ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

APPLICATION OF BLOCKCHAIN FOR SECURING CONFIDENTIAL DATA IN DIGITAL INFORMATION INFRASTRUCTURES

E. MOUNIKA REDDY [1], ILENI SREEMANYA [2], JAKKULLA BRIJANAND [3], KOPPULA SAI GOPINADHREDDY [4], JANGA VISHNU VARDHANREDDY [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— With the rapid advancement of informatization, the security of sensitive data within information systems has become a critical global concern. The widespread adoption of big data, cloud computing, and related technologies has intensified risks of data leakage and privacy breaches. Traditional data protection mechanisms are increasingly inadequate in addressing complex cyber threats and safeguarding data integrity. Blockchain technology, characterized by its decentralization, immutability, and traceability, presents a robust solution for enhancing data security. This paper proposes a system that leverages blockchain to secure sensitive customer data in a financial institution's information system. The proposed system employs the SHA-256 encryption algorithm to ensure data confidentiality and integrity. Additionally, smart contracts are implemented to facilitate secure and transparent sharing of encrypted data among different authorized users, enabling controlled access and real-time auditability. Through encryption, decentralized storage, and programmable access control, the system effectively mitigates risks of data tampering and unauthorized access, thereby significantly improving the overall security and trustworthiness of sensitive information management.

Index Terms – Blockchain, Data Security, Digital Information Infrastructure, Data Privacy, Distributed Ledger Technology, Cryptography, Access Control, Cybersecurity, Smart Contracts, Information Security.

I. INTRODUCTION

With the rapid development of 5G and the Internet of Things, the surge in data volume poses unprecedented challenges to real-time transmission, efficient computing, and secure storage. By 2025, the total number of global IoT connections is expected to reach 24.6 billion [1, 2]. Traditional cloud computing, as one of the key technologies of 5G, faces limitations in IoT applications due to high latency and bandwidth constraints. Currently, in the context of the "big data" era, various industries such as banking, pharmaceuticals, telecommunications, and e-commerce are generating massive amounts of data every day. Take Wal Mart for example, which produces millions of businesses records every week [3]. The global information volume doubles every 20 months, thanks to advances in data collection and storage technology. Faced with a massive flood of information, extracting valuable knowledge is becoming increasingly urgent. Data mining technology emerged in the 1980s, and its function is like an "excavator" that can filter useful information from transaction databases. With the leap of technology and computing performance in the 1990s, data mining technology has developed rapidly, and the accuracy of mining results has been significantly improved. Multi access edge computing (MEC) implements nearby data processing and storage by deploying cloud servers at the edge of the communication network. This innovative strategy significantly reduces the response delay, optimizes the quality of service, and becomes the core driving force for the development of next-generation Internet technology. As a decentralized distributed ledger, blockchain technology has shown outstanding potential in information security due to its tamper proof, transparent, and traceable characteristics. Blockchain eliminates the risk of single point failure and ensures data integrity and availability through multi node data storage [4, 5]. The consensus mechanism enhances system security and significantly reduces the probability of data being maliciously tampered with. Therefore, blockchain technology has become a key research direction for sensitive data security protection. We chose the customer information system of a well-known financial institution as the experimental object because

of its high requirements for data security and privacy protection, which is representative. The system's real-time monitoring requirements for data traffic and abnormal behavior are similar to industries such as the Internet of Things, healthcare, intelligent manufacturing, and e-commerce, and can therefore be extended to these f ields. The research results not only verify the effectiveness of the Bi LSTM model in the financial industry, but also provide reference for other industries with high security requirements, enhancing the universality and applicability of the research. This research aims to achieve complementary advantages through the integration of blockchain and multi access edge computing (MEC). By utilizing blockchain technology, MEC can enhance data security and privacy protection, simplify device management processes, and promote the autonomy of resource markets through transaction functions. By combining MEC's decentralized features with blockchain deployment, the dependency problem in traditional cloud computing models can be solved. The integrated BC MECsystem provides secure, stable, and low latency services, ensuring data integrity and traceability through blockchain technology.

