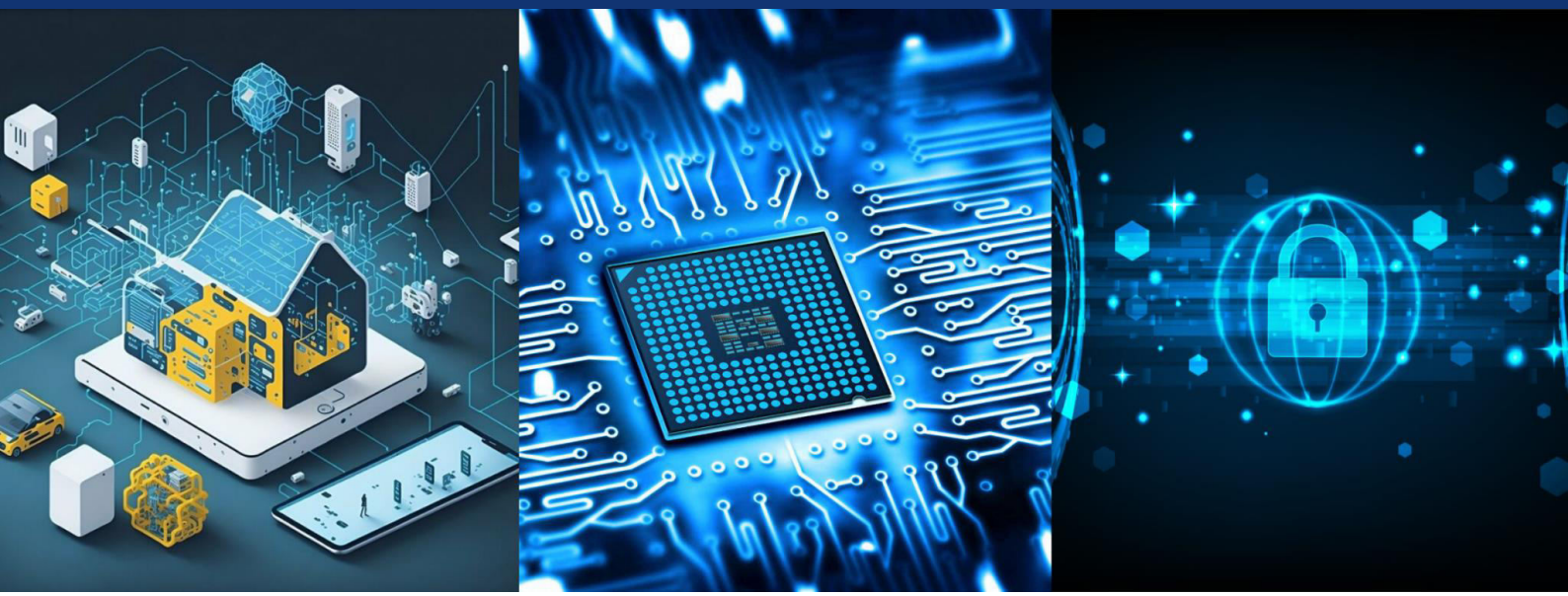
IJIRCCE

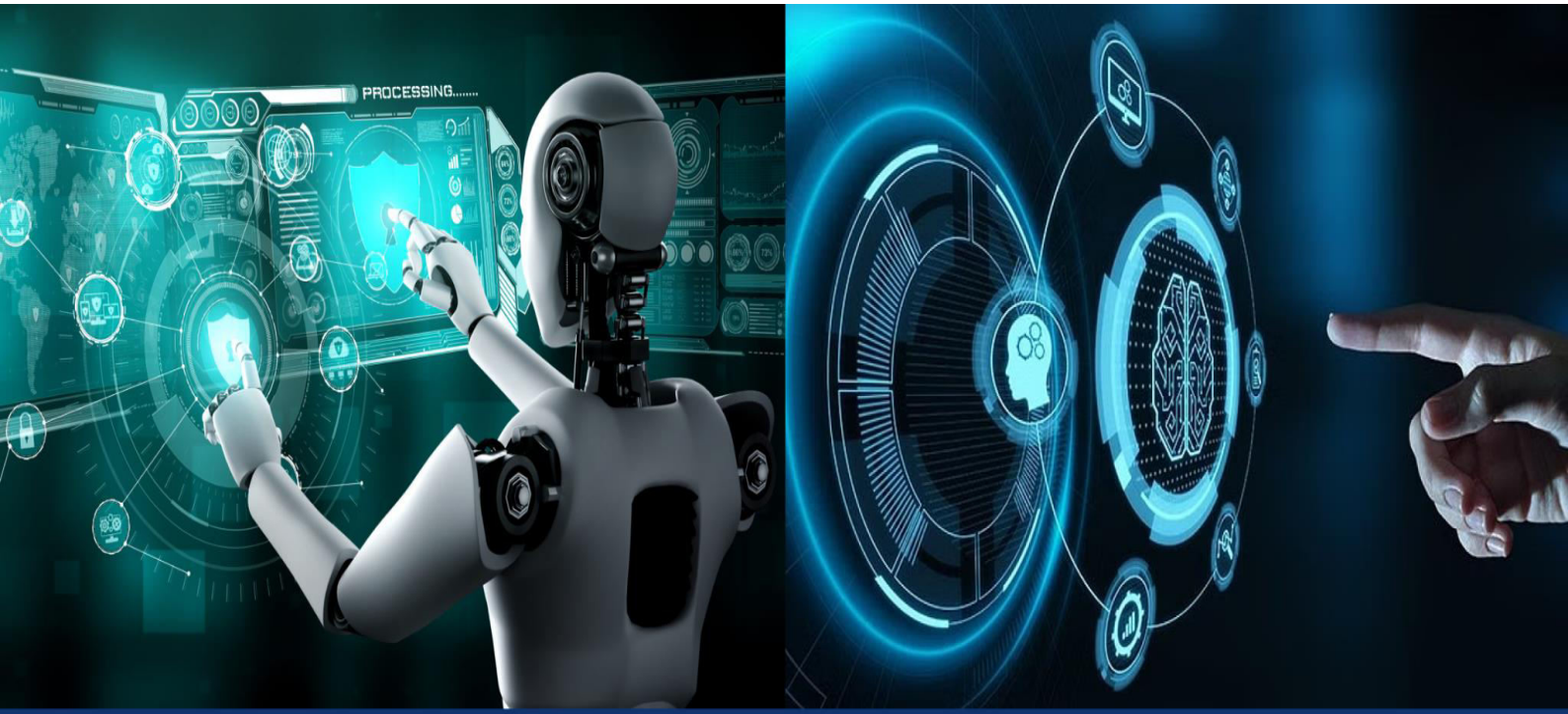
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

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



Impact Factor: 8.771

Volume 14, Issue 4, April 2026

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404017

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

KYC-Chain: Automated and Decentralized KYC

Vuyyuru Venkat Reddy[1], Sanakkayaala Vamsi Krishna[1], Vykuntapu Rajesh[1], Yeruva Rajendra[1], Mr. N. Ashok Kumar[2]

Students, Department of Information Technology, Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India[1]

Assistant Professor, Department of Information Technology, Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India[2]

ABSTRACT: Know Your Customer (KYC) processes are essential for verifying user identities in modern financial systems, yet traditional approaches rely heavily on centralized infrastructures and manual validation procedures. These limitations often lead to increased processing time, higher operational costs, and greater exposure to data security risks. Additionally, users are required to repeatedly submit the same sensitive information across multiple institutions, resulting in inefficiency and reduced user convenience.

This paper introduces KYC-CHAIN, a blockchain-enabled decentralized framework designed to enhance the efficiency and security of KYC operations. The proposed system utilizes distributed ledger technology to maintain tamper-resistant records while eliminating dependence on centralized storage. Smart contracts are employed to automate verification workflows and enforce controlled access to user data. Experimental observations indicate that the system significantly reduces verification time and minimizes redundant data submissions. Overall, the framework offers a scalable, secure, and user-focused solution for modern digital identity management.

KEYWORDS: Blockchain, KYC, Decentralized Architecture, Data Privacy, Identity Verification, Secure Data Sharing.

