







# Towards Decentralized Privacy-Preserving of Encrypted Data Sharing Protocol

Sheng Peng<sup>1,2</sup><sup>a</sup>, Linkai Zhu<sup>3,\*</sup><sup>b</sup>, Wennan Wang<sup>1</sup><sup>c</sup>,  
Shanwen Hu<sup>4</sup><sup>d</sup>, Shiyang Song<sup>5</sup><sup>e</sup> and Baoping Wang<sup>1</sup><sup>f</sup>

<sup>1</sup>Academy of Management, Guangdong University of Science and Technology, Dongguan, China

<sup>2</sup>Zhuhai Yingying Technology Co., Ltd Zhuhai, China

<sup>3</sup>Information Technology School, Hebei University of Economics and Business, Shijiazhuang, China

<sup>4</sup>Institute of Data Science, City University of Macau, Macau

<sup>5</sup>Alibaba Cloud Big Data Application College, Zhuhai College of Science and Technology, Zhuhai, China

**Keywords:** ECC Elliptic, Data Sharing, Blockchain, Privacy-Preserving.

**Abstract:** We propose a blockchain node data secure method based on encryption and blockchain that addresses conventional privacy preserving methods are inaccurate and time-consuming issues. The encrypted data sharing protocol will be established, and the blockchain technology will be used to make the data encrypted in the decentralized ledger based on the data transfer protocol. Private information from non-blockchain sources will be encrypted using the AES symmetric encryption algorithm and securing the privacy. As a result of the simulation experiments, the proposed method is more accurate in privacy preserving and provides faster work efficiency.


## 1 INTRODUCTION


The privacy of network data may be compromised by centralized communication control mechanisms. The privacy preserving is a complex issue in various fields (Bahri et al., 2018). It is possible to find many loopholes in a network system that is not completely protected against security threats. Internet companies still face greater risks, even though some have invested more manpower and material resources in network data security (Javaid et al., 2021). As a non-decentralized system, cloud computing storage poses risks associated with cybersecurity, including private information leakage. Since cloud storage relies on trust, the trust of user is a key point in the network space security.


As described in (Xu et al., 2021) a honeypot encryption algorithm can be used to protect personal privacy data, as well as to address the issue of simple


code for securing bank information for users and digit code using personal electronic wallets. This paper discusses honeypot encryption algorithm security using artificial intelligence algorithm. It has been shown that honeypot encryption has a higher security level than password-based encryption, and decoy messages generated by the algorithm are difficult to distinguish from real messages. In spite of this, privacy data protection takes a long time using the above method.

It is now widely believed that most data exchange and sharing methods are based on the concept of centrally located servers as of today. Among the various cloud computing technologies, the cloud storage and cloud sharing technologies all rely on this technical principle. As an example, if an individual is searching for information about a specific government affairs matter through the government affairs portal platform, the centralized sharing


<sup>a</sup> <https://orcid.org/0000-0001-7007-7722>

<sup>b</sup> <https://orcid.org/0000-0001-7609-3651>

<sup>c</sup> <https://orcid.org/0000-0001-6957-4078>

<sup>d</sup> <https://orcid.org/0000-0001-8517-236X>

<sup>e</sup> <https://orcid.org/0000-0003-4440-781X>

<sup>f</sup> <https://orcid.org/0000-0002-6240-5009>

\* Corresponding Author

platform collects data from each department in accordance with the list of materials related to the matter, or each department sends data on a regular basis to the centre, so that the issue of sharing government affairs information does not arise. There will be plenty of problems arising from the centralization of data sharing, but two of the most pressing ones will be the protection of data privacy and security. It is traditional for data sharing parties to be aware of shared data. A traditional sharing method is prone to several problems including: The traditional method of sharing data makes it easy for the party sharing the data to lose ownership of the data, and once the personal information has been shared, it faces the risk of unlimited dissemination once it has been shared. This makes it difficult to establish liability for data infringement in cases where the data was abused. Consequently, most data owners are not able or unwilling to participate in data exchanges, resulting in a lack of data being exchanged as a consequence. The bottleneck has hindered the sharing of information as well as interaction between users.

