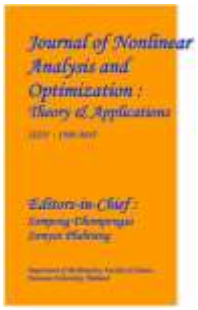
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**



BLOCKCHAIN-BASED MODEL FOR PERSONAL PRIVACY DATA PROTECTION SCHEME FOR CLOUD ENVIRONMENTS

K. UDAY KIRAN[1], **D.N.V.S. AKASH** [2]

[1]Assistant Professor, Dept. of MCA, QIS College of Engineering and Technology, Ongole, Andhra Pradesh.

[2]PG Scholar, Dept. of MCA, QIS College of Engineering and Technology, Ongole, Andhra Pradesh.

ABSTRACT— With the frequent occurrence of private data breaches, it is now more necessary than ever to address how to protect private data. The combination of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and blockchain typically enables secure storage and sharing of data. However, in highdimensional attribute domains, that is, the number of attributes is large, these schemes have issues such as low security of data protection, high computational overhead, and high cost of attribute revocation. This paper proposes a personal privacy data protection scheme for encryption and revocation of high-dimensional attribute domains to address these issues. The proposed scheme is made up of three components. Firstly, Fast High-dimensional Attribute Domain-based Message Encryption (HAD-FME) is proposed to improve data security and reduce computational cost. Secondly, an Attribute Revocation Mechanism Based on Sentry Mode (SM-ARM) is designed in combination with smart contracts. Lastly, a Blockchain-based Model for Personal Privacy Data Protection (BC-PPDP) is proposed by integrating HAD-FME with SM-ARM. The security analysis results show that HAD-FME proposed in this paper is secure under the DLIN assumption, and the attribute revocation satisfies both forward and backward security. Experiments show that HADFME has higher computational efficiency than existing schemes in the high-dimensional attribute domains, SM-ARM has lower revocation cost than existing attribute revocation mechanisms, and smart contracts and blockchain work well.

Index Terms – Privacy data, blockchain, attribute-based encryption, data storage and sharing, attribute revocation.

I. INTRODUCTION

The rapid development of technologies such as cloud computing and the Internet of Things (IoT) has led to the generation of a large amount of personal data worldwide. Enterprises continuously collect and analyze these personal data, providing them with professional services and generating significant economic benefits, enabling users and enterprises to gain huge profits from the information society. Unfortunately, in recent years, enterprises' lack of data protection measures, such as storing data in plaintext on their centralized servers, has led to an increasing number of personal data leakage incidents. Therefore, sharing and storing private data in a secure manner is critical. Blockchain, as a decentralised ledger database, due to its characteristics of decentralization and difficulty in tampering with data, can provide a trustworthy data storage and sharing environment. Currently, many researchers have used blockchain in various fields, including data storage, the Internet of Things, healthcare, transactions, and payments. At the same time, many scholars have done a lot of research on tamper-resistance ledger databases. However, if the data owner explicitly stores information related to private data on the blockchain, any user can access the data information. This may result in the data owner losing control over personal data. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) was proposed as a solution by Bethencourt. In CP-ABE, the data owner can choose the ciphertext access method, in which the access policy is included in the ciphertext and the user attribute set is embedded in the key. The decryption process can only be completed when the user attribute set meets the access policy. In this paper, the set of attributes and the number of attributes is referred to as the attribute domain and attribute domain dimension, respectively. The Fast Attribute-based Message Encryption (FAME) and other CP-ABE algorithms were subsequently proposed Compared with the scheme FAME is constructed using asymmetric prime-order bilinear groups, which have stronger security requirements. In order to achieve secure storage, distribution, and control of personal data, several data protection schemes have been proposed by combining blockchain and CP-ABE. In order to provide access control for IoT data, Zhang et al. proposed a

blockchain-based access control list and paired it with CP-ABE.

In order to provide users with a safe storage environment, Sharma et al. proposed a decentralized cloud storage architecture based on blockchain, which uses CP-ABE to encrypt data. Assuring data security by hybrid encryption of CP-ABE and AES, Lu and Fu proposed a data access control mechanism based on attribute based encryption and blockchain. The CP-ABE schemes used in and are based on symmetric primeorder bilinear groups. If they are directly transformed into an even more secure scheme based on asymmetric prime-order bilinear groups, the computational cost will be significantly greater than that of the present schemes.

