IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115122

DATA INTEGRITY AUDITING WITHOUT PRIVATE KEY STORAGE FOR SECURE CLOUD STORAGE

Sivaganesh.M[1], Priyanka.M[2], Priyadharshini.C[3], Priyadharshini.G[4], Sujitha.A[5]

[1] Assistant Professor, Computer Science Engineering,Paavai Engineering College, Namakkal, Tamilnadu

[2] UG - Computer Science Engineering,Paavai Engineering College, Namakkal, Tamilnadu

[3] UG - Computer Science Engineering,Paavai Engineering College, Namakkal, Tamilnadu

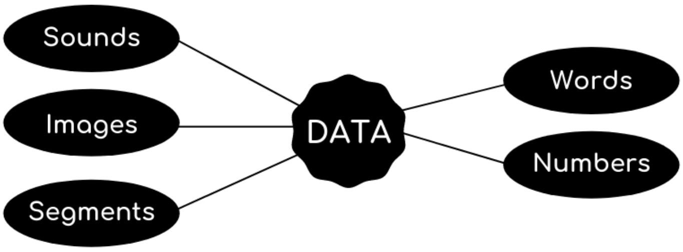
[4] UG - Computer Science Engineering,Paavai Engineering College, Namakkal, Tamilnadu

[5]UG - Computer Science Engineering,Paavai Engineering College, Namakkal, Tamilnadu

Abstract: Cloud storage service has shown its great power and wide popularity which provides fundamental support for rapid development of cloud computing. However, due to management negligence and malicious attack, there still lie enormous security incidents that lead to quantities of sensitive data leakage at cloud storage layer. Once data is stored in the cloud, a client's sovereignty over its data is lost, leaving the data vulnerable to many security threats. From the perspective of protecting cloud data confidentiality, this project proposed a Mimic model Virtual Assistant that combines cloud computing with blockchain that assures data integrity for homomorphic encryption schemes. To establish a secure CSP platform apart from encrypting data homomorphically, there is a need for a robust, tamperproof, and verifiable security architecture. Virtual Assistant will be hired to store and perform computations on client data. Each VA will have to periodically compute a master hash value of their database to be stored on a private blockchain. A client can compare these master hash values to detect if data tampering has occurred. This distributed verification system fulfils the requirements of confidentiality (HE will be used for encryption), and integrity because data modifications by the CSPs can be detected by comparing master hash values stored on the blockchain. The data sharing process is performed via a smart contract, and involved parties have to escrow to encourage honesty. The schemas of data storing and sharing guarantee the security properties including confidentiality, integrity, privacy, non-repudiation, and anonymity.

1. INTRODUCTION

In general, data is a distinct piece of information that is gathered and translated for some purpose. If data is not formatted in a specific way, it does not valuable to computers or humans. Data can be available in terms of different forms, such as bits and bytes stored in electronic memory, numbers or text on pieces of paper, or facts stored in a person's mind.



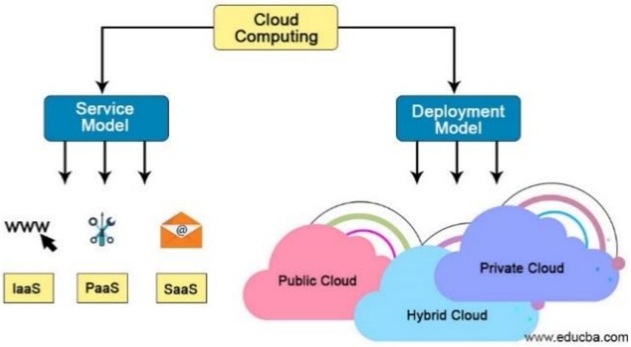
Since the invention of computers, people have used the word data to mean computer information, and this information is transmitted or stored. In a computer's storage, data is stored in the form of a series of binary digits (bits) that contain the) that contain the value 1 or 0. The information can be in terms of pictures, text documents, software programs, audio or video clips, or other kinds of data. The computer data may be stored in files and folders on the computer's storage, and processed by the computer's CPU, which utilizes logical operations to generate output (new data) form input data. As the data is stored on the computer in binary form (zero or one), which can be processed, created, saved, and stored digitally. This allows data to be sent from one computer to another with the help of various media devices or a network connection. Furthermore, if you use data multiple times, it does not deteriorate over time or lose quality.