I. INTRODUCTION

Identity verification plays a critical role in ensuring trust, security, and regulatory compliance within financial ecosystems. Most existing KYC processes rely on centralized data handling, where each organization independently manages user information, leading to inefficiencies and repeated verification steps. This fragmented approach leads to repeated verification processes, increased operational delays, and greater exposure to security vulnerabilities.

With the rapid expansion of digital banking and financial technologies, these inefficiencies have become more evident. Users are often required to submit identical documents multiple times across different platforms, resulting in redundancy and a poor user experience. Although digital KYC solutions have improved accessibility, most still rely on centralized systems, limiting transparency and user control over personal data.

To address these challenges, this work introduces a blockchain-enabled KYC framework that leverages decentralization to enhance data security, reduce duplication, and enable controlled data sharing. By utilizing an immutable ledger and automated mechanisms, the proposed system aims to provide a more efficient and user-centric identity verification process.

II. RELATED WORK

Existing KYC systems typically operate in isolated environments, where each organization maintains its own customer database. This lack of integration leads to repeated verification procedures, increased processing time, and inefficient resource utilization. Furthermore, centralized data storage introduces significant risks, as it becomes a potential target for cyberattacks and unauthorized access.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404017

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

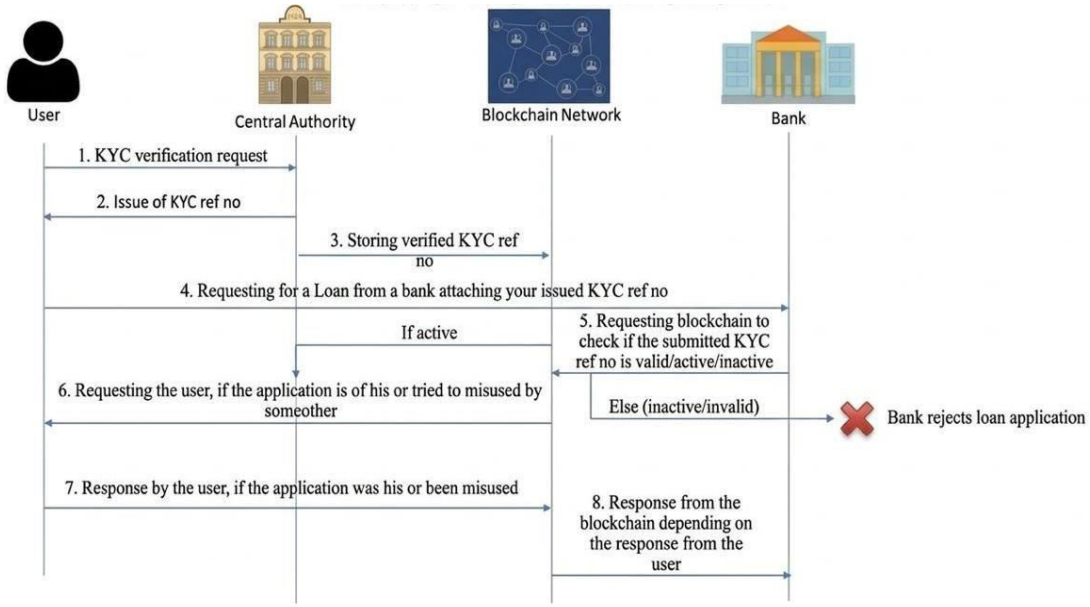
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Recent research has explored the application of blockchain technology in KYC systems, primarily focusing on improving data security through distributed storage and cryptographic methods. While these approaches offer enhanced protection against data tampering, many of them do not fully address the challenges of seamless data sharing and real-time interoperability among institutions. In several cases, user control over personal data remains limited.

The proposed KYC-CHAIN system distinguishes itself by combining secure data storage, automated verification, and controlled data access within a unified framework. This integration not only improves efficiency but also ensures that users retain greater authority over how their information is accessed and utilized.