II. LITERATURE SURVEY

A. DATA PROTECTION SCHEMES

Many privacy data security schemes have been promoted to more expansive fields like medical care and scientific research, as user privacy data is gathered and used in an increasing number of companies. Chen et al. presented an efficient CP-ABE scheme in cloud storage with shared decryption. Instead of simply one specified user, this scheme uses numerous alternate users to decrypt the ciphertext. By utilising an integrated access tree, this decryption approach improves the scheme's security while also reducing the computational cost. Technologies like CP-ABE and symmetrical encryption were used by Lee et al. to protect the privacy and secrecy of blockchain. Wang et al. proposed the RCP-ABE personal privacy data protection system, which substituted conventional third parties with smart contracts to accomplish access control of user data. Kang et al. proposed a traceable and forward-secure attribute-based signature scheme with constant size, it solves the issues of abusing signature and key exposure in existing Attribute-Based Signature (ABS) schemes. Zhang et al. proposed an agricultural products supply chain traceability system based on blockchain and CP-ABE. However, once the security of these schemes in the is enhanced, they will suffer from high computing overhead during the encryption, decryption and key generation phase when used in high dimensional attribute domains.

B. CP-ABE-BASED ATTRIBUTE REVOCATION

One of the main research points of CP-ABE is attribute revocation, Qian et al. proposed a privacy-preserving personal health record using multi-authority attribute-based

encryption with revocation, which supports efficient revocation at both the user and attribute levels. An attributerevocation-compliant cloud storage system was designed by Chen et al. which refreshed the data user's right to access the private data only if their attribute was nonrevoking. The ciphertext was updated by randomly creating a one-time re-encryption key that was connected with the data user's attributes. Lian et al.

proposed a CP-ABE scheme with user attribute revocation. They divided the master key into a delegation key and a secret key and updated the ciphertext and the delegation key by setting the data reencryption algorithm. Li et al. presented user collusion avoidance CP-ABE with efficient attribute revocation for cloud storage, which makes use of attribute groups and binds users' private keys with group keys. It solves the issue of a user's single attribute revocation affecting other users in the system who have the same attributes. A method for using CP-ABE in resource-constrained IoT devices was presented by Fischer et al. which called for an attribute delegation centre to carry out a user key update algorithm and a proxy server to carry out a ciphertext update algorithm. In the attribute revocation schemes the proxy server performs a second encryption on the relevant ciphertexts and updates the user keys, the computational cost of these schemes needs to be reduced.

C. VERIFIABLE LEDGER DATABASES

Regarding the ledger databases, Fekete and Kiss point out they can be divided into two categories. The first is permission blockchain technology-based Decentralised Ledger Technology (DLT). Centralised Ledger Databases (CLD)- based Centralised Ledger Technology (CLT) is the second of them. Gorbunova et al. stated that one of the vital DLT aspects is the capacity to offer an immutable and widely verifiable ledger for larger-scale and highly complex systems. However, DLT has low performance and transaction throughput. To address the problem of low throughput, high latency, and large storage overhead in systems, Yang et al. proposed LedgerDB, a centralised ledger database with tamperevidence and non-repudiation features similar to blockchain. Based on Yang et al. [34] proposed ubiquitous verification in centralised ledger databases to address the shortcoming of high verification cost. In addition, researchers have begun to consider how to construct distributed ledger data with high performance and throughput.

III. PROPOSED SYSTEM

The overview of our proposed system is shown in the below figure.

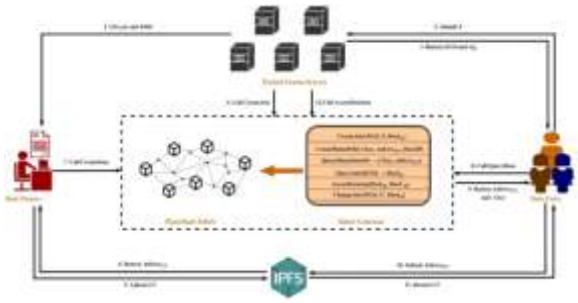


Fig. 1: System Overview

Implementation Modules

IPFS

- In this module, IPFS can login with valid username and password after login successful IPFS can perform some operations are: can view all dataset, view all datasets by blockchain, view all attribute request and respond status, view all revocated users, view all call time results and view call title results.

Data Owner

- In this module, data owner can register and login with valid username and password after login successful data owner can perform some operations are: can upload dataset, view all datasets.

Data User

- In this module, user can register and login with valid username and password after login successful user can request call attributes, find call attribute results and view all attribute request and response.

