ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 01 January 2024

d-KYC SecureChain: Transforming KYC System with Blockchain for Enhanced Customer Authentication

[1] Chitra Jain, [2] Ansul, [3] Puja Das*, [4] Moutushi Singh, [5] Kamal kant

[1] [2] [3] [5] Department of CSE College of Smart Computing COER University Roorkee
[4] Information Technology, Institute of Engineering and Management Salt Lake, Kolkata
Corresponding Author Email: [1] chitra.cj69@gmail.com, [2] ansulpundir2468@gmail.com, [3] pujadas.wbut@gmail.com, [4] moutushi.singh@iemcal.com, [5] dr.kamalverma83@gmail.com

Abstract*— The research design adopts a comprehensive approach, focusing on the seamless integration of blockchain technology and cloud computing to optimize KYC procedures. The methodology encompasses the implementation of advanced encryption algorithms within the cloud infrastructure to fortify data security. This ensures that sensitive customer information remains confidential during storage and transmission, safeguarding against potential security threats. Smart contracts streamline the KYC procedure, reducing manual efforts and increasing efficiency. One pivotal aspect of the research involves leveraging blockchain technology to enhance the reliability of KYC procedures. By employing the decentralized and immutable nature of the blockchain, the study aims to establish a trustworthy and tamper-proof record of identity verification activities. The study indicates that the integration of blockchain and cloud computing in KYC processes can significantly improve data security by implementing encryption algorithms. This also contributes to the integrity of KYC data but also addresses concerns related to data manipulation and unauthorized access. The cloud's scalable infrastructure and blockchain's automation streamline procedures, reducing time consumption and enhancing user-friendliness for a more efficient KYC experience. The anticipated outcomes of this research include a robust framework that combines the security benefits of cloud computing with the reliability and efficiency afforded by blockchain technology. The findings hold implications for industries reliant on stringent identity verification processes, such as finance and healthcare. By contributing to the evolving landscape of secure digital interactions, this research seeks to foster advancements in KYC methodologies and establish a foundation for future developments in the broader context of identity management.

***Index Terms*— Blockchain Technology, Cloud Computing, Smart Contracts, Data Security, KYC.**

I. INTRODUCTION

The digital know-your-customer (d-KYC) process is a regulatory and procedural framework designed to verify the identity of customers or customers, ensuring they are who they claim to be. This process is primarily utilized by banks and other financial institutions to mitigate risks associated with financial crimes, including money laundering, terrorist financing, and fraud, by establishing the identity and legitimacy of individuals or entities. To digitally verify customers, banking institutions have the option of using pre-configured d-KYC (PCd-KYC) software with necessary features or creating a customized solution. They can then implement the system either within their own infrastructure or choose a web-hosted model. With the current trend of externalizing, an increasing number of enterprises are favouring the cloud as their preferred environment for hosting systems and data due to its efficiency and reliability.

In the server-centric d-KYC authentication process, documents must be validated via a centralized server. This setup introduces challenges such as congestion points and a singular point of vulnerability. Moreover, the ability to trace verified transactions is constrained, as the provider exclusively oversees all transactions within the system. In contrast, web-hosted models are essential for ensuring an advanced authentication framework. Beyond enhancing transparency, this approach serves to mitigate potential congestion points and vulnerabilities associated with centralized control. Consequently, it establishes a more resilient and secure system, aligning with the evolving demands of modern authentication processes. However, with web-hosted models, concerns about privacy and security arise due to the d-KYC system residing in the cloud, storing customer data and documents that could be accessed by external cloud users or service providers managing the cloud infrastructure[1]. To tackle this concern, the majority of banks and financial institutions must incorporate an encryption mechanism alongside the robust authentication features offered by service providers. In this regard, banking institutions with a digital Know Your Customer (d-KYC) system should encrypt the corresponding data files prior to uploading them to the cloud. When verification is sought by relying parties, the hosting entity has the option to either conduct the verification by decrypting the file and transmitting the confirmation of the verification result to the requester or by sending the encrypted files along with the decryption key.