Cloud Storage

Cloud storage allows you to save data and files in an off-site location that you access either through the public internet or a dedicated private network connection. Data that you transfer off-site for storage becomes the responsibility of a third-party cloud provider. The provider hosts, secures, manages, and maintains the servers and associated infrastructure and ensures you have access to the data whenever you need it.

DOI: 10.17148/IJARCCE.2022.115122

Cloud storage delivers a cost-effective, scalable alternative to storing files on on-premise hard drives or storage networks. Computer hard drives can only store a finite amount of data. When users run out of storage, they need to transfer files to an external storage device. Traditionally, organizations built and maintained storage area networks (SANs) to archive data and files. SANs are expensive to maintain, however, because as stored data grows, companies have to invest in adding servers and infrastructure to accommodate increased demand.



Cloud storage is available in private, public and hybrid clouds.

2.EXPERIMENTAL METHODS OR METHODOLOGY

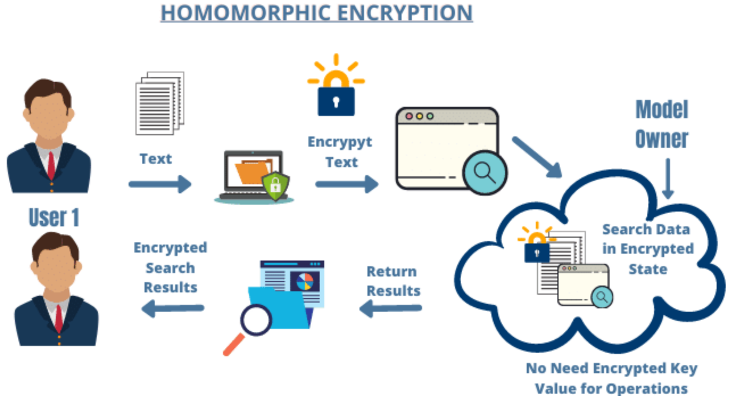
This project proposes a scheme that combines cloud computing with blockchain that assures data integrity in the cloud. The proposed approach in this paper adopts both HE and BC in a unified approach for maintaining data confidentiality in cloud computing.

Mimic Model

Mimic Model is nothing but the substitute of the DO. When a user places a request for data access, the user queries the metadata on the blockchain. The authenticity of the data is verified by checking the signatures of the data owner and the VA. A timestamp is appended if authentication is successful, after which the signed data is sent to the VA in a request for the actual data. The related information on the data is fetched from the cache, while the associated ciphertext is also retrieved from the CSP. The VA performs ciphertext re-encryption and sends the result to the user. The user can now decrypt the ciphertext with his private key. The blockchain beforehand verifies the authenticity of the user by using his signature. The timestamp is verified and the request is stored on the blockchain for auditing purposes.

