International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 03 | March - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Blockchain-Integrated Dual Keypad Authentication System

Sakshi Gaonkar[1], Anushri Pawar[2], Ashwini Jadhav[3], Prof. Sujata Salunkhe[4]

[1,2,3]Students, Department of Computer Engineering, Siddhant College of Engineering, Sudumbare, Pune-412109, India

[4]Assistant Professor, Department of Computer Engineering, Siddhant College of Engineering, Sudumbare, Pune-412109, India

Abstract: With the increasing reliance on cloud storage, securing data against unauthorized access has become crucial. Various algorithms are implemented to maintain data confidentiality, integrity, and availability. However, centralized cloud storage lacks these essential security features. To enhance data storage methods, decentralized cloud storage is employed, with blockchain technology playing a key role in preventing data modification or deletion. Blockchain mitigates the risk of data tampering by storing information in interconnected blocks secured with hash values. The SHA-256 algorithm, widely used in secure banking frameworks, ensures robust hashing functions during data input, making it a preferred choice for implementing blockchain security. Hashing algorithms serve multiple security functions, including message authentication, consensus mechanisms, and mining operations, as well as custom blockchain development. Combining these techniques enhances data security and reliability for users accessing cloud-stored information. Additionally, encryption further strengthens data protection, and the Advanced Encryption Standard (AES) algorithm is specifically utilized in this study for both encrypting and decrypting data due to its strong security attributes.

Keywords: Custom Blockchain, SHA-256 Algorithm, Hashing Functions, Consensus Algorithm, Distributed System, User Data Privacy, etc.

INTRODUCTION

A blockchain system can be regarded as a cryptographic database that is highly resistant to corruption and designed to securely record sensitive user data. The network of computers maintaining this system is accessible to anyone using the software. While blockchain ensures data integrity and is tamper-proof, it operates as a pseudo-anonymous system, raising privacy concerns since all transactions remain publicly visible. To manage private user information across multiple MNC locations and devices, careful planning of the access control system is essential. Blockchain is not inherently designed to function as a large-scale storage system. From the perspective of secure banking frameworks, integrating a decentralized storage solution would significantly address this limitation. Unlike centralized systems, blockchain networks offer greater resilience, as their decentralized nature eliminates the risk of a single point of failure, making them less susceptible to targeted attacks.

However, because all the bitcoin transactions are public and everyone has got right of entry to them, there already exists analytics equipment that picks out the members within the community based on the transaction records [2].

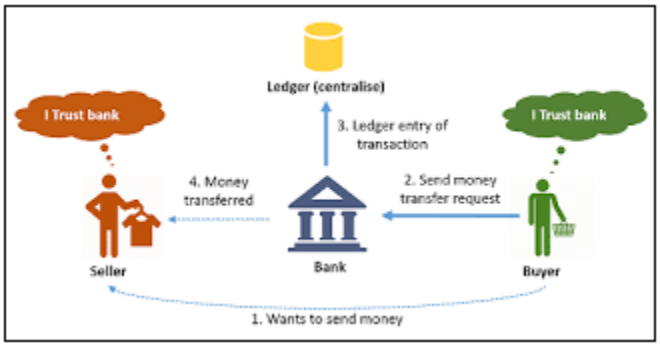

Fig.1: System Overview

The most crucial module of this research project is the blockchain implementation, which includes two types of records: blocks and transactions (fig. 1).Each block contains a timestamp and is linked to its preceding block using a secure hash algorithm. Several algorithms are employed when transaction data is stored in the blockchain system, including SHA for hash generation, mining to determine a valid hash, smart contracts for enforcing system policies, and consensus mechanisms to ensure blockchain validation across all peer-to-peer nodes.The banking application is therefore safer. The second is the accessibility and storage of data. Use content-based cryptography techniques, keywords, and the Secret Shamir hashing technique for this point.

I. RELATED WORK

Data security is less likely in traditional storage, where all data is kept in one location (centralized storage), than in decentralized storage because the owner of centralized storage can keep an eye on the data and it may be stolen or altered. Due to the urgent need for data access, decentralized storage was created because everyone wants to be able to access their data more quickly and securely. Data is stored in multiple data blocks in decentralized storage, which lowers the likelihood that data will be accessed by data thieves. Decentralized storage is popular and widely used because data thieves are unaware of where the rest of the data is stored.