II. RELATED WORK

A. Impact of blockchain technology on information dis closure of competition platforms.

The information regarding agricultural products is crucial to consumers. Blockchain technology theoretically offers a solution to the trust issues surrounding agricultural products by ensuring the credibility of information sources, facilitating trust transmission, and improving information management. Consequently, information plays a pivotal role in consumers' purchasing decisions. This paper investigates strategies for adopting blockchain technology within an agricultural supply chain comprising two competing platforms. Additionally, it analyzes the level of consumer trust in disclosed information and the influence of blockchain adoption costs on strategy implementation.

B. Blockchain Technology, Structure, and Applications: ASurvey.

In the past decade, blockchain technology has become increasingly prevalent in our daily lives. This technology consists of a chain of blocks that contains the history of transactions and information about its users. Distributed digital ledgers are used in blockchain. A transparent environment is created by using this technology, allowing

encrypted secure transactions to be verified and approved by all users. As a powerful tool, blockchain can be utilized for a wide range of useful purposes in everyday life including cryptocurrency, Internet-of-Things (IoT), finance, reputation system, and healthcare. This paper aims to provide an overview of blockchain technology and its security issues for users and researchers. In particular, those who conduct their business using blockchain technology. This paper includes a comparison of consensus algorithms and a description of cryptography. Further, most applications used in blockchain are focused on in this paper also analyzing real attacks and then summarizing security measures in blockchain. Even though Blockchain holds a promising scope of development in several sectors, it is prone to several security and vulnerability issues that arise from different types of blockchain networks which represent a challenge to deal with blockchain. Finally, as a research community, we encourage future research challenges that can be addressed to improve security in blockchain systems.

C. An Agricultural based Supply Chain Management using Blockchain Technology.

Blockchain is a distributed digital ledger technology that allows for the immutable and auditable logging of transactions without needing a central authority or centralized database. First introduced in 2008 as the technology behind the digital currency Bitcoin, blockchain has now found use in a wide range of sectors. Modern agriculture supply networks have emerged to accommodate intricate interactions between regional actors and the agricultural environment. Interactions between various participants in the supply chain, including those involved in manufacturing, processing, and delivery. One of the main reasons fraud happens so often in agriculture is the lack of transparency in the supply chain. Businesses that aren't transparent run the risk of losing money, alienating their customers, and seeing their brands decline in value. To encourage the growth of an efficient and trustworthy trading environment, several fundamental adjustments to the current supply chain architecture are necessary. The potential for blockchain technology to enhance food and agricultural supply chain transparency is well acknowledged. Companies utilize IoT and blockchain to create more equitable, sustainable, and customer-friendly food manufacturing systems. In this current work, a blockchain-based decentralized application (dApp), 'ASBlock', is developed for agricultural-based supply chain management.

The primary focus of this developed application is to bring transparency and security to all participating users of the application; the users of this application include farmers or producers, suppliers or retailers, hotels, and end users. The performance analysis shows that the average gas utilization of the proposed ASBlock dApp is ∼ 2.8 ⋆ 104. The average smart contract execution time for all use cases is ∼ 112sec.

III. PROPOSED METHODOLOGY

The blockchain enhances security, but it may also increase the performance cost of the system, especially in encrypted storage and distributed management processes. The decentralization and consensus mechanism of blockchain may lead to increased system response time and increased consumption of computing resources. The author should balance security and performance in the discussion, consider adopting lightweight blockchain solutions, optimizing consensus algorithms, and allocating computing and storage tasks reasonably to ensure that the system improves performance efficiency while ensuring security. Blockchain is a decentralized, traceable, tamper proof, and multi-party jointly maintained distributed ledger technology. This study is based on the data structure of hash chain, the data update method based on decentralized consensus algorithm, and the design of automated execution of smart contracts.

