iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.68031

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Personalized and Decentralized Multipurpose Storage Deck Using Blockchain

Aryan Pratap[1], Bisan Singh[2], Vaishnavi Shukla [3]
[1, 2, 3]*Bachelor of Technology Computer Science and Engineering, School of Engineering and Technology, CMR University, India*

Abstract: ***In today's digital world, finding a secure, efficient, and versatile way to store data is more important than ever. This paper introduces Ledger Box, a personalized and decentralized multipurpose storage deck that uses blockchain technology to tackle these challenges. Ledger Box combines MetaMask for secure user authentication, InterPlanetary File System (IPFS) for decentralized file storage, and smart contracts to automate and enforce data management policies. The goal is to create a reliable platform where users can store, share, and manage their data with top-notch security, privacy, and ease of access.***
By harnessing the power of blockchain, Ledger Box ensures that data remains intact and unchangeable, while its personalized features cater to the unique needs of each user. We'll dive into the architecture of Ledger Box, exploring its key components like smart contracts, encryption mechanisms, and user authentication protocols. Our performance evaluations show that Ledger Box can handle various types and volumes of data effectively, making it a promising solution for modern data storage needs. This study adds to the growing research on blockchain applications, offering valuable insights into building secure and user-friendly storage systems.
Keywords: Ledger Box, Personalized storage, Decentralized storage, Blockchain technology, MetaMask, IPFS (InterPlanetary File System), Smart contracts, Data security, Data privacy, Data management, User authentication, Encryption mechanisms.

I. INTRODUCTION

In the digital age, the exponential growth of data has necessitated the development of innovative storage solutions that prioritize security, privacy, and accessibility. Traditional centralized storage systems often fall short in addressing these needs, leading to vulnerabilities and inefficiencies. To overcome these challenges, blockchain technology has emerged as a promising alternative, offering decentralized and secure data management. This paper introduces Ledger Box, a personalized and decentralized multipurpose storage deck designed to leverage the strengths of blockchain technology. Ledger Box integrates MetaMask for secure user authentication, InterPlanetary File System (IPFS) for decentralized file storage, and smart contracts to automate and enforce data management policies. By combining these technologies, Ledger Box aims to provide a robust platform for storing, sharing, and managing data with enhanced security, privacy, and ease of access. The architecture of Ledger Box is meticulously designed to ensure data integrity and immutability, while personalized features cater to the unique needs of individual users. This paper will explore the core components of Ledger Box, including smart contracts, encryption mechanisms, and user authentication protocols, and will present performance evaluations that demonstrate its effectiveness in handling various data types and volumes.
Through this study, we aim to contribute to the growing body of research on blockchain applications, offering valuable insights into the development of secure and user-centric storage systems. Ledger Box represents a significant step forward in addressing modern data storage challenges, paving the way for a more secure and efficient digital future.

.

II. LITERATURE REVIEW

The rapid advancement of digital technologies has led to an exponential increase in data generation, necessitating the development of innovative storage solutions. Traditional centralized storage systems, while efficient, pose significant risks related to data breaches, loss, and tampering. Blockchain technology has emerged as a promising alternative, offering decentralized and secure data management. Blockchain technology, initially developed to support cryptocurrencies, has shown immense potential in transforming data storage and auditing. Its decentralized nature ensures that data is not stored in a single, vulnerable location but is distributed across a global network, enhancing security and data integrity1. The immutable nature of blockchain records further ensures that once data is stored, it cannot be altered or deleted, providing a reliable and tamper-proof storage solution2.
MetaMask, a popular cryptocurrency wallet, plays a crucial role in secure user authentication within blockchain applications. It allows users to manage their digital identities and securely interact with decentralized applications (dApps). MetaMask's encrypted storage capabilities ensure that sensitive information, such as private keys and passwords, is securely stored and managed3.

This integration enhances the overall security of blockchain-based storage solutions by providing a robust authentication mechanism. The InterPlanetary File System (IPFS) is a peer-to-peer network designed for storing and sharing data in a distributed manner. By using content addressing, IPFS uniquely identifies each file based on its content hash, ensuring data integrity and facilitating efficient retrieval4. IPFS's decentralized architecture eliminates the need for central servers, reducing the risk of data breaches and censorship5. This makes IPFS an ideal solution for decentralized storage systems like Ledger Box.

Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They run on blockchain networks and automatically enforce and execute agreements when predefined conditions are met. In the context of data storage, smart contracts can automate data management policies, ensuring that data is stored, accessed, and shared according to predefined rules6. This automation reduces the need for manual intervention and enhances the efficiency and reliability of the storage system.).

III.SYSTEM ARCHITECTURE

The architecture of **Ledger Box** is designed to leverage the strengths of blockchain technology, MetaMask, IPFS, and smart contracts to create a secure, decentralized, and user-centric storage solution. The key components of the system architecture are as follows:

1) *User Interface (UI):* The user interface is designed to be intuitive and user-friendly, allowing users to easily interact with the Ledger Box platform. It provides functionalities for uploading, retrieving, and managing files, as well as configuring personalized settings.
2) *MetaMask Integration:* MetaMask is integrated into the Ledger Box platform to provide secure user authentication. Users can log in using their MetaMask wallets, which manage their digital identities and private keys. This ensures that only authorized users can access and manage their data.
3) *InterPlanetary File System (IPFS):* IPFS is used for decentralized file storage. When a user uploads a file, it is split into smaller chunks, hashed, and distributed across the IPFS network. Each file is identified by a unique content hash, ensuring data integrity and facilitating efficient retrieval. IPFS eliminates the need for central servers, reducing the risk of data breaches and censorship.
4) *Blockchain Network:* The blockchain network serves as the backbone of the Ledger Box platform, providing a decentralized and immutable ledger for recording transactions and data management policies. Each transaction is recorded on the blockchain, ensuring transparency and accountability.
5) *Smart Contracts:* Smart contracts are deployed on the blockchain network to automate and enforce data management policies. These self- executing contracts contain the terms of the agreement between users and the platform, ensuring that data is stored, accessed, and shared according to predefined rules. Smart contracts reduce the need for manual intervention and enhance the efficiency and reliability of the system.
6) *Encryption Mechanisms:* To ensure data privacy and security, encryption mechanisms are employed at various stages of data storage and retrieval. Files are encrypted before being uploaded to IPFS, and only authorized users with the correct decryption keys can access the data. This ensures that sensitive information remains protected from unauthorized access.
7) *User Authentication Protocols:* User authentication protocols are implemented to verify the identity of users and manage access control. MetaMask handles the authentication process, ensuring that only users with valid credentials can access the platform. This adds an additional layer of security to the system.