IV. RESULTS

Fig.2: IPFS Login

Fig.3: Data Owner Login

Fig.4: Upload Datasets

Fig.5: View all call time Results

V. CONCLUSION

We have proposed a personal privacy data protection scheme for encryption and revocation of high-dimensional attribute domains, which addresses the issues of low security, significant computational overhead, and high attribute revocation cost of current schemes in high-dimensional attribute domains. Compared with existing data protection schemes, HAD-FME is based on FAME and SM4 with high security, which can reduce the computing overhead and meet the requirements of secure storage and sharing of data in highdimensional attribute domains. We also designed an Attribute Revocation Mechanism Based on Sentry Mode (SM-ARM) to reduce the cost of attribute revocation by updating only the user version key. We have assumed in this paper that STSS is unable to obtain a complete DU private key, and the blockchain system exhibits performance limitations. In the future, we will plan to research multi-authority-based key generation schemes that ensure DU security, while exploring privacy data protection schemes based on high-performance tamper-proof systems to improve the throughput and performance of the schemes.

REFERENCES

[1] P. Patil and M. Sangeetha, ‘‘Blockchain-based decentralized KYC verification framework for banks,’’ Proc. Comput. Sci., vol. 215, pp. 529–536, Jan. 2022, doi: 10.1016/j.procs.2022.12.055.

[2] V. Mani, M. M. Ghonge, N. K. Chaitanya, O. Pal, M. Sharma, S. Mohan, and A. Ahmadian, ‘‘A new blockchain and fog computing model for blood pressure medical sensor data storage,’’ Comput. Electr. Eng., vol. 102, Sep. 2022, Art. no. 108202, doi: 10.1016/j.compeleceng.2022.108202.

[3] M. A. Shaik, A. Kethireddy, S. Nerella, S. Pinninti, V. Kathare and P. Pitta, "Sound Wave Scribe: Bridging Spoken Language and Written Text", 2024 First International Conference on Pioneering Developments in Computer Science & Digital Technologies (IC2SDT), Delhi, India, 2024, pp. 413-417, doi: 10.1109/IC2SDT62152.2024.10696694.

[4] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, and H. Karimipour, ''Secure intelligent fuzzy blockchain framework: Effective threat detection in IoT networks,'' Comput. Ind., vol. 144, Jan. 2023, Art. no. 103801, doi: 10.1016/j.compind.2022.103801.

[5] L. Zhou, K. Qin, C. F. Torres, D. V. Le, and A. Gervais, ''High-frequency trading on decentralized on-chain exchanges,'' in Proc. IEEE Symp. Secur. Privacy (SP), May 2021, pp. 428–445, doi: 10.1109/sp40001.2021.00027.

[6] M. A. Shaik and N. L. Sri, "A Comparison of Stock Price Prediction Using Machine Learning Techniques", 2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2024, pp. 1-5, doi: 10.1109/ICESC60852.2024.10689767.

[7] X. Yang, Y. Zhang, S. Wang, B. Yu, F. Li, Y. Li, and W. Yan, ''LedgerDB: A centralized ledger database for universal audit and verification,'' Proc. VLDB Endowment, vol. 13, no. 12, pp. 3138–3151, Aug. 2020, doi: 10.14778/3415478.3415540.

[8] C. Yue, T. T. A. Dinh, Z. Xie, M. Zhang, G. Chen, B. C. Ooi, and X. Xiao, ''GlassDB: An efficient verifiable ledger database system through transparency,'' Proc. VLDB Endowment, vol. 16, no. 6, pp. 1359–1371, Feb. 2023, doi: 10.14778/3583140.3583152.

[9] Mohammed Ali Shaik, N.Sai Anu Deep, G.Srinath Reddy, B.Srujana Reddy, M.Spandana,B.Reethika, "Graph Based Ticket Classification and Clustering Query Recommendations through Machine Learning", Library Progress International, Vol.44 No.3, July-December 2024, Pp.25828-25837 .

AUTHORS Profile

Mr. K. Uday Kiran is an Assistant Professor in the Department of Master of

Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his Master of Computer Applications (MCA) from Bapatla Engineering College, Bapatla. His research interests include Machine Learning, Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.

Mr. **D.N.V.S. Akash** has received his Degree in B.Sc Electronics from Acharya Nagarjuna University 2022 and pursuing MCA degree in Computer Science at Qis College of Engineering and Technology affiliated to JNTUK in 2023-2025.