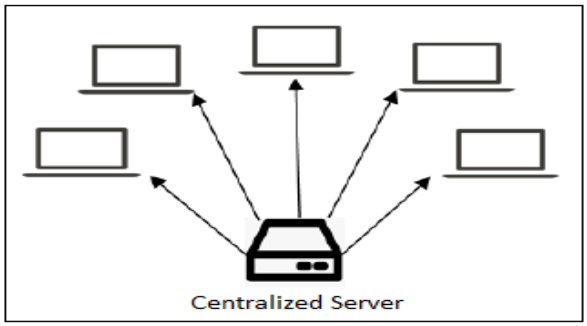

Fig.2: Traditional Centralized Storage

As shown in Fig. 2, every data user depends on a single server for data access. This reliance can create a bottleneck due to the heavy load on the central server, increasing the time needed to retrieve data. Additionally, there is a restriction on the number of users who can connect to the server simultaneously, making it impractical for applications that require large-scale user access. Moreover, if the server experiences a hardware failure or a configuration error, the stored data may become inaccessible. In such cases, data recovery becomes extremely challenging, as the loss could occur without prior warning. This server also requires a lot of maintenance. The fact that they charge their customers the most to use their services is another problem with

this data storage method. Decentralized storage eliminates all of the challenges associated with a centralized structure by resolving all of the issues encountered in centralized storage.

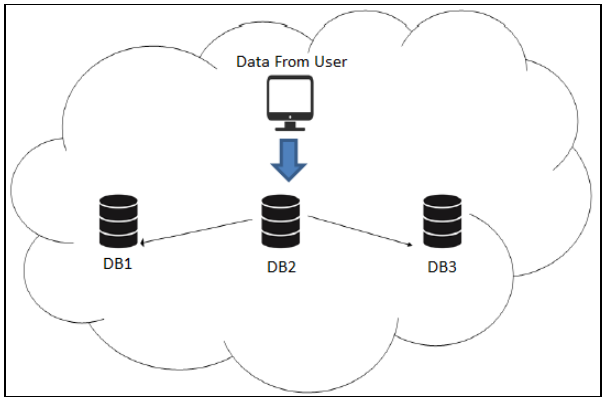

Fig.3: Decentralized Storage

The decentralized storage structure is illustrated in Fig. 3. User data is distributed across multiple databases, with a server assigning replicas to ensure redundancy. When data is stored on different servers, it is fragmented into smaller chunks, maximizing storage capacity while reducing costs. Unlike centralized systems, no single entity owns or controls the data. This approach enhances security, especially against hackers attempting to access cloud-stored data, as they cannot retrieve complete information. While decentralization inherently protects data from loss, encryption methods are necessary to further safeguard it from unauthorized access. Even a single data file is stored at multiple locations with small data blocks, but what if that small block of the file contains sensitive information? For this reason, we need an encryption method to encrypt data. All these storage systems use some sort of algorithm to make data more secure for their customers. Even if a hacker is able to access a piece of data, due to an encryption mechanism used by the service provider's hacker is unable to decrypt the information within the data block. That's why decentralized storage is preferred as compared to a centralized storage structure. [1]

II. ALGORITHMS & METHODOLOGY

A. AES Algorithm (Advanced Encryption Standard):

Cloud storage has become a widely used method for storing and retrieving data over the internet, offering enhanced reliability, security, and availability compared to local storage devices. However, protecting sensitive data from unauthorized access is crucial. To ensure security, encryption is used to convert plaintext into ciphertext, while decryption reverses this process to restore the original data. Encryption algorithms play a vital role in securing information by applying mathematical computations, which can also be demonstrated practically.

During encryption and decryption, data is divided into smaller blocks for processing. Various algorithms are available for this purpose, categorized into two main types. The first is symmetric encryption, where the same key is used for both encryption and decryption. Once encrypted, data becomes unreadable, and only the intended recipient with the correct key can revert it to its original, understandable form through the decryption process.

The second type is asymmetric encryption, which utilizes a pair of keys—one for encryption and another for decryption [5]. Advanced Encryption Standard (AES) is also known as the Rijndael algorithm, which

works up to 128 bits of the block length. This algorithm allows the key length of 128, 192, and 256 bits, three distinct bit lengths. The effectiveness of an encryption algorithm in converting plaintext into ciphertext depends on the key length. To enhance data security, the algorithm undergoes multiple iterations, known as rounds. For a 128-bit key, the process involves 10 rounds, while 192-bit and 256-bit keys require 12 and 14 rounds, respectively. Each round follows the same procedure, except for the final round, which has slight variations. As a result of this process, the encrypted data is transformed into an unreadable format.