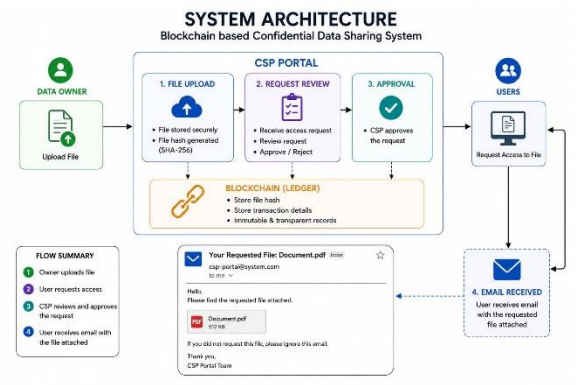
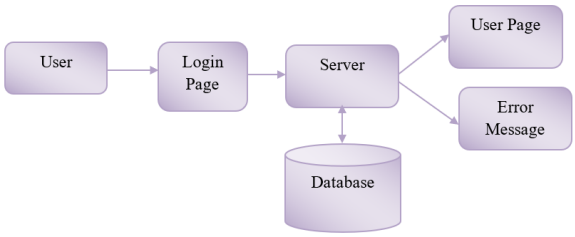


Fig. 1: System Overview

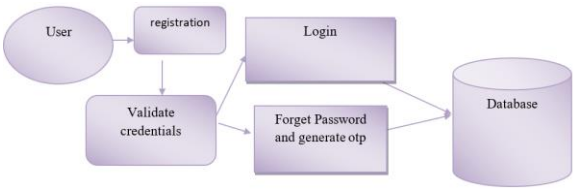
3.1 User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.



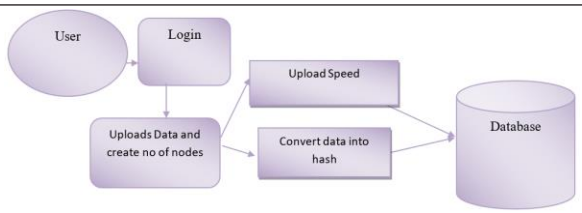
3.2 User Authentication Module

This module manages the registration and login process for users. During sign-up, user credentials are securely stored, and on login, a session is created to track the authenticated user's activity. It ensures that only authorized users can access the system's functionalities. By implementing secure session handling, it prevents unauthorized access and maintains data confidentiality.



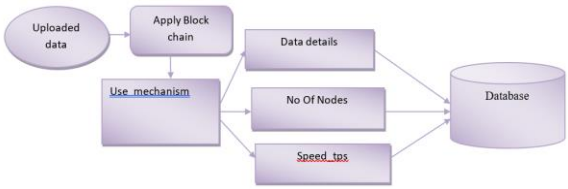
3.3 Data Upload & Storage Module

The data upload module allows users to upload their files into the system. Each file is stored in the database and linked with the cloud service provider (CSP) for secure storage and availability. During upload, the system records essential details such as upload speed, timestamp, and file metadata. This module ensures that data remains accessible, reliable, and ready for blockchain processing.



3.4 Blockchain Processing Module

Once a file is uploaded, this module creates a block containing important information like the file hash, previous hash, timestamp, and node details. Each block is linked to the previous one, ensuring immutability through blockchain technology. The SHA-256 algorithm is applied to generate unique hashes for every file, providing integrity and tamper-proofing. This creates a secure chain of file transactions that cannot be altered.



3.5 Encryption & Decryption Module

Security of the data blocks is ensured through strong encryption and decryption mechanisms. Before being stored, each block is encrypted using keys derived from SHA-256 hashing, which guarantees confidentiality and protection against tampering. When a user requests the data, the encrypted blocks are retrieved and decrypted

only if the requester is authenticated. The decrypted blocks are then reassembled to reconstruct the original dataset or file. This process ensures end-to-end data security and prevents unauthorized access at every stage of data storage and retrieval.

3.6 Consensus Mechanism Module

To validate each transaction and block, this module applies consensus protocols such as Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Delegated Proof of Stake (DPoS). These mechanisms ensure that data is verified by multiple nodes in a decentralized manner. By avoiding single-point failures, the consensus algorithms increase reliability and trust in the system. They also enhance the speed and security of file validation.

3.7 Smart Contract Module

Smart contracts in this module automate rules and access policies for file transactions. They ensure that only authorized users can access or modify data, enforcing security without human intervention. The contracts also manage conditions like approval workflows and automatic verification during uploads. This reduces manual overhead while ensuring transparency, immutability, and fairness in access control.

