Secure File Sharing with Access Control Using Blockchain

M Asha Priyadarshini, Sri Sunith Raju Tatapudi, Sachin Dulla, Rajeev Thomas Saganty and Gopi Krishna Vadlamudi

March 9, 2023

SECURE FILE SHARING WITH ACCESS CONTROL USING BLOCKCHAIN

*Under the guidance of Asha Priyadarshini M, M. Tech,(Ph. D)

(T. Sri Sunith Raju, D. Sachin, S. Rajeev Thomas, V. Gopi Krishna)

Department of Computer Science and Engineering (CSE)

Vignan’s Lara Institute of Technology and Science Vadlamudi,
Guntur district, Andhra Pradesh

Abstract--: There are currently only a few keywords available for blockchain-based crypto searches. Blockchain decentralized storage allows users to decentralize their data without a centralized server. Cloud servers and users experience mutual distrust for fear of losing control of the personal data entrusted to them. Secret service providers are unable to evaluate your personal information in the current circumstances. One of the most common problems was finding an encrypted cloud service.Contrarily, because the traditional cloud storage approach uses centralized storage, a single point of failure might bring the entire system to a standstill. The emergence of blockchain technology has actually led to a greater level of public awareness of decentralized storage. Decentralized storage has several advantages over central storage, including low cost and quick throughput, and it can address the issue of a single point of failure in traditional cloud storage systems. The only person who can download the material and decode it is someone whose features comply with the accessibility policy. The data owner has fine-grained access control over his or her information, and the project offers an attribute-level retraction of a specific data individual without affecting others.To further protect the privacy of the data subject, a cryptographic keyword search is performed upon receipt of the data. We also conducted a thorough analysis of processing and storage costs to demonstrate the effectiveness.

Keywords: Blockchain, encryption, cloud service, ciphertext, high security

I. INTRODUCTION

The latest steps in the grand scheme of technology has become a major part of AI to learn with or to train on. However, the major issue with the advancement is the security and privacy of their users. Consequently, the users tend to share their personal data with the services through a cloud service or any other data-sharing services that were said to be trusted solely based on the service providers. Although, there were barely any reasons for doubting the service providers they all connect to a single dot based on IoT which is vividly proven to be vulnerable to the threats that can break the system which may result in loss of the data that is promised to be kept safe.These details are special and may include private information about a person's life, job, health, and well-being; if private information is seized or unlawfully disclosed and connected to the real identity of the data owner, it can result in a lot of issues for a person. Such loss can cause great damage to a person or to an organization and thus demands exclusive modernization of security as most companies prefer to adopt such vulnerable services, there were a few major steps that supposedly solved the issues with the cloud service. These techniques seem to address the concerns regarding safety and privacy when sharing information. Although these methods address most of the concerns and blindside the problem that arises by considering these techniques. The potential threat of all the protocols is that all the methods heavily depend on a third-party service - CSP(Cloud Service Provider) that provides a functional infrastructure as a service. Such problem is outweighed most of the time by the advantages that they bring to the table to satisfy the demands of security and orchestrate a supposed secure service. However, there can be problems like the following that are inevitable and can barely be addressed.

(1) The possibility of the service providers profiting by selling out the privacy of the data and never coming to the spotlight has always been a concern. Despite the fact that some techniques, such as attribute-based security algorithms, appear to be user-centric and offer user-defined access limits, such methods definitely require a third-party service to manage their keys and hold accountability to the keys. There’s always a potential threat that these companies or services could work together to backstab the user’s trust and privacy but the loss is not for the trust but the data itself.

(2) The Cloud Service Provider maintains the infrastructure and the services that they provide at a single point of the model and is always a potentially vulnerable spot to take over. Recovery of the lost data can be provided using a backup service that the providers tend to give. However, users might not be able to access their data due to multiple factors, like political factors which can cease the service and accessibility of the data through it

(3)The requirement of investing more in the provider’s service and quality there needs to be constant upgrades in the infrastructure and service. Eventually, the provider needs more funds to do so and the impact will be on the user’s affordability and pricing as the entire investment is charged to their users.

OBJECTIVE OF THE PROJECT

Each blockchain, distributed network, and cloud computing have distinct characteristics and face similar network-related challenges. [4] A further level of protection that incorporates numerous network-related technologies may be provided by future assimilation. Despite the possibilities of diverse adversarial tactics, some cyber hazards in cloud computing, such as identity theft and information mining-based assaults, also place on blockchain networks. [5] The data stored in blocks and made available to authorized users hints that mining block data can violate users' privacy. The situation is the same when data is stored on faraway cloud web servers. A successful connection attack on a private cloud dataset could result in privacy leaking. [6] Consequently, two current technologies are in danger due to both internal and external issues. Cloud computing resources are added to the blockchain system to improve security, performance, and solution level.

