Trustworthy E-KYC Systems Using Blockchain

Mr. Suryakant Auti[1], Mr. Kshitij Bhondave[2], Miss. Namodevi Gore[3], Miss. Gitanjali Bhoge[4], Prof. Neeta Gade[5]

[1,2,3,4]Student, Shri Chhatrapati Shivaji Maharaj College of Engineering,
[5]Asst. Professor, Shri Chhatrapati Shivaji Maharaj College of Engineering,

Abstract:
In today's world, Leveraging technological advancements, such as digital identity verification and biometric authentication, has streamlined and modernized KYC processes. These innovations not only enhance efficiency but also contribute to a more user-friendly experience for customers. In this contemporary landscape, staying informed about evolving regulations and industry-specific practices is indispensable for effective KYC implementation. Financial institutions must continuously adapt to the changing regulatory environment and leverage technological solutions to maintain the integrity of their KYC processes. This proactive approach is crucial not only for compliance but also for building trust between customers and stakeholders in an era where financial security and transparency are paramount. KYC procedures have been simplified and brought up to date by utilizing technology innovations like biometric authentication and digital identity verification. These advancements contribute to a more user-friendly experience for customers in addition to increasing efficiency. Keeping up with changing laws and sector-specific procedures is essential for implementing KYC successfully in the modern world. It is imperative for financial institutions to consistently adjust to the dynamic regulatory landscape and utilize technological advancements to uphold the integrity of their KYC procedures. This proactive strategy is essential for both compliance and fostering stakeholder and customer trust in a time when financial stability and openness are critical.

Index Terms – KYC - know your customer, AML - anti-money laundering, CTF - counter-terrorism financing

Keywords – KYC, blockchain, etherium, encryption, compression

I. Introduction

In the dynamic realm of technology, our final-year engineering project represents an exciting foray into innovation. As ambitious students, we are dedicated to implementing an eKYC system using blockchain technology and advanced cryptographic algorithms to expedite identity verification and fortify the security of critical documents. By embracing the potential of blockchain, we create a decentralized, tamper-proof ledger for the secure storage and sharing of user data. This groundbreaking solution is poised to significantly reduce verification times, enhancing efficiency, and protecting user data from unauthorized access and tampering.

While we are not yet experts, we are passionate learners, enthusiastic about the potential of this project. With limited resources and the support of our academic institution, we aim to deliver a functional eKYC system that demonstrates our commitment to innovative engineering solutions. This system will provide valuable insights into the intersection of blockchain and identity verification, offering a glimpse into the future of secure and efficient data management.

II. Motivation

The motivation behind our endeavor is multifaceted. First and foremost, we are driven by the need to provide a more efficient and streamlined experience for our clients. By reducing document verification time, we aim to make their interactions with our organization smoother and more convenient. Additionally, we are deeply committed to safeguarding the sensitive documents and personal information entrusted to us. The security and immutability offered by blockchain technology align with our unwavering dedication to data protection and privacy.

