IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203147 |

# Blockchain A Game Changer for Secure Transferring of Data

**Kandula Surya Prakash, Narayandas Varun Karthikeya, Puppireddy Sai Krishna, M. Sandhya Rani**

Student, Department of CSE, Anurag University, Telangana, India

Student, Department of CSE, Anurag University, Telangana, India

Student, Department of CSE, Anurag University, Telangana, India

Assistant Professor, Department of CSE, Anurag University, Telangana, India

**ABSTRACT**: A consortium of organizations collaborates and exchanges information to create synergies in their operations. Centralized systems of secure transferring of data cannot provide distributed trust and transparency. Blockchain technology can be used to transfer data securely and transparently. This paper proposes a blockchain based secure transferring of data. It can be used by a consortium of organizations to securely exchange files in a distributed fashion. Hyperledger Fabric, an enterprise blockchain framework, is used for blockchain network setup and the development of smart contracts. The Inter Planetary File System (IPFS) is used for storing files in a distributed way. The paper provides the workflow for identity management and file-sharing processes. The proposed system allows a consortium of organizations to share files with confidentiality, integrity, and availability using blockchain.

**KEYWORDS:** Ganache, VSCode , Ethereum, MySQL, RSA

## I. LITERATURE SURVEY

**S. Nakamoto, "bitcoin: A peer-to-peer electronic cash system," 2008.**
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. We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

**Naz M, Al-zahrani FA, Khalid R, Javaid N, Qamar AM, Afzal MK, Shafiq M. A secure data sharing platform using blockchain and interplanetary file system. Sustainability. 2019 Dec 10;11(24):7054.**
In a research community, data sharing is an essential step to gain maximum knowledge
from the prior work. Existing data sharing platforms depend on trusted third party (TTP). Due to the involvement of TTP, such systems lack trust, transparency, security, and immutability. To overcome these issues, this paper proposed a blockchain-based secure data sharing platform by leveraging the benefits of interplanetary file system (IPFS). A meta data is uploaded to IPFS server by owner and then divided into n secret shares. The proposed scheme achieves security

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203147 |

and access control by executing the access roles written in smart contract by owner.

Users are first authenticated through RSA signatures and then submit the requested amount as a price of digital content. After the successful delivery of data, the user is encouraged to register the reviews about data. These reviews are validated through Watson analyzer to filter out the fake reviews. The customers registering valid reviews are given incentives. In this way, maximum reviews are submitted against every file. In this scenario, decentralized storage, Ethereum blockchain, encryption, and incentive mechanism are combined. To implement the proposed scenario, smart contracts are written in solidity and deployed on local Ethereum test network. The proposed scheme achieves transparency, security, access control, authenticity of owner, and quality of data. In simulation results, an analysis is performed on gas consumption and actual cost required in terms of USD, so that a good price estimate can be done while deploying the implemented scenario in real set-up. Moreover, computational time for different encryption schemes are plotted to represent the performance of implemented scheme, which is shamir secret sharing (SSS). Results show that SSS shows the least computational time as compared
to advanced encryption standard (AES) 128 and 256.

**Liu J, Li X, Ye L, Zhang H, Du X, Guizani M. BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. In2018 IEEE Global Communications Conference (GLOBECOM) 2018 Dec 9 (pp. 1-6). IEEE.**

Electronic medical record (EMR) is a crucial form of healthcare data, currently drawing a lot of attention. Sharing health data is considered to be a critical approach to improve the quality of healthcare service and reduce medical costs. However, EMRs are fragmented across decentralized hospitals, which hinders data sharing and puts patients' privacy at risks. To address these issues, we propose a blockchain based privacy-preserving data sharing for EMRs, called BPDS. In BPDS, the original EMRs are stored securely in the cloud and the indexes are reserved in a tamper-proof consortium blockchain. By this means, the risk of the medical data leakage could be greatly reduced, and at the same time, the indexes in blockchain ensure that the EMRs can not be modified arbitrarily. Secure data sharing can be accomplished automatically according to the predefined access permissions of patients through the smart contracts of blockchain. Besides, the joint-design of the CP-ABE-based access control mechanism and the content extraction signature scheme provides strong privacy preservation in data sharing. Security analysis shows that BPDS is a secure and effective way to realize data sharing for EMRs.

