International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 12 | Dec 2023 www.irjet.net p-ISSN: 2395-0072

Blockchain for Enhancing Trust and Privacy in Electronic Know Your Customer

Gannabathula Sri Prabhu Kiran[1], Kakileti Sai Prasanth[2], Pindi Srinivasarao[3], Lakkakula Tarak Sri Chandrahas[4], Shaik Sajid[5]

[1]CST, Sri Vasavi Engineering College(A), Pedatadepalli,Tadepalligudem-534101
[2]CST, Sri Vasavi Engineering College(A), Pedatadepalli,Tadepalligudem-534101
[3]CST, Sri Vasavi Engineering College(A), Pedatadepalli,Tadepalligudem-534101
[4]CST, Sri Vasavi Engineering College(A), Pedatadepalli,Tadepalligudem-534101
[5]CST, Sri Vasavi Engineering College(A), Pedatadepalli,Tadepalligudem-534101

Abstract - *This project presents e-KYC Trust Block, a blockchain-based electronic Know Your Customer (e-KYC) system that enhances trust, security, and privacy in identity verification. Traditional e-KYC systems rely on cloud storage and conventional encryption, leading to key management complexities and security vulnerabilities. To address these challenges, e-KYC Trust Block integrates Ciphertext Policy Attribute Based Encryption (CP-ABE) for fine-grained access control and Interplanetary File System (IPFS) for secure document storage. Additionally, it employs smart contracts to enforce client consent and ensure auditability. By combining symmetric and public-key encryption, the system minimizes communication overhead while maintaining data confidentiality. Experimental results validate its efficiency, scalability, and security, making it a robust solution for privacy-preserving e-KYC processes..*

***KeyWords*: Blockchain, Electronic Know Your Customer (e-KYC), Privacy Preservation, Ciphertext-Policy Attribute-Based Encryption (CP-ABE), Smart Contracts, Interplanetary File System (IPFS), Identity Verification, Decentralized Systems**

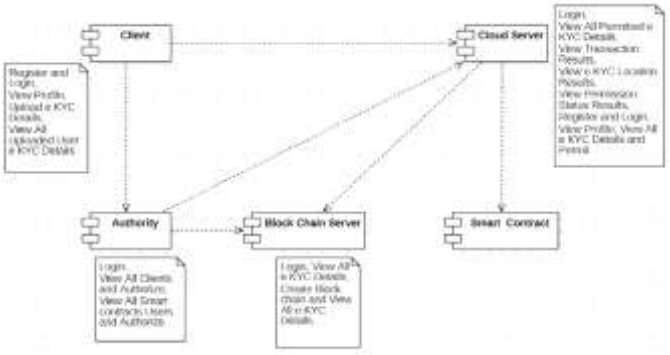
1. INTRODUCTION

In the era of digital transformation, identity verification has become a critical requirement for financial institutions, telecom providers, and various government agencies. The process of Know Your Customer (KYC) ensures that organizations verify the identity of their clients to prevent fraud, money laundering, and other illicit activities. With the advent of digitization, the traditional paper-based KYC processes have evolved into electronic KYC (e-KYC) systems, aiming to streamline verification and improve customer onboarding. However, these conventional e-KYC systems predominantly rely on centralized architectures and standard encryption models, which present major limitations in terms of data privacy, single points of failure, and complex key management.

One of the primary concerns in centralized e-KYC systems is the lack of trust and transparency. Sensitive identity data stored in centralized cloud servers is susceptible to unauthorized access, data breaches, and insider threats. Furthermore, ensuring user consent and controlling access to personal data becomes increasingly difficult in such frameworks. As a result, there is an urgent need for an e-KYC solution that is secure, transparent, privacy-preserving, and aligned with regulatory requirements such as data protection laws (e.g., GDPR, PDPB).

To address these challenges, this paper proposes **e-KYC TrustBlock**, a decentralized, blockchain-based framework designed to enhance the trust, privacy, and security of the e-KYC process. The system utilizes **Blockchain** to ensure immutability and transparency of transactions, **Ciphertext-Policy Attribute-Based Encryption (CP-ABE)** to provide fine-grained access control over encrypted data, and **InterPlanetary File System (IPFS)** for decentralized and tamper-proof storage of sensitive identity documents. Furthermore, **smart contracts** are employed to enforce digital consent, automate authorization policies, and ensure accountability in every data-sharing event.

