ISSN: 2249-7196
IJMRR/April-June. 2025/ Volume 15/Issue 2s/528-537
Mohammad Owais Khan / International Journal of Management Research & Review

Ensuring Secure Sharing Of Identity Information Of Kyc Compliance And Verification

Mohammed Adil[1],Syed Sameer[2],Anas Yousuf [3],Mrs.M.Shilpa[4]
[1,2,3]B.E. Student, Department of IT, Lords Institute of Engineering and Technology, Hyderabad
[4]Assistant Professor, Department of IT, Lords Institute of Engineering and Technology, Hyderabad
shilpa.m@lords.ac.in

ABSTRACT

The growing reliance on centralized servers for storing approximately 70% of user data, including sensitive information like addresses, zip codes, gender, and medical history, poses significant threats due to potential misuse or alteration. To address these risks, a Blockchain-based KYC Sharing system is proposed, leveraging Blockchain's strengths in data encryption, access control, and immutability. Each record in the Blockchain is stored as a transaction or block associated with a unique HASHCODE, ensuring data integrity by verifying the HASHCODE of all preceding records before adding new ones. Users have explicit access control, and whenever an organization accesses their KYC data, Blockchain triggers an automatic email notification, promoting transparency and accountability. Smart Contracts coded in Solidity facilitate efficient data storage and retrieval in the Blockchain. This approach ensures secure sharing of information, mitigates privacy breaches, and provides a more accountable, user-centric data management system, addressing concerns about centralized storage

Keywords: centralized servers, sensitive information, KYC, Blockchain, data encryption, access control, immutability, HASHCODE

I. INTRODUCTION

In our increasingly digitized world, the proliferation of online platforms has resulted in a substantial volume of user data, particularly through identity verification processes like Know Your Customer (KYC). However, the conventional methods of storing and sharing identity information often fall short in terms of security, leaving users vulnerable to data breaches and misuse[1] . The "Secure Sharing of Identity (KYC)" project aims to address these concerns by leveraging advanced technologies to establish a robust and trustworthy framework for managing and sharing sensitive identity information. in the context of KYC, secure sharing of identity involves implementing robust mechanisms to safeguard personal information such as identification documents, addresses, and other relevant data[2]. This helps financial institutions verify the identity of their customers accurately while maintaining data privacy and security. By employing encryption, secure channels, and authentication protocols,

institutions can securely share and verify customer identities without compromising sensitive information[3]. This process not only enhances security but also builds trust between customers and financial institutions. Overall, the secure sharing of identity for KYC is fundamental in today's digital age to combat identity theft, money laundering, and other financial crimes. It's all about striking the right balance between security, efficiency, and customer experience.

Emerging technologies play a crucial role in enhancing secure identity-sharing for KYC. Blockchain enables decentralized and transparent identity verification, reducing reliance on a single repository and mitigating risks associated with data leaks. Similarly, zero-knowledge proofs (ZKP) allow users to verify their identity without exposing personal details, ensuring greater privacy. Biometric authentication methods, such as fingerprint and facial recognition, add another layer of security by reducing dependence on static credentials[4]. With self-sovereign identity (SSI) models, users gain control over their identity data, allowing them to manage and share their credentials without relying on third- party intermediaries. These innovations contribute to a more privacy-centric and efficient KYC process.

Despite its benefits, secure identity-sharing faces challenges such as regulatory variations, user consent mechanisms, and the integration of advanced technology into legacy systems. Governments and institutions must work collaboratively to establish standardized protocols that prioritize both compliance and user privacy. Additionally, ensuring that individuals retain control over their identity data through accessible and transparent platforms will be essential for widespread adoption. Ultimately, secure KYC identity- sharing is vital in combating financial crimes like identity theft and money laundering, promoting safer digital transactions, and enhancing overall trust in the financial ecosystem

As technology continues to evolve, financial institutions must refine their approaches to strike a balance between security, efficiency, and user experience.