**Satapathy U, Mohanta BK, Panda SS, Sobhanayak S, Jena D. A secure framework for communication in internet of things application using hyperledger based blockchain. In2019 10th international conference on computing, communication and networking technologies (ICCCNT) 2019 Jul 6 (pp. 1-7). IEEE.**

In the era of the Internet of Things(IoT) smart devices are connected with wire or wireless way. The IoT devices are capable of sensing the environment and has the ability to transmit that information to the next level. The application area of IoT is Smart city, Smart transportation, Healthcare sector, Agriculture, Monitoring environment. Each of these applications, lots of information are share or transmit among different devices. In the information sharing system among devices, lots of security and privacy challenges exist like data leakage, data modification, device identity. In this paper, authors firstly identify the communication protocols used in IoT application and given their working principle. Secondly, challenges exist in IoT and corresponding Blockchain solution approach are explained, Lastly, the authors proposed a secure architecture based on open Blockchain which can solve some of the challenges in IoT applications. It is anticipated that Blockchain will make far-reaching changes in IoT applications in near future. We have addressed the vulnerabilities occur in secure communication in an IoT application by integrating it with Blockchain. In this paper, we proposed an architecture to communicate securely in IoT Applications using Hyderledger based Blockchain. In IoT application the data sent by various devices stored in a centralized database making it vulnerable for security breaches. Also the authenticity of the sender could not be verified properly making it open for security threats. In this paper we have proposed a secure architecture based on open Blockchain (Hyperledger) for IoT applications. Malicious actor detection will be easy as every node aware of all other node in the Hyperledger network. Concluding it guarantees the security measures for non-repudiation, privacy and scalablity in an IoT application.

## II. METHODOLOGY AND APPROACH

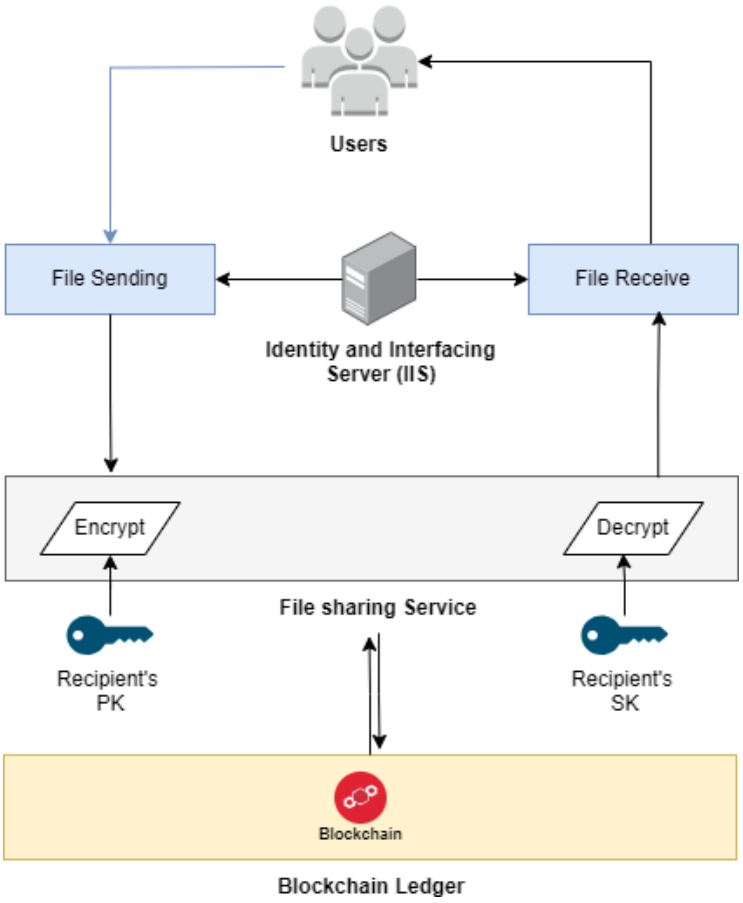
In a consortium of organizations, a number of organizations can share data in the form files and synergies their operations. A blockchain network created among multiple organizations, each of the organizations will host Identity and Interfacing Server (IIS), Smart contract, and blockchain ledger. IIS maintains the identity details in identity database and is also the interfacing point with the smart contract. A smart contract is a program, which contains the business logic