The current landscape of cloud d-KYC environments lacks a comprehensive exploration of key revocation and regeneration in existing research. When customers withdraw consent from banks or financial institutions, these entities are

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 01 January 2024

obligated to expunge the customer's identity data completely, necessitating the revocation of decryption keys. Any institutions sharing a revoked key must regenerate it to ensure that unauthorized entities cannot access customer data stored in the cloud. Furthermore, conventional cloud d-KYC platforms fail to provide shared information for traceability in transactions[2]. Blockchain technology, gaining considerable attention across various industries, including banking and finance, emerges as a solution. Integrating blockchain into d-KYC platforms fosters decentralization, transparency, trustworthiness, and cost-effectiveness. The utilization of smart contracts in the blockchain system facilitates automated execution of system logic, enhancing usability and programmability in a multi-user, multi-provider environment. This advancement reflects a paradigm shift, particularly in the banking and financial sector, with potential implications for transaction processing and management.

SL.No.	Abbreviation	Elaboration
1.	d-KYC	Digital Know-Your-Customer
2.	SFSS	Stellar File Storage System
3.	JTKA	Joint Token Key Access
4.	BI	Business Institutions
5.	AML	Anti-money laundering
6.	CIS	Cloud Infrastructure Source
7.	PCd-KYC	Pre-configured d-KYC
8.	EEK	Encrypted Encryption Key
9.	DHVT	Decentralized Hash Value Table

I. Illustrates the various abbreviations used in the course of the paper.

Over the years, several research endeavours in the realm of blockchain-based KYC have aimed to establish decentralized authentication and verification processes. However, extant works grapple with unresolved issues. Firstly, there is a noticeable gap in solutions providing an electronic customer's consent function with robust assurance against repudiation—a critical necessity under privacy regulations in the KYC registration process[3]. Secondly, the majority of existing works overlook the privacy implications of transactions stored in smart contracts and blockchains. Beyond the encryption of identity documents on cloud storage, preserving the privacy of all d-KYC processing transactions, including transaction status sharing, data origin authentication, and smart contracts containing personal data stored in the blockchain, remains inadequately addressed. Lastly, prevailing works often lack comprehensive features enabling customers to access and update their credentials housed on the cloud service facilitated by financial.

The organization of this paper unfolds as follows, In Section 2, we delve into the existing body of literature concerning our topic. Section 3 elucidates the theoretical framework employed in the development of our proposed methodology. Section 4 elaborates the objectives behind the study. Our suggested system model is detailed in Section 5, while Section 6 offers an in-depth analysis of the security aspects inherent in our devised scheme. The examination of our approach through evaluation analyses and experiments is presented in Section 7. Lastly, Section 8 encapsulates the paper with a summary, concluding remarks, and outlines potential directions for future research endeavours.

II. RELATED WORK

This research attempts to bridge critical gaps by presenting a robust and streamlined blockchain-based d-KYC document registration and verification process, employing lightweight cryptographic protocols within the cloud-based Stellar File Storage System (SFSS). To uphold fundamental privacy prerequisites concerning user agreement acquisition, we have formulated a smart contract designed to generate and enforce digitally endorsed agreements from customers. These agreements are systematically stored in an immutable blockchain, ensuring verifiability. To address data privacy concerns, we implement an advanced cryptographic protocol that combines symmetric and public key encryption to secure user credential files. Additionally, we employ attribute-based encryption with access policies for blockchain transactions. This encryption method, allowing controlled access to multiple institutions within the blockchain, adheres to predefined access policies. To optimize efficiency, we introduce a policy update algorithm, streamlining re-encryption based on a simplified policy tree structure[4].

Our system empowers users to update their d-KYC data with any participating institution in the blockchain. The updated data is distributed across the ledger and managed through a responsible smart contract[5]. This comprehensive framework ensures not only the security and efficiency of the d-KYC process but also compliance with evolving privacy regulations. The integration of SFSS and a strategic blend of cryptographic techniques emphasizes our dedication to a secure, transparent, and customer-centric d-KYC ecosystem, contributing to the progression of digital identity management in the financial sector.

The primary benefit lies in the elevated level of data security achieved through cutting-edge encryption algorithms and a secure cloud infrastructure. This robust security framework ensures the confidentiality and protection of customer information against potential security threats. The decentralized and immutable characteristics of blockchain technology add an additional layer of security, making unauthorized tampering with verified identity records exceedingly challenging[6]. This fortified security structure is indispensable in the context of KYC procedures, given the highly sensitive nature of personal and financial information.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 01 January 2024

Moreover, the integration of these technologies brings about the streamlining of the digital KYC (d-KYC) process, ushering in an era of efficiency and reduced manual efforts. The incorporation of smart contracts automates the verification process, minimizing the need for manual intervention. This, in turn, accelerates turnaround times and enhances overall customer satisfaction, fostering transparency and accountability in the KYC procedures. This transparent approach is crucial in building trust between financial institutions and their customers, ensuring that the KYC process is conducted in a fair, transparent, and accountable manner.