The reverse process of the AES must be applied to encrypted data in order to recover the original data [6].

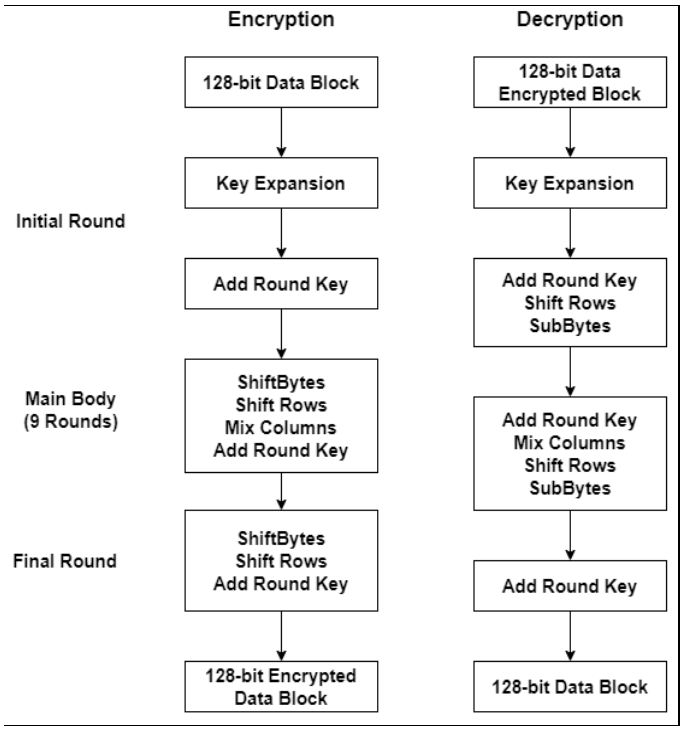

Fig.4: AES Algorithm Structure

To implement such a secure system, we are using the Advanced Encryption Standard to make data more secure and keep data out of reach from attackers.

Figure 4 shows the AES algorithm's overall structure:

a) Data Block: In the first stage, data is split into blocks. As shown in Figure 3, it is arranged in a 4x4 matrix with sixteen bytes, ensuring efficient encryption and secure storage.

b) Key Expansion: This process starts with an initial key, expands it into an array of 44 words, and generates a series of keys for each encryption round.

c) Add Round Key: Key expansion generates 10 keys using a process called key scheduling. This is done by XORing the resulting data to create input for the next round.

d) Substitute bytes: Here, each letter in a word is replaced with the next letter in the alphabet. For example, "hello" becomes "ifmmp."

e) Shift Rows: As the name suggests, each subsequent row is shifted back by one position. The second row moves to the first row's position, the third row moves to the second row's position, and so on.

f) Mix Columns: Each column has some value that is given by the previous stages of the algorithm. Likewise, this mixing of columns is performed.

g) Add Round Key (again): Each block takes input from the previous block and integrates the round key, which is generated at the beginning of the encryption process. At the end of this step, the data becomes fully encrypted. To retrieve the original data, the encryption process is reversed, applying decryption to the encrypted data, ultimately restoring it to its original form [8]. Now, while uploading encrypted data on the cloud server to keep track of the sequence of uploaded

data, blockchain technology is used. Blockchain technology is a technique that records information in such a way that it is impossible to alter the system's transactions of data. It works on the hash function. Each block of data is linked with the next block of data by the hash value, which is shown in fig.5.

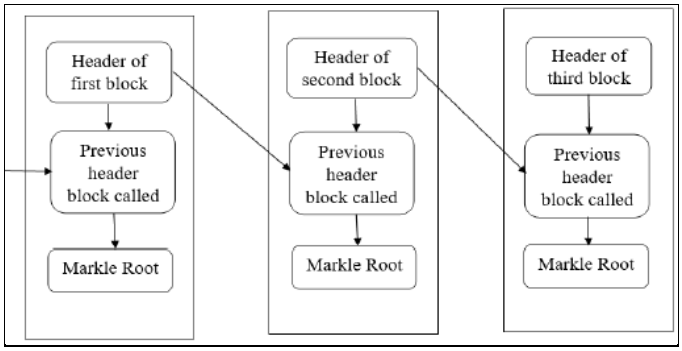

Fig.5: Structure of Blockchain.

