International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at :www.ijsrcseit.com

doi : https://doi.org/10.32628/IJSRCSEIT

Enabling Trust and Privacy Preserving E-KYC System Using Blockchain

Prof. Nalawade V. S., Ahire Kunal, Divate Devendra, Pawar Saurabh

Department of Computer Engineering, S. B. Patil College of Engineering, Indapur, Pune, Maharashtra, India

ARTICLEINFO

Article History:

Accepted: 10 Oct 2023

Published: 30 Oct 2023

Publication Issue

Volume 9, Issue 13

September-October-2023

Page Number

01-09

ABSTRACT

Banks and identity providers use the electronic Know Your client (e-KYC) system to set up client identity verification procedures with reliant parties. Because cloud-based e-KYC systems are more accessible and efficient with resources, many banks choose them. But e-KYC data security in the cloud is a serious issue. Strong authentication and conventional encryption are generally used in existing e-KYC platforms, which results in encryption dependencies and administration overheads when files are uploaded to the cloud. In this work, we introduce the "e-KYC Trust Block," a revolutionary blockchain-based e-KYC solution that improves trust, security, and privacy compliance through the use of ciphertext policy attribute-based encryption (CP-ABE) and client consent enforcement. Furthermore, we present attribute-based encryption to support privacy protection and granular access control for delicate transactions recorded in the blockchain.

KEYWORDS: E-KYC, Authentication, CP-ABE, Identity Verification, Authorization System, blockchain,.

I. INTRODUCTION

By electronically authenticating and validating customer identities, the Electronic Know Your Customer (e-KYC) service helps banks and other financial institutions (FIs) improve the effectiveness and consumer satisfaction of virtual banking activities. Using this technology, FIs can electronically confirm the clients' identity, whether they be private individuals or businesses. FIs can choose to use pre-built e-KYC software that includes all necessary elements or design a customised solution in order to implement the e-KYC system. There are on-premises and cloud-based deployment options.

The majority of businesses now prefer cloud-based platforms to host their e-KYC systems and data as a result of the expanding outsourcing trend. In comparison to host-based authentication, which depends on centralised validation and can result in traffic jams and single points of failure, a cloud-based e-KYC system offers a more effective and adaptable authentication technique. Although customer data documents are stored in the cloud and may be available to other cloud tenants or even the cloud service providers (CSPs), the drawback of a

cloud-based solution is the possible security and privacy problems.For more reliable and secure communication a Cryptographic Key Generationmethods can be used [1]. As per authors[2], two-point information security protection can be provided for cloud storage system [3].

II. LITERATURE SURVEY

Sr. no	Paper title	Author name	Year of Publication	Problem solved in this paper: Existing Problem Statement	The technique used to solve the problem: Existing Problem Solution	What will be future work: Future Scope
1.	Enabling Trustand Privacypreserving e-KYC [5]	Mr. Y. Rajasekhar, K. Chandra Sekhar,G. Ranil, L.V.N. Maneesh, K.Venu	2023	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.	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.	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 feature.
2.	Enabling Trust and Privacy Preservin g e-KYC System Using Blockchai	Viraj Ashok Patil, Akshay Kumar Mishra, Ketan Kishor	2023	A Blockchain based totally protection management device is for offering security to the bank transactions and to implement the KYC manner in an easier	A secure and efficient blockchain-based e-KYC documents registration and verification process with	We have presented the privacy-preserving e-KYC approach based on the block chain In our scheme, the privacy of both

	n[6]	Shinde, Prof A. A. Patil		and secured manner. Blockchain technology is a brand-new technology which is based totally on mathematical, cryptographic and monetary concepts for preserving a database among diverse contributors without the need of any 0.33 party or central authority.	lightweight key cryptographic protocols run in the cloud Interplanetary File System (IPFS). To facilitate the foundational privacy requirement regarding the user's consent collection, we develop a smart contract to generate and enforce the consent to be digitally signed by the customer.	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.
3.	E-KYC System using Blockchain Technology: A Review [7]	Manas Patil, Sakshi Patil, Aaditya Patil, Amir Ahmad, Prof.D.B. Mane	2023	A Blockchain-based security management system is used to secure bank transactions and to make the KYC process more simple and secure. Blockchain technology is a novel technology that uses mathematical, cryptographic, and economic concepts to maintain a database amongst multiple participants without the need for a third party or central authority.	Banks' Know Your Customer (KYC) processes on its consumers are unneeded, inefficient, and costly. As a result, a system is proposed to automate unskilled operations and allow for the sharing of KYC data. Blockchain technology, with its distributed database idea and time-stamped ledgers, can significantly assist banks in improving their KYC procedure.	Today's Blockchain is similar to the Internet in its early 20s in many aspects. Every day, the advancement of information technology and internet commerce has a greater and greater impact on all aspects of contemporary life. Blockchain technology aims to challenge the conventional understanding of how users communicate with one another