The proposed system offers several advantages over existing e-KYC models. It reduces reliance on centralized storage, mitigates risks of unauthorized data access, and improves scalability through distributed technologies. By integrating both **symmetric and asymmetric encryption techniques**, the system achieves secure data handling with minimal communication overhead. The architecture is designed to support secure onboarding, consent-driven data sharing, audit trails, and regulatory compliance.



2.LITERATURE SURVEY

2.1Federated Learning for Privacy-Preserving KYC (2024)

This paper 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. The proposed method enhances privacy and security in KYC processes while reducing risks associated with centralized data storage.

2.2 Enhancing KYC with Behavioural Biometrics in Cloud Environments (2024)

This paper 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.

2.3 Enhancing Privacy in e-KYC Systems Using Zero-Knowledge Proofs (2023)

This study 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.

2.4 A Blockchain-Based Approach for Secure and Efficient Verification (2022)

This paper proposes a blockchain-based system for secure and efficient identity verification. It utilizes 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.

2.5 Blockchain Technology for Secure and Transparent e-Governance Systems (2021)

This research explores the potential of blockchain in e-governance 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.

2.6 A Privacy-Preserving e-KYC System (2020)

This paper presents a privacy-preserving e-KYC system that employs cryptographic techniques, including zero-knowledge proofs, to protect user data during identity verification.

3. EXISTING SYSTEM

Traditional e-KYC systems rely heavily on centralized cloud infrastructure and basic encryption techniques, leading to significant concerns about data privacy, key management, and lack of auditability. These systems often store sensitive customer information in centralized databases, making them attractive targets for cyberattacks. Additionally, user consent and access control mechanisms are typically not verifiable or enforceable in a transparent manner.

3.1 Centralized Architecture:

Current e-KYC implementations depend on centralized cloud storage, creating a single point of failure. This architecture is vulnerable to data breaches, unauthorized access, and internal misuse, compromising the confidentiality of user identity documents.

3.2 Weak Access Control:

Most traditional systems implement role-based or basic access control mechanisms, which lack the flexibility to enforce fine-grained policies. This limitation prevents effective control over who can access specific parts of the data, increasing the risk of data leaks.

3.3 Limited User Consent Management:

Existing solutions often do not offer robust mechanisms to record or verify user consent for data sharing. As a result, user privacy may be compromised, and financial institutions may not comply with privacy regulations effectively.

3.4 No Transparent Audit Trail:

Without blockchain or distributed ledger technology, there is no reliable or tamper-proof way to track data access and modifications. This absence of auditability

reduces trust in the system and complicates regulatory compliance.

4. PROPOSED WORK

The proposed system, e-KYC TrustBlock, introduces a blockchain-based architecture designed to enhance the trust, security, and privacy of electronic Know Your Customer (e-KYC) processes through decentralized technologies.

- The system integrates Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to provide fine-grained access control, enabling clients to control who accesses their KYC data.
- A smart contract framework is implemented to automate the verification, registration, and consent processes. It includes modular contracts for client registration, e-consent generation, and KYC verification.
- The system utilizes the InterPlanetary File System (IPFS) for decentralized and secure storage of encrypted e-KYC documents, ensuring availability and resistance to tampering.
- The system ensures auditability and data integrity by maintaining tamper-proof logs of all activities on a private blockchain ledger.
- A combination of symmetric and asymmetric encryption techniques is used to ensure data confidentiality while maintaining efficient communication.
- The solution is scalable, secure, and generalizable, making it adaptable to a wide range of identity verification use cases in banking and financial domains

5.BENEFITS OF THE PROPOSED SYSTEM

The proposed blockchain-based e-KYC system offers multiple advantages over traditional KYC mechanisms:

- **Enhanced Security:** By integrating CP-ABE and blockchain, the system ensures that only authorized parties can access sensitive user data, reducing the risk of data breaches and unauthorized access.
- **Improved Trust and Transparency**: Smart contracts enforce secure, verifiable, and transparent operations across all actors, enhancing the overall trust in the KYC process.
- **Decentralized Control:** Eliminating single-point control through blockchain ensures no single entity can manipulate or compromise the data.
- **Efficient Consent Management:** Digital e-consent mechanisms allow clients to have complete control over who accesses their data, fostering data privacy and user autonomy.
- **Tamper-Proof Records:** All transactions and credential storage are immutable and auditable, strengthening data integrity and accountability.

