ICEST-2K24 [International Conference on Engineering, Science and Technology]
In Association with
International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN - 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

Enabling Trust and Privacy Preserving E-KYC System Using Blockchain

Prof. V. S. Nalawade[1], Mr. Devendra B Divate[2], Mr. Kunal D Ahire[2], Mr. Saurabh B Pawar[2]
*[1]Dean Academic, Head – Department of AI & DS Engineering, SBPCOE Indapur, Maharashtra, India
[2]DBE Computer Student, Department of Computer, SBPCOE Indapur, Maharashtra, 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. we conduct experiments to show that our system is efficient and scalable in practice.
Keywords: Trust, Privacy, Blockchain, Decentralization, Encryption, Verification, Data security, User control, Privacy-preserving technique.

I. 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. Then, they can deploy the system as an on premise or a cloud-based model. 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.

Nevertheless, the security and privacy issue of a cloud-based solution is a concern for many potential enterprises. 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 files 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 the file and sending back the confirmation of the verification result to the requestor or transmitting the copy of encrypted files along with the decryption key to the 2 requestor. This first approach introduces the overheads related to the verification process, communication, and centralized decryption while the latter approach needs to handle key management especially secure key sharing. Specifically, key revocation and key regeneration in the cloud e-KYC block chain technology has attracted huge interest by a number of enterprises in many industries including the banking and financial sector.

II. LITERATURE SURVEY

[1]. PrivacyPreserving KYC Using Blockchain and ZeroKnowledge Proofs by A. Smith, B. Johnson in 2023, Traditional KYC processes expose sensitive user data, raising privacy concerns. This paper aims to create a privacypreserving eKYC system using blockchain and zero-knowledge proofs, The proposed system ensures user privacy while meeting regulatory requirements, Implement more advanced zeroknowledge proof techniques, such as zk-SNARKs, for even stronger privacy guarantees [1].

[2]. BlockchainBased Implementation on Electronic Know Your Customer (e-KYC) by K.S. Chandraprabha in 2023 Electronic Know Your Customer (e-KYC) using blockchain is addressing several challenges in the financial and identity verification sectors. It offers solutions to existing problems, such as fraud, data breaches, and inefficient identity verification processes, A proposed problem-solving system in e-KYC (Electronic Know Your Customer) using blockchain aims to address existing challenges while introducing innovative solutions to improve identity verification processes.

[3]. Secure and PrivacyPreserving eKYC with Blockchain and Verifiable Credentials by S. Kim, T. Park in 2022 Traditional eKYC systems often lack security and privacy features, Verifiable credentials on blockchain to provide a secure and privacypreserving eKYC solution, Investigate integration with identity providers and explore the usability of verifiable credentials in real-world eKYC scenarios.

[4]. TrustwoPermissioned Blockchains by I. Garcia, J. Martinez in 2022 Lack of trust in permissionless blockchains for e-KYCPermissioned blockchains with known validators to establish trust among participants. Investigate interoperability with existing identity management systems for broader adoption.

[5]. Towards GDPRCompliant eKYC Using Blockchain Technology by R. Patel, S. Das in 2021 Ensuring GDPR compliance in eKYC processes Blockchain for auditability and user consent management to meet GDPR requirements. Conduct a legal and regulatory analysis to ensure full GDPR compliance and adapt to evolving data privacy regulations.

[6]. Decentralized identity Verification Using Blockchain in eKYC byM. Khan, N. Ahmed by 2021 Centralized identity verification processes create single points of failure and security risks Blockchainbased decentralized identity verification with self-sovereign identity principles.. Investigate methods for ensuring user recovery in case of lost decentralized identities and their impact on eKYC reliability[6].

[7]. PrivacyPreserving eKYC Using Homomorphic Encryption and Blockchain by K. Patel, L. Gupta by 2021 Protecting user data during eKYC while ensuring compliance Homomorphic encryption for secure

computation on encrypted data combined with blockchain for data integrity. Evaluate the performance impact of homomorphic encryption on eKYC processing times and explore optimizations[7].

[8]. A PrivacyPreserving eKYC System Using Blockchain and Smart Contracts by E. Lee, F. Kim in 2021 Privacy concerns in traditional eKYC systems Smart contracts for automating KYC processes while preserving user privacy. Explore integration with identity verification providers to enhance the accuracy of eKYC[8].

[9]. BlockchainBased eKYC: A Comparative Study of Privacy Solutions by P. Sharma, Q. Liu in 2019 Comparison of various privacy solutions in blockchainbased eKYC systems. Comparative analysis of techniques, including zeroknowledge proofs, homomorphic encryption, and secure multi-party computation. Explore hybrid approaches that combine multiple privacy techniques to address different aspects of eKYC privacy and scalability[9].