II. LITERATURE SURVEY

Abdullah Al Mamun; Sheikh Riad Hasan; Md Salahuddin Bhuiyan; M. Shamim Kaiser; Mohammad Abu Yousuf [6]

The Know Your Customer (KYC) process plays a crucial role in ensuring financial security and compliance by verifying the authenticity and risk profile of individuals engaging in banking transactions. However, conventional KYC procedures are often burdened by high costs, lengthy processing times, and repetitive verification steps across multiple institutions. To overcome these challenges, this work proposes a secure, efficient, and decentralized KYC verification framework using InterPlanetary File System (IPFS) and blockchain technology[9]. By leveraging blockchain’s immutability,

transparency, and decentralized nature, the system facilitates the seamless exchange of verified identity records among financial institutions while maintaining data integrity and customer privacy.

The proposed IPFS and blockchain-based KYC system transforms the traditional verification process by enabling a customer to complete KYC at one bank and securely share their identity data across multiple institutions using an encrypted hash. Upon generating a unique hash value, the customer's KYC details are stored in the IPFS network, ensuring secure, tamper-proof storage. If the customer wishes to open an account at another financial institution, they can provide their private key, allowing the bank to retrieve and verify their identity without requiring repeated document submissions. This streamlined approach reduces operational costs, prevents redundant verification efforts, and significantly enhances security against fraud and identity theft. By integrating blockchain and IPFS, the system not only ensures data confidentiality and accessibility but also fosters a trustworthy and efficient banking ecosystem, promoting a user-friendly and scalable KYC verification model for future financial applications.

Ujwala Ravale, Aditya Ramakrishnan, Anand Borkar,Suchit Deshmukh. [2]

As digitization continues to expand, individuals frequently use their personal identity documents for various services, often sharing them with third parties without explicit authorization. This widespread practice, coupled with the decentralized storage of identity information across banks,government institutions, and credit agencies, increases the risk of vulnerabilities and security breaches. The financial sector has long sought solutions to improve identity management and reduce exposure to fraud, and blockchain technology has emerged as a promising approach. By shifting KYC verification to a secure, immutable blockchain database, financial institutions can significantly reduce redundant identity checks while enhancing security and efficiency.

Blockchain's decentralized and tamper-resistant architecture ensures that once identity data is recorded, it remains unalterable, preventing fraudulent modifications or unauthorized access. This single-source KYC system would allow banks and financial institutions to collect and verify identity data from authoritative providers, consolidating information into a secure, transparent, and immutable ledger.

By using smart contracts and cryptographic encryption, the Blockchain KYC framework enables real-time identity verification, eliminating the need for repetitive document submissions. As a result, banks can streamline customer onboarding, enhance security, and build a

trusted digital identity ecosystem that reduces risks associated with identity fraud and compliance inefficiencies.

.som chart fugkeaw[3] The electronic Know Your Customer (e-KYC) system is widely adopted by banks and identity providers to streamline customer identity verification processes while ensuring regulatory compliance. With the efficiency and accessibility of cloud computing, most financial institutions implement their e-KYC systems on cloud platforms to enhance scalability and operational efficiency. However, storing sensitive identity- related documents in cloud environments introduces significant security and privacy challenges. Unauthorized access, data breaches, and insufficient encryption mechanisms pose threats to confidential customer information.

Traditional e-KYC platforms primarily rely on strong authentication protocols and standard encryption techniques to maintain security. Typically, the KYC system owner encrypts identity documents using their host's key before uploading them to the cloud. While this ensures basic data protection, it also leads to encryption dependency, complex key management, and communication overhead. To address these concerns, blockchain-based e-KYC solutions are emerging as a promising alternative, incorporating ciphertext policy attribute-based encryption (CP-ABE) and decentralized access control to enhance trust, security, and compliance. By leveraging attribute-based encryption, users gain fine-grained control over their identity data, ensuring privacy while mitigating security risks associated with centralized cloud storage. Future developments will continue to refine these methods, integrating artificial intelligence, biometrics, and distributed ledger technology to further improve secure identity verification processes in digital banking ecosystems. dependency and communication and key management overheads. In this paper, we introduce a novel blockchain based e-KYC scheme called e-KYC TrustBlock based on the ciphertext policy attributebased encryption (CP-ABE) method binding with the client consent enforcement to deliver trust, security and privacy compliance. In addition, we introduce attribute-based encryption to enable the privacy preserving and fine-grained access of sensitive transactions stored in the blockchain. Finally, we conduct experiments to show that our system is efficient and sc.Nazir Ullah; Kawther A. Al-Dhlan; Waleed Mugahed Al-Rahmi[4]