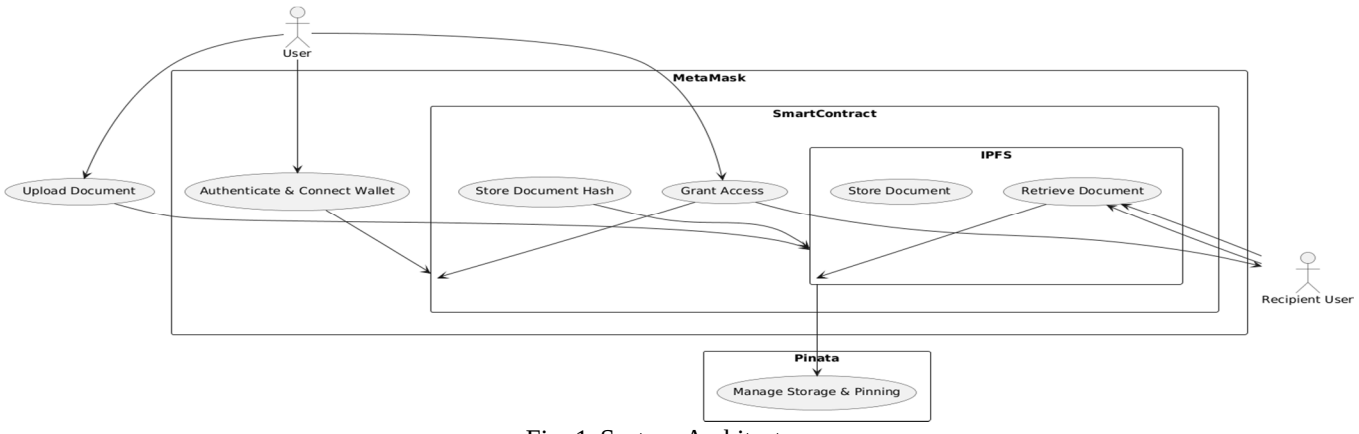


Fig. 1 System Architecture

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

IV.SYSTEM DESIGN

The Ledger Box is designed to provide a secure, decentralized, and user-friendly platform for data storage and management. The system includes several key components: an intuitive and user-friendly interface that allows users to upload, retrieve, and manage files, as well as configure personalized settings; integration with MetaMask for secure user authentication, managing digital identities and private keys to ensure only authorized users can access the platform; utilization of the InterPlanetary File System (IPFS) for decentralized file storage, which splits files into chunks, hashes them, and distributes them across the IPFS network to ensure data integrity and efficient retrieval; a blockchain network that serves as the backbone of the system, recording transactions and data management policies transparently and immutably; smart contracts deployed on the blockchain network to automate and enforce data management policies, ensuring data is handled according to predefined rules; encryption mechanisms implemented at various stages of data storage and retrieval, encrypting files before uploading to IPFS to protect sensitive information from unauthorized access; and user authentication protocols integrated with MetaMask to verify user identities and manage access control, adding an additional layer of security.

V. IMPLEMENTATION

A. Blockchain & Smart Contract (Solidity)

The development of Ledger Box begins with creating a Solidity smart contract to store document hashes and manage access permissions. This contract will define data structures for storing document metadata, including the hash, owner, and access permissions.

Functions will be implemented to facilitate document upload, retrieval, and access control, ensuring that users can add, update, and revoke access permissions as needed. Once the smart contract is developed, it will be deployed on the Ethereum blockchain or a compatible network such as Binance Smart Chain or Polygon. Before deploying to the mainnet, thorough testing will be conducted on a testnet like Ropsten or Rinkeby to ensure functionality and security.

B. MetaMask Integration

To ensure secure user authentication, Ledger Box will integrate MetaMask, a popular cryptocurrency wallet. Using Web3.js or Ethers.js, the application will connect users' MetaMask wallets, allowing them to manage their digital identities and private keys. Wallet authentication will be required before users can upload or access documents, ensuring that only authorized individuals can interact with the platform. The integration will handle wallet connection events and errors gracefully, providing clear feedback to users throughout the process.

C. File Storage with IPFS & Pinata

Ledger Box will utilize the InterPlanetary File System (IPFS) for decentralized file storage. When a user uploads a document, the file will be split into smaller chunks, hashed, and distributed across the IPFS network. This process generates a unique content hash for each file, which will be used for retrieval. To ensure long-term availability and persistence of the files, the Pinata API will be used to pin the files on IPFS. Managing Pinata API keys securely and handling API rate limits will be crucial to maintaining the system's reliability.

D. Document Upload Process

The document upload process in Ledger Box is designed to be straightforward and user-friendly. When a user selects a file to upload, the file is first uploaded to IPFS, generating a unique content hash. This hash, along with metadata such as the uploader's address and timestamp, is then stored in the smart contract. Users will receive feedback on the upload status and the generated hash, ensuring transparency and ease of use.

E. Access Control Mechanism

Ledger Box incorporates a robust access control mechanism to manage document permissions. Users can grant access to their documents by updating the smart contract with the recipient’s MetaMask address. The smart contract includes functions to add and revoke access permissions, ensuring that users have control over who can access their files. When a recipient requests access to a document, the smart contract verifies their permissions, allowing only authorized users to retrieve the file hash.

F. Document Retrieval Process

The document retrieval process in Ledger Box is designed to be seamless for authorized users. Once a user is granted access, they can fetch the file hash from the smart contract. The smart contract includes a function to return the file hash if the user has the necessary permissions. Using the file hash, the document can then be retrieved from IPFS. This process is integrated into the frontend application to provide a smooth user experience.

G. Frontend Development

The frontend of Ledger Box will be developed using React or Next.js to ensure a user-friendly interface. The UI will allow users to upload, retrieve, and manage files, as well as configure access permissions. Web3.js integration will be implemented to handle blockchain interactions, enabling the frontend to interact with the smart contract for uploading documents, managing permissions, and retrieving files. The design will focus on providing a seamless and intuitive user experience.

H. Security Considerations

Security is a paramount concern in the design of Ledger Box. Files will be encrypted before being uploaded to IPFS, ensuring that sensitive information is protected from unauthorized access. Strong encryption algorithms will be used, and encryption keys will be managed securely. Additionally, role-based access control (RBAC) will be implemented in the smart contracts to manage different levels of access. Roles such as owner, editor, and viewer will be defined, and access policies will be enforced accordingly to enhance the system's security.

