IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Decentralized Secure Cloud Storage Using Blockchain

Hod.Rajesh Kolte
Department of Data Science Usha Mittal Institute of Technology
Mumbai, Maharashtra

Sharvee Gharat
Department of Data Science Usha Mittal Institute of Technology
Mumbai, Maharashtra

Srushti Jain
Department of Data Science Usha Mittal Institute of Technology
Mumbai, Maharashtra

Vedika Samant
Department of Data Science Usha Mittal Institute of Technology
Mumbai, Maharashtra

***Abstract*—Cloud storage is one of the leading options to store massive data, however, the centralized storage approach of cloud computing is not secure. On the other hand, Blockchain is a decentralized cloud storage system that ensures data security. Any computing node connected to the internet can join and form peers network thereby maximizing resource utilization. Blockchain is a distributed peer to peer system where each node in the network stores a copy of blockchain thus making it immutable. In the proposed system, the user's file is encrypted and stored across multiple peers in the network using the IPFS (InterPlanetary File System) protocol. IPFS creates hash value. The hash value indicates the path of the file and is stored in the blockchain. This paper focuses on decentralized secure data storage, high availability of data, and efficient utilization of storage resources.**

***Index Terms*—Decentralized Secure Cloud Storage Using Blockchain**

I. Introduction

As per the Forbes article [1], 2.5 quintillion bytes of data are produced each day. Out of the total data in the world over 90 percent of data was produced in the last 2 years. With such a massive increase in the data, cloud storage is required to store the data. Much of the data currently available through the internet is quite centralized and is stored with a handful of technology companies that have the experience and capital to build massive data centers capable of handling this enormous data. The problem with this approach is the security of data. As this data is stored in a centralized manner, if an attacker can gain access to the server he can easily view and modify the data. Another problem with this approach is the privacy of user data. In many instances, this data is used by third parties for data analysis and marketing purposes. Also, the cost incurred in storing data in centralized servers is more and many times users have to pay for the entire plan which they have selected even if they have used only a fraction of storage portion thus it does not provide flexibility to the user to pay only for what they are using. Another issue is the scalability of the system, it is difficult to scale a centralized storage system to meet the increasing demand. With zero trust two parties can transact in Blockchain.

II. Literature Review

2.1 Study on Data Security Policy Based On Cloud Storage
Abstract: Along with the growing popularisation of Cloud Computing. Cloud storage technology has been paid more and more attention as an emerging network storage technology which is extended and developed by cloud computing concepts. Cloud computing environment depends on user services such as high-speed storage and retrieval provided by cloud computing system. Meanwhile, data security is an important problem to solve urgently for cloud storage technology. In recent years, There are more and more malicious attacks on cloud storage systems, and cloud storage system of data leaking also frequently occurred. Cloud storage security concerns the user's data security. The purpose of this paper is to achieve data security of cloud storage and to formulate corresponding cloud storage security policy. Those were combined with the results of existing academic research by analyzing the security risks of user data in cloud storage and approach a subject of the relevant security technology, which based on the structural characteristics of cloud storage system.

2.2 Data security in cloud computing using AES under HEROKU cloud:
Abstract: Cloud security is an evolving sub-domain of computer and network security. Cloud platform utilizes third-party data centers model. An example of cloud platform as a service

(PaaS) is Heroku. It supports several programming languages that are used for web application deployment model. Heroku is based on a managed container system, with integrated data services and a powerful ecosystem, for deploying and running modern apps. One essential issue in cloud computing is data security, which is handled using cryptography methods. A possible method to encrypt data is Advanced Encryption Standard (AES). In this paper, we implement Heroku as a cloud platform, then we implement AES for data security in Heroku. The performance evaluation shows that AES cryptography can be used for data security. Moreover, delay calculation of data encryption shows that larger size of data increases the data delay time for encrypting data.

2.3 Bitcoin: A peer-to-peer electronic cash system

Abstract: A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

2.4 Decentralizing Privacy: Using Blockchain to Protect Personal Data

Abstract: The recent increase in reported incidents of surveillance and security breaches compromising users' privacy call into question the current model, in which third-parties collect and control massive amounts of personal data. Bit coin has demonstrated in the financial space that trusted, auditable computing is possible using a decentralized network of peers accompanied by a public ledger. In this paper, we describe a decentralized personal data management system that ensures users own and control their data. We implement a protocol that turns a block chain into an automated access-control manager that does not require trust in a third party. Unlike Bit coin, transactions in our system are not strictly financial – they are used to carry instructions, such as storing, querying and sharing data. Finally, we discuss possible future extensions to block chains that could harness them into a well-rounded solution for trusted computing problems in society.