Blockchain technology is employed for this purpose and is considered a highly reliable, secure, and efficient solution for applications requiring accurate data logging. Key areas of use include banking, online music platforms, and the Internet of Things (IoT) [3].

B. SHA-256:

The SHA-256 algorithm is a one-way cryptographic hash function designed for secure data processing. It is an improvement over earlier algorithms like SHA-0 and SHA-1. Hashing, also known as a compression function, transforms input data of varying lengths into a fixed-length binary output. The concept of the hashing algorithm is illustrated in Fig. 6.

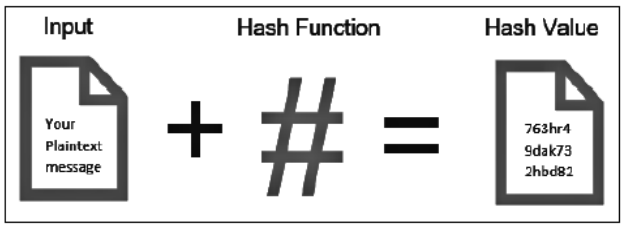

Fig.6: Working of hashing algorithm.

Working of the SHA-256 algorithm is given as follows:

The first step in the SHA-256 algorithm involves padding the input data according to predefined rules, a fundamental process in all hashing algorithms. The algorithm processes the message in 512-bit blocks. Additional bits, typically 128, are appended to the original message to ensure proper formatting. In the SHA-256 construction, data is first absorbed into the sponge structure, followed by an extraction phase known as squeezing. During absorption, the data undergoes an XOR operation, while the squeezing phase involves state transformation to generate the final hashed output. The SHA-256 bit algorithm's actual structure is depicted in fig. 7 below.

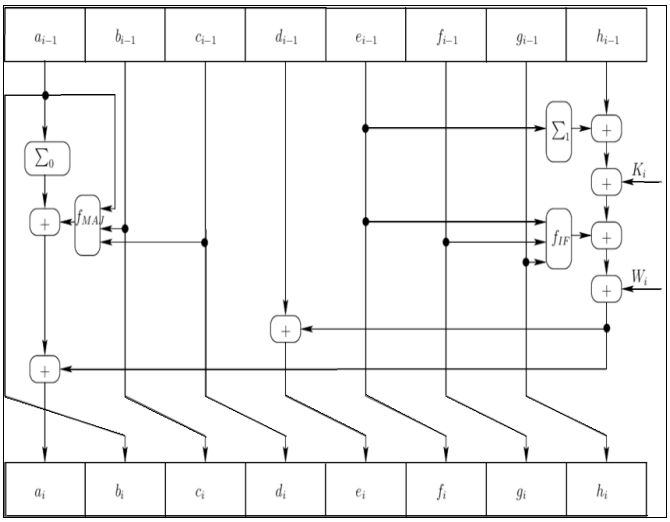

Fig.7: Structure of SHA-256

With the help of AES and Hashing algorithms, we have designed an architecture where users upload data to the cloud server, and with the help of a private key, the receiver can retrieve that data. [4]

C. Consensus Algorithms in Blockchain:

Blockchain operates as a decentralized network that ensures immutability, privacy, security, and transparency. Unlike traditional systems, it does not rely on a central authority to validate and approve transactions. Instead, every transaction within the blockchain is considered secure and verified. This is made possible by the consensus protocol, which plays a fundamental role in maintaining trust and integrity within the blockchain network.

A consensus algorithm is the mechanism through which all peers in a blockchain network agree on the current state of the distributed ledger. These algorithms establish trust within the blockchain community and facilitate coordination among anonymous participants in a decentralized environment. Essentially, the consensus protocol guarantees that each newly added block is the only validated version of the information, unanimously approved by all nodes in the blockchain.

III. PROPOSED SYSTEM

Security is a critical concern in today's digital landscape, with 99% of data being processed online and stored on trusted servers. However, challenges arise when users rely on authorized servers for data storage, as they must ensure data transmission and retrieval occur over a secure communication channel to prevent potential security threats.