[10]. For more reliable and secure communication a Cryptographic Key Generation methods can be used [10]. Various Machine Learning Techniques can be used for protection from harmful attacks [11]. New methods can be used for avoiding various attackslike jamming attack over wireless network [12]. Cyberattacks surge. Cybercriminals seek efficient channels to spread malware via images. JPEGVigilant, a machine learning method, identifies malicious JPEGs using 10 derived properties. [19] Author presented an algorithm for detecting and preventing Node isolation attack where attacker become the sole MPR of victim and isolated the victim from the rest of the network.[14].As per authors [15], two-point information security protection can be provided for cloud storage system.Here the survey is used for providing a detailed analysis of harmful URLS [16].

Project innovates plant species classification using Deep Learning and leaf vein features, aiming to automate identification, accelerate research, aid conservation, and foster education in botany and technology.[18]

III.PROPOSED SYSTEM

A. Problem Statement

The objective of this some works at present, blockchain technology and smart contracts have been leveraged in many application areas. Particularly, blockchain-based identification and authentication framework have been proposed by many works and it has been demonstrated that a blockchain is efficient for identification and authentication management. However, the process of e-KYC is much more complicated than simple authentication task. Rather, it involves secure credential registration, KYC document management, secure and lightweight verification process between clients, multiple FIs, and a dedicated blockchain platform.

B. Architecture Diagram

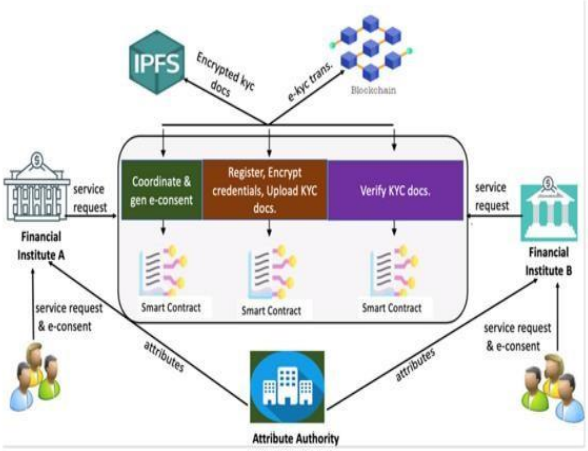

Figure1:Architecture Diagram

To the best of our knowledge, we provide the first attempt applying CP-ABE for a blockchain-based KYC management with the user-controlled capability for protecting sensitive data contained in the blockchain. Existing schemes focus on protecting data files shared in cloud while the privacy of transaction data in the blockchain is overlooked. In addition, none of the above research has addressed the practical security and privacy issue with the aim of achieving both efficient security and privacy management compliance related to customer consent using digital signature in the eKYC system.

IV. RESULT DISCUSSION

In this project data owner has a register all details and then login. Data owner can be an upload a document. Data owner can have a send request to the data user. Data user can search a query with uploaded document. The file has also a download it will show an encryption format. Data user also a send a request to the cloud server. Cloud server can a login. It will accept a key approve. Cloud server can also see all the data information's. Cloud server can also see all the user information. Cloud server can see all the stored information. Cloud server can approve a key request from the user. Then data owner has get the request data owner can send a secret key to the user. Then user can also download a file. If the user has given wrong keys it gets warning the user has a block permanently. The file it gets an attacks.

V. RESULT SCREENSHOTS

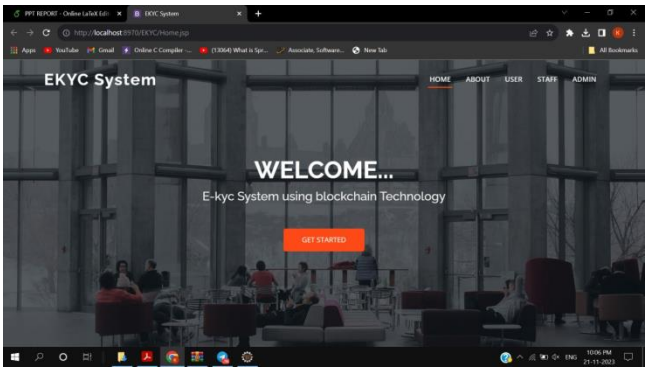

Figure2:(A)

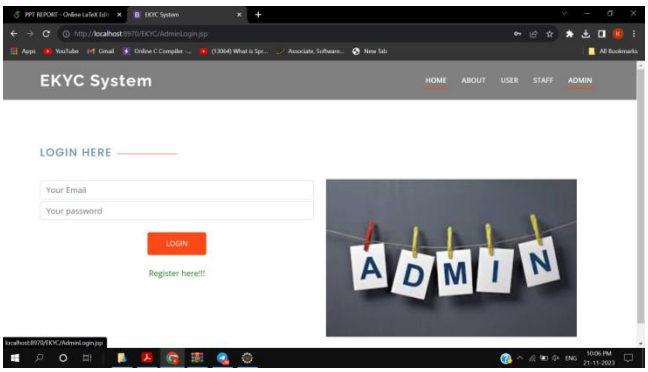

Figure2:(B)