III. SYSTEM ARCHITECTURE

The KYC-CHAIN framework adopts a decentralized architecture designed to enhance security, transparency, and efficiency in identity verification processes. At its core, the system consists of multiple interconnected components that work collaboratively to manage the KYC lifecycle. The user module serves as the primary interface through which individuals can register, upload their identification documents, and manage access permissions for their data. This ensures that users retain control over how and when their information is shared. Complementing this, the administrator module functions as the validation layer, where authorized entities review submitted documents and update the verification status after confirming their authenticity. The blockchain network acts as the foundational layer of the system, storing encrypted data hashes and maintaining an immutable record of all transactions, thereby ensuring data integrity and preventing



unauthorized modifications. In addition, smart contracts play a critical role by automating verification workflows and enforcing strict access control policies, allowing data to be shared only with explicit user consent. By integrating these components into a unified system, the architecture eliminates dependence on centralized authorities while enabling secure, efficient, and user-centric data management.

IV. METHODOLOGY

A. Methodological Overview

The proposed framework for KYC-CHAIN follows a decentralized approach for user verification by utilizing blockchain technology. The proposed methodology aims to replace the conventional centralized approach for KYC systems with a more transparent and user-controlled approach. The proposed framework consists of several phases for user registration, data submission, blockchain-based data storage and verification, and data access.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404017

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

B. KYC Data Submission and Processing

This process starts with the registration of the users, where the users create their account and provide the required identification information as depicted in Fig. 2. The interface is simple and easy to use. After registration, the users will be required to upload their information in the KYC category along with the required identification documents. The information provided is processed and prepared for storage. The information provided is stored in an encrypted form in order to maintain the confidentiality of the information. Each information provided is linked with a specific identifier in order to track the information efficiently.

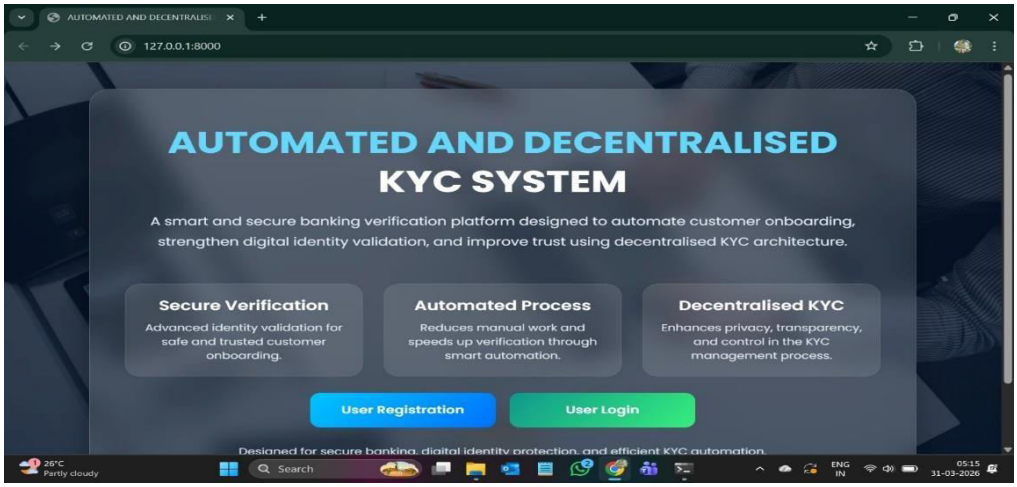


Fig 2. User Registration and Login

C. Blockchain-Based Storage Mechanism

The processed KYC information is stored in a blockchain network in a secure manner with the help of smart contracts, as shown in Fig. 3. Each information is stored in the form of a transaction and is linked together with the help of cryptographic hash functions. After storing the information in the blockchain network, it is not possible to modify it without compromising the integrity of the whole chain. This way, the risk of storing information in a centralized database is eliminated.