2.5 BlockStore: A Secure Decentralized Storage Framework on Blockchain

Abstract: In order to ensure faster audits, higher transparency and security, many applications are being designed using blockchains. We propose BlockStore, a decentralized storage framework using blockchain technology. The primary motivation is efficient utilization of storage resources of users. Users often have un-utilized or underutilized storage in their devices. They can choose to host their storage resources when they are not in use. Users rent storage from the host for a fee for a fixed period of time and release back after the time expires. BlockStore keeps track of un-utilized storage of hosts in Space Wallet, a structure that helps in assigning storage to renters on request. The ownership of storage can be proved by logging all storage transactions in a public ledger (the blockchain), which can be verified by any user. A host cannot host the same storage to two users at the same time, nor can it tamper with the data of the renter. Renters cannot frame a host of cheating. BlockStore uses proofs of storage and data possession to verify that the hosts do not tamper with data and penalizes parties for misbehavior. Users can encrypt data for privacy. Payment and penalty are handled using smart contracts. BlockStore differs from existing solutions, by providing stronger audit that detects and penalizes misbehaving parties earlier than existing schemes.

III. Proposed System

In this initiative, customer data is securely stored using blockchain technology and cloud services. The proposed effort will separate the user file into blocks, encrypt each individual block using the AES technique, and then store each individual block in the IPFS server at various nodes. The memory address of the stored block will be returned by IPFS, and this address will be kept in the blockchain. While downloading, the program will gather all block addresses from Blockchain and send a request to IPFS using those addresses to obtain all file blocks. Once all file blocks have been obtained, all of the blocks will be combined and the client will be able to decrypt and download them.

IV. System Design and Implementation

A. System Architecture

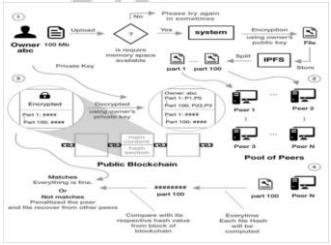

Fig. 1. System Architecture

B. Data Flow Diagram

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.

2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

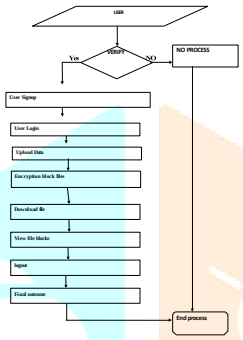

Fig. 2. Data Flow Diagram

C. Use Case Diagram

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

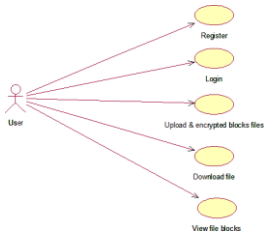

Fig. 3. Use Case Diagram

D. Class Diagram

The class diagram is used to refine the use case diagram and define a detailed design of the system. The class diagram classifies the actors defined in the use case diagram into a set of interrelated classes. The relationship or association between the classes can be either an quot;is-aquot; or quot;has-aquot; relationship. Each class in the class diagram may be capable of providing certain functionalities. These functionalities provided by the class are termed quot;methodsquot; of the class. Apart from this, each class may have certain quot;attributesquot; that uniquely identify the class.

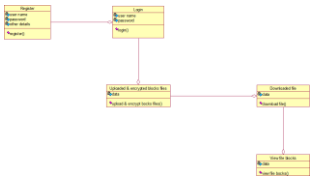

Fig. 4. Class Diagram

E. Activity Diagram

The process flows in the system are captured in the activity diagram. Similar to a state diagram, an activity diagram also consists of activities, actions, transitions, initial and final states, and guard conditions.

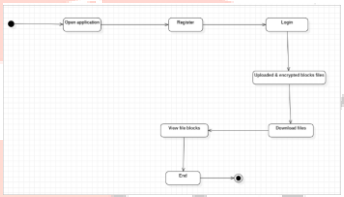

Fig. 5. Activity Diagram

F. Sequence Diagram

A sequence diagram represents the interaction between different objects in the system. The important aspect of a sequence diagram is that it is time-ordered. This means that the exact sequence of the interactions between the objects is represented step by step. Different objects in the sequence diagram interact with each other by passing quot;messagesquot;.

Fig. 6. Sequence Diagram

G. Collaboration Diagram

A collaboration diagram groups together the interactions between different objects. The interactions are listed as numbered interactions that help to trace the sequence of the interactions. The collaboration diagram helps to identify all the possible interactions that each object has with other objects.

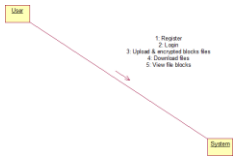

Fig. 7. Collaboration Diagram

H. Component Diagram

The component diagram represents the high-level parts that make up the system. This diagram depicts, at a high level, what components form part of the system and how they are interrelated. A component diagram depicts the components culled after the system has undergone the development or construction phase.

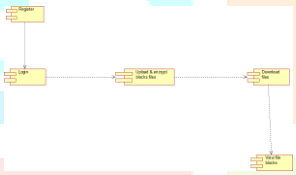

Fig. 8. Component Diagram

I. Deployment Diagram

The deployment diagram captures the configuration of the runtime elements of the application. This diagram is by far most useful when a system is built and ready to be deployed.

V. Conclusion and Future Scope

The proposed system enhances the security of data by encrypting and distributing the data across multiple peers in the system. Implemented system uses the AES 256bit encryption algorithm to encrypt the data ensuring the confidentiality of the user's data. Encrypted data is then distributed and stored across peers in the network using the IPFS protocol. Our system not only solves the privacy and security concerns of centralized cloud storage but also provides a medium for the peer to rent their underutilized storage and earn cryptocurrency in return thereby, maximizing the storage resource utilization.

