International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Virtual Assistant Mimic Model for Cloud Data Security Based on Blockchain

***Dhinesh*[1], *Parthasarathi*[2], *Pasupathi*[3], *Prof Rajakumaran*[4]**

[1]*EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India*
E-Mail: dinsdeepika@gmail.com
[2]*EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India*
E-Mail: partha72692@gmail.com
[3]*EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India*
E-Mail: pasupathikalai7@gmail.com
[4]*Assistant professor, EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India*
E-Mail: rajakumaran@egspec.org

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.

Keywords:Cloud data security, Blockchain, Data security, Virtual assistant

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. There are different kinds of data. such as, Sound, Video, Single character, Number (integer or floating-point), Picture, Boolean (true or false), Text (string). In a computer's storage, data is stored in the form of a series of binary digits (bits) 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 folderson 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 allows you to save data and files in an off-site location that you access either through

* Parthasarathi.Phone.no:+917708883970.
E-mail address: partha72692@gmail.com

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.A data breach is a cyber-attack in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion. Data breaches can occur in any size organization, from small businesses to major corporations. They may involve personal health information (PHI), personally identifiable information (PII), trade secrets or other confidential information.A large percentage of data breaches are not the result of a malicious attack but are caused by negligent or accidental exposure of sensitive data. It is common for an organization's employees to share, grant access to, lose, or mishandle valuable data, either by accident or because they are not aware of security policies.This major problem can be addressed by employee training, but also by other measures, such as data loss prevention (DLP) technology and improved access controls.Social engineering attacks are a primary vector used by attackers to access sensitive data. They involve manipulating or tricking individuals into providing private information or access to privileged accounts.Phishing is a common form of social engineering. It involves messages that appear to be from a trusted source, but in fact are sent by an attacker. When victims comply, for example by providing private information or clicking a malicious link, attackers can compromise their device or gain access to a corporate network.

MODELING AND ANALYSIS

Cloud Server API

The Cloud Server API is a programming interface that allows easy access to all functions of the Cloud Server. This programming interface follows the Flask API design.Cloud applications can be kept smaller by using APIs to hand data to applications or API-based back-end services for processing or analytics computations, with the results handed back to the cloud application.Data stored on cloud services is instantly available to authorized users.Cloud applications offer fine-grained, centralized user and data control. IT departments can manage who has access to data and what they can do with it via a dedicated control interface, reducing the complexity of business software management.

BlockCloud Integration

Blockchain is a core component of our solution.A third-party audit platform between the DU and the CSP is responsible for forwarding and recording the Data user and the CSP interactions during the data integrity verification process. When DO dispute with CSP, the blockchain's records can be submitted to the arbitration institution as valid evidence. All participants jointly maintain the blockchain network, and the behaviour of users and CSP is jointly monitored to ensure the system's normal operation.

Key Generation Centre (KGC)

The KGC generates public and private keys for the system. It is assumed to be semi trusted. The KGC performs legitimate tasks assigned to it by other entities, but it may peek at the data owner's data objects, access control policies, and constraint policies.

Virtual Assistant

Data Retrieval Request- The service provider requests data acquisition. According to the user's labelling, we want to acquire data by creating a valid trapdoor through the connection keyword. Meanwhile, a state channel of data is created. The operation is updated to the latest state and recorded off-chain. **Data Retrieval and Response**- The informant checks the validity of the request. VA verifies that this request's trapdoor is in the data connection keyword set and then distributes the data access token to the node service provider. The final state is distributed on the blockchain as a transaction. VA then decrypt the file with MK_{DO} and re-encrypt with PK_{DU} send to requested DU.

Data flow diagram

The following figure.1 describes the data flow process of the virtual assistant mimic model for cloud data security based on blockchain

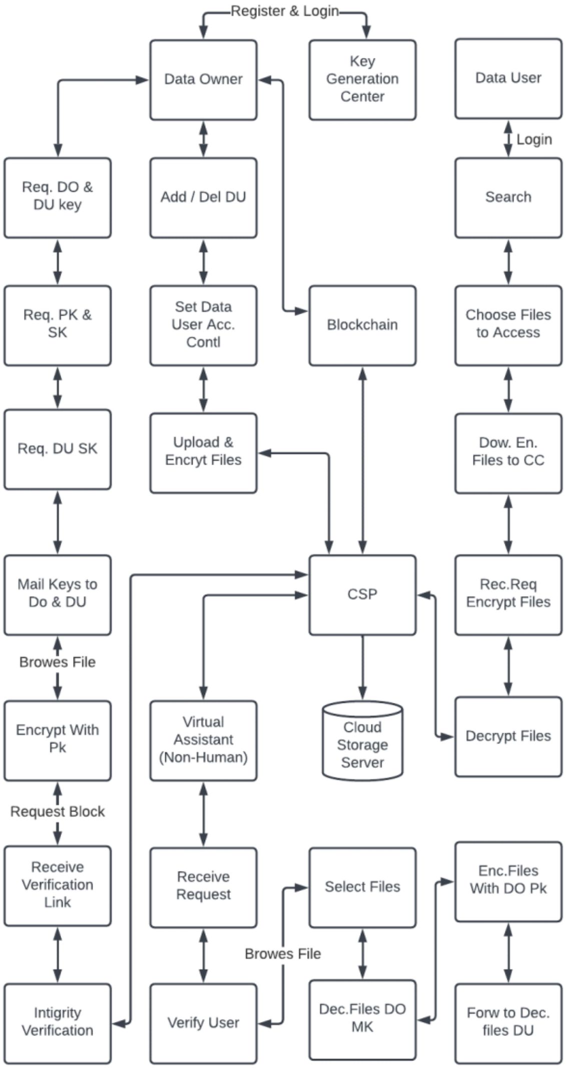

Figure.1 Data flow process of the virtual assistant mimic model for cloud data security based on blockchain