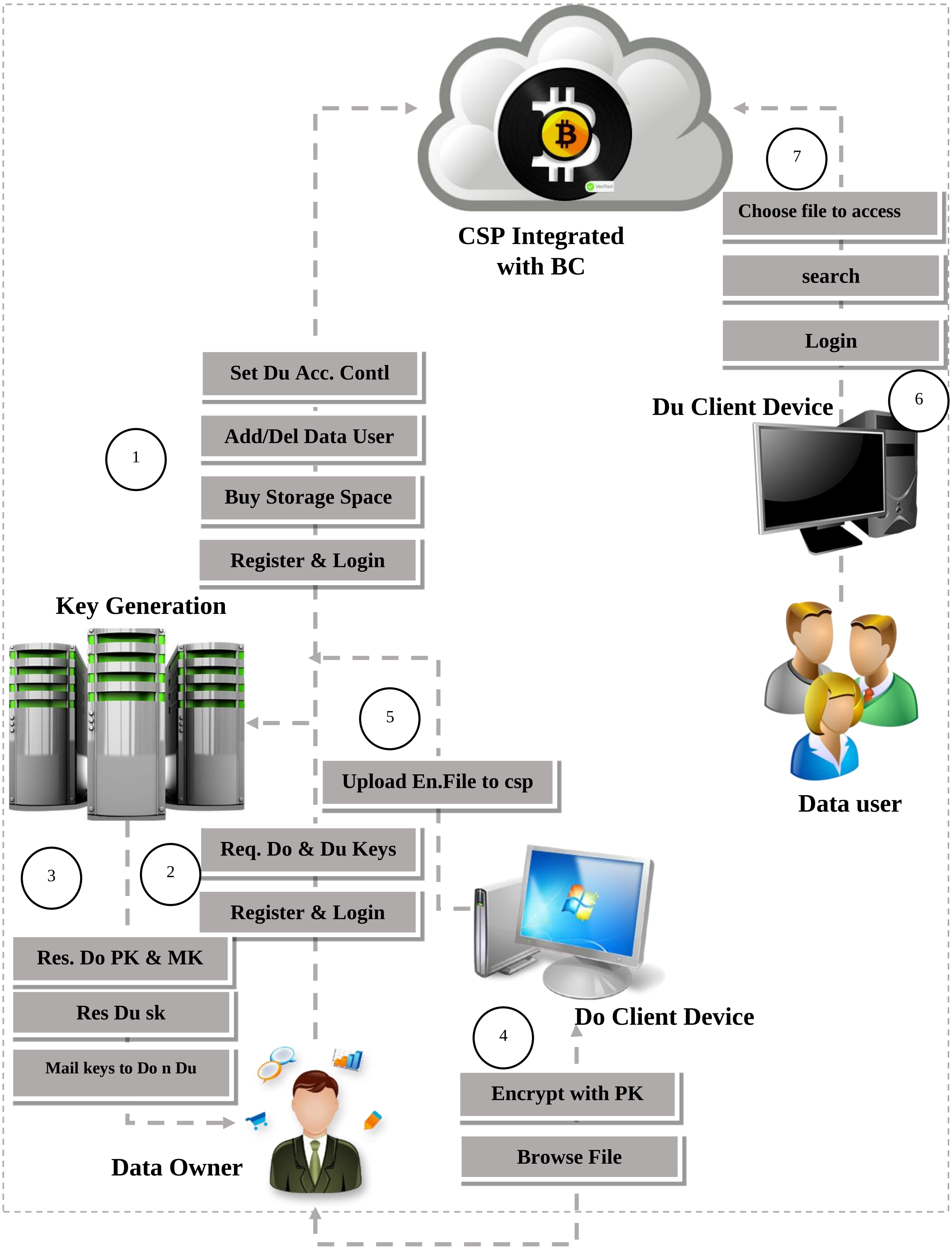
Homomorphic Encryption

Homomorphic encryption (HE) is a kind of encryption that allows computation on encrypted data. In short, HE ensures that performing operations on encrypted data and decrypting the result is equivalent to performing analogous operations without any encryption.



