IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 3, May-June 2025

Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203008

Engaging Trust and Security Saving E-KYC System Using Blockchain

O. Kamal, Dr. Khushbu Doulani

UG Scholars, Department of Computer Science and Engineering, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India

Assistant Professor, Department of Computer Science and Engineering, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India

ABSTRACT: The electronic know your customer (e-KYC) is a system for the banking or identity provider to establish a customer identity data verification process between relying parties. Due to the efficient resource consumption and the high degree of accessibility and availability of cloud computing, most banks implement their e-KYC system on the cloud. Essentially, the security and privacy of e-KYC related documents stored in the cloud becomes the crucial issue. Existing e-KYC platforms generally rely on strong authentication and apply traditional encryption to support their security and privacy requirement. In this model, the KYC system owner encrypts the file with their host's key and uploads it to the cloud. This method induces encryption dependency and communication and key management overheads. In this paper, we introduce a novel block chain-based e-KYC scheme called e-KYC Trust Block based on the ciphertext policy attribute-based encryption (CP-ABE) method binding with the client consent enforcement to deliver trust, security and privacy compliance. In addition, we introduce attribute-based encryption to enable the privacy preserving and fine-grained access of sensitive transactions stored in the block chain. Finally, we conduct experiments to show that our system is efficient and scalable in practice.

KEYWORDS:
1. e-KYC (Electronic Know Your Customer)
2. Identity Verification
3. Cloud Computing
4. Security and Privacy
5. Blockchain
6. Attribute-Based Encryption (ABE)
7. Ciphertext Policy Attribute-Based Encryption (CP-ABE)
8. Client Consent
9. Trust and Compliance

I. INTRODUCTION

Electronic Know Your Customer (e-KYC) systems allow financial institutions (FIs) to verify customer identities electronically, enhancing efficiency and customer experience. While cloud-based e-KYC systems offer flexibility and reduced costs compared to host-based models, they raise concerns over data privacy and security, as sensitive identity documents stored in the cloud could be accessed by unauthorized entities. To mitigate this, banks must encrypt e-KYC files before uploading them and manage decryption keys carefully. However, current systems lack effective mechanisms for key revocation and traceability, especially when users withdraw consent, making it difficult to ensure data deletion and prevent unauthorized access.

Blockchain technology offers a decentralized solution that can enhance transparency, security, and traceability in e-KYC processes. Smart contracts enable automated operations and can help manage identity verification, but existing blockchain-based e-KYC models have notable limitations. These include the absence of secure, non-repudiable digital consent mechanisms, inadequate protection of transaction privacy on the blockchain, and restricted user access to update credentials stored in the cloud.

To address these gaps, this paper proposes a secure, blockchain-based e-KYC registration and verification process using lightweight cryptographic protocols and the Interplanetary File System (IPFS). A smart contract framework is

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203008

introduced to collect and enforce user consent with digital signatures, storing them immutably on the blockchain to ensure auditability and regulatory compliance.

II.SYSTEM MODEL AND ASSUMPTIONS

The proposed system model for the blockchain-based e-KYC framework includes three key entities: customers, financial institutions (FIs), and a blockchain network integrated with decentralized cloud storage using the Interplanetary File System (IPFS). Customers initiate the e-KYC process through FIs, which may act as host or relying parties depending on the verification context. All identity documents are encrypted and stored on the IPFS, while transactions, verification records, and user consents are managed through smart contracts deployed on the blockchain. It is assumed that all entities can access and interact with the blockchain, and that each participant possesses a unique cryptographic identity used for secure communications and digital signatures. The system relies on the immutability of smart contracts and the blockchain to ensure data integrity and auditability. Cloud storage providers cannot access decryption keys, thereby maintaining data confidentiality. Additionally, customers can revoke their consent at any time, and the system is expected to support key revocation and secure deletion of data. These assumptions support a decentralized, secure, and privacy-preserving e-KYC process in compliance with regulations such as GDPR.

III. EXISTING SYSTEM

The For years, a few research works related to block chain-based KYC have proposed to deliver the decentralized authentication and verification process. However, there are shortcomings that have not been fully solved by existing works. First, there are no works that provide electronic client's consent function with the solid nonrepudiation property which is an essential requirement of privacy regulations such as General Data Protection Act (GDPR) in the KYC registration process. Second, most existing works overlook the privacy of transaction stored in the smart contract and blockchain. In addition to the identity or credential documents that are encrypted on the cloud storage, the privacy of all e-KYC processing transactions such as transaction status sharing, data origin authentication, and smart contract that contains personal data stored in the blockchain should be preserved.

