Filed-UP

A web - based application for decentralized file storing using blockchain

MOHITH RAAGESH B

21BCE1840

Project Abstract:

- Our web-based application leverages blockchain technology to create a decentralized file storage system, ensuring the integrity and permanence of files. Users can upload files of any type and size, with each file being stored in a blockchain block that includes metadata such as the username, file size, and file data. This block is then appended to the blockchain, making any subsequent modification or deletion impossible.
- To achieve the required security, our system incorporates a proof-of-work mechanism with a randomly generated nonce, achieving a difficulty level of 3. This ensures that the blockchain remains secure and resistant to tampering. By decentralizing file storage, our application protects against data corruption and unauthorized alterations, providing a robust solution for secure file management.

Literature Survey

1. **"Decentralized and Secure File Storage System Using Blockchain" by A. Sharma et al. (2018)**
   This paper introduces a decentralized file storage system leveraging blockchain technology. It focuses on enhancing data security by distributing file storage across multiple nodes in a peer-to-peer network. The system uses blockchain's inherent immutability to ensure that files cannot be altered or deleted. The authors also discuss the scalability challenges posed by storing large files directly on the blockchain and propose a solution that uses InterPlanetary File System (IPFS) for off-chain storage, with the blockchain storing metadata.
2. **"A Blockchain-Based Decentralized Data Storage and Access Framework for PingER Network" by S. Singh and B. Gupta (2019)**
   Singh and Gupta propose a blockchain-based framework for secure and decentralized data storage within the PingER network. Their system uses

blockchain to store access control policies and file metadata, ensuring that data integrity and access rights are maintained. The paper highlights the efficiency of using a hybrid approach where file data is stored off-chain while the blockchain records the critical metadata. This separation allows for secure and scalable data storage.

3. **"Blockchain for Secure Cloud Storage: A Systematic Review" by J. H. Park et al. (2020)**
   This systematic review explores the integration of blockchain with cloud storage systems to enhance data security and privacy. The paper discusses various blockchain-based storage systems, focusing on how they prevent unauthorized access, data tampering, and deletion. The review highlights the importance of blockchain's immutable ledger in maintaining the integrity of stored files and suggests that blockchain can be a viable solution for decentralized and secure cloud storage.

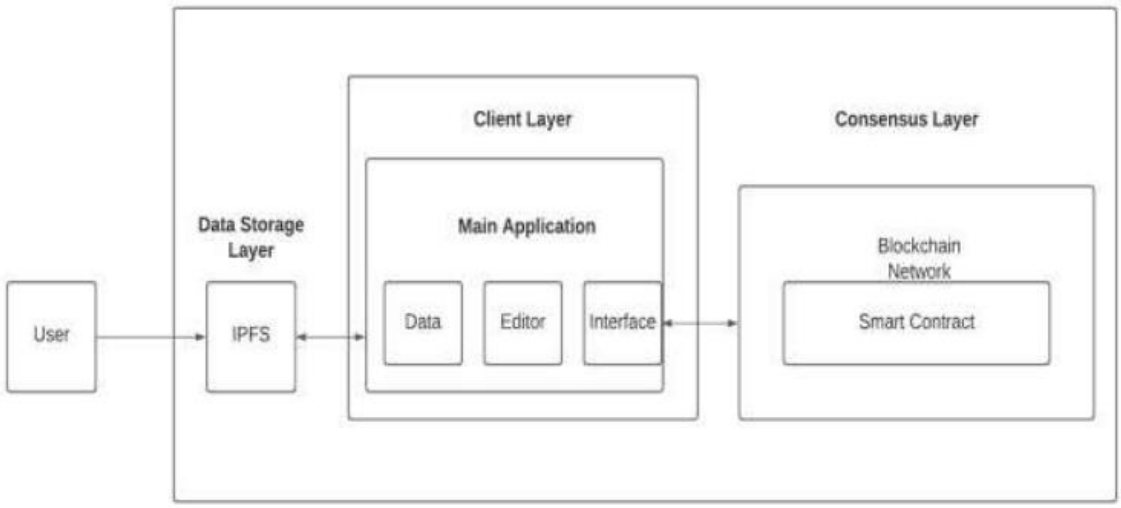
4. **"Filecoin: A Decentralized Storage Network" by Protocol Labs (2017)**
   The Filecoin whitepaper introduces a decentralized storage network where users pay to store their files, and storage providers earn rewards for storing and maintaining these files. Filecoin uses blockchain to record transactions and ensure the integrity and availability of stored data. The network's proof-of-replication and proof-of-spacetime mechanisms ensure that files are stored securely and can be retrieved when needed. This paper serves as a foundation for understanding how blockchain can be used to incentivize decentralized storage and ensure data immutability.