						online.
4.	E-KYC using Blockchain Technology [8]	1angurde Priyanka Sahebrao, 2Kasture Nikita Rajendra, 3Shaikh Saniya Asif, 4Nemade Gunjali Anil, 5V.A. Khairnar	2023	The current KYC process consists of an exchange of documents between the customer and the financial institution that intend to work together. The process includes the collection of basic identity information from all beneficiaries to check for illicit activity and politically exposed persons. The process also includes risk management with regard to on boarding newcustomers, the monitoring of transactions, and specific customer policies for banks.	The presented system introduces effectiveness and time efficiency of operations through its schema simplicity and smart integration of the different technology modules and components. Once the user has logged in, s/he will be asked to fill out the KYC form. This form requires the user to fill His/her name, phone both of which are already filled in by the user and will be retrieved from the database.	The scope of popular KYC methods like eKYC is limited to India, as these methods base their verification process on the Indian Govt. authorized Aadhar Card. Our solution, however, can be applied globally without any restrictions. If a customer wants to apply to any other banks, all s/he needs to do is select it from the list of banks provided in the mobile application. Thus, the entire KYC process can be limited to just one tap, giving the ultimate convenience to customers.
5.	Enabling Trust and Privacy-Preserving e-KYC System Using Blockchain [9]	SOMCHART FUGKEAW , (Member, IEEE)	2022	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	In this model, the KYC system owner encrypts the file with their host's key and uploads it to the cloud. In this paper, we introduce a novel blockchain-based e-KYC scheme called e-	We have presented the privacy-preserving e-KYC approach based on the blockchain. Our proposed scheme delivers secure and decentralized authentication and

				efficient resource consumption and the high degree of accessibility and availability of cloud computing, most banks implement their e-KYC system on the cloud.	KYC TrustBlock based on the ciphertext policy attribute-based encryption (CP-ABE) method binding with the client consent enforcement to deliver trust, security and privacy compliance.	verification of the e-KYC process with the user's consent enforcement feature.
6.	Secured and Privacy preserving e-KYC system Using Blockchain [10]	Viraj Ashok Patil, Akshay Kumar Mishra, Ketan Kishor Shinde, Prof. A.A. Patil	2022	Know Your client (KYC) strategies performed through banks on their clients are needless, unmanageable and highly-priced. therefore, a gadget is proposed to automate unskilled obligations and allow sharing of facts related to KYC. Blockchain technology, with its concept of dispensed database, time-stamped ledgers, can correctly assist banks enhance their KYC technique.	A Blockchain-based totally protection management device is for offering security to the bank transactions and to implement the KYC manner in a easier and secured manner. Blockchain technology is a brand new technology which is based totally on mathematical, cryptographic and monetary concepts for preserving a database among diverse contributors without the need of any 0.33 party or central authority.	In many approaches, Blockchain these days is similar to in which the net was in early 20s. Thedevelopment of facts generation and digital business each day has an increasing number of tremendous impacts on all spheres of the modernexistence.
7.	Privacy-Preserving KYC-Compliant Identity Scheme	Nigang Sun 1 , Yuanyi Zhang 1,2,* and Yining	2022	research proposes a KYC-compliant identity system. It solves the privacy issue of existing solutions and	The scheme includes four entities: users, the KYCprovider,VASPs , and supervisors. In the scheme, there is	This article proposes a KYC compliant identity scheme for Ethereum-based blockchain

