K. M. Junaid, "An improved genetic algorithm optimization fuzzy controller applied to the wellhead back pressure control system," *Mechanical Systems and Signal Processing*, vol. 142, no. 1, article 106708, 2020.

[23] X. Chonghuan, "A novel recommendation method based on social network using matrix factorization technique," *Information Processing & Management*, vol. 54, no. 3, pp. 463–474, 2018.

[24] F. Hu and W. Gang, "Distributed error correction of EKF algorithm in multi-sensor fusion localization model," *IEEE Access*, vol. 8, no. 1, pp. 93211–93218, 2020.

[25] W. Wei, H. Song, W. Li, P. Shen, and A. Vasilakos, "Gradient-driven parking navigation using a continuous information potential field based on wireless sensor network," *Information Sciences*, vol. 408, no. 2, pp. 100–114, 2017.

[26] D. Jiang, G. Li, Y. Sun, J. Kong, and B. Tao, "Gesture recognition based on skeletonization algorithm and CNN with ASL database," *Multimedia Tools and Applications*, vol. 78, no. 21, pp. 29953–29970, 2019.

[27] L. Dong, Q. Guo, and W. Wu, "Speech corpora subset selection based on time-continuous utterances features," *Journal of Combinatorial Optimization*, vol. 37, no. 4, pp. 1237–1248, 2019.

[28] H. Liang, Z. Dialing, L. Zhiling, K. M. Junaid, and Y. Lu, "Dynamic evaluation of drilling leakage risk based on fuzzy theory and PSO-SVR algorithm," *Future Generation Computer Systems*, vol. 95, pp. 454–466, 2019.