A pivotal aspect of this research involves leveraging blockchain technology to enhance the reliability of the KYC procedure. The decentralized and immutable nature of the blockchain aims to establish a trustworthy and tamper-proof record of identity verification activities[7]. Navigating regulatory challenges is crucial for financial institutions to ensure their KYC procedures comply with applicable laws and regulations. Despite the potential advantages, it is imperative to carefully consider challenges and limitations associated with these technologies. Firstly, the integration enhances data security through advanced encryption and a secure cloud infrastructure, ensuring customer information remains confidential[8]. The decentralized nature of blockchain adds an extra layer of security, making it challenging for unauthorized parties to tamper with verified identity records. Secondly, these technologies streamline the KYC process, reducing manual efforts and increasing efficiency, crucial in the digital era where customers expect quick and seamless experiences.

Furthermore, the use of blockchain in KYC enhances transparency and accountability. The decentralized nature ensures no single entity controls identity verification records, eliminating possibilities of data manipulation or fraudulent activities. However, challenges include blockchain scalability issues, potential barriers for smaller institutions due to significant investment requirements, and an evolving regulatory landscape, particularly regarding data privacy, anti-money laundering (AML) compliance, and legal implications.

The integration of blockchain technology and cloud computing in the KYC process holds immense potential to enhance data security, streamline processes, and establish trustworthy records[9]. However, addressing challenges and carefully navigating regulatory landscapes is crucial for successful implementation. Continued research and collaboration across academia, industry, and regulatory bodies are imperative to fully realize the benefits and develop standardized frameworks for implementation.

III. BACKGROUND

Research is framed by the imperative to enhance the efficiency, security, and transparency of Know Your Customer (KYC) procedures in the financial industry. In the current digital landscape, the integration of blockchain technology and cloud computing emerges as a compelling solution to address the inherent challenges in KYC processes[10].

A. Security Requirements

Security is paramount in KYC processes, given the sensitivity of personal and financial information. Traditional methods often fall short in providing robust protection against evolving cybersecurity threats. This research aims to address critical security requirements through advanced technologies.

Confidentiality is a primary security consideration. Customer information must be shielded from unauthorized access, emphasizing the need for cutting-edge encryption algorithms during storage and transmission. The secure cloud infrastructure complements these measures, ensuring customer information remains confidential and protected against potential threats. Data integrity is equally crucial. The research recognizes the importance of establishing an unassailable record of identity verification activities. Blockchain's decentralized and immutable characteristics add an extra layer of security, making verified identity records resistant to unauthorized tampering.

B. Blockchain Integration

Blockchain technology transforms how KYC procedures are conducted. Its decentralized and distributed ledger nature eliminates the need for a central authority, enhancing resilience. The integration of blockchain fortifies security and introduces transparency and accountability.

The study leverages blockchain to streamline the KYC process, particularly in the digital KYC (d-KYC) framework. The decentralized nature ensures no single entity controls identity verification records, eliminating the possibility of data manipulation or fraudulent activities. This transparency builds trust between financial institutions and customers.

C. Encryption Methods for Security

The research employs various encryption methods within the cloud infrastructure to meet advanced security needs. These measures are crucial for safeguarding sensitive customer information against potential threats. Cutting-edge encryption algorithms secure customer information during storage and transmission[6]. This commitment aligns with industry standards for adopting state-of-the-art security measures, especially in KYC procedures, where personal and financial information requires utmost protection.

IV. MOTIVATION AND OBJECTIVES

This research strive to pioneer advancements in Know Your Customer (KYC) processes through the innovative integration of blockchain technology and cloud computing. Motivated by the imperative to enhance the security, efficiency, and transparency of identity verification procedures within the financial sector, our study proposes a

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 01 January 2024

comprehensive framework that redefines the landscape of digital KYC (d-KYC). The primary objective is to fortify data security by employing cutting-edge encryption algorithms and a secure cloud infrastructure while simultaneously leveraging the decentralized and immutable nature of blockchain for enhanced integrity. Our approach introduces a transformative shift, automating and streamlining the KYC process through the incorporation of smart contracts[7]. By fostering a seamless interaction between entities within the system, including customers and Banking Institutions (BIs), our research aims to establish a trustworthy, tamper-proof record of identity verification activities. The motivation behind this study is rooted in the urgency to navigate the challenges posed by traditional KYC methodologies and harness the transformative potential of emerging technologies. Through meticulous examination and implementation, our objective is to contribute to the evolution of KYC practices, setting new standards for security, efficiency, and accountability in the digital age.