Hardware in computer systems refers to any device connected to a blockchain and is just as important as software. [7]

II. RELATED WORK

[1] Zhipeng Cai, Zaobo He, Xin Guan, and Yingshu Li act as the judges for collective data sanitization for social media attacks that aim to suppose delicate details.

The leak of user data from social media networks could seriously violate their privacy. User profiles and friendships are both by their very nature private. Sadly, sensitive information from publicly accessible data can be predicted by data mining technologies. As a result, network data needs to be cleaned up before being published. In this article, we examine how to unleash a logical assault using social networks that combine non-sensitive features and social communications. We relate this challenge to a problem of group categorization and offer a model of group reasoning. Using user accounts and their social connections, an attacker can predict sensitive information about connected victims in a publicly available social media network dataset, according to our method.

Zhipeng Cai, Xu Zheng, and an additional participant from the student audience continue to be present as they discuss [2] a secure and reliable method for posting information in intelligent cyber-physical systems.

Information submission in intelligent cyber-physical systems faces new difficulties in terms of energy conservation and privacy protection in order to enable granular access to various areas of the physical environment. People must send information using the least amount of power possible. However, focusing solely on energy efficiency could result in the extreme disclosure of personal information, especially given that participant-uploaded content is currently more revealing than ever. In this article, we propose a novel information dissemination strategy for intelligent cyber-physical systems that takes into account both power efficiency and privacy protection.

[3] In order for taxi companies to approximate metropolitan website traffic streams, a differential-private structure is required. Jiguo Yu3,4,5, Zhipeng Cai3, Xu Zheng2, and Athors Participant

As a result of the enormous expansion of public transportation systems, cab traffic may now serve as a credible indicator of urban population trends. The general public, city officials, and the actual taxi businesses will all find this information to be of great use. However, the confidential information of taxi firms is seriously at risk if such web content is disseminated carelessly. They will undoubtedly divulge both their own market ratios and the private information of both travelers and drivers. Therefore, in this study, we propose a novel framework for taxi services to share traffic while safeguarding privacy, which takes users' privacy, profits, and justness into account.CURRENT SYSTEM: There is now a structure in place for the storage and exchange of EMR data for cancer patient care. It uses cloud services to store the encrypted data and a permission chain to maintain metadata and accessibility control rules. People can specify their access control policies to ensure information security and accessibility. The blockchain-based data-sharing schemes discussed above provide a great framework, but most of them only outline the strategy without describing how the necessary protocol will actually be put into practice.

SYSTEM RECOMMENDED: Open commerce and information security confirmation are essential in an AI-powered environment.Since the client sends data to the cloud web server for throttling and distribution, standard data exchange steps must be used. The client loses control of the information after it leaves the server, which increases security and raises insurance policy issues. Access control and data security are considered sophisticated improvements for storing certain information on cloud-based internet servers, but their use is limited. However, in most cases, you still rely on cloud providers i.e. 4th parties (CSPs). To solve this problem, we used an interplanetary file system, 3DES cryptography technology, blockchain, and ECC (IPFS).Details of the BTDEC Trible This study focuses on the Elliptic Contour Crypto-system for Personal Data. This customer-driven strategy enhances the decentralization of the system by requiring the information bearer to wait on IPFS while safeguarding the shared data. According to the built-in confirmation mechanism, the shared data area and decryption key will be connected using 3DES and also ECC, and the information owner will distribute his data-related information and transfer it in ways to inform users using blockchain. The only information client are allowed to download, install, and evaluate the information is one whose credit score scores fulfill the verification norms. By enabling the information owner to refuse a specific information customer at a precise measurement without affecting other customers, BTDEC grants the owner of the information fine-grained network access control over his information.They investigated the security of BTDEC and validated the concept by replicating the current technology to the EOS blockchain. In order to maintain the confidentiality of the information consumer, cipher text search is often used when obtaining information. They considered the cost and limitations of the time and found that BTDEC performed well. As a result of the enormous expansion of public transportation systems, cab traffic may now serve as a credible indicator of urban population trends. The general public, city officials, and the actual taxi businesses will all find this information to be of great use. However, the confidential information of taxi firms is seriously at risk if such web content is disseminated carelessly. They will undoubtedly divulge both their own market ratios and the private information of both travelers and drivers. Therefore, in this study, we propose a novel framework for taxi services to share traffic while safeguarding privacy, which takes users' privacy, profits, and justness into account.