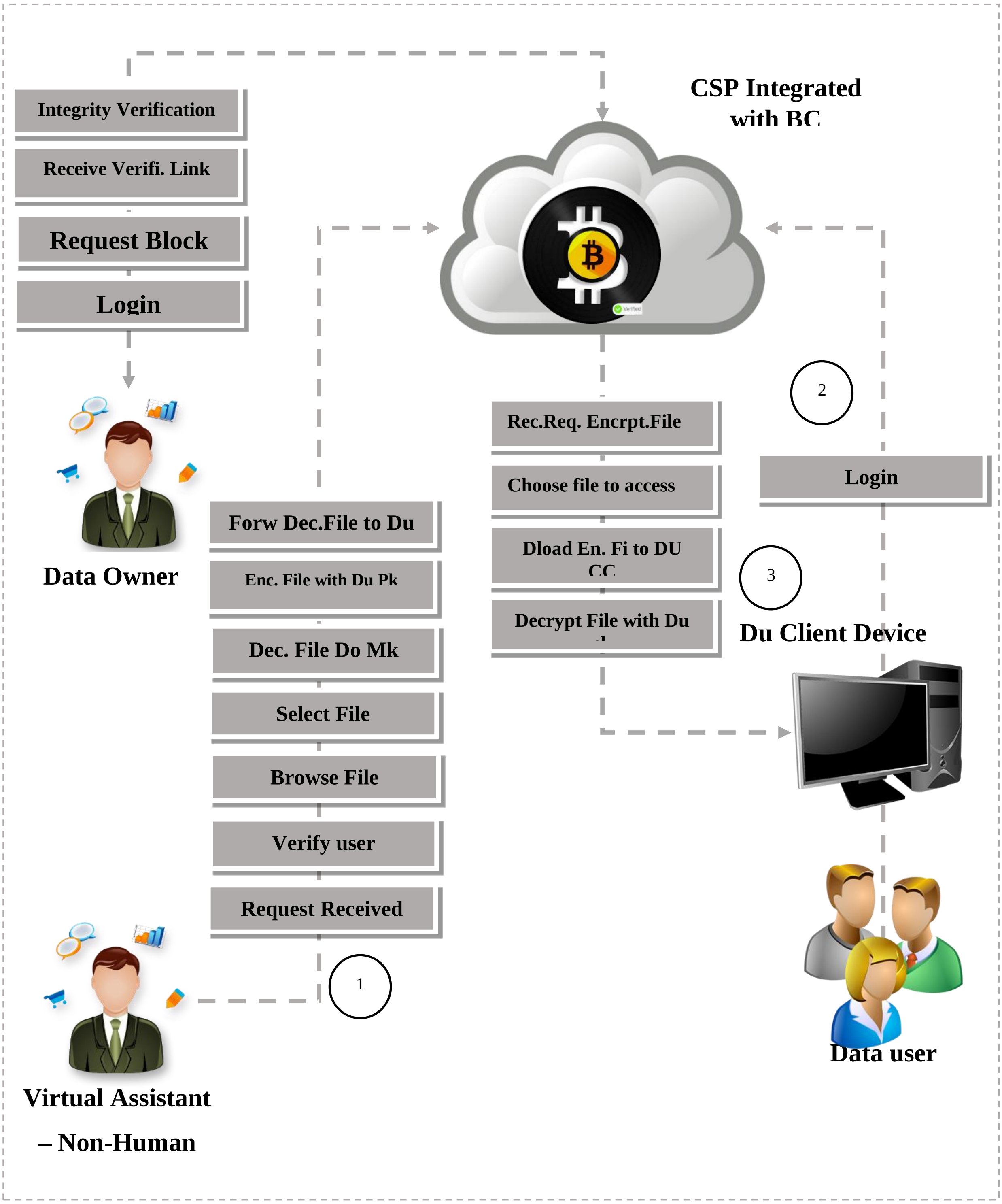
DOI: 10.17148/IJARCCE.2022.115122

system Flow – Homomorphic Encryption & Data user request

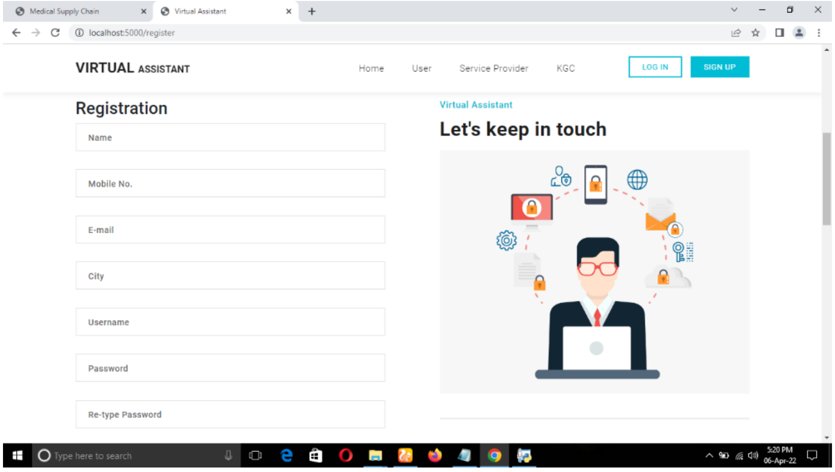


DOI: 10.17148/IJARCCE.2022.115122

System Flow – Mimic Model, Homo.Decryption & Block Verify



RESULTS AND DISCUSSION



Registration

Name

Mobile No.

