(IJRST) 2022, Vol. No. 12, Issue No. IV, Oct-Dec **e-ISSN: 2249-0604, p-ISSN: 2454-180X**

Leveraging Blockchain Technology Centric Tools in Enhancing the Security Safeguards of Documents Storage[1]

Abhishek Dhillon

G D Goenka Public School, Sector-22, Rohini, New Delhi, India

DOI:10.37648/ijrst.v12i04.002

Received: 08 August 2022; Accepted: 20 October 2022; Published: 10 November 2022

ABSTRACT

The most widely used method for exchanging data worldwide is the Internet. Numerous cloud service providers support this sharing by letting customers store and share data over the Internet. However, cloud service providers have consistently failed to guarantee data's 100% security regarding privacy. Data breaches, piracy, and hacking attacks have threatened cloud providers' security mechanisms. However, customer data should be 100% secure because it may contain private information that should only be accessible to the owner and an intended audience. As a result, making this system more secure is critical to maintaining data privacy and cloud provider trust. We present a system that incorporates cloud-based data security into the Blockchain. It permits clients to store information in the cloud and gives a specific access control component that guarantees information security. Users can share data with others with permission by sharing the document's link with the intended user. The owner will have access to logs of all operations performed with the document at any time. This will guarantee the data's true ownership and privacy. A third party or individual will be permitted to access the document with prior authorization. This will increase cloud storage's security and reduce data breaches and attacks.

INTRODUCTION

Most businesses worldwide generate enormous amounts of data through their day-to-day operations. This data must be easily accessible and stored somewhere. These organizations face a significant challenge due to the storage and accessibility of enormous data. The cloud, a recently developed technology, offers a solution to this issue by enabling such organizations to store data on cloud storage and quickly and easily access it via the Internet. Additionally, a significant shift from on-premises to cloud computing occurred. An organization no longer needs to manage its data locally and make it accessible to users via the Internet at any time according to their preferences (public access or private access). Although this appears very effective from an organization's perspective, cloud storage carries several risks. Large cloud providers do not guarantee the security of the data being stored. When selecting cloud storage, the most important consideration should be safeguarding this data's confidentiality, integrity, and security.

A. Block Chain Technology Blockchain technology is a system that uses peer-to-peer nodes to store public transactional records, also known as the block, in multiple databases called "he "ch" in." This type of storage is typically referred to as a "digital ledger."

'The owner's digital signature authorizes every transaction in this ledger, thereby authenticating the transaction and protecting it from tampering. Subsequently, the data the advanced record contains is exceptionally secure.

To put it more succinctly, the digital ledger is similar to a Google spreadsheet shared among many computers in a network. It stores transactional records based on actual purchases. The fact that anyone can view the data without corrupting it is intriguing.

Blockchain combines three prominent technologies:

1) Cryptographic keys, 2) a peer-to-peer network with a shared ledger, and 3) a computing device for storing the network's transactions and records. Cryptography keys are made up of two keys: a private key and a public key. These two keys are what everyone uses to create a safe digital identity reference. These keys make it easier for two parties to carry out successful transactions.

[1] *How to cite the article:* Dhillon A., Leveraging Block Chain Technology Centric Tools in Enhancing the Security Safeguards of Documents Storage, IJRST, Oct-Dec 2022, Vol 12, Issue 4, 7-10, DOI: http://doi.org/10.37648/ijrst.v12i04.002

B. Dapps A decentralized application must be open source because it operates independently without a centralized entity controlling most of its tokens. Additionally, these DApps ought to have a public, decentralized blockchain that the application uses to store a cryptographic record of data, including transactions from the past.

DApps that are entirely closed-source or partially closed-source have emerged as the cryptocurrency industry develops, even though traditional DApps are typically open-source. As of 2019, only 15.7% of DApps are completely open source, compared to 25% of DApps that are completely closed source. This means that there is a smaller percentage of DApps where the application's code and smart contracts are completely available than those of DApps where their code is not disclosed. Transaction volumes are higher in open-source DApps and make the smart contract code available to the public. This suggests that open-source DApps are more popular than closed-source DApps.

C. Cloud Storage A type of computer data storage in which digital data are stored in logical pools, or "on the cloud," is known as cloud storage. Individuals and organizations purchase or lease storage capacity from the providers to store user, organization, or application data. Thev actual capacity traverses' numerous servers (sometimes in various areas), and the actual climate is commonly claimed and overseen by a facilitating organization. The physical environment's security, protection, and operation are the responsibility of these cloud storage service providers. A web service application programming interface (API), a collocated cloud computing service, or applications that use the API can access cloud storage services, such as cloud desktop storage, a cloud storage gateway, or Web-based content management systems.