The traditional Know Your Customer (KYC) process in financial institutions faces several challenges, including security vulnerabilities, high operational costs, and inefficiencies due to redundant verification procedures. As financial services evolve, the adoption of disruptive technologies becomes essential to address these limitations. This study introduces a Hyperledger Fabric network designed to optimize the KYC

process by enhancing security, accelerating verification speed, and improving transparency in identity management.

Hyperledger Fabric, a permissioned blockchain framework, ensures secure data sharing by leveraging cryptographic identity management, smart contracts, and decentralized ledger capabilities. To evaluate the effectiveness of this system, the experiment was conducted using Hyperledger Composer, which provides a structured framework for deploying blockchain applications.

The results confirm that the proposed system significantly reduces processing time for KYC clearance, eliminates duplication of identity verification efforts, and enhances cost-efficiency. Furthermore, the immutability and auditable transparency[7] of Hyperledger Fabric reinforce compliance while mitigating fraud risks. Ultimately, integrating blockchain technology into KYC optimization establishes a more secure, efficient, and reliable financial ecosystem, aligning with future demands for digital identity verification[8] and regulatory compliance of object-oriented software engineering.

The standard is managed, and was created by, the Object Management Group. The goal is for UML to become a common language for creating models of object-oriented computer software.

In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML. The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non- software systems. The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems. The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects

III. PROPOSED WORK

Existing System: The widespread reliance on centralized systems for identity data storage presents significant security challenges, particularly in KYC processes where individuals must disclose highly sensitive information. Traditional centralized databases create a single point of failure, making them attractive targets for cybercriminals seeking unauthorized access or data manipulation. Personal details such as identification numbers, addresses, and financial records are often stored without robust encryption or access controls, leaving them vulnerable to breaches. Once compromised, this information can be exploited for identity theft, fraud, or even unauthorized surveillance, raising serious concerns about user privacy and digital security. Additionally, the lack of transparency regarding how institutions handle and protect this data

further exacerbates the risks, leaving users with little assurance that their personal information is adequately safeguarded. As threats continue to evolve, financial institutions and digital platforms must reassess traditional models of identity storage and adopt more resilient security architectures to mitigate vulnerabilities. To address these risks, decentralized identity frameworks and advanced security technologies offer promising alternatives. By leveraging blockchain-based identity management and cryptographic protections, users can retain greater control over their personal data, eliminating the need for institutions to store large volumes of sensitive information on centralized servers. Self-sovereign identity solutions allow individuals to authenticate themselves without exposing unnecessary details, reducing the chances of data misuse.

Furthermore, adopting secure multi-factor authentication methods, such as biometric verification and encrypted digital credentials, enhances security while streamlining user experiences. Financial institutions can also implement zero knowledge proof mechanisms, enabling verification without revealing actual data, thereby preserving privacy while ensuring compliance.

As digital ecosystems continue to expand, transitioning to decentralized and encrypted identity models will be crucial in safeguarding user information, fostering trust, and redefining secure data sharing in KYC processes.