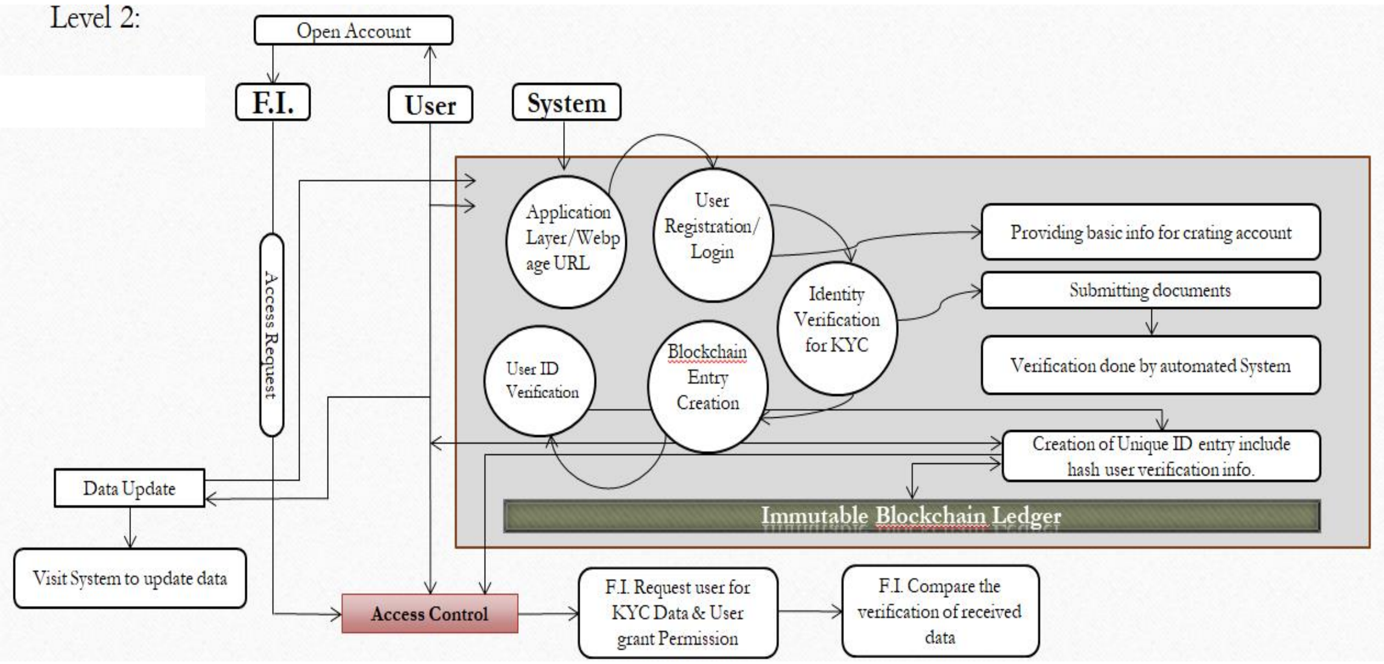
Furthermore, as regulatory landscapes evolve, staying compliant with ever-changing requirements is paramount. Our project will not only expedite the onboarding process but also ensure that we remain in full compliance with the latest regulations. Ultimately, our motivation is rooted in the pursuit of excellence, striving to offer a secure, efficient, and compliant eKYC system that enhances the overall experience for both our clients and our organization.

III. Objectives

The project focuses on the development of a blockchain-based e-KYC system with an integrated live video verification component. The primary objective is to establish a secure and decentralized blockchain infrastructure that ensures the tamper-proof storage and verification of customer data. The inclusion of live video verification aims to enhance identity authentication in real-time, preventing impersonation and bolstering the overall security of the e-KYC process. Regulatory compliance is a key consideration, and the project aims to align with relevant standards, particularly those related to data privacy and financial regulations. The user experience is a focal point, and the project endeavors to create an intuitive interface for both customers undergoing the e-KYC process and administrators managing the system. Seamless integration with financial institutions is a priority, and the development of APIs and integrations is planned to enable efficient and secure data sharing. Smart contracts on the blockchain will be leveraged to automate authorization processes, controlling access to e-KYC data based on predefined criteria. Security measures, including encryption, will be implemented to safeguard sensitive customer information stored on the blockchain. The live video verification process will be optimized for efficiency, ensuring a smooth experience for both customers and verification agents. Rapid customer onboarding is another objective, with a focus on streamlining the e-KYC process to reduce the time and effort required for identity verification. The project also emphasizes scalability, designing the e-KYC system to handle a growing user base and increasing transactions without compromising performance. Regular evaluation of progress against these objectives is deemed essential for the successful development and implementation of the blockchain-based e-KYC system with live video verification.