Data security users face privacy and scalability issues when using blockchain technology. All transactions must be collectively verified through a consensus process before being accepted into a blockchain network (Maldonado-Ruiz et al., 2020). Members maintain copies of their ledgers and each member maintains a copy of the ledger. Internet data security users can benefit from blockchain technology in the following ways. Blockchains eliminate the need for trust between participants because the distributed ledger is tamper-proof. We propose a method based on trusted computing and blockchain to address the issue of low-accurate and consumes a large amount of energy long-term in old privacy preserving methods. The amount of information existing on the blockchain is encrypted using ECC elliptic curve encryption algorithm, while the data that is on the non-block chain is encrypted using AES symmetric encryption algorithm, thus providing complete privacy preserving.

## 2 ENCRYPTED DATA SHARING PROTOCOL

A blockchain-decentralized node must be used to share monitoring data among many terminals that receive data over the network. To ensure the effectiveness and efficiency of the communication system, it is imperative that the communication is

conducted credibly, and security and credibility of each network node are the foundation for it. This protocol is used to hand over and collect encrypted data on a one-to-one basis.

In the data sharing process in blockchain, these steps are as follows:

(1) By signing its own *PCR* using the node identity private key, the next-level blockchain node sends it to the blockchain node; once the signature has been received, the off-chain node confirms the identity key to ensure it was created by the trusted module. The *PCR* value is then compared to the value of a trusted *PCR* stored locally. Based on the consistency of the message, a node in a controlled and safe operation state is determined to be the source.

$$S = f_{PIK_{Pr+LN}}(PCR) \quad (1)$$

$$f_{PIK_{Pr+LN}}(S) = f_{PIK_{Pr+LN}}(f_{PIK_{Pr+LN}}(PCR)) = PCR \quad (2)$$

$$PCR = PCR_{exp} \quad (3)$$

(2) A random value nonce is generated and sent to the blockchain node when it is authenticated.

(3) Blockchain nodes will have relatively little sharing data to share. To encrypt the sharing data, the trusted module generates the symmetric key  $Key_{SM4}$  within the node. After encrypting  $SN_{pub}$  using the digital envelope method,  $Key_{SM4}$  gets  $EKey$  by using the sub-energy router, and  $Updata$  is obtained by stringing these two together.

$$Edata = f_{Key_{SM4}}(SensorData) \quad (4)$$

$$EKey = f_{SN_{pub}}(Key_{SM4}) \quad (5)$$

$$Updata = Edata || EKey \quad (6)$$

(4) As well as encrypting the data, the sensor node calculates *PCR* to obtain the signature *Quote*, then send the signature *Quote* to the blockchain off-chain node.

$$Quote = f_{PIK_{Pr+LN}}(PCR, nonce, Updata) \quad (7)$$

(5) Data  $S$  is received by the decentralized node, and the signature *Quote* is verified. To verify the accuracy and credibility of the data source, we need to verify the signature using the public key of the off-chain node;

$$VerifyQuote = f_{PIK_{Pr+LN}}(f_{PIK_{Pr+LN}}(PCR, nonce, Updata)) = (PCR, nonce, Updata) \quad (8)$$

(6) The information packets and keys are then decrypted, retrieved, and a successful data upload is reported back to the sensor node.

$$Dec(Ekey) = f_{PIK_{Pr+LN}}(Key_{SM4}) = Key_{SM4} \quad (9)$$

(7) If in the event that the blockchain is not able to verify any of the sensor nodes, the data packet will

be discarded, and the sensor nodes will receive an upload failure message.

### 3 PRIVACY PRESERVING IN BLOCKCHAIN SYSTEM

#### 3.1 Blockchain Technology

A blockchain typically has six layers (Zhu et al., 2022), namely the application layer, the data layer, the contract layer, the network layer, the incentive layer, and the consensus layer. Each layer is responsible for a different aspect of the blockchain as a whole. The structure of the privacy preserving blockchain system is shown in Figure 1.

