Ownerbot as a Service for Outsourced Encrypted Data Security In Cloud Based On Blockchain In Networking

Mr.R.Krishnakumar[1],Ms.S.Srimathi[2],Ms.T.V.Janani[3],Ms.N.Ragavi[4],Ms.M.Sharulatha[5],
Dr.R.Umamaheswari[6]
[1],Assistant Professor, [6],Professor, [2,3,4,5],UG Students, Department of CSE,
Gnanamani College of Technology, Namakkal, Tamilnadu, India.

ABSTRACT - Cloud storage services have seen widespread adoption, but with it comes significant security concerns, including management oversights and malicious attacks, leading to sensitive data leakage incidents. This project proposes the integration of the Mimic model OwnerBot, combining cloud computing with blockchain, to ensure data confidentiality through homomorphic encryption. By establishing a secure Cloud Service Provider (CSP) platform and employing distributed verification systems, smart contracts, and escrow mechanisms, this model aims to enhance cloud data security, addressing issues of confidentiality, integrity, privacy, non- repudiation, and anonymity.

Index Terms-Cloud Storage , Block chain , Homomorphic Encryption , Smart Contract, Data Integrity.

I INTRODUCTION

Generally, data is a unique set of data that is collected and translated for a particular purpose. If data isn't formatted in a particular way, it isn't valuable to computers or people. Data can be found in various forms, including bits and bytes, electronic memory, numbers, or text on a piece of paper, or information stored in a person's mind.In a computer's memory, data is stored as a series of binary numbers (bits) that represent the value 1, or 0.The information can be in the form of images, text, software, audio, video, or other types of data. The computer data can be stored in various formats, such as files and folders, on the computer's Data is processed by the computer's CPU which uses logical operations to produce output (new information) as input data. Since the data on the computer is stored in binary format (0 or 1), it can be created, stored, and digitally stored. This enables data to be transmitted from one machine to another using different media devices or network connections. Moreover, data does not degrade over time or suffer from loss of quality.Cloud storage provides a cost-efficient, scalable way to store files on an on-premises hard drive or storage network. A computer hard drive can only hold a limited number of files. When a user runs out of storage space, they must transfer files to external storage devices. Cloud storage allows you to store your data and files on- premise. If your data is moved off-premise, it becomes the responsibility of a third-party cloud provider. The third-party provider hosts, secures, manages, and maintains the servers and associated infrastructure, and ensures that you have access to the data at all times. They use a Service Provider (SP) platform and use distributed verification systems to improve data security and integrity, providing a strong defense against unauthorized access.

III. LITERATURE SURVEY

This article proposed to protect privacy and provide high accuracy in a reasonable amount of time when compared to other state-of-the-art techniques. This article provides detailed information about the neural network model developed for the application under study also show their runtime performance and model accuracy results. This article develops the functionality of the NN network model by using the homomorphic properties of the MORE schemes to complete the work of coding data. The proposed workflow on homomorphic encryption and NN. In the processing stage, the trained data is encoded using a secret key that is not shared. . Finally, it directly supports floating-point calculation with the help of the homomorphic function of the more encrypting scheme, and all the processes achieved on the Attributes. Network is able to train directly on the encrypted text information. This creates a model that gives an encoded prediction that merely the holder of the secret key can decrypt. the convenience of remote data management has brought forth unprecedented challenges. The soaring popularity of cloud services has exposed vulnerabilities, leading to sensitive data leaks from management oversights and malicious attacks Cloud storage, remote data management, and the ever-increasing demand for cloud services have presented unprecedented challenges. As cloud services have become more popular, vulnerabilities have opened the floodgates, allowing for sensitive data leaks due to management oversight and attacks.In order to combat these threats, we have developed the OwnerBot model, which combines the power of cloud computing with the power of blockchain.

To counteract these threats, this project introduces the Mimic model OwnerBot, fusing cloud computing with blockchain. OwnerBot employs homomorphic encryption, establishes a secure Cloud Here the input sample is encoded using the same key used in the training stage. MORE encryption schemes rely on symmetric keys to encrypt plain-text data and decrypt cipher-text data. The design of BC over cloud-RDB is based on simulating BC security components over the RDB stored and processed in cloud servers. This study is an improved proposal of [43] to provide a client self-verification system that detects and restricts internal threats applied to data computations in the cloud

This article has enabled manufacturing resources to be leased and shared on a global scale. However, it has problems arising from its central structure and the need for a reliable 3rd party. Reliability, security, continuity, scalability, data lock-in, single point failure, data manipulation are some of the main problems. Blockchain (BC) is a decentralized and distributed technology. The data stored on the BC network cannot be altered in any way. With these features, we believe that BC- supported cloud manufacturing systems can overcome the aforementioned problems and eliminates the need for a reliable 3rd party. Based on this belief, in this study the agreements and communication are realized with a decentralized application using BC- based smart contracts (scs). The designed application is called the decentralized cloud manufacturing application (dcmapp). Dcmapp does not operate on a fully public BC network, it has a hybrid structure and uses the Ethereum network as a public BC network. These features make dc map different from other BC-based cloud manufacturing applications. This article proposed a decentralized and privacy preserving public auditing scheme, which is secure against the procrastinating third-party auditor and malicious cloud server. Our scheme utilizes two components to generate unpredicted challenge messages. One is generated by the auditor, and the other is a series of decentralized block hashes. Our scheme could resist against the procrastinating auditor, and a malicious cloud server could not retrieve or guess the challenge message ahead of the audit time. Furthermore, our scheme provides better protection of user privacy during the process of verification of the audit response from the cloud server. In the future, cloud storage platforms may be replaced with decentralized storage platforms, such as Inter Planetary File Systems.

