Global Journal of Engineering Innovations & Interdisciplinary Research

Original Article

Blockchain For Enhancing Trust & Privacy in E-KYC

Dr. P. U. Anitha[1], G.Rachana[2], K. Sushmitha[2], A. Sai kumar[2], D. Vijay Kumar[2]

[1]Associate Professor, Department of CSE, Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India
[2]UG Students, Department of CSE, Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India

Correspondence

Dr. P. U. Anitha

Associate Professor, Department of CSE, Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India

- Received Date: 25 Jan 2026
- Accepted Date: 14 Mar 2026
- Publication Date: 20 Mar 2026

Keywords

Blockchain Technology, Distributed Ledger Technology , Smart Contracts, Decentralized Identity Verification, Data Security, User Privacy, Encryption, Immutable Ledger, Tamper proof System, Permissioned Access, Digital Identity Management, Fraud Prevention, Data Sharing Control, Operational Cost Reduction, Trust Enhancement, Secure Authentication.

Abstract

Electronic Know Your Customer (e-KYC) systems play a crucial role in verifying user identities for financial institutions, telecom operators, and other service providers. However, traditional e-KYC frameworks rely heavily on centralized databases, making them vulnerable to data breaches, unauthorized access, single points of failure, and privacy risks. To address these challenges, this paper proposes a blockchain-based e-KYC system that enhances trust, security, and user privacy. The proposed architecture integrates distributed ledger technology with smart contracts to create a transparent, tamper-proof, and decentralized identity verification platform. User data is encrypted and stored securely, while verification records are maintained on an immutable blockchain ledger. Authorized entities can access customer information only through permissioned smart contracts, ensuring controlled data sharing and minimizing exposure. This approach eliminates repeated KYC processes, reduces operational costs, prevents identity fraud, and strengthens user control over personal data.Over all, the blockchain-enabled e-KYC system provides a more reliable, efficient, and privacy-preserving solution compared to conventional centralized models. It significantly improves trust among stakeholders and establishes a secure foundation for digital identity management in modern financial and governmental ecosystems.

Introduction

Electronic-Know Your customer (e-KYC) is a service that banks or financial institutions (FIs) provide virtual banking operation related to authentication and verification of identity electronically to their customers for improving cost efficiency and customer satisfaction. The e-KYC system enables FIs to electronically verify their customer identity and retrieve KYC data for both individual and corporate clients. To implement the e-KYC system, financial institutions either employ off the- shelf e-KYC software fully equipped with necessary functions or develop their own. Due to the trend of the outsourcing model, most enterprises have adopted the cloud as the preferred platform for housing their system and data.

A cloud-based e-KYC system provides a more efficient and flexible authentication method compared to the host based e-KYC authentication method where documents need to be validated via the centralized host. This causes a traffic bottleneck and single point of failure problem. Also, the traceability of the verified transaction is limited since all transactions occurring in the system are entirely managed by the provider.This is because e-KYC system located on the cloud store customer data documents and it might be viewed by any public cloud tenants or even the cloud service providers (CSPs).

To address this concern, most banks and FIs need to implement an encryption mechanism in addition to the strong authentication feature provided by the CSPs. To this end, banks and FIs possessing the e-KYC system need to encrypt the e-KYC data _les before they are uploaded to the cloud. When the relying parties request for verification, the host party can either perform the verification by either decrypting and sending back the confirmation of the verification result to the requestor or transmitting the copy of encrypted _les along with the decryption key to the requestor.

Background

Traditional Know Your Customer (KYC) processes rely on physical document submission and manual verification, making them time-consuming, inefficient, and prone to human errors. With the advancement of cloud computing, electronic KYC (e-KYC) systems have improved efficiency and accessibility; however, they also introduce several challenges, including data privacy concerns, the risk of unauthorized access by cloud service providers, key management issues such as revocation and regeneration, and centralized control that creates single points of failure.Additionally, the integration of smart

Citation: Anitha PU, Rachana G, Sushmitha K, Sai kumar A, Vijay kumar D. Blockchain For Enhancing Trust & Privacy In E-KYC. GJEIIR. 2026;6(3):0179.

contracts automates verification processes, reduces dependency on manual intervention, and strengthens trust among multiple stakeholders, making the system more secure, reliable, and efficient.