IV. System Architecture

The architecture of the blockchain-based e-KYC system, featuring integrated live video verification, is designed to establish a secure, decentralized, and user-friendly environment. At its core is a blockchain infrastructure ensuring tamper-proof storage of e-KYC data, with smart contracts automating authorization processes. The user interface is intuitively crafted to provide a seamless experience, particularly during live video verification sessions. The system incorporates APIs for smooth integration with financial institutions, a robust security layer to safeguard sensitive information, and a compliance module to adhere to regulatory standards. This scalable architecture is supported by a database for efficient data handling, and monitoring tools ensure optimal system performance. This comprehensive design aims to enhance security, streamline user interactions, and meet regulatory requirements for a successful implementation of the e-KYC system. The system architecture of a blockchain-based e-KYC (Know Your Customer) system with integrated live video verification is designed to ensure a secure, efficient, and decentralized environment. The architecture involves several key components working in concert to achieve the project's objectives:


Level 2:
Open Account
F.I.
User
System
Access Request
Application Layer/Webpage URL
User Registration/ Login
Identity Verification for KYC
User ID Verification
Blockchain Entry Creation
Providing basic info for crating account
Submitting documents
Verification done by automated System
Creation of Unique ID entry include hash user verification info.
Immutable Blockchain Ledger
Data Update
Visit System to update data
Access Control
F.I. Request user for KYC Data & User grant Permission
F.I. Compare the verification of received data

Blockchain based e-kyc system architecture

IV.I Blockchain Infrastructure

The blockchain infrastructure of the e-KYC system serves as its foundational framework, providing a secure and decentralized ledger for the storage and management of customer identity data. This distributed ledger technology ensures that information is stored across a network of nodes, enhancing security by eliminating a single point of failure and making it resistant to unauthorized alterations. Each transaction, or in this case, each update or verification within the e-KYC process, is recorded in a block that is cryptographically linked to the previous one, creating an immutable chain. This design not only enhances data integrity but also fosters transparency, allowing authorized parties to trace and validate each step of the e-KYC journey. Smart contracts, self-executing code stored on the blockchain, play a crucial role in automating and enforcing predefined rules and authorization processes, such as controlling access to e-KYC data based on specific criteria. The decentralized nature of the blockchain ensures that no single entity has unilateral control, contributing to a trustless environment where parties can transact and verify identities without relying on a central authority. Overall, the blockchain infrastructure forms the backbone of the e-KYC system, providing the security, transparency, and efficiency necessary for a robust and reliable identity verification process.

VI.II Smart Contracts

Smart contracts, integral to the architecture of the blockchain-based e-KYC system, represent self-executing, programmable agreements stored on the blockchain. These contracts automate and enforce predefined rules and conditions without the need for intermediaries, ensuring a trustless and transparent execution of processes. In the context of the e-KYC system, smart contracts play a pivotal role in facilitating and securing authorization processes. These contracts govern the access to e-KYC data based on specific criteria, such as verifying a user's identity or granting permission for data sharing. Through the use of if-then logic, smart contracts automatically execute actions when predefined conditions are met, enhancing the efficiency and reliability of the e-KYC process. Their execution on the decentralized blockchain ensures that the terms of the contracts are immutable, transparent, and tamper-proof. This not only streamlines the e-KYC workflow but also minimizes the risk of fraud or unauthorized access, contributing to the overall integrity and security of the identity verification system.

VI.III User Interface

The user interface (UI) of the blockchain-based e-KYC system with integrated live video verification plays a pivotal role in shaping the user experience for both customers and administrators. For customers undergoing the e-KYC process, the UI is meticulously designed to be intuitive and user-friendly, guiding them seamlessly through each step of identity verification. The interface incorporates clear and concise instructions for the live video verification sessions, ensuring that users can easily navigate and understand the process. It features responsive and visually appealing design elements, optimizing the presentation of information and enhancing overall usability. Additionally, the UI provides real-time feedback during the live video sessions, assuring users that the verification process is underway. For administrators, the UI offers a comprehensive dashboard with functionalities for managing and monitoring the e-KYC system. This includes tools for reviewing verification sessions, accessing audit logs, and responding to any flagged issues. The goal of the UI is to create a positive and efficient interaction between users and the e-KYC system, fostering trust, ease of use, and overall satisfaction with the identity verification process. Regular user testing and feedback loops are integral to refining and optimizing the UI to meet the evolving needs of both customers and administrators.