3.8 Analytics & Visualization Module

This module provides real-time insights into system performance and user activity. It generates graphical reports on upload speed, the number of nodes created, time differences between file uploads, and hash variations. By visualizing blockchain activities and consensus results, users and administrators can monitor the system effectively. This not only improves usability but also helps in identifying patterns and detecting abnormal behaviors.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The proposed blockchain-based framework for securing confidential data in digital information infrastructures was evaluated using metrics such as security strength, transaction processing time, data integrity, and system throughput. Experimental results demonstrated that the use of Blockchain Technology significantly improved protection against unauthorized access, data tampering, and single points of failure. The decentralized architecture ensured secure and transparent data sharing while maintaining high reliability and traceability of transactions. The analysis confirms that the proposed approach provides enhanced

confidentiality, integrity, and availability of sensitive information with acceptable computational and communication overhead.

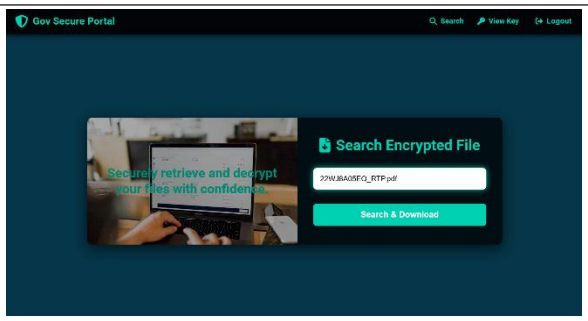


Fig. 5: Search Encrypted File

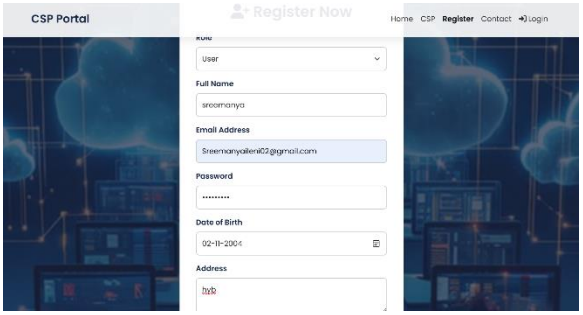


Fig. 2: Registration

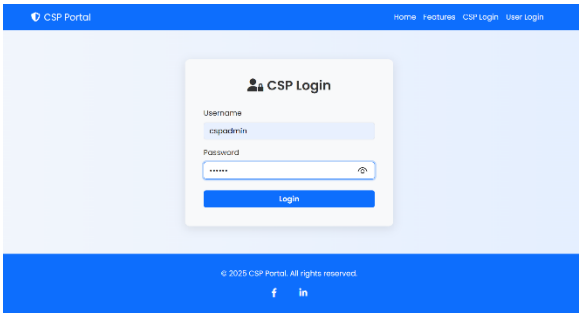


Fig. 6: CSP Login

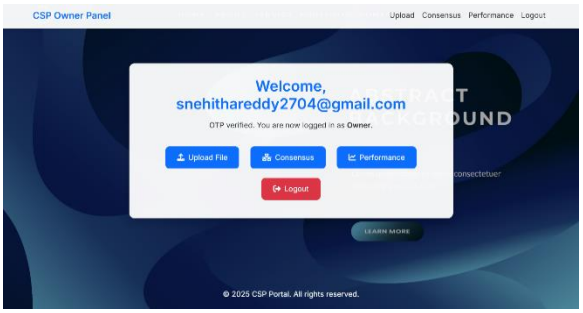


Fig. 3: Home Page

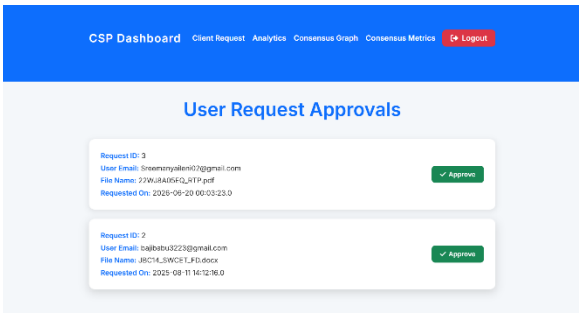


Fig. 7: User Request Approvals

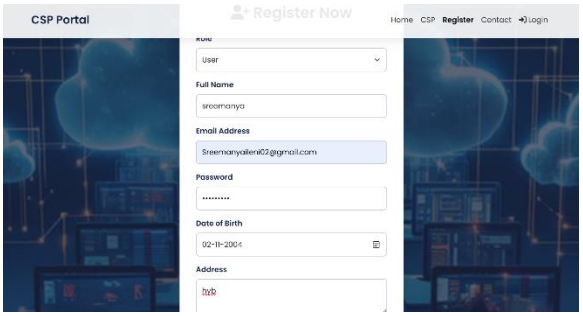


Fig. 4: Registration

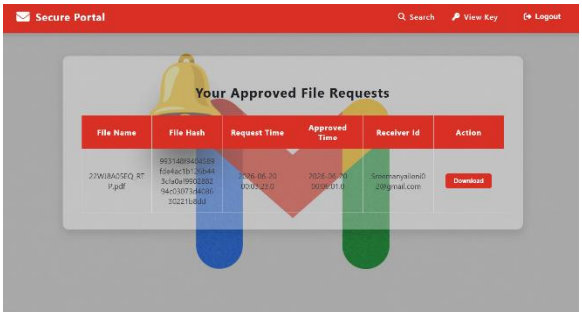


Fig. 8: User Approved Requests

V. CONCLUSION

This project demonstrates the effective integration of blockchain technology with SHA-256 hashing, consensus mechanisms (PoS, PBFT, DPoS), and cloud storage to ensure secure, transparent, and reliable management of sensitive data. By employing blockchain-backed user and operator registration, encrypted block-level storage, and immutable ledger validation, the system provides end-to-end confidentiality, integrity, and accountability for all uploaded datasets. The use of smart contracts strengthens access