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203147 |

of the proposed file-sharing mechanism, is installed on each of the organizations. The blockchain ledger maintains transactions in the form of blocks. The following Figure illustrates the high-level view of the proposed system.




**Modules**

**Identity and Interfacing Server**

For sharing files among the users of the participant or organizations, the concerned users need to be registered with the blockchain through the smart contract. A key pair (pki, ski) is generated by the end user application. The private key ski is kept with the user machine and the public key along with user details like name, email, organization, password, etc is sent to the IIS. IIS admin verifies the user identity registration request. Upon successful verification the hash of the password is written to the identity database.

**Blockchain Ledger**

IIS sends the user registration request to the smart contract with public key $pk_i$ and user details. The smart contract generates the blockchain identifier $BCID_i$ and inserts $BCID_i$, userdetails, $pk_i$ into blockchain ledger. The blockchain update status(success/failure) and BCIDi is sent to IIS. IIS sends the user identity registration status and $BCID_i$ to the end user application.

**File Sharing**

Once the user is registered with blockchain, he can securely share files with any other registered user. The user logs in using the user authentication process. The user selects the file to be shared and specifies the file receivers. The end user application generates the symmetric key, K and encrypts file, M to be shared using K. The encrypted file M is uploaded to the IPFS distributed storage. IPFS returns content ID of the uploaded file, $M_{cid}$ to the end user application. The end user application generates file identifier, $M_{fid}$ for the unique identification of the file. The end user application requests the public keys of (R1, R2, ...Rn) i.e., the receivers with whom the file is to be shared.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203147 |

In this project we will be using VSCode and Ganache.
There are mainly 4 instructions that we use to connect code, transfer data and execute in blockchain.
Connect Ganache with VS Code: Typically, Ganache is a standalone application that runs on your local machine. To interact with it from VS Code, you might need to ensure that your project is configured to connect to the local blockchain provided by Ganache. This might involve configuring your project settings or updating your Ethereum provider settings to point to Ganache's RPC endpoint.

Run migrations: Once your Django project is set up and configured to connect to Ganache, you'll want to run migrations to create database tables based on your Django models. You can do this by running the command python manage.py migrate in the terminal within VS Code. This ensures that your database schema is up to date with your Django models.