CURRENT SYSTEM: There is now a structure in place for the storage and exchange of EMR data for cancer patient care. It uses cloud services to store the encrypted data and a permission chain to maintain metadata and accessibility control rules. People can specify their access control policies to ensure information security and accessibility. The blockchain-based data-sharing schemes discussed above provide a great framework, but most of them only outline the strategy without describing how the necessary protocol will actually be put into practice.

SYSTEM RECOMMENDED: Open commerce and information security confirmation are essential in an AI-powered environment.Since the client sends data to the cloud web server for throttling and distribution, standard data exchange steps must be used. The client loses control of the information after it leaves the server, which increases security and raises insurance policy issues. Access control and data security are considered sophisticated improvements for storing certain information on cloud-based internet servers, but their use is limited. However, in most cases, you still rely on cloud providers i.e. 4th parties (CSPs). To solve this problem, we used an interplanetary file system, 3DES cryptography technology, blockchain, and ECC (IPFS).Details of the BTDEC Trible This study focuses on the Elliptic Contour Crypto-system for Personal Data. This customer-driven strategy enhances the decentralization of the system by requiring the information bearer to wait on IPFS while safeguarding the shared data. According to the built-in confirmation mechanism, the shared data area and decryption key will be connected using 3DES and

also ECC, and the information owner will distribute his data-related information and transfer it in ways to inform users using blockchain. The only information client is allowed to download, install, and evaluate the information is one whose credit score scores fulfill the verification norms. By enabling the information owner to refuse a specific information customer at a precise measurement without affecting other customers, BTDEC grants the owner of the information fine-grained network access control over his information.They investigated the security of BTDEC and validated the concept by replicating the current technology to the EOS blockchain. In order to maintain the confidentiality of the information consumer, cipher text search is often used when obtaining information. They considered the cost and limitations of the time and found that BTDEC performed well.

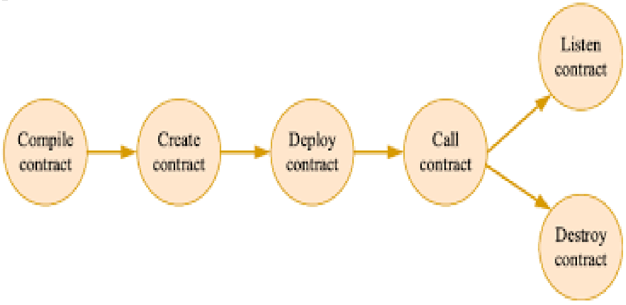

Fig.1. Blockchain model.

III. METHODOLOGY

In fact, they created the following technology. IPFS, Blockchain, Information Owners, and Data Consumers are the four components of BTDEC. The DO quickly shared his information with IPFS, stored it as a blockchain smart contract, and unlocked the key with a decryption tool. Granular access control is implemented using 3DES and ECC. Since the traded information is compressed in the DO blockchain, only those who meet customs clearance requirements can receive and decrypt it. Processes are distributed throughout.Data is maintained and stored on IPFS to ensure information security and transparency. The immutable DOs and DUs are stored on the blockchain.

The following operations are explicitly managed and performed in these four locations. Building secure and reliable storage solutions with IPFS. The driving force's organizational structure ensures that IPFS' expertise can never be limited.

Blockchain: The blockchain governs all new information added to the plan and all information currently available to the general public.A similar method may have originally been used to pass secure and secure messages from DO to DU. You won't find a single real outsider, but this is your main tactic. BTDEC basically has two types of smart contracts. DSContract receives information about the client from UMContract, which tracks the client.

Owner of the data: according to the approach, this individual is in charge of directing the creation and distribution of the Smart Arrangement. The DO's institutional capabilities and the systems he has in place for disseminating information to those who have access to it are both open to question. A data person (DU) can also ask for entrance permissions, which the DO might grant or deny, in order to use common data. The location and also approach to obtaining the common knowledge will be made known when DU's characteristics link to the strategy indicated in the ciphertext. The entire client ID was only provided as part of the 3DES, ECC mechanism to handle authorization denial. The countersign ciphertext search provided by BTDEC helped it operate.

The following overview discusses each novel element:

1 The Division of the Interior is in charge of creating and disseminating innovative agreements. Each person in our setup has two Smart Agreements. Because of the value of the administrators, the inventiveness of the board, and the involvement of the users, UMContract is well-liked. DSContract keeps an eye on all information transmission, access plan changes, authorization denials, and information retrieval operations.

After the DO generates the setup personal keys and also the residential properties public key on the area, the structure public trick is saved in DSContract.

IV. CONCLUSION

In the AI-driven future, a stakeholder-sharing perspective is presented to promote comprehension while ensuring data security. By merging the blockchain, BTDEC, and IPFS, I proposed a blockchain-based security sharing information system for reasonably effective authorization management as well as additional approval cancellation. The DO uses the approved approach to submit his information to IPFS while keeping it secure. He then encrypts the technique and uses 3DEECS to decode the return address. DUs that meet the requirements of the admission procedure is required to gather information and encrypt it. This method has no built-in control center and DOs have complete discretion over the information they share, ensuring both security and personal privacy. To illustrate this point, they created this framework on the EOS blockchain. Defense and execution evaluations show this strategy's reasonability, vigor, and dependability. It might also make use of virtual currency to increase the scope of this approach and create a system of trade for information. Besides that, there are a few issues with this strategy. For instance, the 3DEECS, which were created with revocable authorization, are insufficient. On BTDEC, numerous research assignments have been completed. For this method, a 3DEECS with an additional obvious execution would be beneficial. 'the's' is an a. For each and every information transmission, it would also be necessary to manage a huge number of datasets, but this effort might be accomplished more quickly. Blockchain has been suggested as a solution to the reasonableness issue with the present document encryption technology by a number of researchers.

V. REFERENCES

[1] Bodziony, Norbert, Pawe Jemioo, Krzysztof Kluza, and Marek R. Ogiela. 2021. "Blockchain-Based Address Alias System" in Journal of Theoretical and Applied Electronic Commerce Research 16, no. 5: 1280-1296. https://doi.org/10.3390/jtaer16050072

[2] N. Nizamuddin, H. R. Hasan, and K. Salah, “Ipfs-blockchain-based authenticity of online publications,” in Proc. International Conference on Blockchain, Seattle, Wash., USA, Jul. 2018, pp. 199–212..

[3] Ethereum White-Paper. Online: https://github.com/ethereum/wiki/wiki/ White-Paper, 2019..

[4] Cui, Shujie, Muhammad Rizwan Asghar, and Giovanni Russello. "Towards blockchain-based scalable and trustworthy file sharing." 2018 27th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2018.

[5] Y. H. Ho, Z. Cheng, P. M. F. Ho, and H. C. Chan, “Mobile intercloud system with blockchain,” in Proc. of the International MultiConference of Engineers and Computer Scientists, vol. 1, Hong Kong, China, Mar. 2018, pp. 100–105.Z. Cai, Z. He, X. Guan, and Y. Li, “Collective data-

sanitization for preventing sensitive information inference attacks in social networks," in IEEE Transactions on Dependable and Secure Computing, 2018, vol. 15, no. 4, pp. 1–590.

[6] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," in IEEE Transactions on Network Science and Engineering, 2020, vol. 7, no. 2, pp. 766–775.

[7] X. Zhou, W. Liang, K. Wang, R. Huang, and Q. Jin, "Academic influence aware and multidimensional network analysis for research collaboration navigation based on scholarly big data," in IEEE Transactions on Emerging Topics in Computing, no. 1, 2018.

[8] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flow estimation via taxi companies," in IEEE Transactions on Industrial Informatics, 2019, vol. 15, no. 12, pp. 6492–6499.

[9] M. Steichen, B. Fiz, R. Norvill, W. Shbair and R. State, "Blockchain- Based, Decentralized Access Control for IPFS," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1499-1506, doi: 10.1109/Cybermatics_2018.2018.00253.

[10] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Zeng, "A blockchain-enabled de-duplicatable data auditing mechanism for network storage services," in IEEE Transactions on Emerging Topics in Computing, 2020.

[11] M. A. Harlev, H. Sun Yin, K. C. Langenheldt, R. R. Mukkamala, and R. Vatrapu, "Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning," in Proceedings of the 51st Hawaii International Conference on System Sciences, 01 2018.

[12] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," in Computers & Security, 2018, vol. 72, pp. 1–12.

[13] P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, E. Izumchenko, A. Aliper, K. Romantsov, A. Zhebrak et al., "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," Oncotarget, vol. 9, no. 5, p. 5665, 2018.

[14] Cui, Shujie, Muhammad Rizwan Asghar, and Giovanni Russello. "Towards blockchain-based scalable and trustworthy file sharing." 2018 27th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2018.

[15] J. Sun, X. Yao, S. Wang and Y. Wu, "Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS," in IEEE Access, vol. 8, pp. 59389-59401, 2020, doi: 10.1109/ACCESS.2020.2982964.