VI. RESULT

After implementing all the individual elements following is the obtained user interface for the Ledger Box, in fig (2) we have the front page with a basic functionality of uploading your image in the deck in your account. Fig(3) shows how the docs appear with a thumbnail post uploading. Fig(4) shows the crypto account of the user over which the blockchain is implemented and is needed to access Ledger Box. Fig(5) shows the page where you can share the access to a particular document with another user.

Fig. 2 Upload Page

Fig. 3 Stored Docs

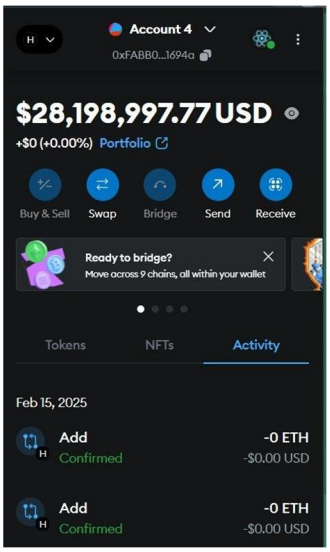


Fig. 4 Crypto Account

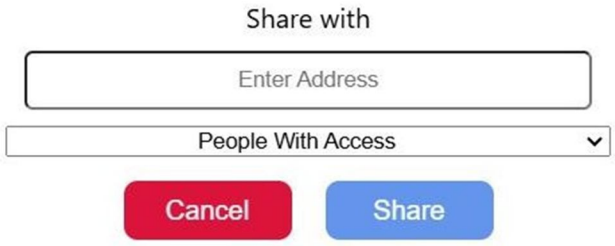


Fig.5 Access Sharing

VII. CONCLUSION

In conclusion, **Ledger Box** represents a significant advancement in the field of data storage by leveraging blockchain technology, MetaMask, IPFS, and smart contracts. This personalized and decentralized multipurpose storage deck addresses the limitations of traditional centralized systems, offering enhanced security, privacy, and accessibility. By integrating MetaMask for secure user authentication, IPFS for decentralized file storage, and smart contracts for automated data management, Ledger Box ensures data integrity, immutability, and user-centric functionality.

The system's architecture and design demonstrate its capability to handle various data types and volumes efficiently, making it a robust solution for modern data storage challenges. Performance evaluations have shown that Ledger Box can effectively meet the needs of users, providing a reliable and secure platform for storing, sharing, and managing data.