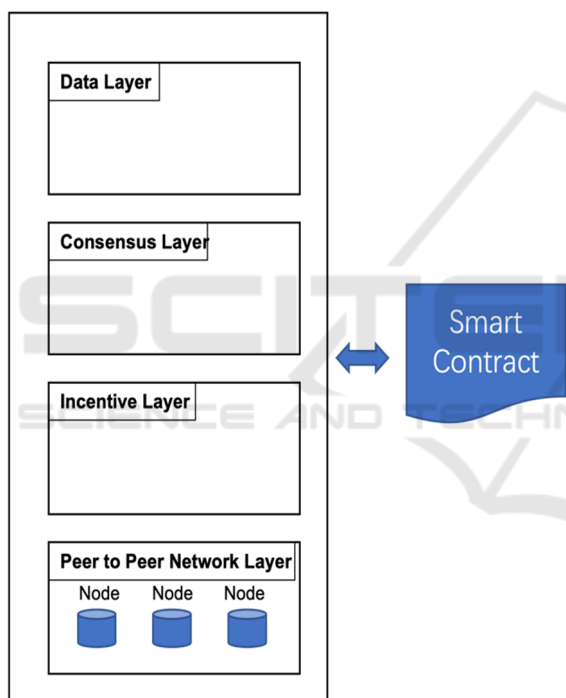


Figure 1: Blockchain network structure

A number of advantages can be attributed to blockchain technology.

(1) Traceability. It is convenient for collaborators to conduct reliable auditing, tracing and tracking of data changes in the blockchain since each data change in the blockchain will record the author's clear identification, time and other relevant information.

(2) Data uniformity. Rather than relying on scattered data sources that require constant verification, different participants in the blockchain utilize a unified data source.

(3) Data sharing. In order to improve coordination and collaboration between all parties, blockchain technology allows participants to upload and share the latest statuses, views, and business information in real time, thereby enhancing communication and coordination between all parties.

A practical Byzantine algorithm (PBFT) (Javaid et al., 2021) consists of having each node in the network emulate the transaction contents of a new block in order after it is added to the current block chain. The nodes in the blockchain network receive the contents of the new block and emulate their transactions in order. In the network, every node receives information regarding the transactions contained in the latest block and emulates these transactions in order. The hash value of the block is calculated by taking the results of these runs and then distributing them to all the nodes in the network as soon as the runs are completed. The existence of this node will then be communicated to all the nodes in the network. It is important to mention that the Byzantine algorithm is practical because it operates even in the presence of a few malicious nodes and still maintains the security of the system.

Despite the presence of a few malicious nodes in a network, the practical Byzantine algorithm is able to maintain the security and proper operation of the system, allowing the system to have fault tolerance, and also making the In spite of a few malicious nodes in the network, the Byzantine algorithm maintains the security and proper operation of the system. This algorithm, however, is not successful when there are more than 30% of malicious nodes in a network and therefore has limitations when most of the nodes are malicious.

#### 3.2 Blockchain Data Privacy Preserving Method

An important prerequisite to facilitate active data sharing among parties without a trust base on the Internet is the ability to exchange trust-based data between the parties. The cryptography-based system is able to prevent data leakage and untrustworthiness during data exchange by effectively preventing privacy data leaks. To present a data trustworthy exchange scheme involving asymmetric encryption, multiple signatures and homomorphic encryption in cryptography, this chapter proposes a combination of asymmetric encryption, multiple signatures, and homomorphic encryption under the decentralized platform of block ripen in order to achieve data traceability, encryption and decryption, and data security sharing. In addition, we ensure the

confidentiality of the shared data by encrypting it and obtaining its ciphertext in order to protect the private data that can't easily be disclosed, and using an improved homomorphic encryption algorithm, we are able to ensure that the data is kept confidential. By calculating the ciphertext, we are able to achieve the desired result without disclosing the original data, and as a result, the data holders can share and exchange the data without infringing on their ownership.

On Information on blockchain nodes is protected by a secure sharing protocol, which ensures that the privacy of the information is preserved (Peng et al., 2021). This method of mathematically verifying the authenticity of electronic documents and information is called a digital signature. The verifier can be confident that the identity of the sender of the data and that the data has not been altered by a legitimate digital signature. In other words, by utilizing digital signature technology, both the origin and ownership of the data file, as well as the integrity of the data file, can be verified. Blockchain technology can be utilized in order to protect private data from outside invasion and intruders in addition to offering two types of encryption algorithms. The first is the ECC elliptic curve encryption algorithm, which encrypts data already on the blockchain, while the second is the AES symmetric encryption algorithm, which protects non-blockchains.