	forAccounts on All Public Blockchains [11]	Liu 3		therefore does not affect the anonymity of theblockchain. The solution supports all public blockchains and only needs to be deployed on an EVM-compatible blockchain. It addresses the limitations of existing solutions that require extra work to support new blockchains.	only one KYC provider but there may be multiplesupervisors. TheKYC provider is a government department that manages users' identities. The supervisors are government departments different from the KYC provider, such as inspection agencies responsible for crime investigation. VASPs include exchanges, OTC (over-the-counter)platforms, etc.	wallet accounts using Merkle trees and smart contracts. First, in order to solve the above privacy issues, the scheme divides the IdP of the three-party model into supervisors and KYC providers and uses a four-party model consisting of supervisors, KYC providers, users, and VASPs. The supervisor is responsible for identitytracking, and the KYC provider is responsible for checking the user's identity.
8.	Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity [12]	Vincent Schlatt, Johannes Sedlmeir, Simon Feulner, Nils Urbach	2021	KYC processes place a great burden on banks, because they are costly,inefficient, and inconvenient for customers. While blockchain technology is often mentioned as apotential solution, it is not clear how to use the technology's advantages without violating dataprotection regulations and	To comprehensively address the challenges of the KYC process (as identified in Section 2),stage 2 in our DSR process involved the derivation of objectives to be met by a useful SSI-basedeKYC framework. We derived these objectives from the literature on the	To improve on the current shortcomings in theKYC process through an end-to-end digital process that leverages blockchain-based SSI. Research on SSI is still in its infancy, and little has been published on the design of applications for SSI.

				customer privacy.	KYC process, KYC-related regulatory requirements, and three formative interviews with experts.	

III.LIMITATIONS OF EXISTING WORK

Using blockchain technology to enable trustworthy and privacy-preserving e-KYC systems has several drawbacks.

1. **Scalability:** When it comes to processing a huge volume of transactions fast, blockchain networks, especially open ones like Ethereum, may experience scalability challenges. This scalability issue may compromise the effectiveness of the system because e-KYC operations necessitate many verifications.
2. **Performance Overhead:** Compared to conventional centralised systems, blockchain transactions require a consensus mechanism, which might result in performance overhead. The speed of e-KYC processes can be impacted by how long it takes to validate transactions.
3. **Privacy Issues:** Although blockchain offers data immutability, it also makes all transaction data on the ledger publicly accessible. Even using encryption approaches like CP-ABE (Ciphertext-Policy), it can be difficult to guarantee the privacy of sensitive customer data and transactions.
4. **Regulatory Compliance:**E-KYC procedures frequently must adhere to stringent legal standards, which can differ by jurisdiction. The use of blockchain technology can make it challenging and possibly much more difficult to comply with these rules.
5. **Key Administration:** Data confidentiality must be managed with security while managing encryption keys. Key management issues may arise with blockchain systems, particularly in ensuring that only authorised parties have access to the required decryption keys.
6. **Interoperability:**Different blockchain platforms or versions may be used by diverse institutions and systems. It can be challenging to achieve interoperability between various systems, which could cause the e-KYC ecosystem to become fragmented.

IV.CONCLUSION

We have outlined the blockchain-based, privacy-preserving e-KYC solution. Our suggested solution provides user consent enforcement together with secure, decentralised authentication and verification of the e-KYC procedure. In our system, the sensitive transaction data kept in the blockchain is protected using symmetric key encryption and CP-ABE, while the privacy of both customers' identification documents saved in the cloud is guaranteed by public key and symmetric key encryption. The data owner or the customer may also amend the KYC data using our system.We also developed an algorithm for updating access policies to support dynamic access authorization. Regarding computation cost, communication cost, and performance, we conducted comparison analysis between our scheme and similar works for the evaluation. According to the experimental data, our method performs better than other current schemes.

V. REFERENCES

[1]. 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.

[2]. 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.

[3]. 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.

[4]. Mr. Y. Rajasekhar, K.ChandraSekhar,G.Ranil, L.V.N. Maneesh, K.Venu 2023Enabling Trust and Privacy preserving e-KYChttps://www.indusedu.org/pdfs/IJREISS/IJREISS_4120_14404.pdf

[5]. Viraj Ashok Patil, Akshay Kumar Mishra, KetanKishorShinde, Prof A. A. Patil 2023Enabling Trust and Privacy Preserving e-KYC System Using Blockchain https://ijsrem.com/download/enabling-trust-and-privacy-preserving-e-kyc-system-using-blockchain-2/

[6]. Manas Patil, Sakshi Patil, Aaditya Patil, Amir Ahmad, Prof.D.B.Mane 2023E-KYC System using Blockchain Technology: A Review https://ijcrt.org/papers/IJCRT2304818.pdf

