WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

A Decentralized Data Using a Block Chain Technique

Md. Khizer Mohinuddin[1], Ambadi Narendra[2], Harsha Vardhan[3], Mr. Suyash Agrawal[4]

[1,2,3] Computer Science and Engineering (Internet of Things), Guru Nanak Institutions Technical Campus, Telangana, India
[4]Asst. Professor, Computer Science and Engineering (Internet of Things, Guru Nanak Institutions Technical Campus, Telangana, India
[1]khizermd2003@gmail.com, [2]narendraambadi677@gmail.com, [3]harshavardhan933@gmail.com, [4]Suyash.agrawal1983@gmail.com

ABSTRACT -

A cloud-based storage system is one of the best options for storing large amounts of data, however, the centralized storage approach of cloud computing is not secure. The Block Chain is, on the other hand, a decentralized cloud storage system that ensures the security of data. A peer network can be formed by any computer connected to the Internet, thus maximizing the utilization of resources. It is a distributed peer-to-peer system in which every node in the network stores a copy of the block chain, making it immutable. The proposed system encrypts the user's file and stores it across multiple peers using IPFS (Interplanetary File System). Hash values are generated by IPFS. A hash value indicates the path of a file and is stored in the block chain. We focus on decentralized secure data storage, high availability of data, and efficient storage resource utilization in this paper.

Keywords - ***Blockchain Technology, Ethereum, Smart Contracts, IPFS Protocol, Hybrid Cloud, Encryption, Secure Transactions, Decentralized Cloud Storage***.

I. INTRODUCTION-

According to the Forbes article, 2.5 quintillion bytes of data are generated every day. The world's total data production has increased by more than 90 percent in the last two years. With such a massive increase in data, cloud storage is required to store the data. The majority of the data available through the internet today is centralized and is stored by a few technology companies that have the experience and capital to build large data centers capable of handling this vast amount of data. Data security is a problem with this approach. Data stored in a 5centralized manner makes it easy for an attacker to view and manipulate the information if he is able to gain access to the server. The privacy of user data is also a problem with this approach. This information is often used by third parties for the purposes of data analysis and marketing. The cost associated with storing data in centralized servers is also higher, and many users are required to pay for the entire plan even when they have used just a fraction of the storage space. Thus, the user does not have the flexibility to pay only for the amount of storage they use. It is also difficult to scale a centralized storage system to meet the increasing demand. It is possible for two parties to transact on a blockchain with zero trust. There are two types of transactions in the proposed system, namely, Access and Tata. Access is used for the control of permission for accessing the data, which will be set by the respective user who is in possession of the data, and Tata is used for the storage of the data. Third parties are prevented from accessing the data due to the shared encryption key. The author of Caching discusses the architecture of hyper ledger blockchain fabric, limitations of electronic coins, the operation of hyper ledger fabric, and the proof of work consensus algorithm. The Hyperledger Fabric is a permission-based blockchain network that allows only a limited number of nodes to add new nodes

An overview of the architecture of Ethereum and smart contracts is presented in the paper. Initially, Bitcoin was used primarily to send and receive cryptocurrency without adding any business logic. We discuss Ethereum applications such as decentralized file storage and decentralized autonomous systems. A decentralized framework using blockchain technology is proposed by Raj, Sushmita to enhance the security and transparency of transactions between peers (hosts and renters). Using proof of storage and proof of work, the system verifies that no host or donor tampers with data in the blockchain. Currently, the proposed system does not encrypt or decrypt data before uploading it to peers, which poses a threat to confidentiality and privacy. A peer-to-peer file transfer protocol called IPFS (Interplanetary File System) was introduced by Juan Benet et al. IPFS utilizes a content-based addressing system. IPFS offers content-addressed block storage along with content-addressed hyperlinks, according to the author. Li, Dagan, discusses how blockchain based applications differ from traditional applications in terms of data sharing. It has been pointed out by the author that data sharing in decentralized architectures can be cumbersome. The author proposes Meta-key for the secure sharing of data in a decentralized storage system based on blockchain technology, and he also proves its collusion-free property. According to Wohrer et al., the solidity used to create smart contracts on blockchains and their difficulty is explained. The following security issues have been resolved: The Checks-Effects Interaction, Stopping in case of emergency, speed bump, limit on the rate, mutex limit on the balance.