5. **"A Secure Data Sharing Scheme in Public Clouds Using Blockchain" by H. Li et al. (2018)**
   Li et al. propose a secure data-sharing scheme that combines blockchain and public cloud storage. Their approach uses blockchain to manage access control and ensure that data cannot be tampered with once shared. The system stores encrypted files on the cloud, with the blockchain recording encryption keys and access rights. This method ensures that only authorized users can access and decrypt the stored files, providing a high level of data security and integrity.

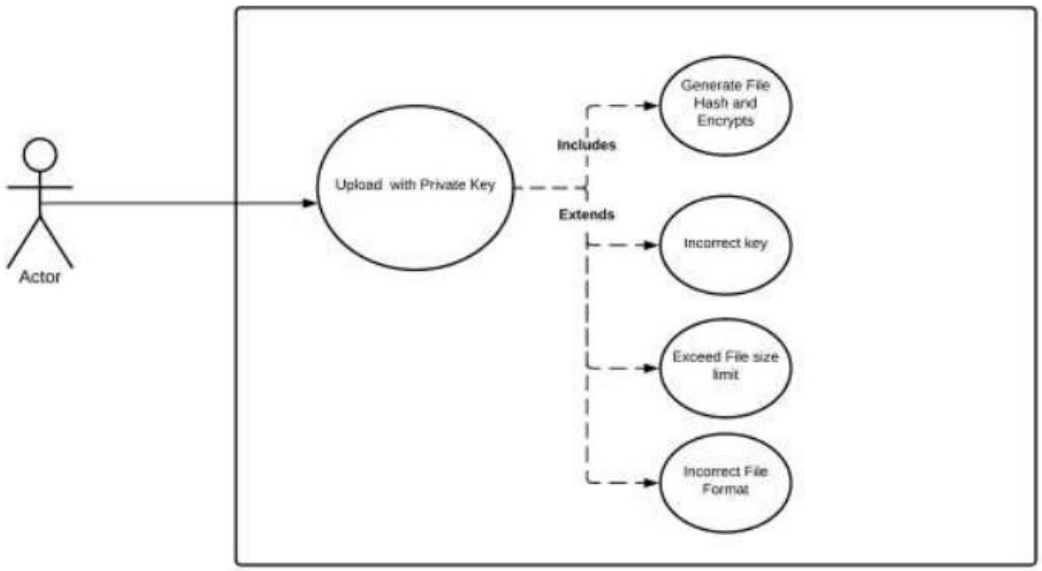
6. **"Proof of Work and Bread Pudding Protocols: Incentives for Security in Blockchain Systems" by M. Castro and A. Clement (2019)**
   This paper explores the proof-of-work (PoW) concept in blockchain systems, discussing its role in ensuring security and consensus. The authors analyze various PoW mechanisms and their effectiveness in preventing attacks on the blockchain. They also discuss the trade-offs between security and

computational overhead, which is critical for systems like decentralized file storage that rely on PoW to secure data blocks. The insights from this paper are directly applicable to your project, as it highlights the importance of designing a PoW system that balances security with performance.