[7]. Sairise, Raju M., Limkar, Suresh, Deokate, Sarika T., Shirkande, Shrinivas T. , Mahajan, RupaliAtul& 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, DOI: 10.47974/JDMSC-1825

[8]. E-KYC using Blockchain Technology 2023GangurdePriyankaSahebrao, Kasture Nikita Rajendra, Shaikh Saniya Asif, NemadeGunjali Anil, 5V.A. Khairnar https://www.ijirmps.org/papers/2023/3/230138.pdf

[9]. SOMCHART FUGKEAW , (Member, IEEE) 2022Enabling Trust and Privacy-Preserving e-KYC System Using Block chain https://ieeexplore.ieee.org/iel7/6287639/9668973/09770032.pdf

[10]. Viraj Ashok Patil, Akshay Kumar Mishra, KetanKishorShinde,Prof. A.A. Patil 2022

[11]. Secured and Privacy preserving e-KYC system using Blockchain https://www.irjmets.com/uploadedfiles/paper//issue_2_february_2023/33872/final/fin_irjmets1677561174.pdf

[12]. Gaikwad, Yogesh J. "A Review on Self Learning based Methods for Real World Single Image Super Resolution." (2021).

[13]. V. Khetani, Y. Gandhi and R. R. Patil, "A Study on Different Sign Language Recognition Techniques," 2021 International Conference on Computing, Communication and Green Engineering (CCGE), Pune, India, 2021, pp. 1-4, doi: 10.1109/CCGE50943.2021.9776399.

[14]. Vaddadi, S., Arnepalli, P. R., Thatikonda, R., &Padthe, A. (2022). Effective malware detection approach based on deep learning in Cyber-Physical Systems. International Journal of Computer Science and Information Technology, 14(6), 01-12.

[15]. Thatikonda, R., Vaddadi, S.A., Arnepalli, P.R.R. et al. Securing biomedical databases based on fuzzy method through blockchain technology. Soft Comput (2023). https://doi.org/10.1007/s00500-023-08355-x

[16]. Rashmi, R. Patil, et al. "Rdpc: Secure cloud storage with deduplication technique." 2020 fourth international conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC). IEEE, 2020.

[17]. Khetani, V., Gandhi, Y., Bhattacharya, S., Ajani, S. N., &Limkar, S. (2023). Cross-Domain Analysis of ML and DL: Evaluating their Impact in Diverse Domains. International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 253-262.

[18]. Khetani, V., Nicholas, J., Bongirwar, A., &Yeole, A. (2014). Securing web accounts using graphical password authentication through watermarking. International Journal of Computer Trends and Technology, 9(6), 269-274.

[19]. Nigang Sun, Yuanyi Zhang and Yining Liu 2022Privacy-Preserving KYC-Compliant Identity Scheme for Accounts on All Public Blockchains https://mdpi-res.com/d_attachment/sustainability/sustainability-14-14584/article_deploy/sustainability-14-14584-v2.pdf?version=1667898781

[20]. Kale, R., Shirkande, S. T., Pawar, R., Chitre, A., Deokate, S. T., Rajput, S. D., & Kumar, J. R. R. (2023). CR System with Efficient Spectrum Sensing and Optimized Handoff Latency to Get Best Quality of Service. International Journal of Intelligent Systems and Applications in Engineering, 11(10s), 829-839.

[21]. Nagtilak, S., Rai, S., & Kale, R. (2020). Internet of things: A survey on distributed attack detection using deep learning approach. In Proceeding of International Conference on Computational Science and Applications: ICCSA 2019 (pp. 157-165). Springer Singapore.

[22]. Mane, Deepak, and AniketHirve. "Study of various approaches in machine translation for Sanskrit language." International Journal of Advancements in Research & Technology 2.4 (2013): 383.

[23]. Shivadekar, S., Kataria, B., Limkar, S. et al. Design of an efficient multimodal engine for preemption and post-treatment recommendations for skin diseases via a deep learning-based hybrid bioinspired process. Soft Comput (2023). https://doi.org/10.1007/s00500-023-08709-5

[24]. Shivadekar, Samit, et al. "Deep Learning Based Image Classification of Lungs Radiography for Detecting COVID-19 using a Deep CNN and ResNet 50." International Journal of Intelligent Systems and Applications in Engineering 11.1s (2023): 241-250.

[25]. Vincent Schlatt, Johannes Sedlmeir, Simon Feulner, Nils Urbach 2021Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity https://arxiv.org/pdf/2112.01237