Many blog articles and grey literature articles address these issues. In addition to providing scalability, security, and sustainability, blockchain technology is also helpful for transforming the way businesses operate. A comprehensive survey is presented in this paper on the technical and application of

blockchain technology by discussing its structure with respect to different consensus algorithms. According to the author, the structure of a blockchain consists of data, timestamps, and addresses of previous blocks. The timestamp records the time at which the block was created. It is a hash function that generates a unique output from an input of any length. A hash value of the previous block is contained in each block. As a result, Blockchain provides an increased level of security.

OBJECTIVE-

Providing security to user data storage is the objective of this project. Our objective in this paper is to develop a decentralized storage system that is reliable, efficient, and has a high level of data availability. The implemented system utilizes the AES 256-bit encryption algorithm in order to encrypt user data and ensure its confidentiality. IPFS is used to distribute and store encrypted data across peers in the network.

SCOPE OF THE PROJECT-

The purpose of this research is to not only resolve the privacy and security concerns associated with centralized cloud storage, but also provide a means for peers to rent their underutilized storage, maximizing the utilization of storage resources.

II. METHODOLOGIES-

1**. User Interface Design**

In this module, we'll design login windows to ensure secure access. Users will need to provide their username and password to connect to the server. New users can register with their email address to create an account and track their data usage.

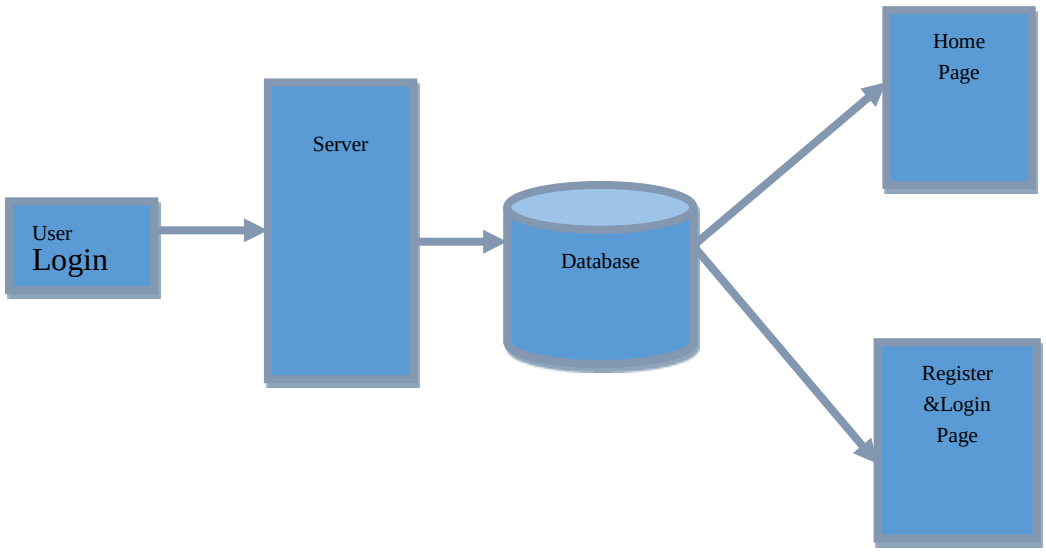

Figure 1: User Interface design

2. Cloud Storage

This is the first module of the project, which focuses on the Cloud Storage system. In this module, the Cloud Storage system serves as the central component with complete control over all operations. Key functionalities include:

•The ability for the Cloud Storage system to log in.