E-mail

City

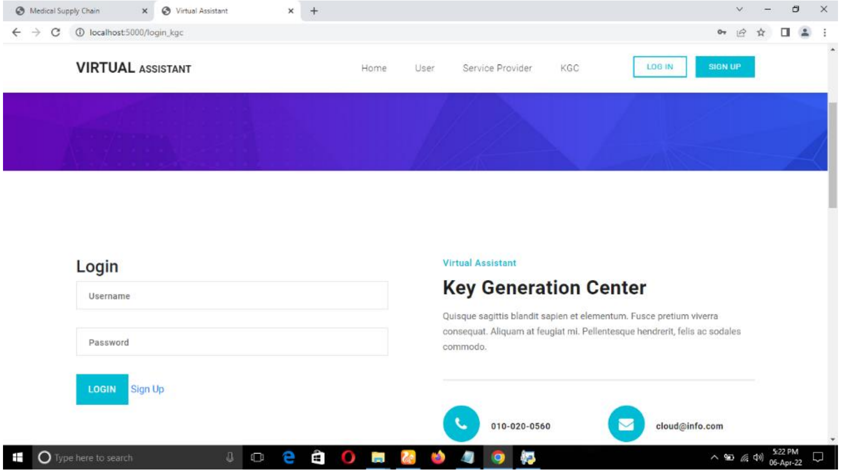
Username

Password

Re-type Password

Virtual Assistant

Let's keep in touch



Login

Username

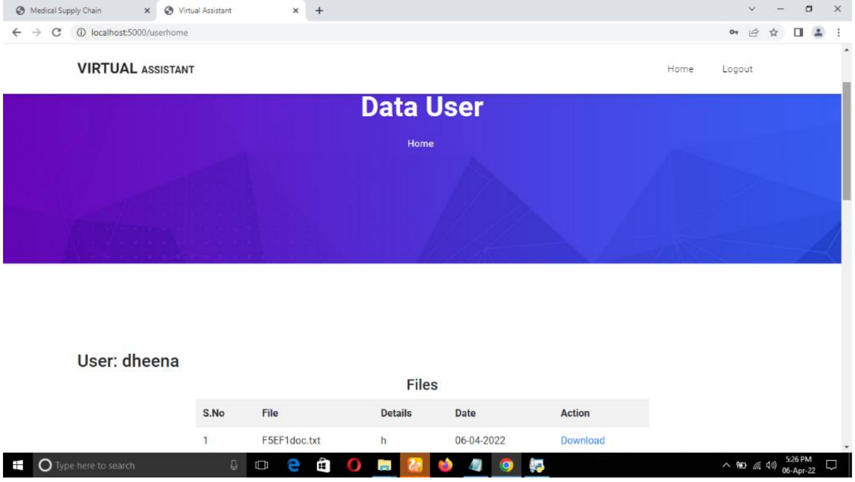
Password

Virtual Assistant

Key Generation Center

Quisque sagittis blandit sapien et elementum. Fusce pretium viverra consequat. Aliquam at feugiat mi. Pellentesque hendrerit, felis ac sodales commodo.

010-020-0560 cloud@info.com



Data User

User: dheena

Files

S.No	File	Details	Date	Action
1	F5EF1doc.txt	h	06-04-2022	Download

CONCLUSION

Cloud databases should have a reliable authority control security apparatus to follow data modifications. Specifically, cloud databases are problematic since they can be manipulated even without the acknowledgement of the data owner. To guarantee data confidentiality, integrity, and privacy, we propose a secure homomorphic-based FHE data-sharing scheme in a cloud computing environment. Secure data sharing is realized with FHE technique, which allows the data owners to store their encrypted data in the cloud and share them with legitimate users efficiently. Due to resource constraints, a