Disadvantages

1. Complexity: Implementing secure identity-sharing mechanisms introduces technical and operational complexities, requiring sophisticated encryption protocols and advanced authentication frameworks. The integration of these systems can sometimes lead to delays in customer onboarding, as institutions must ensure compatibility across various platforms while maintaining strict security standards. 2.Cost: Enhancing security measures for identity sharing demands significant financial investment in cutting-edge technologies, including encryption tools, blockchain-based authentication systems, and artificial intelligence-driven fraud detection solutions. Alongside infrastructure costs, financial institutions must allocate resources to ongoing maintenance, compliance audits, and staff training, which can further escalate operational expenses. Smaller financial entities or startups may struggle to implement these solutions due to budgetary constraints, potentially limiting their ability to offer the same level of security as larger institutions. Despite the high costs, prioritizing secure identity-sharing mechanisms is essential to mitigating fraud risks and preserving consumer trust.

3.User Experience**:** While strong security measures enhance data protection, overly stringent verification protocols can create friction in the user experience. Customers may find excessive authentication steps, such as multi-factor authentication and complex verification procedures, cumbersome and time consuming.

4. A poorly optimized interface can lead to

frustration and discourage individuals from completing KYC processes, affecting customer retention rates. Financial institutions must strike a delicate balance between security and ease of use by integrating intuitive interfaces and seamless authentication methods while maintaining robust protection against potential threats.

Proposed System

The "Secure Sharing of Identity (KYC)" project is a pioneering initiative that harnesses blockchain technology to centralized data storage while providing users with greater autonomy over their personal information. As financial institutions and digital platforms continue to adopt this innovative model, they not only safeguard customer identities but also enhance trust and reliability in online interactions. With the growing need for secure and seamless identity verification, this initiative represents a crucial step toward redefining KYC processes and shaping the future of digital authentication.

Advantages: Data Protection: Secure sharing of identity data plays a vital role in safeguarding personal and financial information from unauthorized access and cyber threats. By implementing encryption techniques and decentralized identity frameworks, institutions can ensure that sensitive data remains tamper-proof and resistant to breaches.

This minimizes the risk of identity theft and fraudulent activities, reinforcing security across digital transactions. Additionally, controlled access mechanisms allow users to share only necessary details with authorized entities, preventing unnecessary exposure of personal information Additionally, employees require extensive training to manage and execute these technologies efficiently, adding to the administrative burden of financial organizations. Balancing security with efficiency is crucial to ensuring that customers experience a seamless verification process without unnecessary delays.

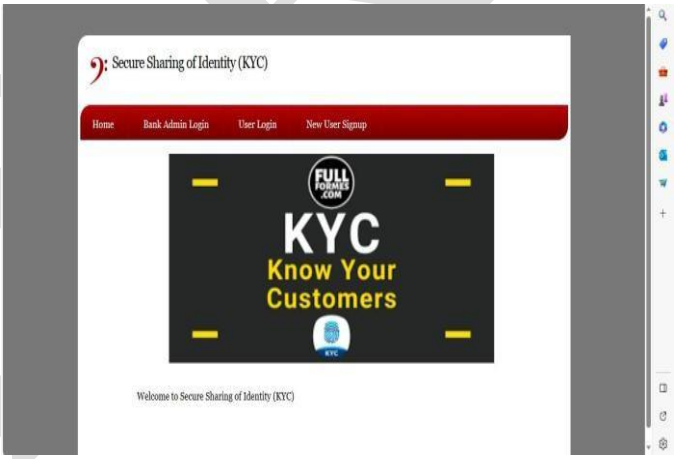
As digital ecosystems continue to grow, prioritizing robust data protection strategies helps individuals maintain privacy while benefiting from seamless and secure financial interactions.