EXISTING METHODOLOGIES

In the proposed system, we incorporate cloud-based data security into the Blockchain. The consequences of the framework vow to give the greatest security to the information put away on the cloud. The permission-based access control increases the data's security while making the system more trustworthy and reliable.

The presented results demonstrate that the proposed system effectively addresses cloud data security issues. The user-accessible logs guarantee that the actual owner of the data is aware of every data access operation, including read, write, and delete. The data remain intact thanks to this. Likewise, it guarantees that the permissioned client is ready to get to the information.

The logs will be responsible for providing this information to the data owner. Additionally, unauthorized access to data is discovered by the logs and reported to the owner. In a nutshell, the system and all of its features address several cloud data storage-related issues. Can defend against attacks based on collaboration is a current proposal.

A. Authentication and Login In this module, user credentials are entered and verified. As the initial step of verification, the username of the client and passwords are gathered through web shapes and are approved using the foundation process. To keep credentials safe, they are kept in a secure location.

Existing Systems	Proposed system
There are Many theories that have proposed the use of encrypted documents	There is no overhead of encryption and decryption
Cryptography is involved and it requires secure channel for sharing of various keys	There is no overhead of sharing keys as Cryptography is not Involved
There is no Involvement of Blockchain	The benefit of blockchain ledger, Consensus and its tamper proof nature is used for achieving more security
There are no logs generated and stored for every operation performed on each document	Here Logs are stored on Blockchain for every document and User can access these Logs stored on Blockchain
Cloud providers have sole right on document storage. He might perform unsecure operations on the document	As cloud database triggers are involved cloud provider has to take permission from user before doing any operation on document
The shared document links can be shared further to anyone, and User is unaware of who is using the link	If a document link is shared with anyone other than the trusted entity it will notify and request permission from the owner of the document
If User's account is hacked, he will lose full control of his account	Here even if the account is hacked the owner of the document will be notified on his mobile before any unethical operation is performed on the document

First, you must authenticate users before using the application. A straightforward registration form requires an email address and password for access. The same credentials should be used for cloud login whenever the s3 bucket's data is needed.

After successfully registering, users can use their email and password to log in. If a user forgets their password, the application allows them to change it safely by verifying their email first. Can use only registered mail to access the link to reset your password. The user must also be able to reset their credentials so that they can reset them whenever they forget their password.

B. Home Page When a user successfully logs in, the initial page of our application with a single button for uploading a new file is displayed. This button allows the user to upload the file to the cloud. Additionally, a search box and a view button are available, allowing the user to access documents from other users by entering the file's corresponding code C. Uploading Documents As soon as the user selects a file, an alert is displayed, prompting the user to confirm whether or not he consents to this action.

This application must use a meta mask to access the Blockchain. He must also confirm the transaction using the meta mask. The file is uploaded to the cloud after the transaction is completed. Last but not least, the log is saved on the Blockchain for future file creation.