Existing System Disadvantages:

- Decentralized authentication.
- Verification process.

IV. PROPOSED SYSTEM

In this model, the KYC system owner encrypts the file with their host's key and uploads it to the cloud. This method induces encryption dependency and communication and key management overheads. In this paper, we introduce a novel blockchain-based e-KYC scheme called e-KYC Trust Block based on the cipher text policy attribute-based encryption (CP-ABE) method binding with the client consent enforcement to deliver trust, security and privacy compliance. In addition, we introduce attribute-based encryption to enable the privacy preserving and fine-grained access of sensitive transactions stored in the blockchain. Finally, we conduct experiments to show that our system is efficient and scalable in practice.

PROPOSED SYSTEM ADVANTAGE

- Attribute-based encryption to enable the privacy preserving.
- Induces encryption dependency and communication.
- Key management overheads.

V. METHODOLOGIES

The methodology for implementing a secure and efficient blockchain-based e-KYC system involves integrating blockchain technology, smart contracts, and decentralized cloud storage (IPFS) to address privacy, security, and traceability concerns. The process begins with customer registration, where identity documents are encrypted locally and uploaded to IPFS. A unique digital signature and consent are generated and stored on the blockchain via a smart contract to ensure non-repudiation and auditability. Financial institutions interact with the system to either verify customer data directly through the host party or retrieve encrypted files along with decryption keys for local verification. Smart contracts manage consent collection, access permissions, and transaction logs, ensuring

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203008

transparency and compliance with regulations like GDPR. Key management protocols are applied to securely handle key generation, sharing, revocation, and regeneration, especially when consent is withdrawn. Throughout the process, the blockchain ensures data immutability and integrity, while IPFS ensures efficient, scalable, and decentralized storage, forming a robust and privacy-preserving e-KYC ecosystem.

MODULES EXPLANATION

1. User Registration Module

This module enables new customers to register by submitting their identity documents. Before upload, documents are encrypted locally using a cryptographic key. A digital signature is created by the user to ensure authenticity. The module then triggers a smart contract to store the user's consent and basic metadata on the blockchain, establishing a tamper-proof record of the registration.

2. Document Management Module

Responsible for handling secure storage of identity documents. Encrypted documents are stored on the decentralized IPFS cloud. This module manages upload, retrieval, and deletion processes, ensuring that documents are only accessible by authorized parties with valid decryption keys.

3. Verification and Authentication Module

This module facilitates the identity verification process. When a financial institution requests verification, the module either performs the verification internally and sends the result back or shares the encrypted document and a secure decryption key. This dual approach offers flexibility while maintaining security.

4. Transaction Logging Module

All actions related to e-KYC—such as document submission, access requests, and consent changes—are logged on the blockchain. This module ensures traceability and transparency by maintaining an immutable audit trail that can be reviewed for compliance or dispute resolution.

5. Consent Management Module

This module manages customer consent, a critical requirement under privacy laws like GDPR. Smart contracts are used to collect, validate, and enforce digital consent. Customers can also revoke consent, and the system updates access rights accordingly, ensuring that no unauthorized access occurs after consent withdrawal.

6. Key Management Module

Handles the secure lifecycle of encryption keys used in the system. It includes key generation, secure sharing between parties, revocation when access is withdrawn, and regeneration when keys are compromised, or access rules change. This ensures continued confidentiality and controlled access to user data.

VI. RESULTS AND DISCUSSION

The proposed privacy-preserving e-KYC scheme demonstrates significant improvements over existing solutions in terms of security, efficiency, and compliance with regulatory requirements. Through a series of experiments and comparative analysis, the system was evaluated based on computation cost, communication cost, and overall performance. The results show that the integration of symmetric key encryption, public key encryption, and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) ensures robust protection of both identity documents in the cloud and sensitive transaction data on the blockchain.