Problem Statement

The existing Know Your Customer (KYC) and electronic KYC (e-KYC) systems largely depend on centralized architectures and cloud-based storage, which expose sensitive user data to significant security and privacy risks. These systems are vulnerable to data breaches, unauthorized access, and misuse by third-party providers. Additionally, centralized control creates single points of failure, making the system less reliable and more susceptible to cyberattacks. Traditional KYC processes are also repetitive, time-consuming, and inefficient, leading to increased operational costs and poor user experience. Furthermore, challenges related to key management, such as secure storage, revocation, and regeneration, remain inadequately addressed. Therefore, there is a need for a secure, decentralized, and privacy-preserving e-KYC solution that ensures data integrity, enhances user control over personal information, minimizes redundancy, and improves overall trust and efficiency in identity verification systems.

Literature Survey

- **Federated Learning for Privacy-Preserving KYC (2024):** It explores the use of federated learning to enable privacy-preserving KYC processes without centralizing sensitive data. It leverages differential privacy techniques to ensure data protection while allowing financial institutions to verify identities securely.
- **Enhancing KYC with Behavioural Biometrics in Cloud Environments (2024):** Investigates the use of behavioural biometrics and machine learning to strengthen KYC verification. By analysing user behaviour patterns, the system provides an additional layer of security for identity verification, particularly for mobile users. The approach ensures data owner control while improving authentication accuracy and reducing fraud risks in cloud-based KYC solutions.
- **Enhancing Privacy in e-KYC Systems Using Zero Knowledge Proofs (2023):** It demonstrates how zero-knowledge proofs (ZKPs) can improve privacy in e-KYC systems by allowing identity verification without revealing sensitive data. It employs data anonymization techniques to enhance security and protect users' personal information. The proposed solution effectively reduces the risk of identity theft while maintaining compliance with privacy regulations.
- **A Blockchain-Based Approach for Secure and Efficient Verification (2022):** It proposes a blockchain-based system for secure and efficient identity verification. It utilize smart contracts and data encryption to ensure transparency and prevent fraudulent activities.By decentralizing the verification process, the system improves security, enhances trust, and eliminates reliance on third-party intermediaries
- **Blockchain Technology for Secure and Transparent eGovernance Systems (2021):** This research explores the potential of blockchain in egovernance for secure and transparent identity verification. By leveraging blockchain's decentralized nature, the system enhances security and reduces the risks associated with centralized identity management. The proposed approach strengthens transparency and trust in e-governance systems.

Proposed system

The proposed system introduces a secure and efficient blockchain-based e-KYC document registration and verification framework that leverages lightweight cryptographic protocols and the Interplanetary File System (IPFS) for decentralized storage. The encrypted data is stored in IPFS, while only the corresponding hashes and transaction records are maintained on the blockchain to ensure immutability and integrity.

To address privacy and user consent requirements, a smart contract is developed to generate, manage, and enforce user consent. Customers digitally sign their consent, which is then recorded on the blockchain in a tamper-proof manner, enabling transparent auditing and accountability. For enhanced data privacy and fine-grained access control, the system employs Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to secure blockchain transactions. This allows multiple authorized financial institutions to access encrypted user data based on predefined access policies without compromising confidentiality

Modules Used

The system consists of key modules including the Authority, Client, IPFS, Blockchain, and Smart Contracts working together for secure e-KYC processing. The Authority manages keys, clients provide encrypted data with consent, while IPFS stores encrypted documents and blockchain maintains tamper-proof transaction records. Smart contracts automate registration, consent management, and verification, ensuring secure, efficient, and decentralized identity management.

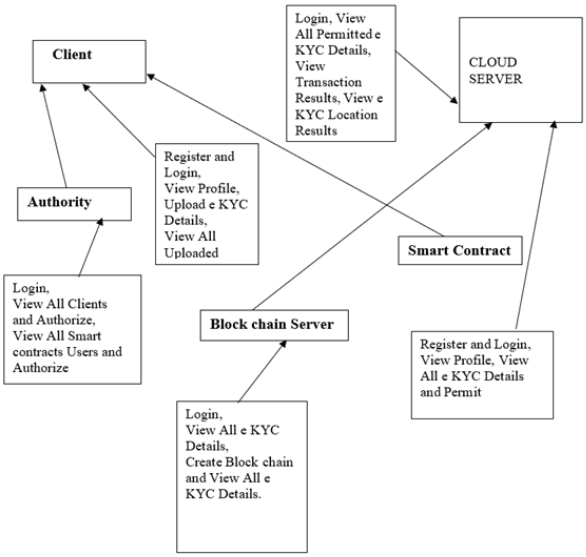
Manufacturers

In the blockchain-based e-KYC system, the "manufacturers" module can be interpreted as the key system participants who register and operate within the platform. These include Financial Institutions (such as banks and telecom providers) that must first register and obtain authorization from the authority before performing any operations. After successful registration and approval, they can log in using their credentials and access the system to perform actions such as requesting KYC verification, viewing customer profiles, accessing approved KYC data, and managing verification requests. These participants interact with the blockchain and smart contracts to securely verify identities, access encrypted user information, and maintain transaction records in a controlled and authorized manner

