A Seminar on

Decentralized File Sharing: Blockchain and Cryptography

Team Details

1. K. Preetham(20EG105122)
2. M. Ananya(20EG105132)
3. P. Bhanuprakash(20EG105140)
4. S. Harshitha(20EG105144)

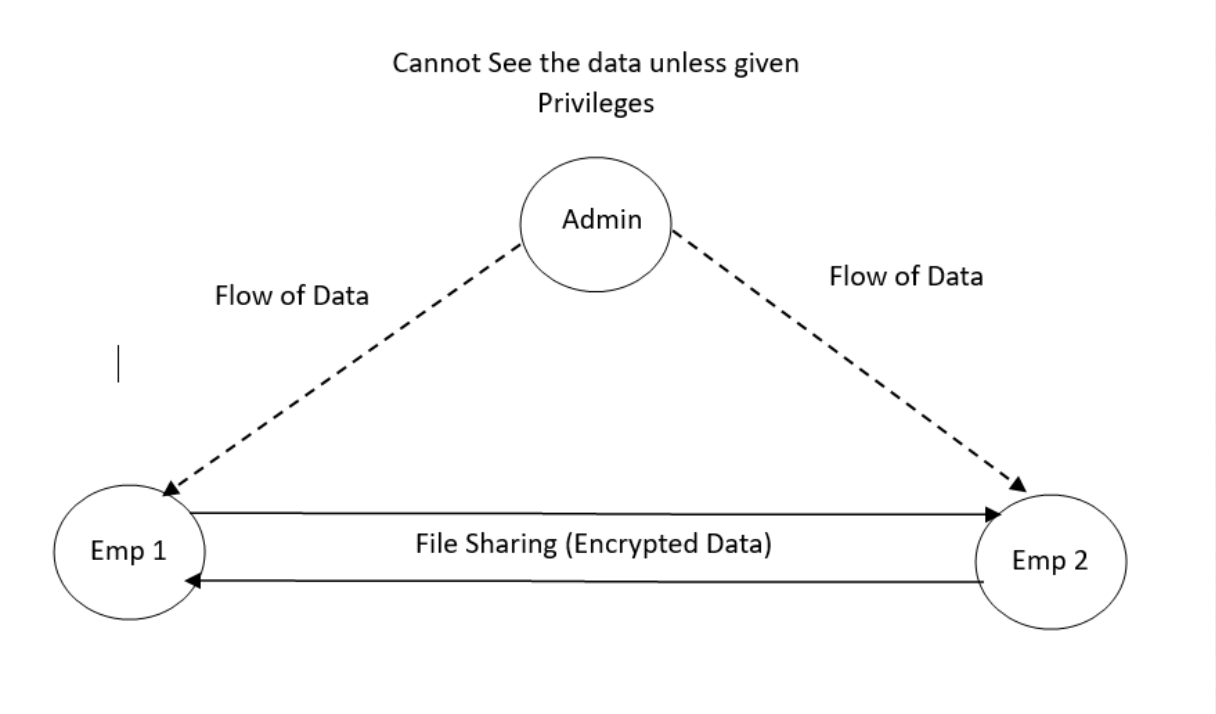
Project Supervisor

Dr. G. Prabhakar Raju
Assistant Professor

Introduction

- This method introduces a new way for organizations to securely share files within a group.
- Traditional methods often lack trust, transparency and traceability.
- To overcome this, we suggest using blockchain technology, which ensures security and transparency.
- Our system allows organizations to exchange files securely and transparently by leveraging blockchain.
- We use Hyperledger Fabric to set up the blockchain network and manage contracts.
- This approach ensures that files are shared confidentially, with integrity and availability, benefiting consortiums by enhancing trust, efficiency and transparency.

Concept Tree



Literature

S. No.	Paper Name	Publisher and year	Author(s)	Method	Merits	Demerits
1	FILE SHARING USING BLOCKCHAIN	IEEE - 2023	N Jeenath Laila Dr. G Tamilpavai S Sarvana Kumar	Cryptography Blockchain Technology	Security Decentralization Data Integrity	Scalability Complexity Privacy
2	Blockchain-Based Anonymous Data Sharing With Accountability for Internet of Things	IEEE - 2023	Tong Wu Weijie Wang Chuan Zhang Weiting Zhang Liehuang Zhu Keke Gai Haotian Wang	Blockchain Technology IoT	Security Privacy Accountability	Scalability Complexity
3	A Secure Framework for Communication in Internet of Things Application using Hyperledger based Blockchain	IEEE - 2020	Utkalika Satapathy Bhabendu Ku. Mohanta Soumyashree S Panda Srichandan Sobhanayak Debashis Jena	Blockchain Technology Hyperledger IoT and Communication Protocols	Decentralization Trust lessness Security and Privacy	Complexity Resource Intensiveness Integration Challenges

Literature(cont..)