In recent years, fields such as healthcare, e-commerce, internet banking, education, and business applications have processed vast amounts of data. Since these services operate online, they are vulnerable to various cyber threats. To mitigate these risks, we have developed a secure framework for online banking in the public cloud, incorporating multi-factor authentication within a blockchain-based security system. This approach enhances protection against potential attacks, as illustrated in Fig. 8.

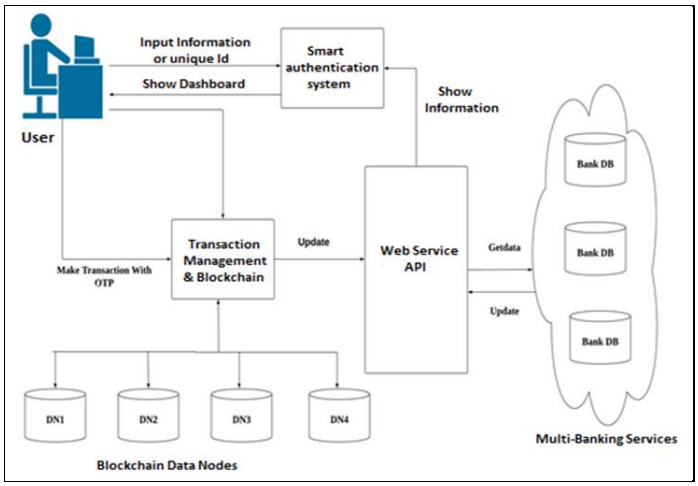

Fig. 8: System Architecture

As shown in Fig. 8, these methods focus on creating a custom blockchain to securely store transaction records. By integrating a dynamic smart contract with a consensus algorithm, the system improves transaction transparency and reliability for users. This ensures that each transaction is verified and recorded in an immutable manner. Moreover, the security of data records is achieved solely through a software-based system, eliminating the reliance on external hardware while maintaining data integrity and

confidentiality. This approach reinforces trust and security in digital transactions by leveraging blockchain's decentralized and tamper-proof nature.

IV. CONCLUSION

This research presents a blockchain-driven security framework for cloud storage, overcoming the vulnerabilities of conventional centralized systems. By integrating AES encryption and SHA-256 hashing, the proposed model guarantees secure data storage and retrieval while ensuring data integrity and confidentiality. The decentralized nature of the system enhances security, reducing the risk of unauthorized access and cyber threats, particularly in financial transactions. Future studies can explore advancements in consensus mechanisms to improve blockchain efficiency and further fortify security measures, making the system more robust and scalable for real-world applications.

V. REFERENCES

[1] Kumar, R., & Singh, M. (2020). "Blockchain Technology in Banking and Finance: A Review." Journal of Financial Services Research, 58(1), 1-22.

[2] Smith, A., & Jones, B. (2019). "Enhancing Online Security with Multi-Factor Authentication: A Comprehensive Review." Journal of Cyber Security Technology, 3(4), 200-215.

[3] Williams, T., & Brown, C. (2021). "Cloud Security Challenges and Solutions: An Overview." International Journal of Cloud Computing and Services Science, 10(1), 45-58.

[4] Lee, H., & Zhang, Y. (2022). "Integrating Blockchain with Multi-Factor Authentication for Enhanced Security." IEEE Access, 10, 8700-8712.

[5] Adams, R., & Clark, J. (2023). "Practical Applications of Blockchain in Financial Services: Case Studies and Lessons Learned." Financial Technology Review, 15(2), 100-120.

[6] Harris, J. (2020). "Blockchain Technology and Its Application in Secure Banking Systems." Journal of Financial Technology, 7(3), 150-164.

[7] Patel, N., & Sharma, R. (2021). "Blockchain-Based Multi-Factor Authentication for Cloud Applications." Cloud Computing Journal, 11(2), 78-91.

[8] Morris, L., & Thompson, G. (2022). "Enhancing Data Security in Public Cloud with Blockchain Technology." International Journal of Information Security, 21(5), 367-380.

[9] Nguyen, T., & Nguyen, H. (2020). "Secure Online Banking Using Blockchain Technology: A Survey." Journal of Information Security and Applications, 55, 102-115.

[10] Jones, P., & Lee, K. (2023). "Blockchain and MFA: A Synergistic Approach to Online Banking Security." IEEE Transactions on Network and Service Management, 20(1), 35-49.