A private key is represented by *privateKey*, and a public key is represented by *publicKey*. Here are the expressions:

$$privateKey = SHA256(message) \quad (10)$$

$$publicKey = Secp256(privateKey) \quad (11)$$

There are two algorithms involved in every block of the blockchain, Secp256 and SHA256, both of which represent elliptic curve algorithms commonly found in blockchain technology.

A symbiotic relationship exists between several factors, which involves the duration of each round, the size of the block, the pace at which transactions propagate, the block generation interval, and the security of each block, all of which are influenced by the restriction relationship. Therefore, Block size, round length, transaction propagation speed, and the way blocks are generated should all be adapted to the specific restrictions. By using both the public key and the private key, network data is protected on a periodic basis.

## 4 SIMULATION EXPERIMENT ANALYSIS

Data for the experiment is taken from a company that provides electricity of power user information database. There are two thousand records in the privacy database. Several levels and tuples of privacy data sets are classified within the privacy data sets. Considering the fact that power users have access to information that can be used for conducting privacy experiments, the number 10 is chosen using the method described in this paper and the method of differential protection proposed in the literature.

In Using the method discussed in this paper to protect 2000 private data, we compare and analyse the time required to protect the data in this paper to the time required by the privacy preserving method proposed in the literature (Diallo et al., 2022) using differential protection in software development databases. In Figure 2, we can see the result of the comparison;

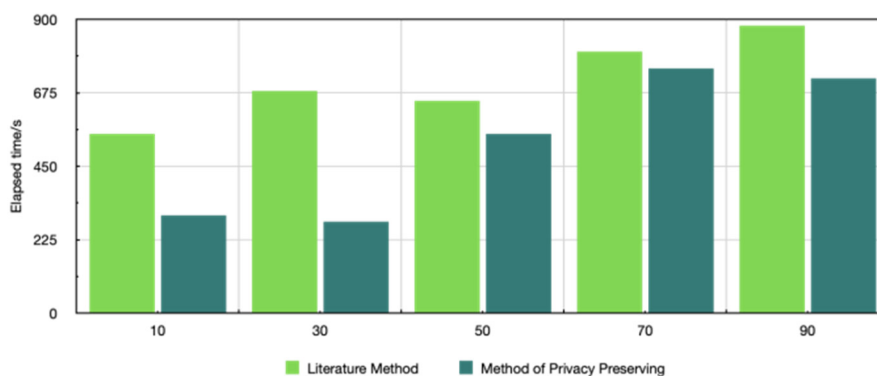


Figure 2: Comparison results of consumption time

The experimental results indicate that the method in this paper consumes more time as the private data

set tuples increase, it is important to note, however, that the rate of increase of private data set tuples is

slower, and the maximum consumption of private data sets is around 750s. It becomes increasingly difficult to maintain software development databases as the level of privacy is raised.

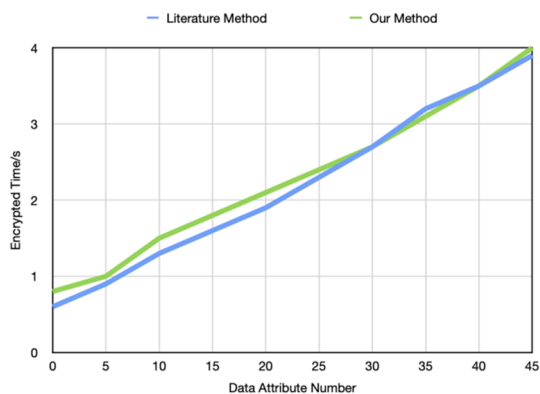


Figure 3: The relationship between the running time of the encryption algorithm and the number of data attributes

It can be observed from Figure 3 that an increasing number of attributes causes the encryption algorithm to take longer to run, thereby increasing its running time. The actual message can still be decrypted within a shorter time period than the scheme proposed in the literature as the literature scheme encrypts not only the actual message, but also a random message for verification, whereas this scheme only encrypts the actual message. This paper shows that the method is faster and more efficient, because the number of information tuples increases promptly, approximately 900 seconds are consumed during the process. Our proposed method consumes significantly less time than the comparison method as the number of experiments increases. This solution has been proven to be safe and efficient after rigorous security analysis and performance analysis has been performed.