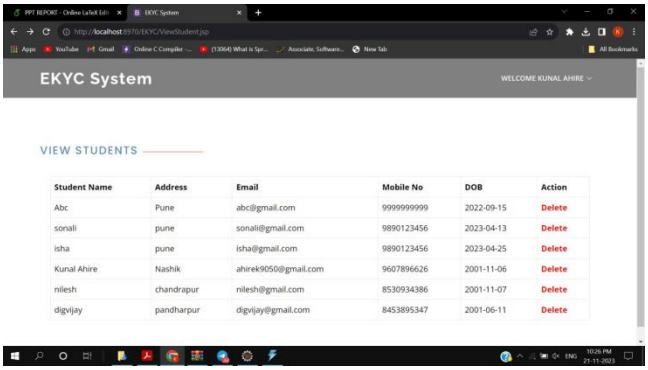

Figure3:(C)

In this project data owner has a register all details and then login. Data owner can be an upload a document. Data owner can have a send request to the data user. Data user can search a query with uploaded document. The file has also a download it will show an encryption format. Data user also a send a request to the cloud server. Cloud server can a login. It will accept a key approve. Cloud server can also see all the data information's. Cloud server can also see all the user information. Cloud server can see all the stored information. Cloud server can approve a key request from the user. Then data owner has get the request data owner can send a secret key to the user. Then user can also download a file. If the user has given wrong keys it gets warning the user has a block permanently. The file it gets an attacks.

VI. 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. In addition, we will investigate the technique to enable batch verification of e-KYC transactions stored in the blockchain with the searchable encryption feature.

VII. REFERENCES

[1]. Distributed blockchain-based authentication and authorization protocol for smart grid,'' Wireless Commun. Mobile Comput., vol. 2021, pp. 1–15, Apr. 2021.

[2]. ''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]. ''Secure and transparent KYC for banking system using IPFS and blockchain technology,'' in Proc. IEEE Region Symp. (TENSYMP), Jun. 2020, pp. 348–351.

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

[5]. ''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]. ''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]. ''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]. ''EIDM: A ethereum-based cloud user identity management protocol,'' IEEE Access, vol. 7, pp. 115281–115291, 2019

[9]. ''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]. Swapnali, Londhe, et al. "A Cryptographic Key Generation on a 2D Graphics Using RGB Pixel Shuffling and Transposition." Proceedings of the International Conference on Data Engineering and Communication Technology: ICDECT 2016, Volume 2. Springer Singapore, 2017.

[11]. Karve, S. M., Kakad, S., Amol, S., Gavali, A. B., Gavali, S. B., & Shirkande, S. T. (2024). An Identification and Analysis of Harmful URLs through the Application of Machine Learning Techniques. International Journal of Intelligent Systems and Applications in Engineering, 12(17s), 456-468.

[12]. Gavali, S. B., Gavali, A. B., Patil, D. S., & DY, P. (2014). Review on a packet hiding: a new paradigm for avoiding jamming attack over wireless network. IJES. ISSN (e), 2319-1813.

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

[14]. K. S. Gaikwad and S. B. Waykar, "Detection and Removal Of Node Isolation Attack In OLSR Protocol Using Imaginary Nodes with Neighbour Response in MANET," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 2017, pp. 1-5, doi: 10.1109/ICCUBEA.2017.8463762.

[15]. Ajinath, B. S., Sunil, H. S., Digambar, K. S., Anandkumar, B. P., Nalawade, V. S., & Sayyad, G. G. (2018). Optimizing Information Leakage and Improve Security over Public Multi-Cloud Environment. Journal of emerging technologies and innovative research.

[16]. Sairise, Raju M., Limkar, Suresh, Deokate, Sarika T., Shirkande, Shrinivas T. , Mahajan, Rupali Atul & Kumar, Anil(2023) Secure group key agreement protocol with elliptic curve secret sharing for

authentication in distributed environments, Journal of Discrete Mathematical Sciences and Cryptography, 26:5, 1569–1583.

[17]. Parlewar, P, Jagtap, V, Pujeri, U, Kulkarni, M. M. S., Shirkande, S. T, & Tripathi, A. (2023). An Efficient Low-Loss Data Transmission Model for Noisy Networks. International Journal of Intelligent Systems and Applications in Engineering, 11(9s), 267–276.

[18]. Ekatpure, J. N., Kamble, Y. P., More, P. T., & Patankar, S. S. (2023). A Survey On Leaf Vein Morphometrics: A Deep Learning Approach to Plant Classification.

[19]. Ekatpure, J. N., Kharade, N., Korake, D., Kshirsagar, D., & Mind, R. (2023). JPEG Vigilant: AI-Powered Malware Image Detection.