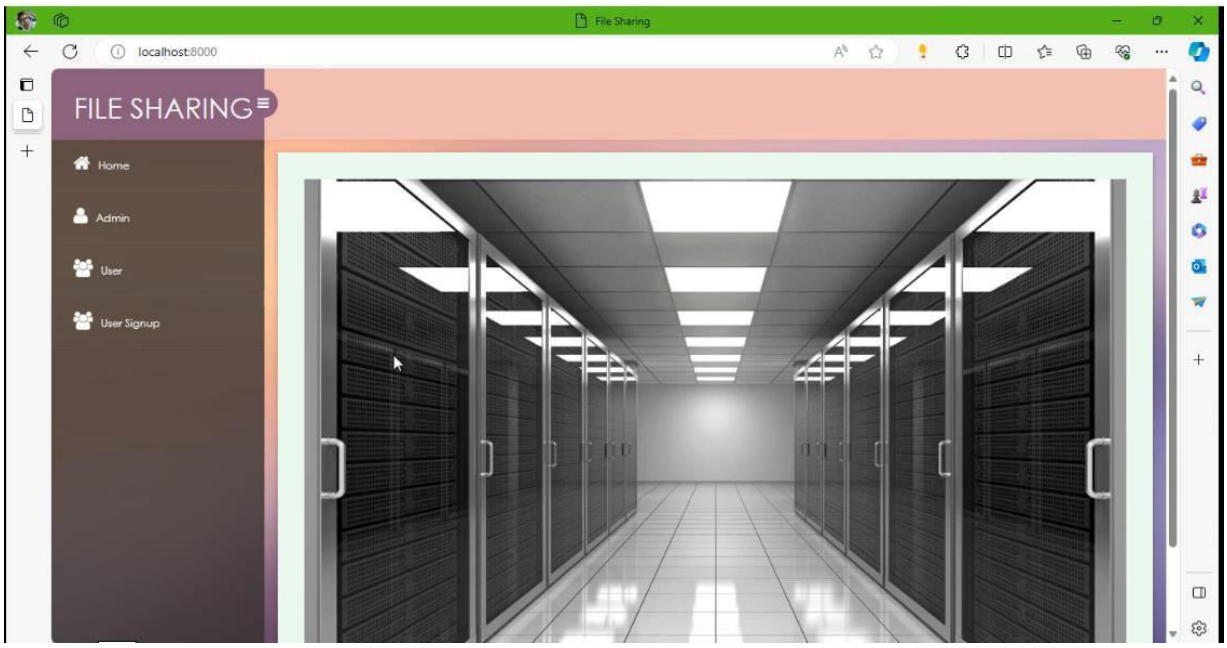
Run the development server: After successfully migrating your database, you can start the Django development server using the command python manage.py runserver. This command starts the server, allowing you to access your Django project from a web browser.

Access the web browser: Once the server is running, you can open a web browser and navigate to the address where your Django project is hosted. By default, this is usually http://localhost:8000/. From there, you should be able to interact with your Django application.

Remember to make sure that your Django project is configured properly to work with Ganache and that your Ethereum-related code interacts correctly with the local blockchain provided by Ganache. Additionally, ensure that your Django project is set up with appropriate Django models, views, and templates to serve the content you want on the web browser.

## III. RESULTS AND DECLARATION

Here you can see the website after redirecting to the web browser
**Home Screen**

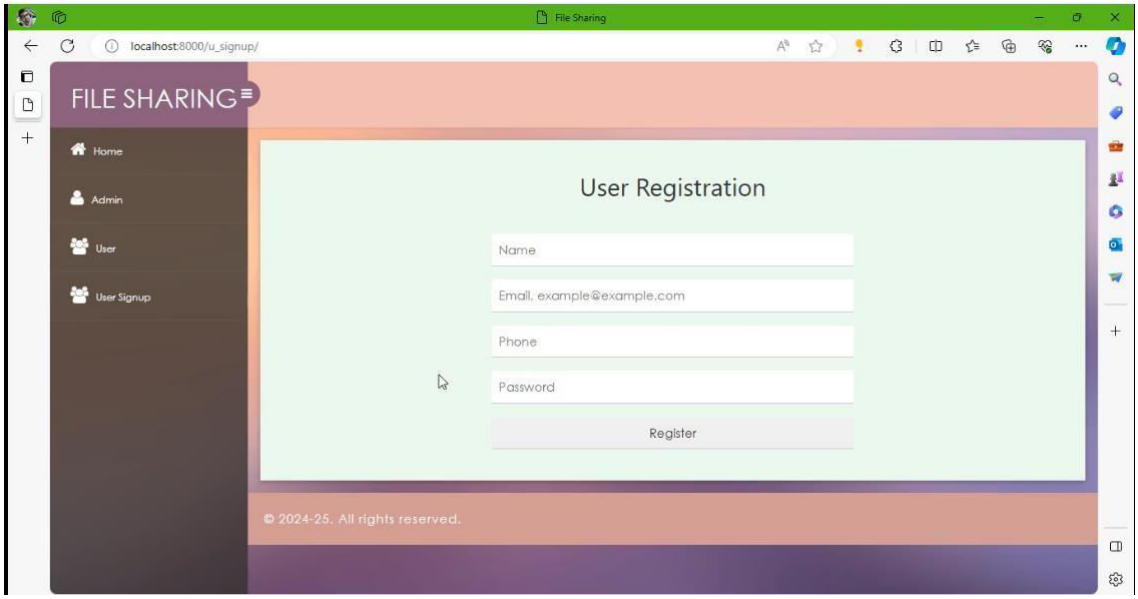


| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

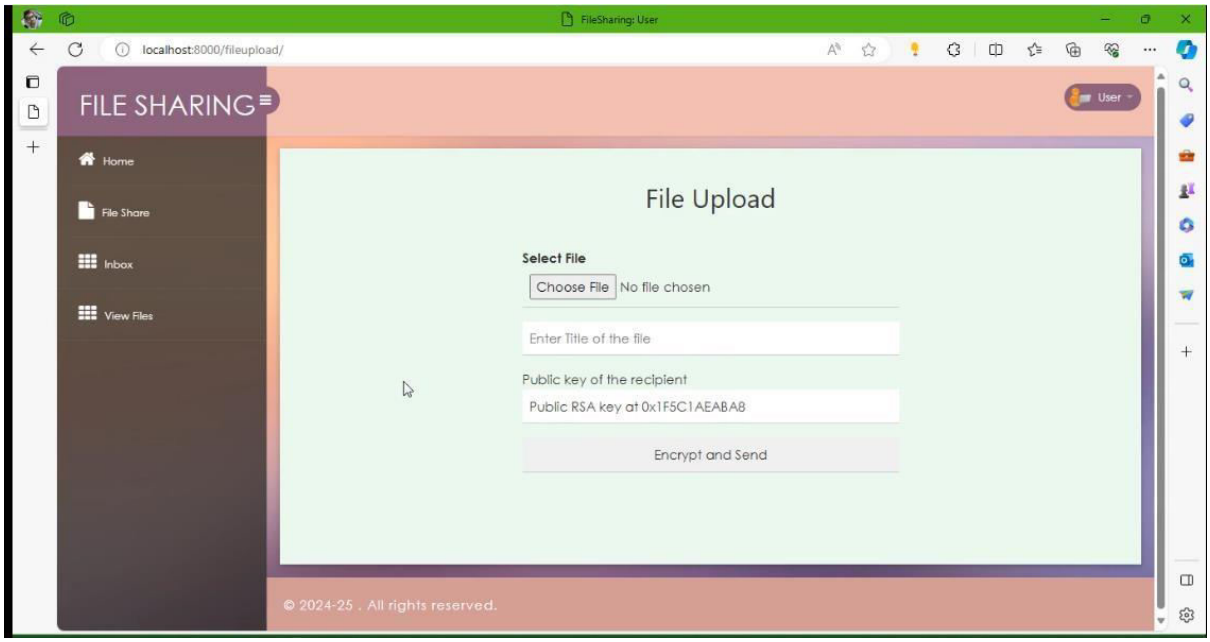
|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203147 |