The primary objective of this research is to establish a robust and streamlined blockchain-based digital Know Your Customer (d-KYC) document registration and verification process. This entails the utilization of lightweight cryptographic protocols within the cloud-based Stellar File Storage System (SFSS)[8]. The focus is on upholding fundamental privacy prerequisites through the creation and enforcement of digitally endorsed agreements from customers via a smart contract[8]. These agreements are systematically stored in an immutable blockchain, ensuring verifiability[8]. To address data privacy concerns, an advanced cryptographic protocol is implemented, combining symmetric and public key encryption to secure user credential files. Attribute-based encryption with access policies for blockchain transactions is also employed, allowing controlled access to multiple institutions within the blockchain, adhering to predefined access policies. The optimization of efficiency is achieved through the introduction of a policy update algorithm, streamlining re-encryption based on a simplified policy tree structure. A key objective is to empower users to update their d-KYC data with any participating institution in the blockchain. The updated data is distributed across the ledger and managed through a responsible smart contract[9]. This framework ensures not only the security and efficiency of the d-KYC process but also compliance with evolving privacy regulations.

V. PROPOSED WORK

The study's methodology includes the implementation of advanced encryption algorithms within the cloud infrastructure to fortify data security[10]. Encrypting sensitive customer information during storage and transmission ensures its confidentiality and protection against potential security threats. The use of smart contracts in the KYC process has proven to be a significant factor in increasing efficiency and reducing manual efforts[11]. Automation through smart contracts eliminates the need for manual intervention, reducing the chances of errors or delays and providing a faster and more streamlined KYC process.

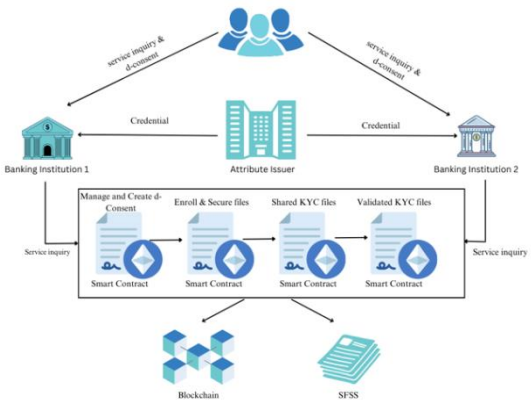

Fig 1. This figure illustrates the configuration of the framework designed to instill confidence and reliability in data transactions.

A. Customer Authentication

The foundational security paradigm integrates Attribute-Based Encryption with Ciphertext Policy (ABE-CP), ensuring robust customer authentication. E-consent generation through smart contracts, coupled with customer signatures, establishes a non-repudiation mechanism, aligning with data privacy standards.

The user starts the enrolment process by registering within the system as shown in Fig 1. and providing essential identity information and a cryptographic key. Following this, the wallet system of the blockchain platform generates a unique key pair, including a public key (PubQ Customer_ID) and a private key (PrivQ Customer_ID), specifically designed for the customer. The banking institution (BI) then activates the Central contract, enabling the creation and authorization of a decentralized consent (d-consent). The customer, using their private key connected to Customer_ID, digitally endorses this consent.

The banking institution proceeds by invoking the Register contract, formally enrolling the customer in the system, and the customer submits their credential documents (Creds docs), which are securely stored in the institution's internal database[12][13].

Subsequently, the Register contract generates an AES encryption key for securing the d-KYC document. The customer, following the instructions, encrypts this key using their public key (PublicKey Customer_ID), resulting in an encrypted file containing all credentials (Encrypt-CredsFile). This encrypted file, along with the encrypted encryption key (EEK), is stored in SFSS storage and the blockchain, respectively.