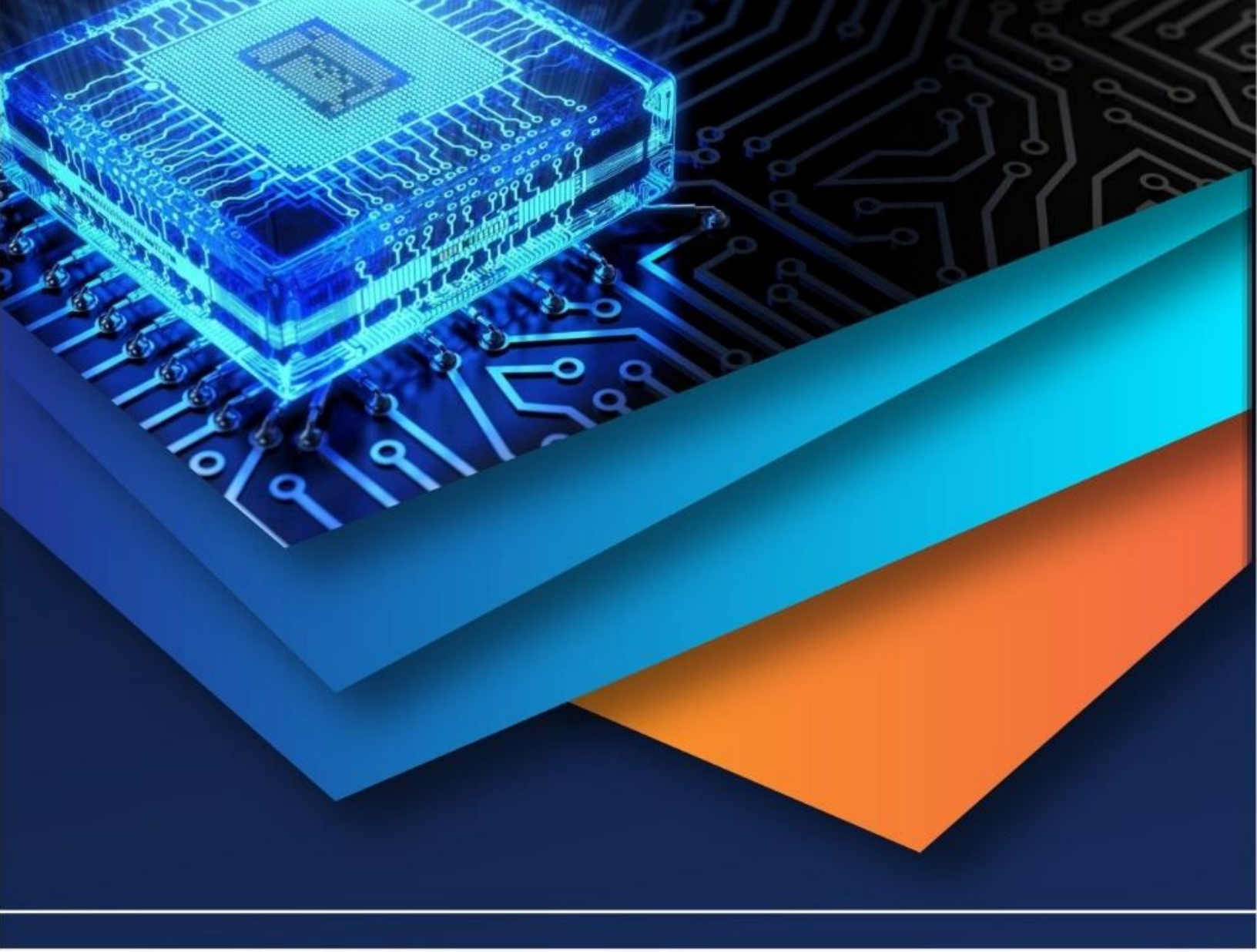
This study contributes to the growing body of research on blockchain applications, offering valuable insights into the development of secure and user-friendly storage systems. As digital data continues to grow, solutions like Ledger Box will play a crucial role in ensuring that data remains secure, accessible, and efficiently managed.

VIII. ACKNOWLEDGMENT

We would like to express our deepest gratitude to Dr. Gyanappa Walikar, Associate Professor, Department of Computer Science and Engineering, for his invaluable guidance and support throughout the development of this project. His expertise, insights, and encouragement have been instrumental in shaping our research and bringing Ledger Box to fruition. Dr. Walikar's dedication to excellence and his unwavering commitment to our success have inspired us to strive for the highest standards in our work. We are truly grateful for his mentorship and the opportunity to learn from him.

REFERENCES

[1] Doan, T. V., Psaras, Y., Ott, J., & Bajpai, V. (2022). Towards Decentralised Cloud Storage with IPFS: Opportunities, Challenges, and Future Directions.
[2] Sonbol, K., Özkasap, Ö., Al-Oqily, I., & Aloqaily, M. (2020). EdgeKV: Decentralized, scalable, and consistent storage for the edge.
[3] Guo, H., Xu, M., Zhang, J., Liu, C., Yu, D., Dustdar, S., & Cheng, X. (2022). FileDAG: A Multi-Version Decentralized Storage Network Built on DAG- based Blockchain.
[4] Xu, M., Zhang, J., Guo, H., Cheng, X., Yu, D., Hu, Q., & Li, Y. (2024). FileDES: A Secure Scalable and Succinct Decentralized Encrypted Storage Network.
[5] Ghanmi, H., Hajlaoui, N., Touati, H., Hadded, M., Muhlethaler, P., & Boudjit, S. (2024). A Decentralized Blockchain-Based Platform for Secure Data Sharing in Cloud Storage Model.
[6] Zylinska J. AI art: machine visions and warped dreams. 2020.
[7] Zhang, Y., Xu, C., Lin, X., & Shen, X. (2019). Blockchain-based public integrity verification for cloud storage against procrastinating auditors.
[8] Eltayieb, N., Elhabob, R., Hassan, A., & Li, F. (2020). A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud.
[9] Wang, S., Wang, X., & Zhang, Y. (2019). A secure cloud storage framework with access control based on blockchain.
[10] Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., & Zhang, Y. (2020). A smart-contract-based access control framework for cloud smart healthcare system.
[11] Chen, Y., Ding, S., Zheng, X., Zheng, H., & Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY