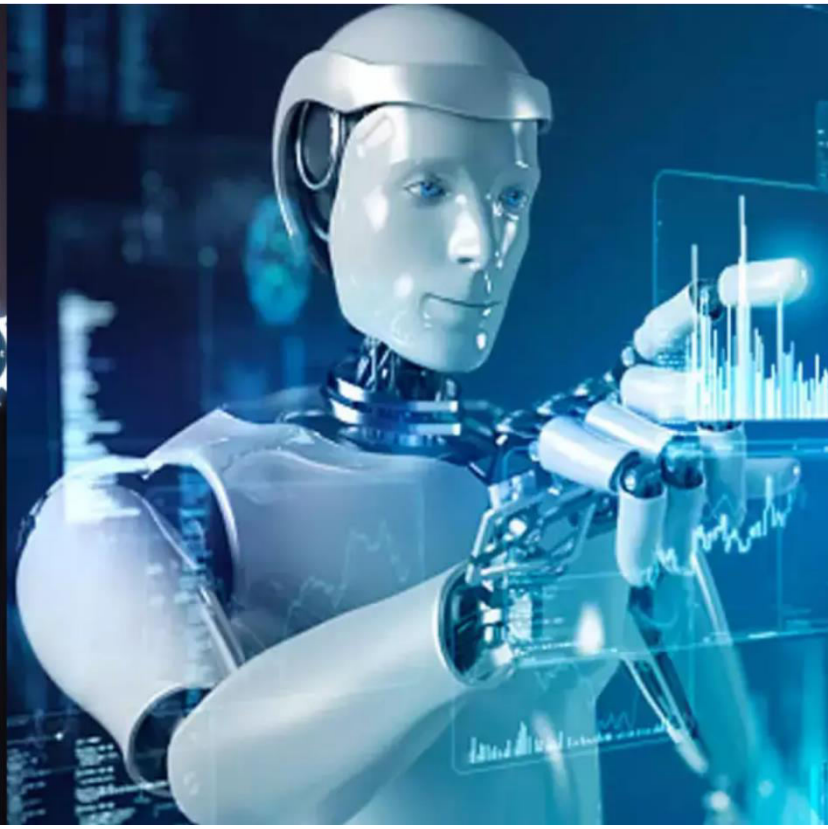
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405347|

Blockchain-Enhanced Secure Data Storage: An Experimental Approach to Decentralization and Integrity

Manoj Gowda K S[1], Mithun R P[1], Dr.Nagarathna[2], Dr.Deepika[3], Mithun Dev M[1], Madhav Adithya M S[1]

U.G. Student, Dept. of CSE, PES College Engineering, Mandya, Karnataka, India[1]

Professor, Dept. of CSE, PES College Engineering, Mandya, Karnataka, India[2]

Assistant Professor, Dept. of CSE, PES College Engineering, Mandya, Karnataka, India[3]

ABSTRACT: This experiment investigates the development and testing of a secure, blockchain-based storage system, called Secure Store. The system employs decentralised architecture, cryptographic hashing, and peer-to-peer networking to ensure data integrity, security, and privacy. Through implementation and testing, we evaluated the system's performance, security, and scalability, with a focus on encryption, data retrieval, and transaction handling. Results show that the system effectively secures data and processes transactions efficiently, making it a viable solution for sensitive data storage.

KEYWORDS: Blockchain, Secure Data Storage, Decentralization, Cryptographic Hashing, and Proof-of-Work (PoW).

I. INTRODUCTION

With the growing dependency on digital platforms, secure data management has become a critical need across various industries. Traditional centralised storage systems, while effective to an extent, remain vulnerable to data breaches, manipulation, and single points of failure. Blockchain technology, introduced in 2008 with Bitcoin by Satoshi Nakamoto, provides a decentralised alternative where data is distributed across a network of nodes, making unauthorised tampering virtually impossible. Each transaction or data entry in a blockchain is recorded on blocks that are cryptographically linked to one another, creating an immutable chain of records. This immutable and decentralised nature of blockchain technology not only enhances security but also ensures transparency and accountability.

The Secure Store project explores these essential aspects of blockchain, such as block creation, transaction handling, cryptographic hashing, and consensus mechanisms like proof-of-work (PoW)[1]. By implementing these features, this project aims to build a robust blockchain-based storage system that securely stores and retrieves sensitive information without reliance on central authorities. Such a system is particularly beneficial in sectors like finance, healthcare, and supply chain management, where data integrity and security are paramount. Through this experiment, the Secure Store project provides a practical demonstration of blockchain's capabilities in handling sensitive data and securing it against unauthorised access and tampering.

This experimental paper documents the development, testing, and evaluation of the Secure Store system. The focus is on building a blockchain from scratch, emphasising core functionalities without introducing complex features like smart contracts. Instead, the paper seeks to highlight the efficiency and reliability of fundamental blockchain mechanisms in managing data security. Additionally, the project evaluates the strengths and limitations of the blockchain structure through rigorous testing under various conditions, with a specific focus on performance and security.

Ultimately, this research not only serves as an educational tool for understanding blockchain technology but also investigates its applicability and feasibility in real-world applications. By implementing a decentralised storage system,

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405347|

we can better understand the advantages and challenges blockchain technology presents, paving the way for further innovations in secure data management.

II. SYSTEM DESIGN

2.1 System Architecture

The system design of Secure Store leverages blockchain's decentralised infrastructure to establish a robust, secure storage platform. By distributing data across multiple nodes in a blockchain network, Secure Store achieves resilience against single points of failure and ensures data remains secure and immutable. The primary components of Secure Store include a blockchain network for decentralised data storage, an encryption module for data protection, a client application for user interactions, and a database for secure metadata management. These components are integrated to form a cohesive system that provides end-to-end data security and ensures that only authorised users can access stored information.

The architecture of Secure Store is fundamentally decentralised, relying on blockchain to store data across multiple nodes. Each data entry is stored as a block within the chain, and every block contains encrypted data, a timestamp, and a hash of the previous block, which collectively ensure data integrity and immutability. This chain of blocks prevents unauthorised data modifications, as altering a single block would require changing all subsequent blocks, an impractical task without consensus from the network.

The system also includes a **Proof-of-Work (PoW)** mechanism, which functions as a consensus protocol to validate new blocks before they are added to the blockchain. PoW requires nodes to solve complex cryptographic puzzles, making it computationally challenging for malicious actors to tamper with the blockchain. This consensus mechanism not only secures the network but also ensures that all participating nodes agree on the current state of the data.

Secure Store's architecture is designed to accommodate growth, allowing additional nodes to join the network as needed, which increases decentralisation and enhances data availability. This modular and scalable architecture forms the backbone of Secure Store, allowing it to handle data efficiently and securely across a peer-to-peer network.

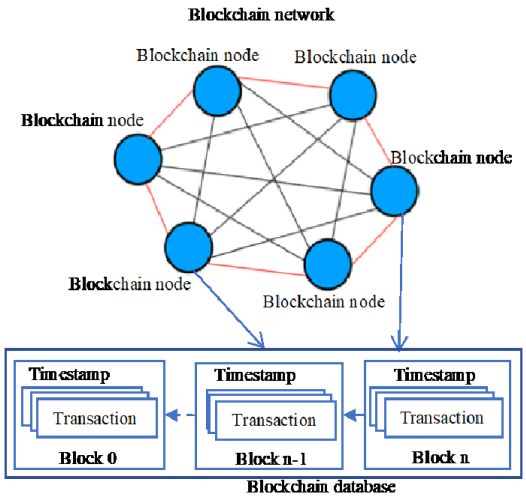


Fig. 1 System Architecture Diagram [1]

2.2 Key Components

To achieve its objectives, the Secure Store system incorporates the following components:

Blockchain Network: The blockchain serves as a decentralised ledger that records all transactions and data blocks. Each block is cryptographically linked to the preceding block using a hash function, ensuring the immutability of stored data[4]. The use of a distributed ledger eliminates the need for a central authority, making data tampering nearly

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405347|

impossible without consensus across the network. This structure enhances transparency and provides a tamper-resistant audit trail, critical for secure data management.

Encryption Module: Data security is paramount in Secure Store, and the encryption module plays a vital role in protecting sensitive information. The system employs AES-256 encryption, a highly secure encryption standard, to encode data before storing it on the blockchain[2]. When users retrieve their data, the module decrypts it, ensuring that even if a block is accessed, the information within remains unreadable without the decryption key[6]. By encrypting data before it is added to the blockchain, Secure Store ensures that sensitive information remains private and protected throughout its lifecycle.

Client Application: The client application acts as the user interface, allowing users to interact with the blockchain network. Built using ReactJS for frontend development, it provides a responsive and intuitive user experience. Flask, a lightweight Python framework, serves as the backend, managing requests, processing transactions, and coordinating interactions with the blockchain. Through the client application, users can store, retrieve, and manage their data seamlessly, with minimal technical knowledge required, making blockchain technology accessible and user-friendly[5].
Database: In addition to the blockchain network, Secure Store employs a MongoDB database to store metadata and user credentials securely. MongoDB is a NoSQL database known for its flexibility and scalability, making it well-suited for dynamic blockchain applications[2]. The database manages non-sensitive data, such as user authentication information and access logs, to streamline data retrieval and enhance system performance. By offloading metadata to MongoDB, the system can efficiently handle data-heavy applications without overloading the blockchain network.

III. IMPLEMENTATION

3.1 Backend Development

Python was chosen for its simplicity and extensive library support. Flask was used for backend services, with libraries such as PyCryptodome for cryptography and Web3.py for blockchain interaction. The backend manages user authentication, encryption, and transaction handling via RESTful APIs.

3.2 Frontend Development

The client-side application was developed using ReactJS for its modular structure and ease of integration with Web3.js, enabling interaction with the Ethereum blockchain. TailwindCSS was used for designing a responsive and user-friendly interface.

3.3 Beeple NFT Exploit (2021)

To ensure security, the system uses SHA-256 hashing for block linking, while AES-256 encryption is applied to user data. These cryptographic methods provide a strong layer of protection, ensuring that even if intercepted, data cannot be deciphered without the correct keys[7].

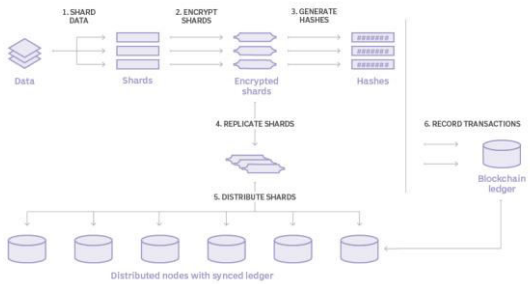


Fig. 2 Backend Structure Diagram

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405347|

IV. TESTING AND EVALUATION

4.1 Testing Methodology

The system was subjected to rigorous testing, including unit tests, integration tests, performance tests, and security evaluations. Testing was done to ensure the smooth functioning of each component and its interoperability within the entire system

4.2 Unit Testing

Backend functionalities were tested using PyTest to ensure encryption, decryption, and API endpoints worked as expected.

Frontend unit tests were conducted with Jest to validate UI components and blockchain interaction using Web3.js

Test Case	Expected Output	Obtained Output	Status
Data encryption	Data encrypted successfully	Data encrypted successfully	Passed 100%

Table 1: Unit Testing Results

4.3 Integration Testing

Integration tests were conducted using Postman and simulated blockchain environments (using Ganache). Tests focused on ensuring that the frontend and backend interact seamlessly with the blockchain

Test Case	Expected Output	Obtained Output	Status
Data retrieval	Data retrieved successfully	Data retrieved successfully	Passed 100%

Table 2: Integration Testing Results

4.4 Performance Testing

Performance testing was done using Apache JMeter, subjecting the system to increasing loads. Metrics such as response time, throughput, and error rates were measured. The system maintained performance at user loads of up to 1000, with minimal error rates and acceptable response times.

Security was a key focus, tested using OWASP ZAP for vulnerabilities like SQL injection and cross-site scripting (XSS). Blockchain transaction integrity was maintained through hashing and consensus validation.

Test Case	Status	Vulnerability Level	Mitigation
SQL Injection	Passed	Low	Input Validation

Table 4: Security Testing Results

V. PROOF-OF-WORK (POW) ALGORITHM COMPARISON

Two different PoW algorithms were implemented and compared based on running times and difficulty levels. The second algorithm exhibited superior performance under higher difficulty, with faster execution times.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405347|

Difficulty	First Algorithm	Second Algorithm
Level 2	0.00022 ms	0.00035 ms
Level 5	4.06034 ms	0.04427 ms

Table 5: Proof-of-Work Algorithm Comparison Results

VI. DISCUSSION

The results from the performance, security, and integration testing validate that the Secure Store system achieves its core objective: providing a secure, decentralised storage solution capable of protecting sensitive data. The implementation of blockchain's foundational mechanisms—block creation, cryptographic hashing, proof-of-work (PoW), and decentralised storage—significantly enhances data security and integrity. Through multiple rounds of testing, Secure Store has demonstrated its ability to mitigate vulnerabilities associated with centralised storage, thereby offering a promising alternative for industries that prioritise data security and confidentiality.

6.1 Security and Data Integrity

One of the primary strengths of the Secure Store system is its ability to maintain data integrity through blockchain's immutable ledger[8]. By linking each block with a cryptographic hash of the previous one, the system ensures that any attempt to alter data within a single block would require changing all subsequent blocks, a task that is computationally prohibitive without network consensus. This immutability makes Secure Store highly resistant to unauthorised tampering, offering significant advantages for sectors such as finance and healthcare, where data accuracy and security are critical.

The encryption module, which employs AES-256, provides an additional layer of protection by encoding data before it is stored on the blockchain[3]. This approach ensures that even if data is intercepted or accessed by unauthorised entities, it remains unreadable without the decryption key. Together, these mechanisms create a robust framework that secures data from external threats, demonstrating the potential for blockchain to enhance data privacy and protection.

6.2 Performance and Scalability Challenges

While Secure Store successfully achieves its security objectives, scalability remains a challenge, particularly when the system operates under extreme load conditions. The proof-of-work consensus mechanism, while effective for securing the network, is computationally intensive and can lead to slower processing times and higher energy consumption as more nodes join the network. Performance testing highlighted that response times increased and throughput decreased under heavy loads, indicating potential bottlenecks in the system's current design.

To address these scalability issues, future implementations could consider integrating alternative consensus mechanisms, such as Proof-of-Stake (PoS). Unlike PoW, PoS relies on validators who are selected to create new blocks based on the number of tokens they hold, reducing the computational burden associated with block validation. By transitioning to PoS or a hybrid approach combining PoW and PoS, the system could enhance processing efficiency and reduce latency under high-transaction scenarios, making it better suited for applications with significant data handling demands.

6.3 Usability and Accessibility

Another consideration in the Secure Store design is usability. While blockchain-based systems are generally complex and require specialised knowledge to operate, the client application interface was developed with simplicity in mind, ensuring that users can securely store and retrieve data with minimal technical expertise. The use of ReactJS for the frontend has enabled a responsive, user-friendly interface that accommodates a broader audience, making blockchain's benefits accessible to users who may be unfamiliar with decentralised systems.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405347|

However, there remains room for improvement in terms of accessibility and user onboarding. Implementing detailed onboarding guides, tutorials, and tooltips within the application could further lower the barrier to entry, allowing a wider range of users to harness blockchain's security benefits without needing extensive technical knowledge. These enhancements could also foster greater user adoption, especially among businesses seeking user-friendly solutions for secure data management.

6.4 Integration with Existing Systems

A key observation during integration testing was the importance of compatibility between blockchain and conventional systems. Secure Store's integration with MongoDB for metadata management reflects a hybrid approach, where blockchain stores critical, immutable data, and MongoDB manages flexible, non-sensitive data. This structure allows the system to achieve a balance between blockchain's security and a database's efficiency for rapid data retrieval. Such a dual-structure setup could be beneficial in various real-world applications, as it allows organisations to leverage blockchain security while retaining some characteristics of traditional databases.

Further integration with enterprise systems could be explored to enable seamless adoption in larger organisations. This could include support for API-based connections with other databases, cloud storage solutions, or enterprise resource planning (ERP) systems, which would make Secure Store adaptable for businesses with established infrastructure.

6.5 Broader Implications and Future Applications

The success of the Secure Store project underscores blockchain's potential in fields beyond finance and cryptocurrency. For instance, healthcare providers could use similar systems to store patient records securely, ensuring that sensitive data remains protected from unauthorised access. Similarly, supply chain management could benefit from blockchain's traceability, allowing stakeholders to track goods and verify data integrity across the production process.

However, blockchain adoption also presents broader challenges, such as regulatory and compliance issues. Blockchain's decentralised nature complicates adherence to certain data privacy regulations, especially those requiring the erasure or modification of personal data, as data on a blockchain is inherently immutable. Addressing these challenges requires balancing regulatory compliance with blockchain's security features, possibly through solutions like private blockchains or permissioned access to meet industry standards while ensuring data security.

VII. CONCLUSION

The Secure Store project effectively showcases blockchain's potential for secure, decentralised data storage. By integrating block creation, cryptographic hashing, proof-of-work, and AES-256 encryption, the system ensures data integrity, security, and resilience against tampering. This approach is especially valuable for sectors needing strong data protection, such as finance and healthcare.While Secure Store demonstrates significant strengths, its reliance on proof-of-work affects scalability. Future versions could explore Proof-of-Stake to enhance performance. Additionally, incorporating smart contracts could expand Secure Store's functionality, allowing for automated access controls and enhanced data management.Overall, Secure Store provides a promising framework for secure data storage, balancing blockchain's benefits with user accessibility and practical integration options. With improvements in scalability and interoperability, this approach could become a viable solution for real-world applications needing secure, reliable storage.

REFERENCES

[1] Y. Hu, J. Shen, S. He, G. Xu and H. Yang, "Research on Secure Data Sharing Technology of Block Chain," 2022 6th Asian Conference on Artificial Intelligence Technology (ACAIT), Changzhou, China, 2022, pp. 1-10, doi: 10.1109/ACAIT56212.2022.10137979.

[2] Cao et al., "TreePIR: Efficient Private Retrieval of Merkle Proofs via Tree Colorings with Fast Indexing and Zero Storage Overhead," in 2025 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2025, pp. 32-32, doi: 10.1109/SP61157.2025.00032.

[3] A. M. Alniamy and H. Liu, "Blockchain-Based Secure Collaboration Platform for Sharing and Accessing Scientific Research Data," 2020 3rd International Conference on Hot Information-Centric Networking (HotICN), Hefei, China, 2020, pp. 34-40, doi: 10.1109/HotICN50779.2020.9350856.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405347|

[4] Verma, Garima & Kanrar, Soumen. (2023). Secure digital documents sharing using blockchain and attribute-based cryptosystem. Multiagent and Grid Systems. 18. 365-379. 10.3233/MGS-221361.
[5] M. M. Taha and M. Alanezi, "Cryptocurrencies in Blockchains Environment: The Verification Trip," in 4th International Conference on Current Research in Engineering and Science Applications, ICCRESA 2022, Institute of Electrical and Electronics Engineers Inc., 2022.
[6] Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management, 15(1), 70-83.
[7] R. Sarkis-Onofre, F. Catalá-López, E. Aromataris, and C. Lockwood, "How to properly use the PRISMA Statement," Systematic Reviews, vol. 10, no. 1. BioMed Central Ltd, Dec. 01, 2021.
[8] F. AyotundeAlaba, H. A. Sulaimon, M. Ifeyinwa Marisa, and O. Najeem, "Smart Contracts Security Application and Challenges: A Review," Cloud Computing and Data Science, vol. 5, 2024.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details