•Tracking and managing data accessed by users.

•Storing and maintaining block data information.

•Managing a database of data owners and their details.

•Keeping records of data users in the database.

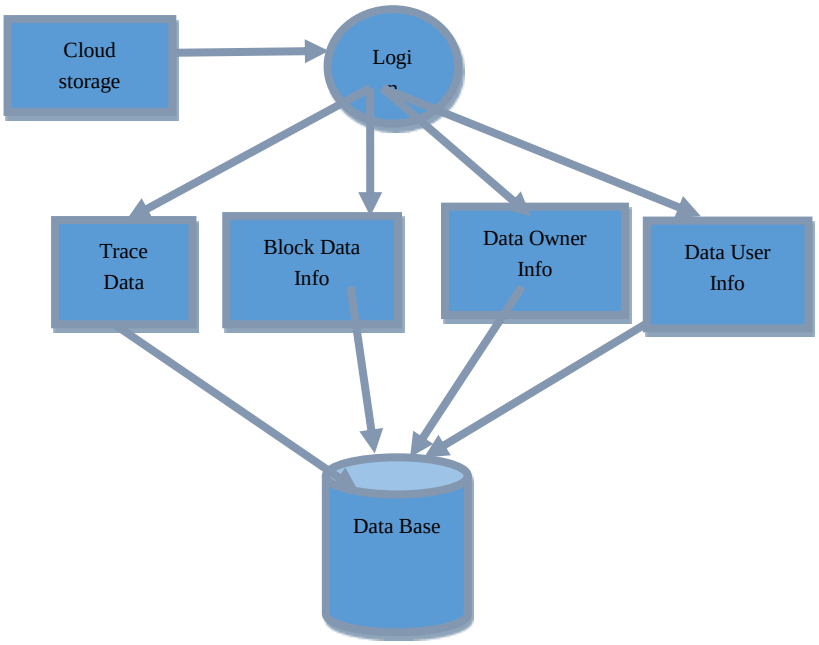

Figure 2: Cloud Storage

3. Data Owner-

In this module, the data owner registers and logs in, uploads and views files, reviews user access requests, and sends encryption keys to users

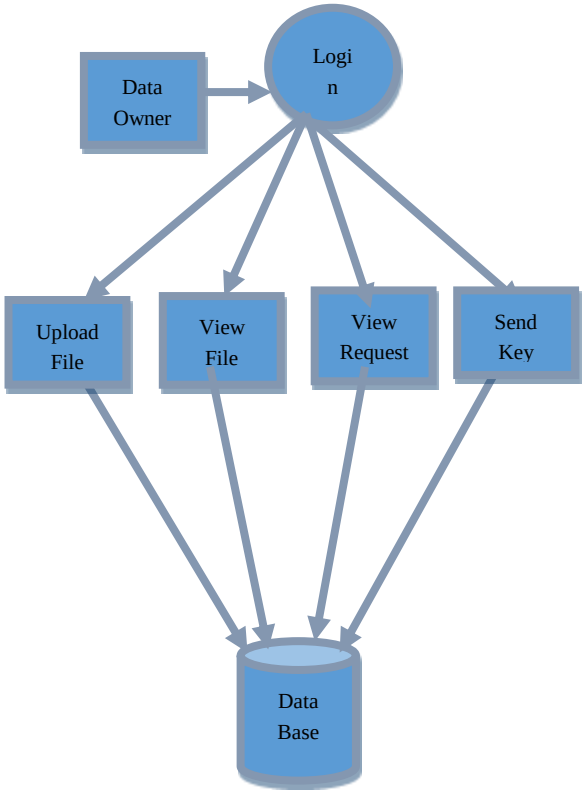

Figure 3: Data Owner

4. Data User

In this module, the user registers and logs in, searches files by name, and views responses from the database.