The SFSS storage system carefully stores the data file in a designated data storage node, generating a hash value through SHA-256 that encapsulates both the file and

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 01 January 2024

customer details. This hash value (HV) serves as a dynamic index, linking to the EncryptCredsFile located in SFSS. Additionally, it is automatically returned and stored in the DHVT table and the Central contract.

B. Validation Process

Our innovative scheme employs symmetric and asymmetric encryption for d-KYC documents, fortifying their integrity. Robust access controls, combining symmetric and ABE-CP encryption, validate transactions securely, substantiated by the system's resilience against collaborative attacks[14].

The process of d-KYC verification commences with the client furnishing their customer ID to the pertinent Banking institution (BI). Subsequently, the requesting Banking Institution (BI) computes a hash value and transmits it to the Verify contract. The Verify contract subsequently compares the newly submitted hash value to the stored one in the Central contract. Upon verification of a match, the Verify contract retrieves file addresses from the Decentralized Hash Value Table (DHVT) in the Secure File Storage System (SFSS) by utilizing the hash value. It procures the corresponding EncryptCreds document and its correlated Encrypted Encryption Key (EEK). The Verify contract then requests the Central contract to produce a d-consent, which is dispatched alongside the EncryptCreds file and EEK to the BI seeking KYC verification. The customer is obligated to digitally sign the d-consent, decrypt the EEK using their private key, and employ the session public key to decrypt the EncryptCredsFile. The requesting BI securely stores the client's Credential File in its internal database, and the system logs the verified transaction while updating the smart contracts' state within the blockchain.

C. Securing Crucial Data

Transparent audit trails on the blockchain meticulously record user access, providing enduring records for authorized Banking Institutions (BIs) and auditors. The integration of ABE-CP ensures the confidentiality of sensitive transactional data, safeguarding against unauthorized access attempts[15][16].

Blockchain technology guarantees the integrity and immutability of data, creating a tamper-proof ledger for KYC records. Cloud computing facilitates secure storage and access, ensuring scalability and availability. ABE-CP encryption adds an extra layer of security by granting access based on specified attributes, providing fine-grained control over who can access specific information[17][18].

Additionally, Joint Token Key Access enhances security by requiring multiple authentication tokens for data access, reducing the risk of unauthorized access. By integrating these technologies seamlessly, our framework not only meets but exceeds industry standards for securing private data, offering a comprehensive solution to safeguarding the confidentiality and integrity of KYC information.

VI. RESULTS

Within this segment, we expound on the security assessment of our proposed framework by delineating the foundational security paradigm and its associated characteristics.

1. Foundational Security Framework

Our model operates on the premise that the d-KYC platform seamlessly integrates with a blockchain. All entities within the system, including blockchain nodes and the cloud, are assumed to be honest but inherently inquisitive. The cornerstone of our cryptographic protocol rests on an advanced encryption technique denoted as Attribute-Based Encryption with Ciphertext Policy (ABE-CP). A comprehensive exposition of the security model and its corroboration can be found in.

2. Integral Security Attributes

Complementing the foundational security framework, our innovative scheme encapsulates several pivotal security attributes. Fig 2. depicts a clear correlation between file magnitude and encryption time, revealing a positive trend. Larger file sizes correspond to longer encryption times, highlighting the algorithm's sensitivity to data magnitude. Fig 3. illustrates a discernible correlation between file magnitude and decryption time, indicating a positive trend. Longer decryption times are observed with larger file sizes, underscoring the algorithm's responsiveness to variations in data magnitude. This sensitivity emphasizes the algorithm's performance characteristics in relation to different data sizes.

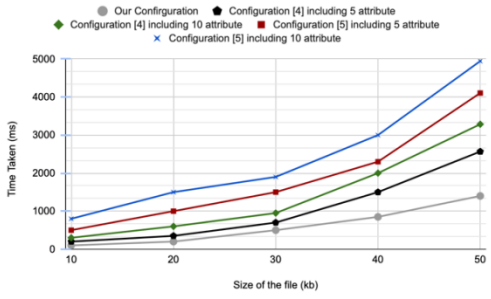

Fig 2. This figure demonstrates the correlation between the file magnitude and the corresponding encryption time.