4	Bitcoin: A Peer-to-Peer Electronic Cash System	IEEE - 2020	Satoshi Nakamoto	Proof-of-Work (PoW) Blockchain Technology Peer-to-Peer Network	Decentralization Trust lessness Global Accessibility	Scalability No Anonymity Privacy Concerns
5	A Secure File Sharing System Based on IPFS and Blockchain	IEEE - 2022	Hsiao-Shan Huang Tian-Sheuan Chang Jhih-Yi Wu	Cryptography Blockchain Technology	Decentralized Access Control Group Management	Complexity Size Limitations
6	A peer-to-peer file storage and sharing system based on consortium blockchain	IEEE - 2022	Shaoliang Peng Wenxuan Bao Hao Liu Xia Xiao Jiandong Shang Lin Han Shan Wangde Xiaolan Xie Yang Xu	Blockchain Technology Peer-to-Peer	Security Fault Tolerance Privacy Protection	Scalability Complexity
7	Blockchain based Security Framework for P2P Filesharing system	IEEE - 2022	Srikanta Pradhan Somanath Tripathy Sukumar Nandi	Blockchain Technology	Decentralization Incentive Mechanism	Scalability Complexity

Problem Statement

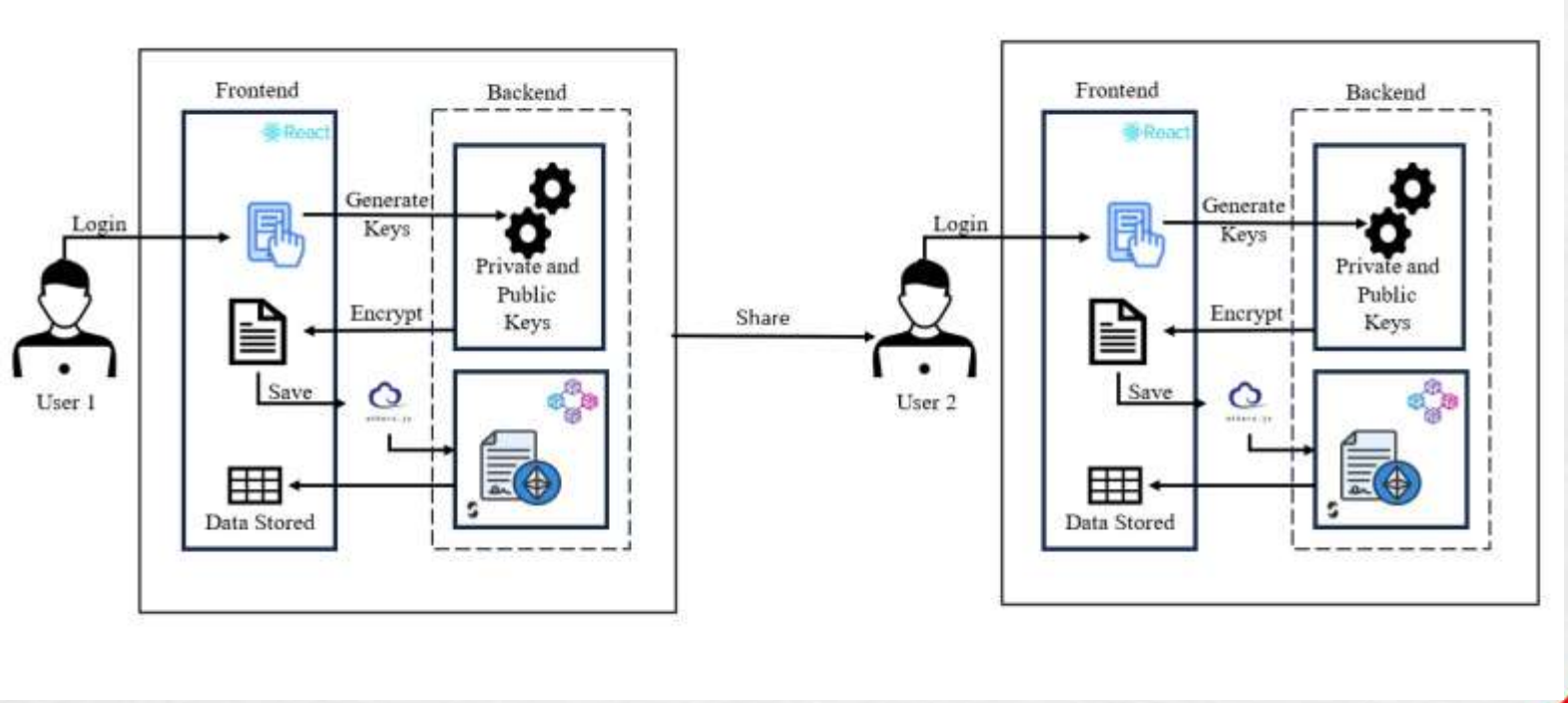
- The major underlying problem in research data sharing is the fear of researchers regarding misuse and **misinterpretation of data.**

- The solution proposed to this problem is the protection of identities of every individual and controlled access to the data rather than making all the data open access.
- **“These solutions cannot provide trust, immutability to digital data, and traceability regarding data usage.”**

Proposed Method

- The proposed system provides secure file-sharing across a consortium of organizations using blockchain.
- It provides confidentiality, integrity, and availability of shared files. It ensures end to end encryption of the files.
- The content ID of the shared file is stored on the blockchain in a tamper resistant way.
- The encrypted file and file metadata is stored in a distributed fashion on the distributed storage and blockchain ledger respectively.