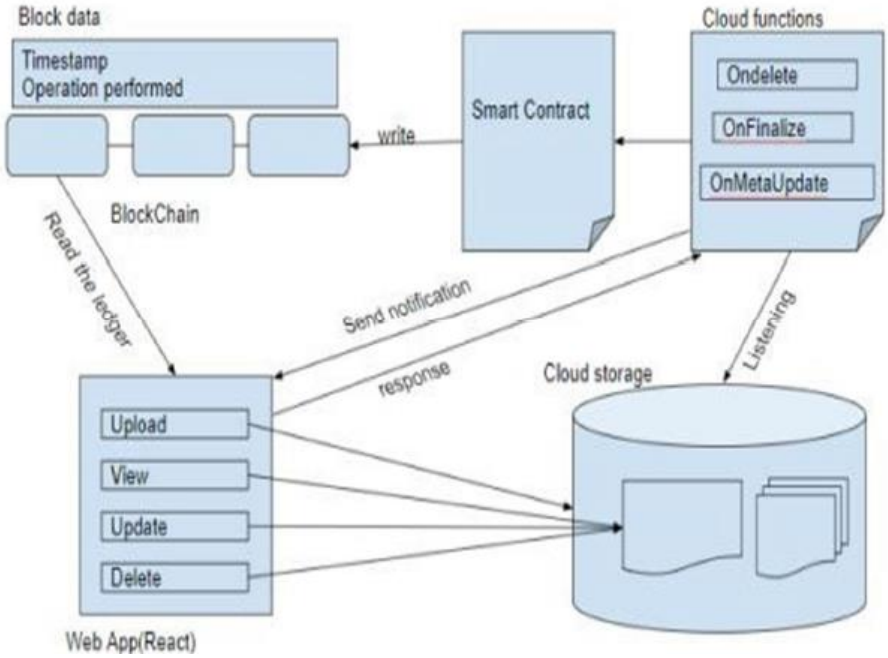

Fig 1: Architecture for Proposed Work

EXPERIMENTAL RESULTS

We have implemented a working prototype of the system and demonstrated how it functions with the additional security cloud providers offer. In our Framework, encryption, decoding and creating the hash for extraordinarily distinguishing the records in Blockchain isn't required as archives are put away for what it's worth with the simple expansion of triggers, and we use Client ID to extraordinarily distinguish the records on the Blockchain.

The time required to generate links, encrypt, and decrypt cloud-based documents will be saved by our system. It will save the memory space and energy expected for encryption and decoding. Users can refer to tamper-proof logs stored on the Blockchain for all operations and securely share data using two-factor authentication. The first step is sharing the link with a trusted entity.

CONCLUSION

Generating links, encrypting, and decrypting cloud-based documents will take less time with our system. Additionally, it will conserve the energy and memory space required for encryption and decryption. Users can refer to tamper-proof logs stored on the Blockchain for all operations and securely share data using two-factor authentication. The first step is sharing the link with a trusted entity.

The second step is to approve the notification for granting permission to prevent unauthorized access. This makes our system less expensive, more secure, and faster. This policy can be used in the future by any organization that uses public or private cloud storage to

store data more securely and protect it. By assigning user roles, you can safely store data in the cloud without concern for security breaches.

REFERENCES

1. Maximilian Wöhrer, Uwe Zdun, "Smart contracts: Security patterns in the ethereum ecosystem and solidity", International Workshop on Blockchain Oriented Software Engineering (IWBOSE), IEEE, 2018.
2. Qiwu Zou, Yuzhe Tang, Ju Chen, Kai Li, Charles A. Kamhoua, Kevin Kwiat, Laurent Njilla, "ChainFS: Blockchain-Secured Cloud Storage", IEEE 11th International Conference on Cloud Computing (CLOUD), 2018.
3. Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues", Elsevier, 2018
4. R.Gowthami Saranya, A.Kousalya, "A comparative analysis of security algorithms using cryptographic techniques in cloud computing", IEEE, 2017.
5. Ilya Sukhodolskiy, Sergey Zapechnikov, "A Blockchain Based Access Control System for Cloud Storage," IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2018.
6. Shubham Desai, Rahul Shelke, Omkar Deshmukh, Harish Choudhary, Prof. S. S. Sambhare "Blockchain Based Secure Data Storage and Access Control System using Cloud" IEEE - ICCUBEA 2019.
7. Gurudatt Kulkarni, Rani Waghmare, Rajnikant Palwe, Vidya Waykule, Hemant Bankar, Kundlik Koli, "Cloud Storage Architecture", IEEE 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA) Google Cloud Platform Documentation: https://cloud.google.com/docs AWS Documentation: https://docs.aws.amazon.com/
8. Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen, "A Survey on the Security of Blockchain Systems", Beijing university China, 2018.
9. Rongzhi Wang, "Research on data security technology based on cloud storage", 13th Global Congress on Manufacturing and Management, GCMM, 2016.
10. Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", IEEE 6th International Congress on Big Data, 2017.
11. Julija Golosova et.al. "The Advantages and Disadvantages of Blockchain Technology", IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), 2018.
12. Mr Anup R. Nimje et.al. "Blockchain Attribute Based Encryption Techniques in Cloud Computing Security : An Overview " IJCTT Volume 4, Issue 3-2013
13. Sangsuree Vasupongayya -"Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems", Research Article, 2019
14. Naresh vurukonda, B.Thirumala Rao, -"A Study on Data Storage Security Issues in Cloud Computing", 2nd International Conference on Intelligent Computing, Communication & Convergence , (ICCC-2016), 2018.
15. Guang Chen, Bing Xu1, Manli Lu1 and Nian-Shing Chen, -"Exploring blockchain technology and its potential applications", [Elsevier] 2018