Advantages Of Proposed System

- The advantage of having ciphertext policy attribute-based encryption(cp-abe) is to protect the data from external attacker.
- The system is very safe and secure since it is implemented with blockchain in identity management system.
- Smart contracts automate the KYC verification process, reducing manual intervention and human errors
- It enables fine-grained access control, allowing only authorized financial institutions to access user data based on defined policies.
- The use of encryption techniques enhances user privacy by keeping sensitive information confidential.
- It reduces the need for repeated KYC verification across multiple organizations, saving time and effort.
- Operational costs are minimized by reducing paperwork, manual verification, and redundancy.

System Architecture



Results

The proposed blockchain-based e-KYC system demonstrates significant improvements over traditional KYC and cloud-based models in terms of security, efficiency, and reliability. By integrating blockchain technology with IPFS and advanced cryptographic techniques, the system ensures secure storage and tamper-proof management of user data. The implementation successfully enables encrypted storage of KYC documents in IPFS, while only hash values and transaction records are maintained on the blockchain, ensuring data integrity and privacy.

Conclusion

We have presented the privacy-preserving e-KYC approach based on the block chain. Our proposed scheme delivers secure and decentralized authentication and verification of the e-KYC process with the user's consent enforcement feature. In our scheme, the privacy of both customers' identity documents stored in the cloud is guaranteed by the symmetric key and public key encryption while the sensitive transaction data stored in the block chain is encrypted by symmetric key encryption and CP-ABE. Our scheme also allows the KYC data to be updated by the data owner or the customer. In addition, we devised an access policy update algorithm to enable dynamic access authorization. For the evaluation, we performed comparative analysis between our scheme and related works in terms of the computation cost, the communication cost, and performance.

Future scope

The proposed blockchain-based e-KYC system can be further enhanced to improve its overall efficiency, security, and scalability. AI/ML-based document verification can be integrated to automatically authenticate identity documents and detect forgeries, significantly reducing manual verification efforts. Incorporating biometric authentication—such as fingerprint, iris, or facial recognition—can strengthen identity accuracy and minimize impersonation risks.To optimize blockchain performance, large documents can be stored securely in off-chain repositories like IPFS, while only hashed references are maintained on-chain. Privacy-preserving technologies such as zero- knowledge proofs (ZKP) can be adopted to validate user information without revealing sensitive data. Additionally, developing a dedicated mobile application can enhance user accessibility, allowing seamless verification and permission management. Real-time fraud detection mechanisms can also be integrated to identify suspicious activities and prevent fraudulent attempts, ensuring a more robust and trustworthy e-KYC ecosystem.

References

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
2. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain technology: Beyond Bitcoin,” Applied Innovation Review, vol. 2, pp. 6–19, 2016.
3. G. Zyskind, O. Nathan, and A. Pentland, “Decentralizing privacy: Using blockchain to protect personal data,” in Proc. IEEE Security and Privacy Workshops, 2015, pp. 180–184.
4. M. Conti, S. K. Sandeep, C. Lal, and S. Ruj, “A survey on security and privacy issues of blockchain technology,” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 116– 133, 2019.
5. A. Al-Heeti, M. Ahmad, and R. M. Noor, “AI-driven document forgery detection using deep learning: A comprehensive review,” IEEE Access, vol. 12, pp. 98734–98752, 2024.
6. ISO/IEC 30107-1:2016, “Information technology — Biometric presentation attack detection — Part 1: Framework,” International Organization for Standardization, 2016.
7. J. Benet, “IPFS – Content Addressed, Versioned, P2P File System,” IPFS Whitepaper,2014.
8. E. Ben-Sasson et al., “Succinct non-interactive zero knowledge for a von neumann architecture,” in Proc. USENIX Security Symposium, 2014, pp. 781–796.
9. A. Putra, L. Lin, and F. R. Yu, “Fraud detection in digital identity management using machine learning: A survey,” IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2345–2362, 2023.