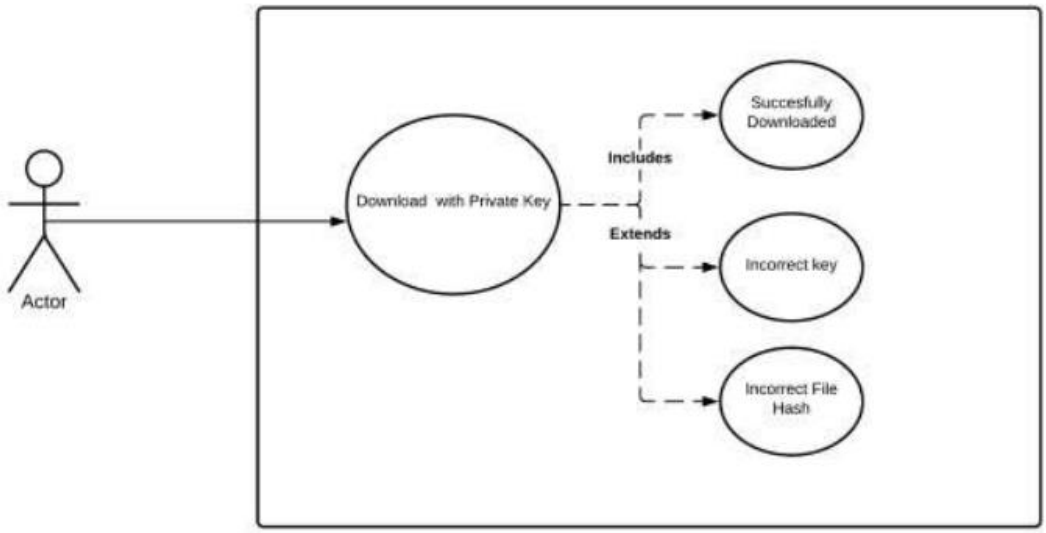
System Architecture Diagram



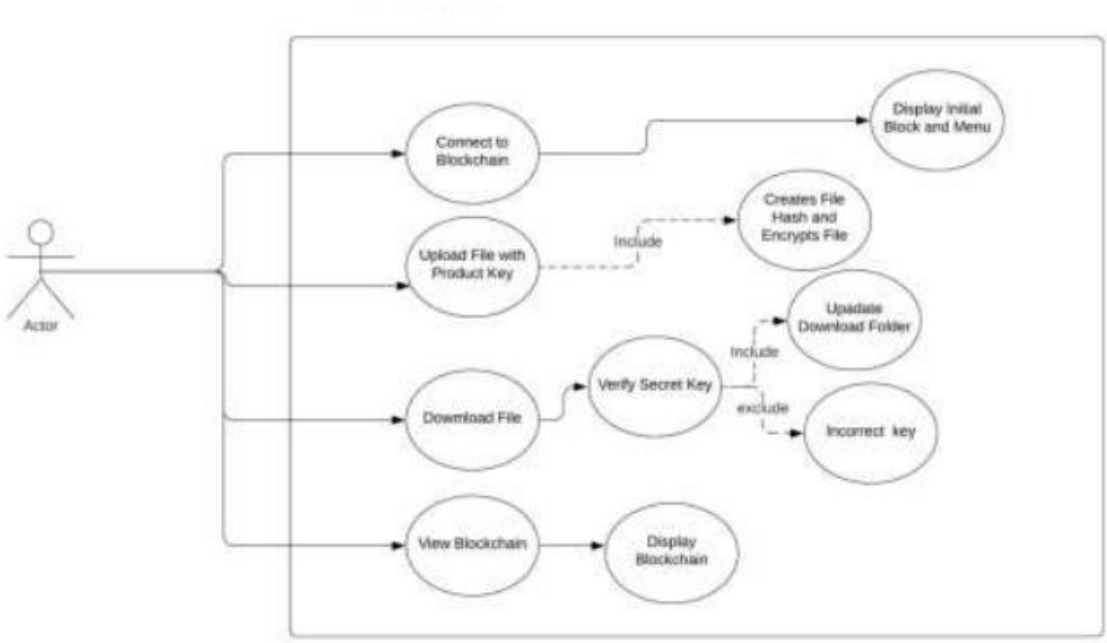
Upload Use Case diagram



Download Use case diagram



System use case diagram



Done by,

B Mohith Raagesh

21BCE1840