6.METHODOLOGY:

1. **RequirementAnalysis:**
   Identify and understand the requirements of a secure, privacy-compliant e-KYC system. Define the roles of Clients, Financial Institutions, the Central Authority, Blockchain Server, and Smart Contracts. Determine the need for secure data storage, consent-based sharing, and access control using cryptographic techniques like CP-ABE.
2. **SystemDesign:**
   Design the overall architecture involving user roles and their interaction with the system. Develop a modular architecture using IPFS for decentralized storage and blockchain for immutability. Define the workflow for user registration, data upload, authorization, and KYC verification through smart contracts. Design the interfaces using JSP and Java Servlets.
3. **Database and Blockchain Setup:**
   Use MySQL to store non-sensitive metadata such as user activity logs and access permission history. Blockchain is used to store encrypted hash values of KYC data, ensuring immutability and traceability. Implement CP-ABE to encrypt sensitive documents before uploading to IPFS.
4. **Implementation:**
   Develop the system using Java, JSP, and Servlets.
   Implement modules for each actor:

   4.1 Clients: Register, login, and upload encrypted e-KYC documents. Clients digitally sign consent forms allowing FIs to access their data.

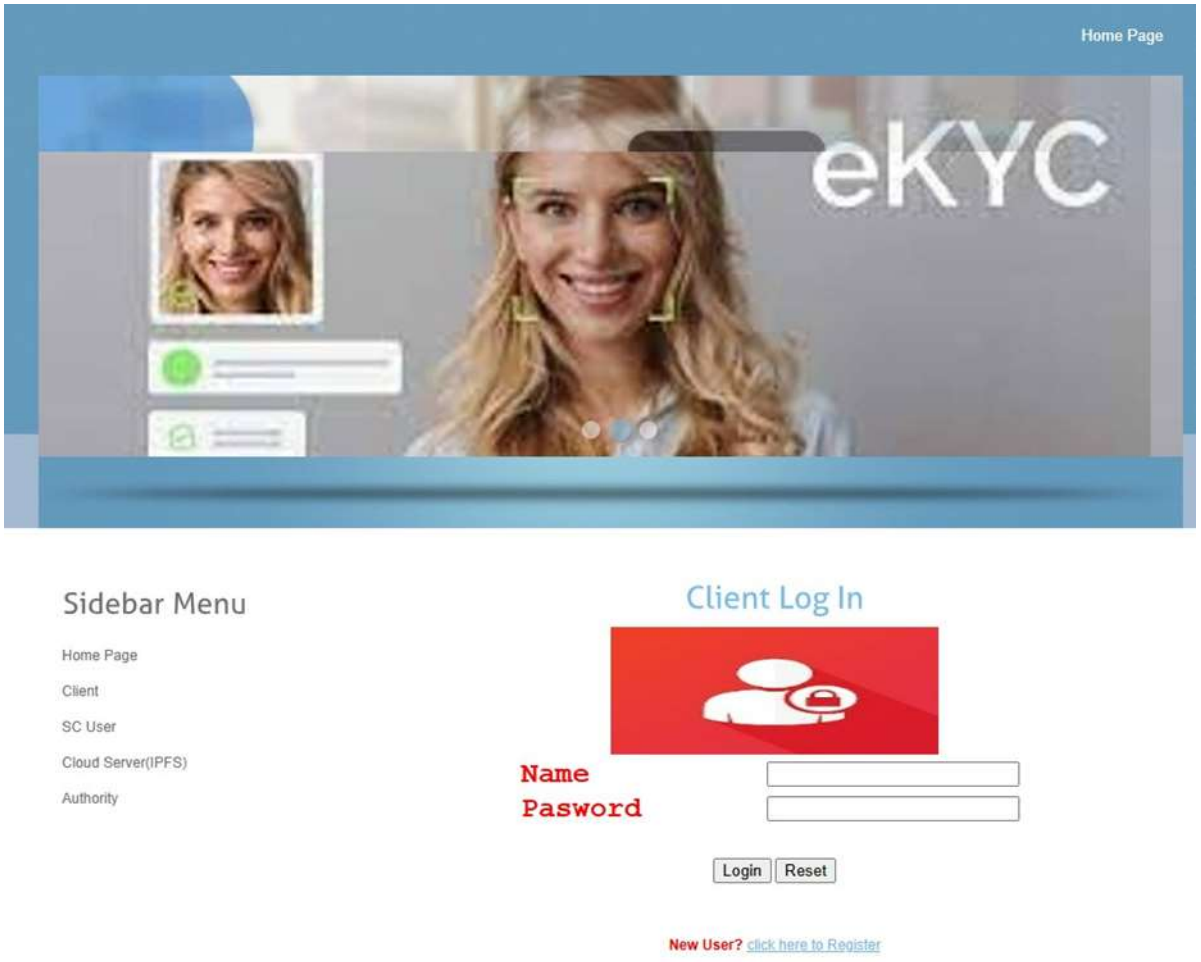
   4.2 Authority: Generates system keys, distributes secret keys using CP-ABE, and manages access control and user authorization.