Architecture



Parameters

Each user generates a key pair

i.e. public and private key using the following steps:

- *each user selects two large primes at random -* ***p, q***
- *compute their system modulus* ***n=p.q***
- *calculate* ***ø(n)****, where* ***ø(n)=(p-1)(q-1)***
- *selecting at random the encryption key* ***e****, where* ***1<e<ø(n)****,and* ***gcd(e,ø(n))=1***
- *solve following equation to find decryption key* ***d: e.d=1 mod ø(n)*** *and* ***0≤d≤n***
- *publish their public encryption key:* ***KU={e,n}***
- *keep secret private decryption key****: KR={d,n}***

Experiment Environment

Hardware Requirements

Technology	Python 3.6
Operating System	Windows Family
IDE	VS Code
Technology	Python, Django
Database Server	MySQL
Front Design Technology	HTML, CSS, JS

Software Requirements

RAM	4 GB Minimum
Processor	i3 Minimum
Hard disk	250 GB HDD Min

Project status

S.No	Functionality	Status (Completed /in-progress/Not started)
1.	Front-End	Completed
2.	Database	In-Progress
3.	Smart Contract	Not Started

References

- N. Jeenath Laila, G. Tamilpavai, S. Saravana Kumar, "File Sharing Using Blockchain," Assistant Professor, Department Of CSE, GCE, Tirunelveli-7, India. Professor, Department Of CSE, GCE, Tirunelveli-7, India. Student, Department Of CSE, GCE, Tirunelveli-7, India. DOI: https://www.doi.org/10.56726/IRJMETS41190.
- T. Wu, W. Wang, C. Zhang, W. Zhang, L. Zhu, K. Gai, and H. Wang, "Blockchain-Based Anonymous Data Sharing with Accountability for Internet of Things," Tong Wu - Member, IEEE. Weijie Wang - Chuan Zhang - Member, IEEE. Weiting Zhang - Member, IEEE. Liehuang Zhu - Senior Member, IEEE. Keke Gai - Senior Member, IEEE. Haotian Wang.
- U. Satapathy, B. K. Mohanta, S. S. Panda, S. Sobhanayak, and D. Jena, "A Secure Framework for Communication in Internet of Things Application using Hyperledger based Blockchain," Department of Computer Science and Engineering, IIT Bhubaneswar, Odisha, India, 751003. Emails: A117010@iiit-bh.ac.in (Utkalika Satapathy), C116004@iiit-bh.ac.in (Bhabendu Ku. Mohanta), C117011@iiit-bh.ac.in (Soumyashree S Panda), srichandan@iiit-bh.ac.in (Srichandan Sobhanayak), debasish@iiit-bh.ac.in (Debashis Jena).

References

- S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System."
- H.-S. Huang, T.-S. Chang, J.-Y. Wu, "A Secure File Sharing System Based on IPFS and Blockchain," Department of Electronics Engineering, National Chiao-Tung University, Telecommunication Laboratories, Chunghwa Telecom Co., Ltd., Hsinchu, Taiwan. Emails: tschang@mail.nctu.edu.tw (Tian-Sheuan Chang), ian_wu@cht.com.tw (Jhih-Yi Wu), phm@cht.com.tw (Hsiao-Shan Huang).
- S. Wang, Y. Zhang, and Y. Zhang, "A Blockchain-Based Framework for Data Sharing with Fine-Grained Access Control in Decentralized Storage Systems," School of Science, Xi'an University of Technology, Xi'an 710048, China. School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China. Corresponding author: Yinglong Zhang (ylzhang3550@gmail.com). This work was partly supported by the National Natural Science Foundation of China under Grants 61572019 and 61173192, and partly by the Key Project of Natural Science Foundation of Shaanxi Province of China under Grant 2016JZ001.

References

- S. Pradhan, S. Tripathy, and S. Nandi, "Blockchain-based Security Framework for P2P Filesharing System," Department of Computer Science & Engineering, Indian Institute of Technology Patna, India. Email: srikanta.pcs16@iitp.ac.in (Srikanta Pradhan), som@iitp.ac.in (Somanath Tripathy), sukumar@iitg.ernet.in (Sukumar Nandi).

Thank you