Compliance: Financial institutions must adhere to stringent data protection regulations and KYC requirements, making secure identity sharing an essential component in regulatory compliance. By adopting advanced security frameworks, banks can ensure that their data-sharing mechanisms align with legal standards, protecting users while mitigating the risk of non-compliance penalties. Automated verification tools and blockchain-based identity management streamline compliance efforts by creating transparent and auditable data records that enhance accountability. Additionally, staying ahead of evolving regulations enables institutions to proactively address

enhance privacy, security, and efficiency in digital identity verification. Blockchain’s decentralized architecture eliminates the reliance on vulnerable centralized databases, ensuring that identity records remain tamper-proof and resistant to unauthorized access. Each identity transaction is

securely encrypted and assigned a unique identifier, creating an immutable audit trail that guarantees data integrity. Smart contracts further streamline the verification process by automating secure data exchanges, allowing only verified entities to access specific identity details. This approach not only strengthens security but also simplifies compliance for financial institutions, making KYC procedures more transparent and effective. In addition to leveraging blockchain, the project incorporates advanced notification mechanisms that empower users with real-time oversight of their identity data. Whenever an entity requests access to personal information, users receive instant alerts, allowing them to monitor and control their data transactions proactively. This transparency ensures that individuals remain informed about how their information is being utilized, reducing concerns about unauthorized access or data exploitation. Furthermore, integrating multi factor authentication and biometric verification enhances security, making unauthorized breaches nearly impossible. By combining blockchain's protective features with user-centric monitoring tools, the project fosters a more secure and resilient digital identity ecosystem. Ultimately, the "Secure Sharing of Identity (KYC)" project establishes a new standard for digital identity management by prioritizing security, privacy, and efficiency. Its decentralized framework minimizes risks associated with emerging security concerns, demonstrating their commitment to responsible data handling and reinforcing trust among stakeholders.

1. Customer Trust**:** Trust is a cornerstone of successful financial services, and secure identity sharing directly contributes to strengthening the customer-bank relationship. When individuals are assured that their identity information is handled with the utmost security and transparency, they are more likely to engage confidently with financial institutions. Features such as real-time access notifications, encrypted authentication, and decentralized data storage empower users with



control over their personal information, fostering a sense of security. This proactive approach enhances customer confidence in banking services, encouraging long-term engagement and loyalty. By prioritizing secure identity sharing, financial institutions not only protect their users but also cultivate a trustworthy and reliable reputation in an increasingly digital financial landscape.

Fig.1. Home page

ISSN: 2249-7196
IJMRR/April-June. 2025/ Volume 15/Issue 2s/528-537
Mohammad Owais Khan / International Journal of Management Research & Review