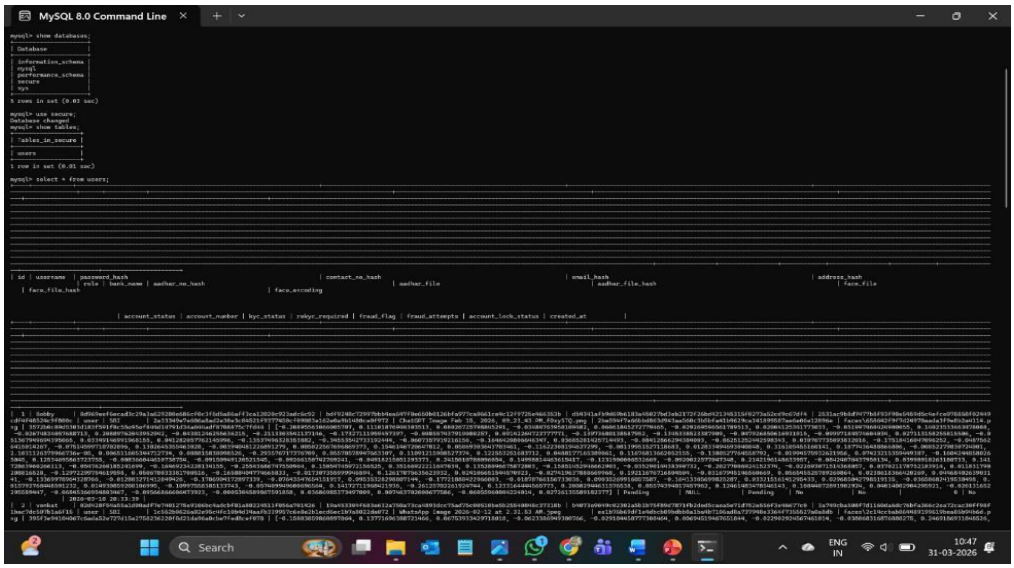


Fig 3. User Data Storage in Encrypted Form Using SHA-256

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404017

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

D. Verification and Status Management

The authorized administrators are responsible for verifying the provided information in the KYC data. This is demonstrated in Fig. 4. The verification process involves validating user information as well as supporting documents. According to the verification results, the user information will be updated as either verified or rejected. The verified information will be regarded as valid for use and sharing purposes.

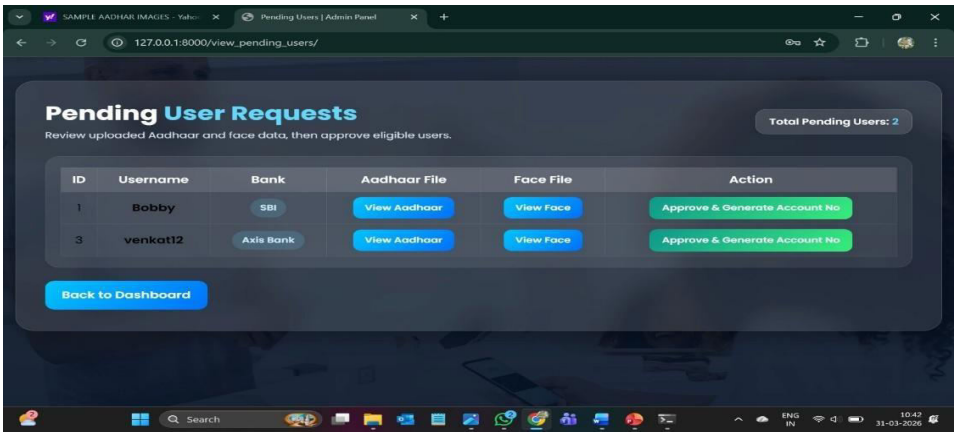


Fig 4. Verification and Status Management in Admin Portal

E. Access Control Mechanism

The proposed framework, as shown in Fig 5, incorporates a permission-based access control system to allow only authorized entities to access KYC information stored on the blockchain. The access request is verified before allowing data access. The system is intended to support user-controlled data sharing, where users can accept or deny access. Although user-level approval is not included in this proposed framework, it ensures secure and limited access to verified KYC information.