DOI: 10.17148/IJARCCE.2022.115122

Virtual Assistant as the proxy to handle the intensive computations instead of DO role. The scheme also incorporates the features of Cloud to proficiently deliver cached content, timely response, thereby improving the quality of service and making great use of the network bandwidth. Then, we present a blockchain-based system model that allows for flexible authorization on encrypted data. Fine-grained access control is achieved, and it can help data owners achieve privacy preservation in an adequate way. The analysis and results of the proposed model show how efficient our scheme is, compared to existing schemes. Furthermore, Blockcloud enables blockchain systems to suit dynamic network with higher efficiency and easier scalability

FUTURE SCOPE

In the future, we will focus on improving blockchain performance. We consider introducing VA and zero-knowledge proof to further simplify the management of patients' medical files and improve privacy protection.

REFERENCES

1. V. Hemamalini, G. Zayaraz, and V. Vijayalakshmi, “Bspc: blockchainaided secure process control for improving the efficiency of industrial internet of things,” Journal of Ambient Intelligence and Humanized Computing, pp. 1–14, 2022.
2. P. A. Lobo and V. Sarasvathi, “Distributed file storage model using ipfs and blockchain,” in 2021 2nd Global Conference for Advancement in Technology (GCAT). IEEE, 2021, pp. 1–6.
3. J. Chi, Y. Li, J. Huang, J. Liu, Y. Jin, C. Chen, and T. Qiu, “A secure and efficient data sharing scheme based on blockchain in industrial internet of things,” Journal of Network and Computer Applications, vol. 167, p. 102710, 2020.
4. C. Chen, J. Yang, W.-J. Tsaur, W. Weng, C. Wu, and X. Wei, “Enterprise data sharing with privacy-preserved based on hyperledger fabric blockchain in iiot's application,” Sensors, vol. 22, no. 3, p. 1146, 2022
5. N. Z. Benisi, M. Aminian, and B. Javadi, “Blockchain-based decentralized storage networks: A survey,” Journal of Network and Computer Applications, vol. 162, p. 102656, 2020.
6. M. J. H. Faruk, H. Shahriar, M. Valero, S. Sneha, S. I. Ahamed, and M. Rahman, “Towards blockchain-based secure data management for remote patient monitoring,” in 2021 IEEE International Conference on Digital Health (ICDH). IEEE, 2021, pp. 299–308.
7. A. Al Mamun, M. U. F. Jahangir, S. Azam, M. S. Kaiser, and A. Karim, “A combined framework of interplanetary file system and blockchain to securely manage electronic medical records,” in Proceedings of International Conference on Trends in Computational and Cognitive Engineering. Springer, 2021, pp. 501–511.
8. M. Naz, F. A. Al-zahrani, R. Khalid, N. Javaid, A. M. Qamar, M. K. Afzal, and M. Shafiq, “A secure data sharing platform using blockchain and interplanetary file system,” Sustainability, vol. 11, no. 24, p. 7054, 2019.
9. X. Lu, S. Fu, C. Jiang, and P. Lio, “A fine-grained iot data access control scheme combining attribute-based encryption and blockchain,” Security and Communication Networks, vol. 2021, 2021.
10. S. Niu, L. Chen, J. Wang, and F. Yu, “Electronic health record sharing scheme with searchable attribute-based encryption on blockchain,” IEEE Access, vol. 8, pp. 7195–7204, 2019
11. M. Du, Q. Wang, M. He and J. Weng, "Privacy-preserving indexing and query processing for secure dynamic cloud storage", IEEE Trans. Inf. Forensics Security, vol. 13, no. 9, pp. 2320-2332, Sep. 2018.
12. Y. Li, K. Gai, L. Qiu, M. Qiu and H. Zhao, "Intelligent cryptography approach for secure distributed big data storage in cloud computing", Inf. Sci., vol. 387, pp. 103-115, May 2017.
13. W. Shen, J. Qin, J. Yu, R. Hao and J. Hu, "Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage", IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 331-346, Feb. 2019.
14. Y. Zhang, C. Xu, X. Lin and X. S. Shen, "Blockchain-based public integrity verification for cloud storage against procrastinating auditors", IEEE Trans. Cloud Comput., Mar. 2019.ss