   4.3 Smart Contracts: Automate the operations such as registration, consent verification, and data validation. Separate contracts handle registration, consent, and verification.

   4.4 Blockchain Server: Stores all KYC-related activities and hashes. Ensures data immutability and maintains transaction history.

   4.5 Cloud Server (IPFS): Stores encrypted documents and responds to queries by authorized users through hash lookups.

7.User Interface:



8.CONCLUSION:

This paper presents a secure and privacy-preserving e-KYC system leveraging blockchain and CP-ABE encryption. The proposed system enhances trust, security, and transparency by decentralizing the storage and verification of user credentials through smart contracts and encrypted cloud storage. It enables users to retain control over their data with a digital consent mechanism, while ensuring tamper-proof records and access control. The architecture demonstrates a scalable, efficient, and privacy-compliant solution to modernize KYC processes. Future enhancements can integrate zero-knowledge proofs and layer-2 scalability solutions for even greater performance and privacy.

9. REFERENCES:

[1] Y. Zhong *et al.*, "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 *et al.*, "Blockchain technology the identity management and authentication service disruptor: A survey," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, pp. 1735–1745, Sep. 2018.

[3] A. A. Mamun *et al.*, "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, "RemoteKYC: Attacks and countermeasures," 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] R. Norvill *et al.*, "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.

[7] 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.

[8] 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.

[9] 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.

[10] N. Kapsoulis *et al.*, "Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture," *Future Internet*, vol. 12, no. 41, pp. 1–13, 2020.

[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Secur. Privacy*, Oakland, CA, USA, May 2007, pp. 321–334.

[12] I. Gutierrez-Aguero *et al.*, "Burnable pseudo-identity: A non-binding anonymous identity method for ethereum," *IEEE Access*, vol. 9, pp. 108912–108923, 2021.

[13] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," [Online]. Available: https://bitcoin.org/bitcoin.pdf. Accessed: Jan. 8, 2022.

[14] J. P. Moyano and O. Ross, "KYC optimization using distributed ledger technology," *Bus. Inf. Syst. Eng.*, vol. 59, no. 6, pp. 411–423, Dec. 2017.

[15] A. Chowdhary, S. Agrawal, and B. Rudra, "Blockchain based framework for student identity and educational certificate verification," in *Proc. 2nd Int. Conf. Electron. Sustain. Commun. Syst. (ICESC)*, Aug. 2021, pp. 916–921.

[16] GDPR European Union Guidelines. [Online]. Available: https://gdprinfo.eu/. Accessed: Aug. 12, 2021.

[17] G. Bramm, M. Gall, and J. Schütte, "BDABE-blockchain-based distributed attribute based encryption," in *Proc. 15th Int. Conf. e-Bus. Telecommun.*, 2018, pp. 99–110.

[18] Y. Fan *et al.*, "TraceChain: A blockchain-based scheme to protect data confidentiality and traceability," *Softw., Pract. Exper.*, vol. 52, no. 1, pp. 115–129, Jan. 2022, doi: 10.1002/spe.2753.

[19] C. Yuan *et al.*, "Blockchain with accountable CP-ABE: How to effectively protect the electronic documents," in *Proc. IEEE 23rd Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2017, pp. 800–803.

[20] A. Wu *et al.*, "Efficient and privacy-preserving traceable attribute-based encryption in blockchain," *Ann. Telecommun.*, vol. 74, nos. 7–8, pp. 401–411, Aug. 2019.

[21] L. Guo, X. Yang, and W.-C. Yau, "TABE-DAC: Efficient traceable attribute-based encryption scheme with dynamic access control based on blockchain," *IEEE Access*, vol. 9, pp. 8479–8490, 2021, doi: 10.1109/ACCESS.2021.3049549.

[22] M. Barati *et al.*, "Privacy-aware cloud auditing for GDPR compliance verification in online healthcare," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 4808–4819, Jul. 2022, doi: 10.1109/TII.2021.3100152.