Our experiments reveal that the system introduces lower computation overhead compared to traditional centralized systems and other blockchain-based approaches. The lightweight cryptographic protocols used in our scheme allow faster encryption, decryption, and access control operations, making the solution suitable for real-time KYC processing. Moreover, the dynamic access policy update algorithm provides flexible and scalable access control, enabling authorized entities to access customer data securely and efficiently as needed while preserving privacy. Another important feature is the support for user-controlled data updates and consent revocation, which enhances user autonomy and aligns with privacy regulations such as GDPR. The ability to log all actions on the blockchain ensures traceability and auditability without compromising confidentiality, due to encryption of sensitive information stored on-chain. Overall, the proposed system achieves a well-balanced trade-off between security, efficiency, and compliance. It outperforms existing schemes by delivering faster response times, scalable key management, and enhanced privacy

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203008

features. These results confirm the viability and effectiveness of the blockchain-based e-KYC model in modern financial environments.

VII. CONCLUSION

We have presented the privacy-preserving e-KYC approach based on the blockchain. 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 blockchain 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. The experimental results showed that our scheme outperforms existing schemes in terms of performance, comprehensive KYC compliance features, and the scalable access control mechanism. For future works, we will test a larger sample of data in the real cloud environment and measure the throughput of the system in accommodating high number of e-KYC registration and verification requests. In addition, we will investigate the technique to enable batch verification of e-KYC transactions stored in the blockchain with the searchable encryption.

REFERENCES

[1] Y. Zhong, M. Zhou, J. Li, J. Chen, Y. Liu, Y. Zhao, and M. Hu, ''Distributed blockchain-based authentication and authorization protocol for smart grid,'' Wireless Commun. Mobile Comput., vol. 2021, pp. 1–15, Apr. 2021, doi: 10.1155/2021/5560621.

[2] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F. Ang, and R. Ismail, ''Blockchain technology the identity management and authentication service disruptor: A survey,'' Int. J. Adv. Sci. Eng. Inf. Tech., vol. 8, pp. 1735–1745, Sep. 2018.

[3] A. A. Mamun, A. Al Mamun, S. R. Hasan, S. R. Hasan, M. S. Bhuiyan, M. S. Bhuiyan, M. S. Kaiser, M. S. Kaiser, M. A. Yousuf, and M. A. Yousuf, ''Secure and transparent KYC for banking system using IPFS and blockchain technology,'' in Proc. IEEE Region Symp. (TENSYMP), Jun. 2020, pp. 348–351.

[4] M. Pic, G. Mahfoudi, and A. Trabelsi, ''Remote KYC: Attacks and counter measures,'' in Proc. Eur. Intell. Secur. Informat. Conf. (EISIC), Nov. 2019, pp. 126–129.

[5] W. Shbair, M. Steichen, and J. François, ''Blockchain orchestration and experimentation framework: A case study of KYC,'' in Proc. 1st IEEE/IFIP Int. Workshop Manag. Managed Blockchain (Man Block), Jeju Island, South Korea, Aug. 2018, pp. 23–25.

[6] Pareek, C. S. FROM PREDICTION TO TRUST: EXPLAINABLE AI TESTING IN LIFE INSURANCE.

[7] R. Norvill, M. Steichen, W. M. Shbair, and R. State, ''Demo: Blockchain for the simplification and automation of KYC result sharing,'' in Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC), May 2019, pp. 9–10, doi: 10.1109/BLOC.2019.8751480.

[8] T. Mikula and R. H. Jacobsen, ''Identity and access management with blockchain in electronic healthcare records,'' in Proc. 21st Euromicro Conf. Digit. Syst. Design (DSD), Prague, Czech Republic, Aug. 2018, pp. 699–706.

[9] S. Wang, R. Pei, and Y. Zhang, ''EIDM: A ethereum-based cloud user identity management protocol,'' IEEE Access, vol. 7, pp. 115281–115291, 2019, doi: 10.1109/ACCESS.2019.2933989.

[10] N. Ullah, K. A. Al-Dhlan, and W. M. Al-Rahmi, ''KYC optimization by blockchain based hyperledger fabric network,'' in Proc. 4th Int. Conf. Adv. Electron. Mater., Comput. Softw. Eng. (AEMCSE), Mar. 2021, pp. 1294–1299.

[11] N. Kapsoulis, A. Psychas, G. Palaiokrassas, A. Marinakis, A. Litke, and T. Varvarigou, ''Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture,'' Future Internet, vol. 12, no. 41, pp. 1–13, 2020.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com