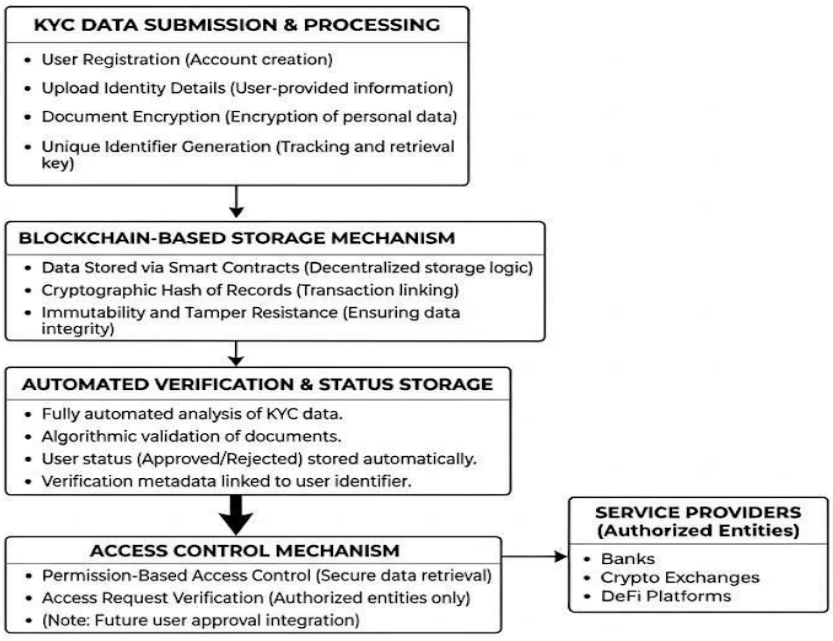


Fig 5. Flowchart of the proposed System

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

V. IMPLEMENTATION

The proposed system was developed as a full-stack web application seamlessly integrated with a blockchain-based backend to ensure both usability and security. The frontend was designed to provide an intuitive and responsive user interface, allowing users to easily register, upload their KYC documents, and manage data-sharing permissions. On the backend, robust communication mechanisms were implemented to interact with the blockchain network, ensuring secure processing and storage of user data. Smart contracts were developed using Solidity to handle critical operations such as verification logic, status updates, and access control. These contracts act as autonomous and tamper-proof programs that execute predefined rules, thereby eliminating the need for manual intervention and reducing the chances of human error.

For testing and development purposes, the system was deployed in a local blockchain environment using tools such as Truffle and Ganache. This setup enabled efficient simulation of blockchain transactions, testing of smart contract functionality, and analysis of system behaviour under controlled conditions. It also allowed for rapid debugging and optimization before considering deployment on a live network. To strengthen data security, advanced cryptographic techniques were employed. User documents were protected using AES encryption prior to transmission, ensuring that sensitive information remains confidential even if intercepted. Additionally, SHA-256 hashing was used to generate unique cryptographic hashes of the data, which were stored on the blockchain to maintain integrity and prevent tampering.

The system was further evaluated under simulated operational conditions to assess its performance, reliability, and scalability. Various scenarios were tested, including multiple user requests and concurrent verification processes, to ensure that the system could handle real-world workloads efficiently. The results demonstrated that the integration of blockchain technology with automated smart contracts significantly enhances the speed, security, and transparency of the KYC process, making it a viable solution for modern digital identity management systems.

VI. RESULTS AND DISCUSSION

The The proposed system successfully demonstrated efficient and reliable handling of the KYC verification process across all stages of the identity lifecycle. Experimental observations revealed a substantial improvement in processing time when compared to traditional KYC systems, which typically rely on manual verification and repeated document submissions. In conventional approaches, the verification process can take several hours to days due to administrative delays and inter-institutional dependencies. However, in the proposed framework, once the user's identity is initially verified and securely recorded on the blockchain, subsequent verification requests can be completed within a few minutes. This significant reduction in processing time is achieved by reusing previously validated identity records, thereby eliminating redundant verification efforts.

Moreover, the integration of blockchain technology plays a crucial role in enhancing the overall security and robustness of the system. By shifting from centralized databases to a decentralized ledger, the framework effectively removes the single point of failure that is commonly exploited in traditional systems. This ensures that even if a part of the network is compromised, the integrity and availability of the data remain unaffected due to the distributed nature of the blockchain. Additionally, the use of cryptographic techniques such as hashing and encryption safeguards sensitive user information from unauthorized access and tampering.