RESULTS AND DISCUSSION

Existing System

Threshold Proxy Re-encryption Scheme

In thisexisting system is constructed around the proposed scheme named Threshold Proxy Re-Encryption. In the beginning the cloud storage system stores user details in some database. The user needs to get registered in the database, by entering his data like user name, user gender, user location, user password, user birthdate, and user e-mail address. The user then logs into the system using his credentials that were initially registered. The file is forwarded contained in a folder along with the user and recipients name, a security question for decryption access, the file containing the key for decryption and the status of the message. The file is transferred using the receiver’s email and public key. After the file is received by the receiver, the selected file is downloaded. But before downloading the file, he has to download the key file that was sent in the same folder.

Disadvantages

- Security risks, such as identity privacy and data privacy disclosure.
- Inflexibility of access control policy
- Authority abuse of group managers
- Collusion attacks during user revocation.
- Computation burden of users' systems
- Difficulty in user revocation.
- Whenever owner wants to change the access right of user, it is not possible to do efficiently.
- For sending private key requires secure channel.
- IBE scheme may depend on cryptographic techniques that are insecure against code breaking attack.

Proposed System

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 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 associatedciphertext 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.

Advantages

- Provides confidentiality, decentralization, audit availability, and the secure sharing of file integrity monitoring results, without overloading.
- Possibility of auditing all stages of the file storage and integrity check processes.
- Immutability, inviolability and resilience provided by the Blockchain technology.
- Virtual Assistant plays major role of Data Owner for time consumption process.
- Fine-grained access to data.
- Guarantee data owners' complete control over their data

Use Case Diagram

The following figure 2. describes the process of virtual assistant mimic model for cloud data security based on blockchain

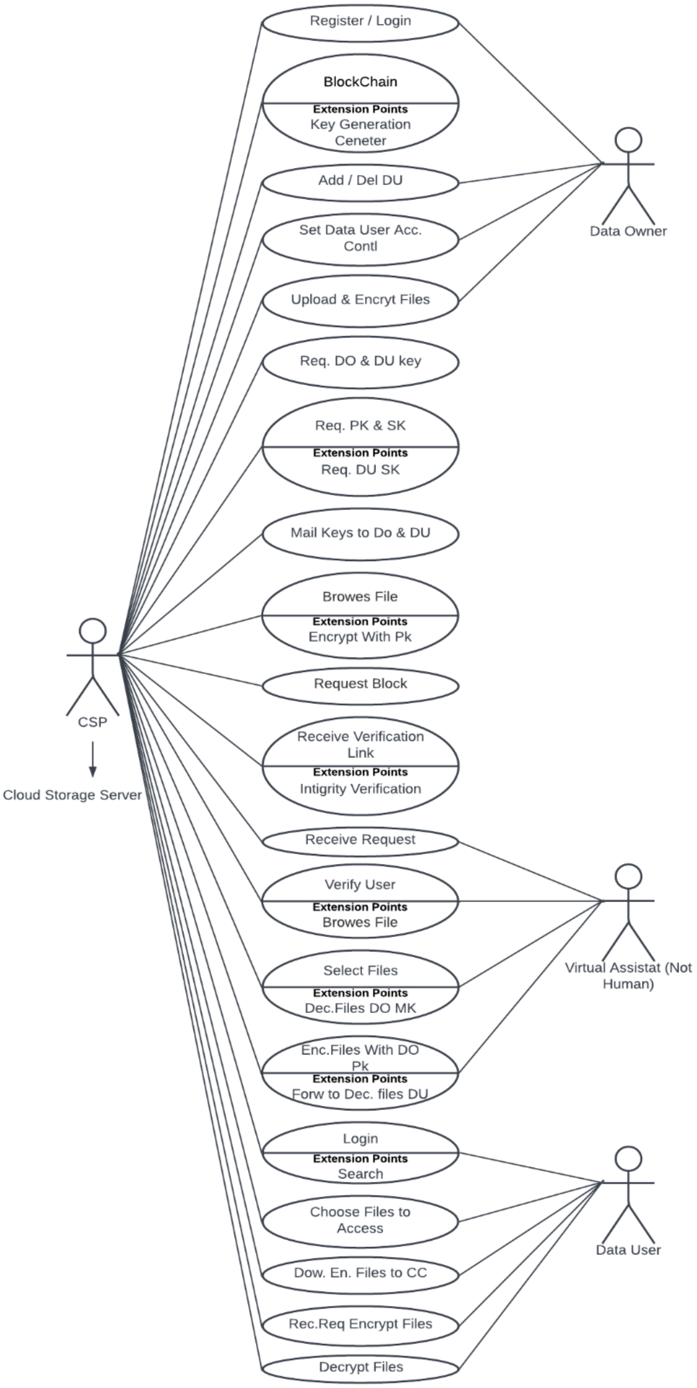

Figure 2. Virtual assistant mimic model for cloud data security based on blockchain

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 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, Block cloud enables blockchain systems to suit dynamic network with higher efficiency and easier scalability.

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