## 5 CONCLUSIONS

A large amount of data is generated every second by a wide variety of Internet-connected devices. The privacy of users will be a major concern with this data. People's private data will be increasingly collected and processed, posing serious security and privacy concerns. Security and privacy challenges are exacerbated by several inherent deficiencies of the blockchain network, including centralization is lacking and heterogeneous equipment resources. A major issue of the Internet is the security of data and

privacy of users, which inhibits the deployment of the Internet on a large scale. As a result of the existing data exchange platform, it is not easy for users and enterprises to share their private data with one another. A third-party platform is able to easily backup and restore the most important data, and it faces the threat of being mishandled by malicious users or organizations after sharing the data, which means the data owners lose the ownership of important information, and face a difficult time pursuing redress if the private information is compromised. The purpose of this paper is to propose methods to solve the problem of privacy data leakage and the problem of data security in the process of sharing data in traditional platforms using data encryption and decryption, traceability authentication and secure exchange functions. Also, it is to explore and demonstrate a method for protecting private data with trusted computing and blockchain technologies that prevents the leakage of personal information due to an unauthorized access by third parties, while also guaranteeing the security of private data, thus creating a stable basis for the protection of network data.

## ACKNOWLEDGEMENTS

This research is supported by the project funded by Zhuhai Industry University Research Cooperation and Basic and Applied Basic Research Project in 2020: Research on Key Technologies of Cross-domain Data Compliance and Mutual Trust Computing in Zhuhai and Macao (No. ZH22017002200011PWC), in part by MOST-FDCT Projects (0058/2019/AMJ,2019YFE0110300) (Research and Application of Cooperative Multi-Agent Platform for Zhuhai-Macao Manufacturing Service), and in part by the National Natural Science Foundation of China and Macao Science and Technology Development Joint Fund (0066/2019/AFJ).

Part of the material has been used in the article (Zhu et al., 2021). This work adds many contents and also modifies the shortcomings of the previous version.

## REFERENCES

Bahri, L., Carminati, B., & Ferrari, E. (2018). Decentralized privacy preserving services for Online Social Networks. *Online Social Networks and Media*, 6, 18–25. <https://doi.org/10.1016/j.osnem.2018.02.001>



- Diallo, E., Dib, O., & Al Agha, K. (2022). A scalable blockchain-based scheme for traffic-related data sharing in VANETs. *Blockchain: Research and Applications*, 3(3), 100087. <https://doi.org/10.1016/j.bcr.2022.100087>
- Javaid, M., Haleem, A., Pratap Singh, R., Khan, S., & Suman, R. (2021). Blockchain technology applications for Industry 4.0: A literature-based review. *Blockchain: Research and Applications*, 2(4), 100027. <https://doi.org/10.1016/j.bcr.2021.100027>
- Maldonado-Ruiz, D., Torres, J., & El Madhoun, N. (2020). 3BI-ECC: A Decentralized Identity Framework Based on Blockchain Technology and Elliptic Curve Cryptography. 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 45–46. <https://doi.org/10.1109/BRAINS49436.2020.9223300>
- Peng, S., Zhu, L., Cai, Z., Liu, W., He, C., & Tang, W. (2021). Dynamic Optimization of Government Data Transmission Based on Blockchain Technology. *Mobile Information Systems*, 2021, e8948323. <https://doi.org/10.1155/2021/8948323>
- Xu, L. D., Lu, Y., & Li, L. (2021). Embedding Blockchain Technology Into IoT for Security: A Survey. *IEEE Internet of Things Journal*, 8(13), 10452–10473. <https://doi.org/10.1109/JIOT.2021.3060508>
- Zhu, L., Peng, S., Cai, Z., Liu, W., He, C., & Tang, W. (2021). Research on Privacy Data Protection Based on Trusted Computing and Blockchain. *Security and Communication Networks*, 2021, e6274860. <https://doi.org/10.1155/2021/6274860>
- Zhu, L., Song, S., Peng, S., Wang, W., Hu, S., & Lan, W. (2022). The Blockchain and Homomorphic Encryption Data Sharing Method in Privacy-Preserving Computing. 2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD), 84–87. <https://doi.org/10.1109/BCD54882.2022.9900530>