**User Registration**




**Key Generation**

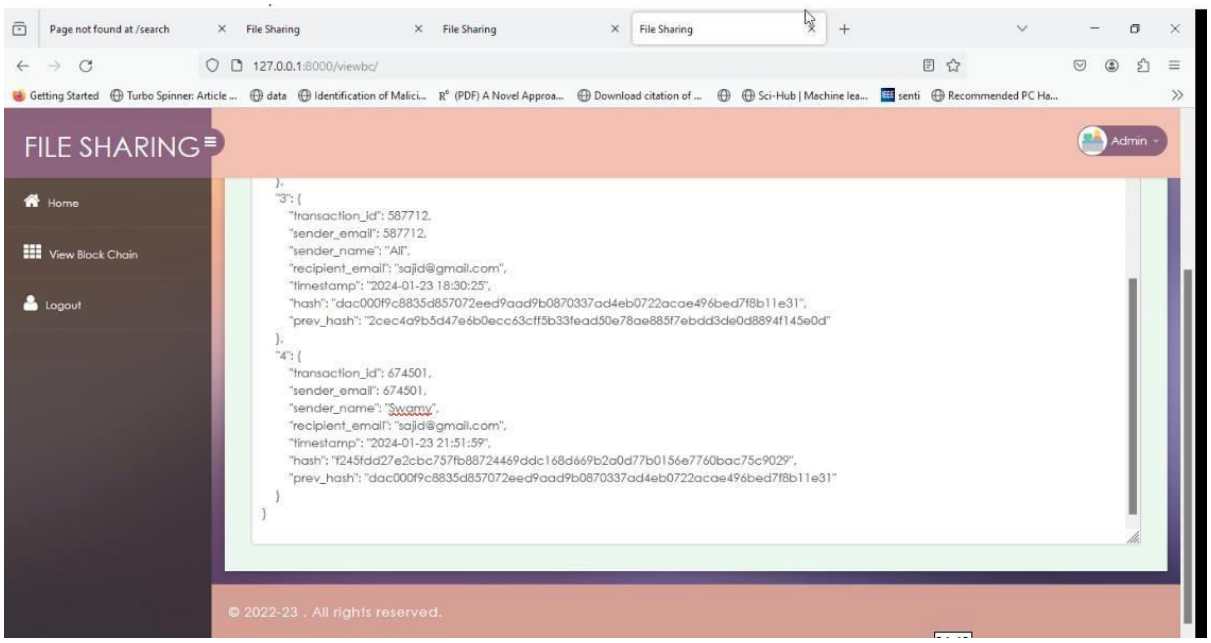


| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203147 |

**View Block Chain**




## IV. CONCLUSION

The proposed system provides secure transferring of data 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 IPFS storage and blockchain ledger respectively. The system is realized using open source blockchain framework Hyperledger Fabric and tested using Hyperledger Caliper tool.

## REFERENCES

[1] S. Nakamoto, “bitcoin: A peer-to-peer electronic cash system,” 2008.
[2] ”Hyperledger Fabric Documentation, Release main”, ttps://readthedocs.org/projects/hlf/downloads/pdf/latest/, accessed on Dec 2022
[3] Naz M, Al-zahrani FA, Khalid R, Javaid N, Qamar AM, Afzal MK, Shafiq M. A secure data sharing platform using blockchain and interplanetary file system. Sustainability. 2019 Dec 10;11(24):7054.
[4] Liu J, Li X, Ye L, Zhang H, Du X, Guizani M. BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. In2018 IEEE Global Communications Conference (GLOBECOM) 2018 Dec 9 (pp. 1-6). IEEE.
[5] Satapathy U, Mohanta BK, Panda SS, Sobhanayak S, Jena D. A secure framework for communication in internet of things application using hyperledger based blockchain. In2019 10th international conference on computing, communication and networking technologies (ICCCNT) 2019 Jul 6 (pp. 1-7). IEEE.
[6] YSari L, Sipos M. FileTribe: blockchain-based secure file-sharing on IPFS. InEuropean Wireless 2019; 25th European Wireless Conference 2019 May 2 (pp. 1-6). VDE.
[7] Benet J. Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561. 2014 Jul 14.
[8] ”Hyperledger Caliper Documentation, Getting Started”, ”https://hyperledger.github.io/caliper/v0.5.0/getting-started/”, accessed on Dec 2022
[9] ”Apache Couch Database Documentation: Release 3.3.0”, ”https://docs.couchdb.org/ /downloads/en/latest/pdf/”, accessed on Dec 2022
[10] Buterin, Vitalik. ”A next-generation smart contract and decentralized application platform.” white paper 3, no. 37 (2014): 2-1.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details