control, ensuring that only authorized entities can retrieve or manage data, while analytics dashboards provide insights into upload speed, block creation, hash verification, and system performance. Overall, the project proves that blockchain-enabled storage combined with cryptographic hashing and decentralized consensus can significantly reduce risks of data tampering, unauthorized access, and single-point failures, making it an efficient and secure solution for modern information systems.

VI REFERENCES

[1] Jin, Y., and Hu, S. Impact of blockchain technology on information dis closure of competition platforms. Procedia Computer Science, vol. 242, pp. 742–748, 2024.

[2] Moosavi, N., Taherdoost, H., Mohamed, N., Madanchian, M., Farhaoui, Y., and Khan, I. U. Blockchain Technology, Structure, and Applications: ASurvey. Procedia Computer Science, vol. 237, pp. 645–658, 2024.

[3] Panigrahi, A., Pati, A., Dash, B., Sahoo, G., Singh, D., and Dash, M. ASBlock: An Agricultural based Supply Chain Management using Blockchain Technology. Procedia Computer Science, vol. 235, pp. 1943–1952, 2024.

[4] Aljarrah, E. AI-based model for Prediction of Power consumption in smart grid-smart way towards smart city using blockchain technology. Intelligent Systems with Applications, vol. 24, pp. 200440, 2024.

[5] Bamakan, S. M. H., and Far, S. B. Distributed and trustworthy digi tal twin platform based on blockchain and Web3 technologies. Cyber Security and Applications, vol. 3, pp. 100064, 2025.

[6] Boumaiza, A., and Maher, K. Leveraging blockchain technology to enhance transparency and efficiency in carbon trading markets. Inter national Journal of Electrical Power & Energy Systems, vol. 162, pp. 110225, 2024.

AUTHORS Profile



Mrs. E. MOUNIKA REDDY has received her B.Tech from JNTUH, Hyderabad in 2015, M.Tech degree in Computer science from JNTUH, Hyderabad in 2017. She is dedicated to teaching field from the last 8 years. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Ms. ILENI SREEMANYA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. JAKKULLA BRIJANAND pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. KOPPULA SAI GOPINADHREDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026



Mr. JANGA VISHNU VARDHANREDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.