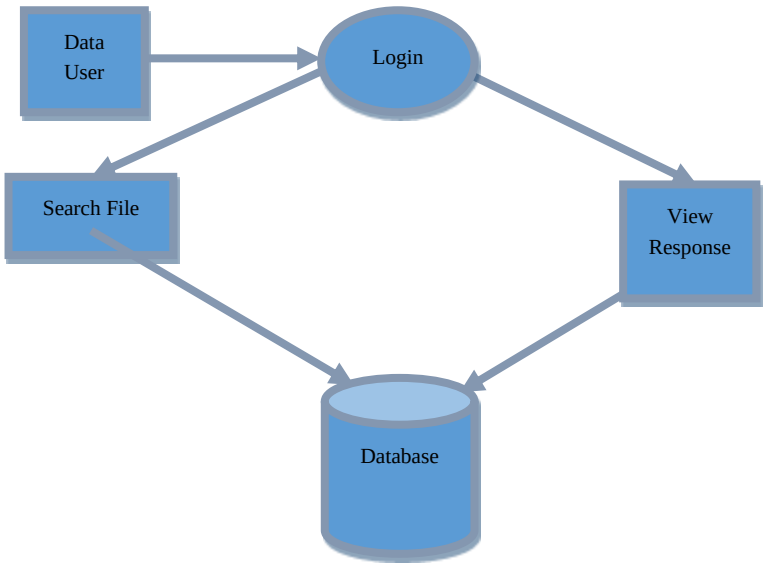

Figure 4: Data User

AES Algorithm-

The Advanced Encryption Standard (AES) is a widely used symmetric block cipher for encrypting sensitive data in software and hardware globally. Critical for government security, cybersecurity, and electronic data protection, AES employs 128-bit, 192-bit, or 256-bit key lengths to encrypt and decrypt 128-bit message blocks, using the same key for both processes.

SHA Algorithm-

SHA algorithms generate a fixed-size hash, or digest, from any input, typically represented in hexadecimal. They operate as:

- Hash Functions: Converting input data of any size into a fixed-size hash.
- One-Way Functions: Preventing the reverse derivation of input from the hash.
- Collision-Resistant Mechanisms: Making it difficult to find two inputs with the same hash.
- Output Varies by Version: For example, SHA-256 produces a 256-bit hash.
- Widely used in modern cryptography, SHA ensures data integrity, authenticity, and security. Selecting the right SHA version based on security needs and monitoring vulnerabilities is critical for robust cryptographic systems.

III. Related Work Area-:

I.Kumar,J.Singh., explains Smart contracts on blockchain, particularly Ethereum, eliminate trusted third parties by embedding contract terms in code. Writing secure contracts in Solidity is challenging. Using Grounded Theory, researchers identified security patterns to address common vulnerabilities. These patterns help Solidity developers mitigate typical attack scenarios and enhance contract performance and security.

G. Thompson, H. Nguyen., explains Decentralized Finance (DeFi) is a new paradigm in the creation, distribution, and utilization of financial services via the integration of blockchain technology. Our research conducts a comprehensive introduction and meticulous classification of various DeFi applications. Beyond that, we thoroughly analyze these risks from both technical and economic perspectives, spanning multiple layers. We point out research gaps and revenues, covering technical advancements, innovative economics, and sociology and ecology optimization.

E. Wang, F. Zhang., explains This paper surveys blockchain adoption in supply chain management (SCM), analyzing 97 publications. It highlights blockchain's role in improving transparency, traceability, trust, and anti-counterfeiting while addressing SCM issues like security and fraud. Applications, benefits, and research challenges are explored, providing insights and future directions for blockchain integration in SCM.

A. Smith, B. Johnson., explains the surveys blockchain-based healthcare solutions, analyzing over 40 systems through a systematic framework covering interactions, components, challenges, and benefits. Blockchain's decentralization, transparency, and smart contracts address data security, privacy, and interoperability issues. It discusses regulatory compliance with GDPR and HIPAA, emphasizing blockchain's potential in secure health data sharing.