Fig. 9. Deployment Diagram

Future Scope:

While our proposed system lays a solid foundation for decentralized secure cloud storage, there are several avenues for further research and development to explore:

1. Scalability Enhancement: Investigate scalability solutions such as sharding, layer 2 protocols, or off-chain storage to accommodate the growing volume of data and transaction throughput within the network.
2. Interoperability and Standards: Explore interoperability between different blockchain networks and standardization of protocols to enable seamless data exchange and interoperability across decentralized storage platforms.
3. Enhanced Privacy and Confidentiality: Research advanced cryptographic techniques such as zero-knowledge proofs, homomorphic encryption, and differential privacy to enhance privacy-preserving capabilities and protect sensitive data.
4. Usability and User Experience: Focus on improving user interfaces, accessibility, and user experience to make decentralized storage solutions more user-friendly and intuitive for individuals and businesses.
5. Regulatory Compliance and Governance: Address regulatory challenges and compliance requirements, such as GDPR, HIPAA, and data sovereignty laws, to ensure legal compliance and governance within decentralized storage networks.
6. Integration with Emerging Technologies: Explore integration with emerging technologies such as artificial intelligence, Internet of Things (IoT), and edge computing to enhance the functionality and applicability of decentralized storage solutions in diverse domains.
7. Real-World Adoption and Implementation: Conduct pilot projects and real-world deployments to evaluate the feasibility, performance, and practicality of decentralized secure cloud storage solutions in enterprise environments and everyday use cases.

By pursuing these avenues of research and development, we can further advance the capabilities, scalability, and adoption of Decentralized Secure Cloud Storage Using Blockchain, ultimately realizing its potential to revolutionize data storage and management in the digital age.

Acknowledgment

Gratitude is extended to all those who made it possible to complete this report.Special appreciation is given to the project guides, HOD Rajesh Kolte and Dr. Santoshi Pote for their invaluable contributions in providing stimulating suggestions and encouragement to coordinate the project and guide the team towards achieving the goal.

Heartfelt thanks are also extended to the team members, Sharvee Gharat, Srushti Jain, Vedika Samant, who worked tirelessly to assemble the project and provided valuable suggestions to enhance its quality.

Guidance and support provided by other supervisors and panels, especially in the paper presentation, were also appre-

ciated for helping to develop presentation skills and improve overall performance.

Lastly, appreciation is expressed to Usha Mittal Institute of Technology for providing the opportunity to complete this project within the stipulated time.This project was a valuable learning experience, and the support and encouragement received throughout its completion were greatly appreciated.Sincere gratitude is extended to everyone who played a role in the completion of this report, and whose support was crucial to its success

REFERENCES

[1] Bernard Marr, ”How Much Data Do We Create Every Day? The MindBlowing Stats Everyone Should Read.” Forbes, 2018.”

[2] Zhe, Diao, ”Study on Data Security Policy Based On Cloud Storage” 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids) IEEE, 2017.”

[3] Lee, Bih-Hwang, Ervin Kusuma Dewi, and Muhammad Farid Wajdi. ”Data security in cloud computing using AES under HEROKU cloud.” 2018 27th Wireless and Optical Communication Conference (WOCC). IEEE, 2018.”

[4] Nakamoto, Satoshi,”Bitcoin: A peer-to-peer electronic cash system”, (2008). [5] Zyskind, Guy, and Oz Nathan,” privacy: Using blockchain to protect personal data”,IEEE Security and Privacy Workshops. IEEE, 2015.”

[5] Cachin, Christian,” Architecture of the hyperledger blockchain fabric”, Workshop on distributed cryptocurrencies and consensus ledgers. Vol. 310. 2016.”

[6] Buterin, Vitalik, ”A next-generation smart contract and decentralized application platform”, white paper (2014).”

[7] Ruj, Sushmita, et al, ”BlockStore: A Secure Decentralized Storage Framework on Blockchain” 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA). IEEE, 2018.”

[8] Benet, Juan, “IPFS - Content Addressed, Versioned, P2P File System.” 2014. [10] Li, Dagang, et al. Meta-Key: ”A Secure Data-Sharing Protocol Under Blockchain-Based Decentralized Storage Architecture”, IEEE Networking Letters 1.1 (2019): 30-33.”

[9] Wohrer, Maximilian, and Uwe Zdun,”a Smart contracts: security patterns in the ethereum ecosystem and solidity”, International Workshop on Blockchain Oriented Software Engineering (IWBOSE). IEEE, 2018.”

[10] Sum, V. “SECURITY AND PRIVACY MECHANISM USING BLOCKCHAIN.” Journal of Ubiquitous Computing and Communication Technologies (UCCT) 1.01 (2019): 45-54

[11] Sivaganesan, D. “BLOCK CHAIN ENABLED INTERNET OF THINGS.” Journal of Information Technology 1.01 (2019): 1-8.