VI.IV APIs and Integrations

APIs (Application Programming Interfaces) and integrations play a pivotal role in the architecture of the blockchain-based e-KYC system with integrated live video verification. These components serve as the conduits for seamless communication between the e-KYC system and external entities, particularly financial institutions. APIs are designed to expose specific functionalities, allowing these entities to securely access and interact with the e-KYC system's features. Integrations facilitate the smooth exchange of data, ensuring that the e-KYC system can efficiently share information with external systems and vice versa. The APIs enable standardized and secure connections, allowing for the retrieval and updating of e-KYC data as needed for various financial processes. These interfaces not only enhance the interoperability of the e-KYC system but also contribute to the broader goal of creating a connected financial ecosystem. By integrating with external systems, the e-KYC system can provide a more comprehensive view of customer information, enabling financial institutions to make informed decisions while ensuring the integrity and security of sensitive data. The careful design and implementation of APIs and integrations are crucial for achieving a cohesive and efficient blockchain-based e-KYC system that aligns with industry standards and regulatory requirements. Regular monitoring and updates to these interfaces are essential to adapt to evolving technologies and maintain the system's effectiveness in a dynamic financial landscape.

VI.V Live Video Integration

The live video integration in the blockchain-based e-KYC system plays a pivotal role in elevating the identity verification process to a more robust and real-time level. This module incorporates advanced video streaming capabilities, leveraging cutting-edge technologies such as facial recognition algorithms and biometric authentication. During the live video verification sessions, customers engage with a secure platform that facilitates direct communication with verification agents. This not only adds an extra layer of authentication by verifying the user's identity in real-time but also significantly reduces the risk of impersonation or fraudulent activities. The live video integration ensures a dynamic and secure verification process, enhancing the overall reliability and accuracy of the e-KYC system. Furthermore, it contributes to a more user-friendly experience, as customers can undergo identity verification conveniently from their preferred locations, promoting accessibility without compromising security.

VI.VI Regulatory Compliences

On the regulatory compliance front, the e-KYC system incorporates a dedicated module to ensure adherence to stringent data protection and financial regulations. This module is designed to accommodate evolving compliance requirements, providing a framework for the systematic collection, storage, and sharing of customer data in accordance with legal standards. It includes features such as audit trails, encryption protocols, and secure data transmission channels. By maintaining a comprehensive record of user interactions and transactions, the regulatory compliance module not only facilitates transparency but also aids in regulatory reporting. Regular updates and monitoring mechanisms are integrated to adapt swiftly to changes in regulations, ensuring that the e-KYC system remains aligned with industry-specific legal frameworks. This commitment to regulatory compliance not only safeguards the interests of users but also fosters trust in the system, a critical factor in the success of a blockchain-based e-KYC platform in the financial landscape.

VI.VII Scalable Architecture

The scalable architecture of the blockchain-based e-KYC system is foundational to accommodate growth, increased user activity, and evolving demands. It involves the strategic design and implementation of systems capable of handling rising workloads without sacrificing performance. Key elements include load balancing mechanisms, which distribute incoming traffic efficiently across servers, preventing bottlenecks during peak usage. Additionally, the architecture incorporates distributed processing, enabling tasks to be spread across multiple servers or nodes, optimizing resource utilization. This approach ensures that the e-KYC system can seamlessly scale horizontally by adding more servers or nodes to the network, meeting the demands of a growing user base while maintaining responsiveness and reliability.