The system also contributes significantly to improving the user experience by introducing a more streamlined and user-centric approach to data sharing. Instead of repeatedly submitting the same documents to different institutions, users can rely on a single verified identity that can be securely shared when required. Through smart contract-based permission mechanisms, users maintain full control over their data, granting access only to authorized entities. This not only reduces user effort but also enhances transparency and trust in the verification process. Overall, the proposed system presents a highly efficient, secure, and scalable solution for modern KYC requirements.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

Parameter	Traditional KYC System	Proposed KYC-CHAIN System
Verification Time	24–48 hours	5–10 minutes
Data Redundancy	High (Repeated submissions)	Very Low (One-time verification)
Data Security	Moderate (Centralized storage)	High (Blockchain-based security)
User Control	Limited	Full user-controlled access
Data Sharing	Manual and repetitive	Automated with user permission
Risk of Data Breach	High	Low
Transparency	Low	High
System Scalability	Limited	High

Fig: Comparison Between Traditional KYC and Proposed KYC-CHAIN System

VII. CONCLUSION

This paper presented KYC-CHAIN, a blockchain-based framework designed to improve the efficiency and security of identity verification processes. By minimizing repetitive document submissions and leveraging a decentralized ledger, the system enables faster verification while maintaining data integrity and resistance to tampering. The integration of smart contracts further automates key operations, reducing reliance on manual intervention and improving overall reliability.

The proposed approach demonstrates notable improvements over traditional KYC systems, particularly in terms of processing speed, data security, and user experience. By allowing controlled data sharing, the system empowers users to manage access to their personal information more effectively. Future work may focus on deploying the system at scale, incorporating biometric authentication mechanisms, and exploring advanced privacy-enhancing techniques to further strengthen data protection and adaptability in real-world scenarios.

REFERENCES

[1] M. A. Hannan et al., “A systematic literature review of blockchain-based e-KYC systems,” IEEE Access, 2023.
[2] V. Schlatt et al., “Designing a framework for digital KYC processes built on blockchain-based identity,” Information & Management, vol. 59, no. 3, 2022.
[3] B. Karadag et al., “Blockchain-Based KYC Model for Secure Banking Systems,” IEEE Access, 2023.
[4] T. Tanchangya et al., “Mapping blockchain applications in financial services,” Information (MDPI), 2024.
[5] A. Vaziry et al., “A systematic review on blockchain-based identity systems,” arXiv, 2024.
[6] U. Arshad et al., “Web3-Based Identity and KYC Innovations,” ACM Digital Library, 2024z
[7] M. Elveny et al., “Blockchain-enabled KYC integration for secure customer data management,” Future Business Journal (Elsevier), 2025.
[8] F. Piper et al., “Privacy-preserving KYC data sharing mechanisms,” arXiv, 2025.
[9] I. Ahmed et al., “Blockchain-enabled e-KYC systems: Challenges and opportunities,” TechRxiv, 2023. [10]A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in IoT: Challenges and solutions,” IEEE Internet of Things Journal, vol. 6, no. 5, 2019.
[11] R. Norvill et al., “A security and privacy focused KYC data sharing platform,” in Proc. ACM BSCI, 2020.
[12] N. Kshetri, “Blockchain’s roles in strengthening cybersecurity and protecting privacy,” Telecommunications Policy, vol. 46, no. 2, pp. 102–118, 2022.
[13] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
[14] M. Swan, Blockchain: Blueprint for a New Economy, O’Reilly Media, 2015.
[15] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.
[16] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

Paper, 2014.
[17] A. M. Antonopoulos, Mastering Bitcoin, O'Reilly Media, 2017.
[18] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," NIST, 2018.
[19] J. Bonneau et al., "SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies," IEEE Symposium on Security and Privacy, 2015.
[20] Z. Zheng et al., "Blockchain challenges and opportunities: A survey," International Journal of Web and Grid Services, vol. 14, no. 4, 2018.
[21] M. Pilkington, "Blockchain technology: Principles and applications," in Research Handbook on Digital Transformations, 2016.
[22] H. Treiblmaier, "The impact of blockchain on the supply chain: A theory-based research framework," Supply Chain Management, 2018.
[23] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, 1976.
[24] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, 1978.
[25] E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," ACM EuroSys, 2018.
[26] J. Benet, "IPFS – Content addressed, versioned, P2P file system," arXiv, 2014.
[27] K. Croman et al., "On scaling decentralized blockchains," Financial Cryptography and Data Security, 2016.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

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