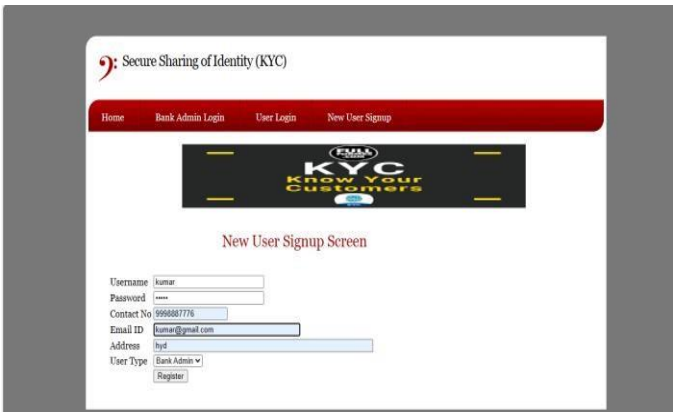


Fig.2. Signup Page

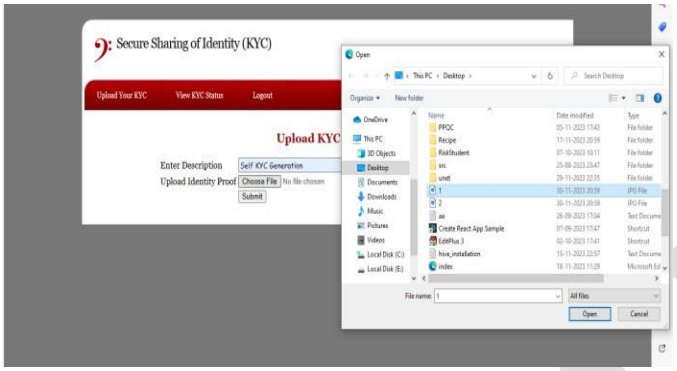


Fig.3. Upload KYC

Fig.4. Admin page

IV.CONCLUSION AND FUTURE WORK

The Secure Sharing of Identity (KYC) project represents a significant advancement in identity management, addressing vulnerabilities in traditional KYC processes by integrating blockchain technology, encryption, and decentralized verification systems. Conventional identity-sharing mechanisms often involve storing sensitive user data in multiple locations, increasing the risks of data breaches and unauthorized access. By leveraging immutable ledger technology, this project ensures that identity data remains tamper-proof, transparent, and accessible only to authorized entities, reducing reliance on centralized servers.

The use of smart contracts and automated notifications further enhances security by allowing users to retain control over their personal information while ensuring seamless identity verification. Additionally, InterPlanetary File System (IPFS) is incorporated to store encrypted KYC data efficiently, eliminating redundancy and reducing verification costs across multiple financial institutions.

The project ultimately streamlines identity authentication while minimizing fraud risks, enhancing regulatory compliance, and optimizing KYC processes for financial service providers. Looking ahead, the future of secure identity-sharing for KYC is poised to undergo significant transformations with the integration of biometrics, artificial intelligence (AI), and quantum encryption.

As cybersecurity threats evolve, the financial sector will need adaptive security models to mitigate new risks and prevent identity fraud more effectively.

The emergence of self- sovereign identity (SSI) solutions will empower individuals to manage and share their identity credentials without relying on third-party providers, enhancing privacy and security. Additionally,

governments and financial institutions may work toward standardizing digital KYC protocols to ensure interoperability across jurisdictions, simplifying compliance procedures. Ongoing advancements in machine learning- driven fraud detection and real-time threat analysis will help institutions proactively counter security vulnerabilities, fostering a more trustworthy, efficient, and user-friendly KYC ecosystem. As digital transactions become increasingly prevalent, refining identity-sharing mechanisms will be crucial to strengthening global financial security and building a resilient digital identity framework for the future.

V.REFERENCES

[1]J. P. Moyano and O. Ross, "KYC optimization using distributed ledger technology", Business & Information Systems Engineering, vol. 59, no. 6, pp. 411-423, 2017.

[2]N. K. Ostern and J. Riedel, "Know-Your-Customer (KYC) Requirements for Initial Coin Offerings", Business & Information Systems Engineering, pp. 1-17, 2020.

[3]D. De Smet and A. L. Mention, "Improving auditor effectiveness in assessing KYC/AML practices: Case study in a Luxembourgish context", Managerial Auditing Journal, 2011.

[4]R. Syah, M. K. Nasution, M. Elveny and H. Arbie, "Optimization model for customer behavior with MARS and KYC system", Journal of Theoretical and Applied Information

Technology, vol. 98, no. 13, 2020.

[5]I. Bashir, Mastering Blockchain: Distributed ledger technology decentralization and smart contracts explained, Packet Publishing Ltd, 2018.

[6]G. Wood, "Ethereum: A secure decentralized generalized transaction ledger", Ethereum project yellow paper, vol. 151, no. 2014, pp. 1-32, 2014.

[7]E. Andreoulakis et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains", Proceedings of the thirteenth EuroSys conference, pp. 1-15, 2018.

[8]W. Shbair, M. Steichen and J. François, "Blockchain orchestration and experimentation framework: A case study of KYC", IEEE/IFIP Man2Block 2018-IEEE/IFIP Network Operations and Management Symposium, 2018.

[9]N. Sundareswaran, S. Sasirekha, I. J. L. Paul, S.Balakrishnan and G. Swaminathan, "Optimised KYC Blockchain System", 2020 International Conference on Innovative Trends in Information Technology (ICITIIT), pp. 1-6, 2020.

[10]S. Nakamoto, "Re: Bitcoin P2P e-cash paper", The Cryptography Mailing List, 2008. Conference on Intelligent Computing and Control Syste