VI.VIII Database

The database module within the e-KYC system serves as a crucial component supporting efficient data management and retrieval. While the primary e-KYC data is securely stored on the blockchain for its decentralized and tamper-resistant properties, a supporting database complements this setup. This database is optimized for quick query responses and specific functionalities, enhancing the overall performance of the system. The integration between the blockchain and the database is carefully orchestrated to maintain data consistency, ensuring that updates and changes are synchronized seamlessly. This dual-layered approach combines the security of the blockchain with the speed and efficiency of a dedicated database, providing a robust foundation for managing customer information in a dynamic and evolving environment.

VI.IX Monitoring and Analytics

Monitoring and analytics are integral aspects of the e-KYC system, contributing to its resilience, performance optimization, and the derivation of valuable insights. Monitoring tools are implemented to track the system's health, identify potential issues, and ensure optimal resource utilization. Real-time alerts and notifications help in promptly addressing any anomalies or performance bottlenecks. On the analytics front, data derived from user interactions, system usage, and live video verification sessions are processed to gain valuable insights. These insights can inform strategic decisions, improve user experience, and identify areas for system enhancement. The combination of robust monitoring and analytics capabilities not only ensures the smooth operation of the e-KYC system but also positions it for continuous improvement and adaptation to evolving requirements and user behaviors.

V. Algorithms

1. NLP (Natural Language Processing):

Natural Language Processing involves the interaction between computers and human languages. It combines computational linguistics and computer science to enable machines to understand, interpret, and generate human-like language. Applications include language translation, sentiment analysis, and chatbots.

2. ECC (Elliptic Curve Cryptography):

Elliptic Curve Cryptography is a public-key cryptography system based on the mathematics of elliptic curves. It provides a secure method for key exchange, digital signatures, and encryption. ECC is known for its ability to provide strong security with relatively short key lengths compared to other cryptographic methods.

3. ECDSA (Elliptic Curve Digital Signature Algorithm):

ECDSA is a digital signature algorithm based on elliptic curve cryptography. It is commonly used to verify the authenticity and integrity of digital messages. ECDSA is efficient and provides a level of security comparable to other digital signature algorithms with longer key lengths.

4. PoW (Proof of Work):

Proof of Work is a consensus algorithm used in blockchain networks. It requires participants (miners) to solve complex mathematical problems to validate transactions and create new blocks. PoW is resource-intensive, providing security through the computational work required to add blocks to the blockchain.

5. ZK-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge):

ZK-SNARKs are cryptographic proofs that allow one party to prove possession of certain information without revealing the information itself. They are used to enhance privacy in blockchain transactions, enabling verification of the validity of a statement without disclosing the details of the statement.

6. ERC-20 (Ethereum Request for Comment 20):

ERC-20 is a standard for creating and implementing fungible tokens on the Ethereum blockchain. These tokens can represent various assets, and ERC-20 defines a set of rules and functions that tokens on the Ethereum network must follow to be supported.

7. DIDs (Decentralized Identifiers):

Decentralized Identifiers are a new type of identifier that is created, owned, and controlled by the subject of the identifier (individual, organization). DIDs are fundamental to self-sovereign identity systems, providing a way for individuals to have control over their digital identities.

Each of these algorithms and concepts plays a significant role in various domains, from cryptography and blockchain technology to artificial intelligence and decentralized identity systems.

VI. Conclusion

The proposed solution effectively addresses the issue of redundant registration in the current KYC process. It incorporates the use of the AES encryption algorithm and random key generation, providing customers with control over their KYC data and ensuring its confidentiality. The system has the potential to reduce storage requirements by approximately 20%. Looking ahead, future iterations of this system could assign separate access keys to individual fields, offering users enhanced control over their private data. A comprehensive examination of all encryption and compression techniques could lead to a more efficient solution in a real-world decentralized environment.