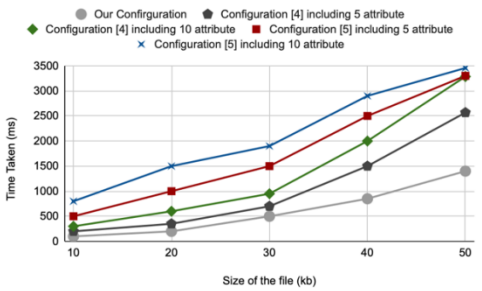

Fig 3. This figure demonstrates the correlation between the file magnitude and the corresponding decryption time

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 01 January 2024

A. Confidential d-KYC Credentials with Customer Accord:

Our approach amalgamates cutting-edge symmetric and asymmetric encryption methods to fortify d-KYC documents prior to their integration into cloud storage. To align with prevailing standards governing data privacy and auditing in cloud environments, the pertinent smart contract orchestrates the generation of e-consent. Customers are then prompted to affix their signature, granting the Banking Institution (BI) permission to utilize and securely store their personal data. This not only ensures privacy preservation but also incorporates a robust non-repudiation mechanism.

B. Robust and Nuanced Access Control to Transactional Data:

Leveraging a combination of symmetric and ABE-CP encryption, our framework ensures the confidentiality of transactional data by encrypting it, along with the secret keys of Banking Institutions (BIs). This guarantees that only legitimate BIs can access sensitive transactional data. The robustness of ABE-CP is substantiated in the original literature.

C. Resilience Against Collaborative Attacks:

In the hypothetical scenario where two distinct BIs collude, our system remains steadfast. Even though these BIs possess secret keys with disparate attribute sets, the Cloud Infrastructure Source (CIS) issues them a Joint Token Key Access (JTKA). However, their inability to amalgamate attributes prevents access to the encrypted data, owing to the inherent properties of ABE-CP and the stipulated access policy.

D. Transparent Audit Trail:

Every user access activity, irrespective of customer or participating BI, is meticulously recorded within the blockchain. Authorization details and smart contract states serve as enduring records of transactions that can’t be changed. Authorized BIs and third-party auditors can discern the actors involved in these activities, eliminating any scope for denial of access operations. Additionally, legitimate BIs possess the capability to identify and thwart unauthorized access attempts through meticulous verification.

VII. DISCUSSION

The comprehensive security measures embedded in our proposed d-KYC framework and the fusion of advanced encryption techniques, customer accord mechanisms, nuanced access controls, resilience against collaborative attacks, and a transparent audit trail collectively contribute to a robust security paradigm, ensuring the integrity, confidentiality, and accountability of d-KYC processes integrated with blockchain technology.

Our system exhibits resilience against collaborative attacks, addressing a hypothetical scenario where two distinct BIs collude. Despite possessing secret keys with disparate attribute sets, the issuance of Joint Token Key Access (JTKA) by the Cloud Infrastructure Source (CIS) is rendered ineffective due to the inherent properties of ABE-CP. This resilient architecture ensures that even in collaborative attack scenarios, unauthorized access to encrypted data is thwarted, maintaining the integrity of the d-KYC system.

This research is motivated by the necessity to evolve KYC procedures in the digital era. The integration of blockchain technology and cloud computing serves as a transformative solution, addressing security requirements, streamlining processes, and establishing transparency. The research methodology integrates advanced encryption algorithms, leverages blockchain's decentralized nature, and harnesses the potential of cloud computing to revolutionize KYC in the digital age.

VIII. CONCLUSION

This study has explored the potential of integrating blockchain technology and cloud computing to optimize KYC procedures. The research design adopted a comprehensive approach, focusing on the seamless integration of these two technologies to enhance data security, streamline the KYC process, and establish a trustworthy and tamper-proof record of identity verification activities. The amalgamation of blockchain technology and cloud computing in the KYC framework yields multifaceted advantages. Foremost among these is the heightened level of data security achieved through the utilization of cutting-edge encryption algorithms and secure cloud infrastructure. This robust security framework ensures the confidentiality and safeguarding of customer information against potential security threats. The decentralized and immutable characteristics of the blockchain contribute to an additional layer of security, rendering unauthorized tampering with verified identity records exceedingly challenging. Moreover, the integration of these technologies facilitates the streamlining of the d-KYC process, ushering in a new era of efficiency and reduced manual efforts. The incorporation of smart contracts automates the verification process, minimizing the need for manual intervention, thereby accelerating turnaround times and enhancing overall customer satisfaction. This is crucial in building trust between different types of organizations and their customers, as it ensures that the KYC process is conducted in a transparent and accountable manner. The integration of blockchain technology and cloud computing in the KYC process offers several benefits. Further research and collaboration between academia, industry, and regulatory bodies are needed to fully realize the benefits of this integration and develop standardized frameworks for its implementation.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 01 January 2024

REFERENCES

[1] Chandraprabha, K. S. "Blockchain-Based Implementation on Electronic Know Your Customer (e-KYC)." In Intelligent Communication Technologies and Virtual Mobile Networks, pp. 281-297. Singapore: Springer Nature Singapore, 2023.