IV. PROBLEM STATEMENT

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. 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. Ransomware is a major threat to data in companies of all sizes. Ransomware is malware that infects corporate devices and encrypts data, making it useless without the decryption key. Attackers display a ransom message asking for payment to set release the key, but in many cases, even paying the ransom is ineffective and the data is lost. The major challenge of cloud computing, which is security and privacy.Cloud services are susceptible to attacks Biggest cloud security concern is data loss/leakage. Cloud computing involves third-party providers, can lead to a huge loss of data enterprises. Erasing/misusing data from anyone's computer.

V. ALGORITHM

FHBE Scheme

In this subsection, we propose a FHBE scheme based on lattice as follows. Suppose that the plaintext M D= {m1; m2; _ _ _; mx} € {0; 1} $^{x.}$ Our scheme consists of the following four algorithms.

Setup

The algorithm takes security parameters as input, and system generates public key PK and master key MK. The public key PK is very important in the HBE scheme, which is used to generate the secret key sk and cipher text. In our scheme, the attribute is associated with the cipher text, and the access structure of the attribute is associated with the secret key sk. If and only if the attribute of the cipher text meets the access structure of the secret key, the user can decrypt the cipher text to recover the plaintext.

Keygen

The algorithm takes PK, MK and attribute access control policy W as input. The system generates secret key sk for users.

Encrypt

The algorithm takes PK, user attribute ati €T and plaintext M as input and outputs ciphertext C.

Decrypt

The algorithm takes the public key, private key sk and cipher- text C as inputs. Only if access control policy W matches the user attribute policy T, the algorithm outputs plaintext M.

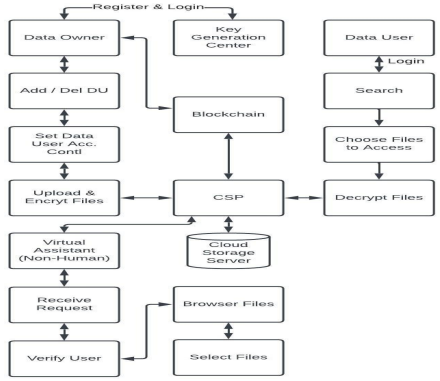
Block Cloud Algorithm

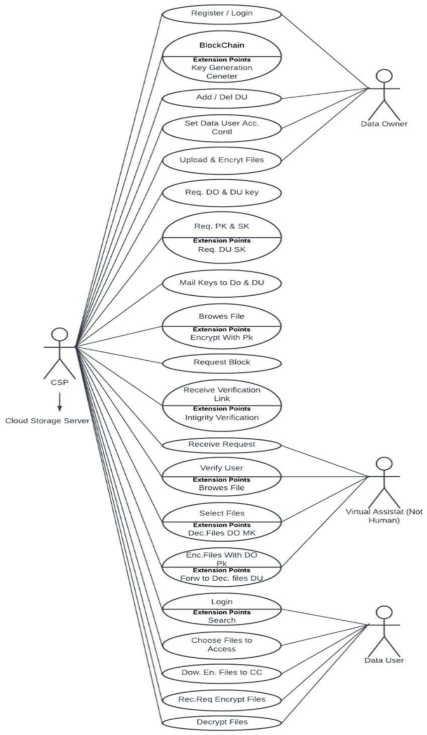
Incentive based IPFS Data Storage & Sharing

1. Upload IoT data to IPFS
2. Reward with Digital currency
3. Event Generation
4. Update Existing User
5. Delete file from IPFS

Block diagram

This is a Block Diagram for Ownerbot as a service for Encrypted data security in Cloud based on Blockchain in Networing .It shows the Login/signup for the dataowner (do).It add the data user then set the data for user account .Now we can upload and encrypt the data files. The Block Diagram shows the Flow Diagram for how the owner login and add user then upload encrypt files. So now the data user can search and choose files to access and Decrypt files. Easily we can understand about the working process for Ownerbot as a service for Encrypted data security in cloud based on Blockchain in Networking.





CONCLUSION

The project proposes a robust framework for securing cloud data through the integration of cloud computing and blockchain technology. By leveraging homomorphic encryption and blockchain-based verification mechanisms, the project provides a comprehensive solution for ensuring the confidentiality and integrity of data stored in the cloud. This addresses longstanding concerns regarding data breaches and tampering incidents. The implementation of smart contracts and distributed verification systems enables data owners to retain control and sovereignty over their data, even when stored and processed by cloud service providers. This fosters trust and transparency in data transactions.

REFERENCE

[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] 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 Explore opportunities to integrate emerging technologies such as quantum computing, advanced cryptography, or decentralized identity solutions into the project. This could enhance security, scalability, and privacy capabilities. Customize the project's framework to cater to specific industry verticals such as finance, healthcare, supply chain, or IoT.

[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] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[7] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[8] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[9] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[10] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter" Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[11] Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay" Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022

[12] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash "Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756

[13] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, "Perfromance Investigation of T-Source Inverter fed with Solar Cell" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749

[14] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007

[15] M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022

[16] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, "Physiochemical Analysis of Ground later used for Domestic needs in the Area of Perundurai in Erode District", International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019

[17] 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.

[18] A. Al Mamun, M. U. F. Jahangir, S. Azam, M.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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,

[24] 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.

[25] A. Al Mamun, M. U. F. Jahangir, S. Azam, M.

[26] 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.

[27] VI. 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.
[28] 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.
[29] 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.