VII. References

1. José Parra Moyano and Omri Ross, "KYC Optimization using Distributed Ledger technology", Springer -Business & Information systems Engineering, , pp-411-423, vol.59,2018.
2. G. Zyskind, O. Nathan and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data", IEEE Security and Privacy Workshops, San Jose, CA, 2015.
3. Mauro Isaja and John Soldatos, Distributed ledger technology for decentralization of manufacturing processes,IEEE Conference on Industrial Cyber-Physical Systems (ICPS) 2018 at, St. Petersburg, Russia, pp 696- 701,2018..
4. Rui Yuan, Yu-Bin Xia, Hai-Bo Chen, Bin-Yu Zang, Jan Xie and ShadowEth: Private Smart Contract on Public Blockchain, Springer, Journal of Computer Science and Technology, Issue 3, pp 542–556. vol 33,2018.
5. XiaoqiLi , PengJiang, ,XiapuLuo,TingChen and QiaoyanWen, "A survey on the security of blockchain systems”, Elsevier Future Generation Computer systems", ,Aug 2017
6. Sein Myung, Jong and Hyouk Lee, Ethereum smart contract-based automated power trading algorithm in a microgrid environment, Springer Journal of Super computing, PP 1-11,2018
7. Petar Maymounkov and David Mazieres, "Kademlia: A peer-to- peer information system based on the xor metric", Business & Information Systems Engineering Journal, 2002
8. S.Nakamot, “Bitcoin: A peer-to-peer electronic cash system”, International Conference on Financial Cryptography and Data Security, 2009
9. Shbair, Wazen & Steichen, Mathis & François, Jérôme and State, Radu“Blockchain Orchestration and Experimentation Framework: A Case Study of KYC”, IEEE/IFIP Network Operations and Management Symposium
10. Liehuang Zhu, Yulu Wu, Keke Gai, Kim-Kwang and Raymond Choo "Controllable and trustworthy

blockchain-based cloud data management", Elsevier, Future Generation Computer Systems, pp. 527-535, vol 91, 2019

11. PaulJ.Taylor, Tooska Dargahi,Ali Dehghantanha,Reza,M.Parizi,Kim Kwang and Raymond Choo, ,A systematic literature review of blockchain cyber security.,DigitalCommunication and networks,", Elsevier Feb 2019
12. Wjatscheslav Baumung, and Vladislav Fomin, Framework for enabling order management process in a decentralized production network based on the blockchain-technology, Elsevier, Procedia CIRP, PP 456-460, vol 79, 2019,
13. J.Uthayakumar,T.Vengattaraman and P.Dhavachelvan, A survey on data compression techniques: From the perspective of data quality, coding schemes, data type and applications, Elsevier, Journal of king saud university Computer and Information Sciences, ,pp 1-22, May 2018
14. KenanKalajdzic,SamaherHusseinAli and AhmedPatel Rapid lossless compression of short text messages Elsevier, Computer Standards & Interfaces, , PP 53-59, vol 37, 2015
15. SuryaPrakashMishra,Col.GurmitSingh and RajeshPrasad, A review on compressed pattern matching, Elsevier, Perspectives in Science, PP 727-729, vol 8, 2016
16. Kosba A, Miller A, Shi E, Wen Z K, Papamanthou and C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proc. IEEE Symp. Security and privacy, PP-839-858, 2016
17. Zhang F, Cecchetti E, Croman K, Juels A, Shi E. Town crier: An authenticated data feed for smart contracts. In Proc. the 23rd ACM SIGSAC Conf. Computer and Communications Security, ,pp.270-282, 2016
18. NishthaMathuraRajeshBansodeb, AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection, Elsevier, Procedia Computer Science PP 1036-1043, vol79, 2016
19. Rashmi Ramesh Rachh, P. V. Ananda Mohan and B. S. Anami Efficient Implementations for AES Encryption and Decryption, Springer, Journal of Circuits, Systems and Signal Processing, pp 1765–1785, vol.31,2012
20. Fatimah Alkhudhayr, Shouq Alfarraj, Buthina Aljameeli, Salim Elkhdhiri, “ Information security: A review of information security issues and Techniques,”IEEE International conference on computer applications& Internet security,2019