C. Lee, D. Patel.,explains the proposes a blockchain-based decentralized identity management system using self-sovereign identity, decentralized identifiers, and verifiable credentials. It eliminates central authorities, enhances user control over data, ensures secure identity verification, reduces verification time, enables permissioned data sharing, and verifies data origin, addressing privacy and security issues of centralized systems.

IV. Result-

A decentralized data storage system leveraging blockchain technology to address the limitations of centralized cloud storage, such as security vulnerabilities, privacy concerns, and scalability issues. The proposed system integrates blockchain with the Interplanetary File System (IPFS) for distributed storage, ensuring high data confidentiality through AES-256 encryption. By fragmenting and storing data across network peers, the system enhances security, availability, and resource utilization, allowing peers to share unused storage. It eliminates centralized control, enabling cost-effective, pay-as-you-use storage solutions. Key techniques include AES encryption, SHA hashing for file integrity, and Proof-of-Work for transaction validation. The system design incorporates distinct components for cloud storage, data owners, and data users, with encryption keys managed securely and shared only with authorized users. Developed using Java, J2EE, and MySQL, the system underwent rigorous testing to ensure reliability and robust functionality. Future enhancements include adaptive scheduling for frequent file access and advanced consensus mechanisms to improve scalability. This study demonstrates the potential of blockchain to revolutionize cloud storage by offering a secure, efficient, and user-centric alternative.

V. Conclusion:

This research presents a decentralized data storage system leveraging blockchain and IPFS protocols to address the challenges of centralized cloud storage. By integrating AES-256 encryption and SHA algorithms, the proposed solution ensures enhanced security, data privacy, and integrity while optimizing resource utilization. The decentralized architecture eliminates reliance on single points of failure, providing scalability and high availability. This system demonstrates significant potential for applications in sectors requiring secure and transparent data management. Future advancements, such as adaptive scheduling and further optimization of access mechanisms, can enhance the system's efficiency and usability, paving the way for broader adoption of blockchain-based decentralized storage solutions.

REFERENCES-

[1]A. S. Masurkar, X. Sun and J. Dai, "Using Blockchain for Decentralized Artificial Intelligence with Data Privacy," 2023 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA,2023,pp.195-201,doi: 10.1109/ICNC57223.2023.10074247.

[2] Sum, V. “SECURIT Y AND PRIVACY MECHANISM USINGBLOCKCHAIN.” Journal of Ubiquitous Computing and Communication T technologies (UCCT) 1.01 (2019): 45 -54

[3] Siva Ganesan, D. “BLOCK CHAIN ENABLED INT ERNET Font HINGS.” Journal of Information T technology 1.01 (2019): 1-8.

[4]Li, Dagan, et al. Meta-Key: ”A Secure Data-Sharing Protocol Under Blockchain-Based Decentralized Storage Architecture”, IEEE Networking Letters 1.1 (2019)

[5]Bernard Marr, ”How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read.” Forbes, 2018.

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

[7]Wuhrer, 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

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

[9]Zha, Diao, ”Study on Data Security Policy Based on Cloud Storage”2017 ire 3rd international conference on big data security on cloud(bigdata security), ire international conference on high performance and smart computing (hips), and ire international conference on intelligent data and security (ids) IEEE, 2017.

[10] Caching, Christian,” Architecture of the Hyperledger blockchain fabric”, Workshop on distributed cryptocurrencies and consensus ledgers. Vol.310. 2016.

[11]Ziskind, Guy, and Oz Nathan,” privacy: Using blockchain to protect personal detainee Security and Privacy Workshops. IEEE, 2015.

[12] Benet, Juan, “IPFS - Content Addressed, Versioned, P2P File System.”2014

[13] Butlerin, Vitali, ”A next-generation smart contract and decentralized application platform”, white paper (2014).

[14] Nakamoto, Satoshi, ”Bitcoin: A peer-to-peer electronic cash system”,(2008).