[2] Barati, Masoud, Gagangeet Singh Aujla, Jose Tomas Llanos, Kwabena Adu Duodu, Omer F. Rana, Madeline Carr, and Rajiv Ranjan. "Privacy-aware cloud auditing for GDPR compliance verification in online healthcare." IEEE Transactions on Industrial Informatics 18, no. 7 (2021): 4808-4819.

[3] Kulkarni, Vikrant, and Awadhesh Pratap Singh. "Sustainable KYC through blockchain technology in global banks." Annals of Dunarea de Jos University of Galati. Fascicle I. Economics and Applied Informatics 25, no. 2 (2019): 34-38.

[4] 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.

[5] S. Gao, G. Piao, J. Zhu, X. Ma, and J. Ma, ‘‘TrustAccess: A trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain,’’ IEEE Trans. Veh. Technol., vol. 69, no. 6, pp. 5784–5798, Jun. 2020.

[6] Al Mamun, Abdullah, Sheikh Riad Hasan, Md Salahuddin Bhuiyan, M. Shamim Kaiser, and Mohammad Abu Yousuf. "Secure and transparent KYC for banking system using IPFS and blockchain technology." In 2020 IEEE region 10 symposium (TENSYMP), pp. 348-351. IEEE, 2020.

[7] Malhotra, Diksha, Poonam Saini, and Awadhesh Kumar Singh. "How blockchain can automate KYC: systematic review." Wireless Personal Communications 122, no. 2 (2022): 1987-2021.

[8] Kumar, Manoj, P. Anand Nikhil, and P. Anand. "A blockchain based approach for an efficient secure KYC process with data sovereignty." Int J Sci Technol Res 9 (2020): 3403-3407.

[9] Schlatt, Vincent, Johannes Sedlmeir, Simon Feulner, and Nils Urbach. "Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity." Information & Management 59, no. 7 (2022): 103553.

[10] Patil, Pradnya, and M. Sangeetha. "Blockchain-based Decentralized KYC Verification Framework for Banks." Procedia Computer Science 215 (2022): 529-536.

[11] Sun, Nigang, Yuanyi Zhang, and Yining Liu. "A privacy-preserving kyc-compliant identity scheme for accounts on all public blockchains." Sustainability 14, no. 21 (2022): 14584.

[12] Patel, Dhiren, Hrishikesh Suslade, Jayant Rane, Pratik Prabhu, Sanjeet Saluja, and Yann Busnel. "KYC as a Service (KASE)—A Blockchain Approach." In Advances in Machine Learning and Computational Intelligence: Proceedings of ICMLCI 2019, pp. 795-803. Springer Singapore, 2021.

[13] Hannan, Md Abdul, Md Atik Shahriar, Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, and Mohammad Shahriar Rahman. "A systematic literature review of blockchain-based e-KYC systems." Computing (2023): 1-30.

[14] Rajasekhar, Mr Y., K. Chandra Sekhar, G. Ranil, L. V. N. Maneesh, and K. Venu. "ENABLING TRUST AND PRIVACY PRESERVING E-KYC."

[15] Biradar, Raghavendra R., and M. Dakshayini. "Blockchain enabled KYC solutions using hyperledge fabric." In 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), pp. 1-3. IEEE, 2020.

[16] Alfozan, Thalaya, and Mr Ghaleb Aoude. "Cloud Computing and its Impact on Kuwait's Banking Sector." (2021).

[17] Algamdi, Abdelmageed. "„KYC and Blockchain Onboarding Process for Banks.“." International Journal of Innovation, Creativity and Change 15, no. 9 (2021).

[18] Rankhambe, Bharti Pralhad, and Harmeet Kaur Khanuja. "Hassle-Free and Secure e-KYC System Using Distributed Ledger Technology." International Journal of Next-Generation Computing 12, no. 2 (2021).