IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

KYC Verification Using Ciphertext Policy Attribute-Based Encryption and Blockchain Technology

[1]Dhinagaran.V, [2]Aruna Kumari. S

[1] Student (BE-final yr.), [2]Supervisor assistant professor,
[1]Computer Science and Engineering
[1] IFET College of Engineering, Villupuram, India

Abstract: The Know Your Customer (KYC) process plays a vital role in the financial industry, especially for banks and other financial institutions. Its main objective is to verify customers' identities, ensuring their legitimacy. This verification is essential to prevent illicit activities such as money laundering and terrorism financing, which can have severe repercussions for both the financial sector and society. Historically KYC procedures have heavily relied on manual methods that are now considered outdated and problematic. These methods entail the collection and validation of various identification documents from customers, often involving extensive paperwork and in-person visits to physical bank branches. The manual nature of these procedures results in time-consuming processes and a heightened risk of errors In contrast blockchain-based KYC verification presents an innovative solution. It offers decentralization, immutability, and heightened security. Blockchain technology makes use of advanced encryption algorithms like Ciphertext-Policy Attribute-Based Encryption (CPABE) to reinforce security measures. The immutability of blockchain ensures the integrity and accuracy of KYC data. Once customer information is recorded on the blockchain, it becomes impossible to alter or delete it without proper authorization. This eliminates the risk of fraud and data tampering, addressing common issues in traditional KYC procedures. Financial institutions can rely on the precision of customer data and their adherence to regulatory requirements.

Keywords-- Dated, Time-consuming, Less Secure, Blockchain-based KYC Verification, Decentralized, Immutable, Secure Features, CPABE Algorithm

I. INTRODUCTION

In the ever-evolving landscape of the financial sector, ensuring customer legitimacy and preventing illicit activities is a top priority. Financial institutions, particularly banks, have a substantial role in the global economy, and they carry both a moral and regulatory responsibility to protect their services from exploitation by criminals engaged in activities such as money laundering, drug trafficking, and terrorism financing.[1] To fulfill this obligation, banks implement the "Know Your Customer" (KYC) procedure, serving as a critical defense to identify and verify their customers' authenticity The KYC procedure is a fundamental component of the financial industry, essential for maintaining the integrity of the banking system. Its primary objective is to establish a thorough understanding of each customer, ensuring their true identity and the legitimacy and transparency of their financial activities. This approach enables financial institutions to mitigate the risks associated with criminal activities and comply with regulatory requirements The traditional manual KYC procedure, which has long been the standard for customer verification, faces various challenges that impede its effectiveness. [2]This manual process relies on cumbersome paperwork, time-consuming administrative tasks, and limited security measures. As financial crimes become more sophisticated, the shortcomings of this outdated method become increasingly evident. Additionally, manual KYC procedures can be burdensome for customers, involving in-person visits to physical bank branches and extensive documentation Recognizing the limitations of the traditional KYC process, the financial industry is at a crossroads, seeking innovative and secure solutions to modernize customer verification. In this pursuit, blockchain technology has emerged as a promising solution. Blockchain, a decentralized and immutable ledger, possesses features that align well with the evolving needs of KYC verification.

Blockchain's decentralized and immutable ledger ensures the highest level of security for KYC data. It guards against data breaches, tampering, and unauthorized access, contributing to a robust defence against financial crimes. The CPABE algorithm

integrated into blockchain-based KYC systems ensures that sensitive customer information remains confidential. It provides privacy controls while allowing authorized access.
The immutability of blockchain ensures the integrity and accuracy of KYC data, reducing the risk of fraud and manipulation. Blockchain-based KYC [3] offers customers a more seamless and convenient onboarding experience, promoting trust and satisfaction with financial institutions.

II. RELATED WORK

Banks have long criticized existing KYC processes for being unreliable and expensive, highlighting the need for safer and more effective verification techniques. Considering Blockchain's reputation for security and dependability, this study investigates it as a possible remedy.[6] The research focuses on secure data storage and tries to understand how incorporating Blockchain could change the banking industry, with a particular emphasis on KYC document verification. The research emphasizes how urgent it is to put in place a Blockchain-based KYC system since it should improve security and dependability while addressing issues with scalability and data privacy. In addition, the study performs a thorough examination of earlier research and studies on the topic. It is anticipated that this earlier research will offer insightful information on the benefits and difficulties of incorporating Blockchain technology into KYC procedures. Crucially, the study shows how Blockchain technology can do away with the requirement for middlemen, which will lower the likelihood of mistakes and malicious activity that are typically connected to conventional KYC procedures.

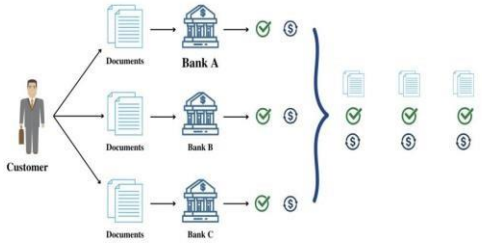

Fig1. The architecture of the existing system

The present KYC system used by the banking sector has difficulties including exorbitant fees, drawn-out onboarding, worries about data security, restricted accessibility, complicated regulations, fraud threats, and issues with transparency.[8] By lowering costs, bolstering fraud resistance, improving accessibility, enhancing data security, streamlining compliance, and boosting transparency, integrating Blockchain technology can address these issues and eventually improve the security and efficiency of the KYC process in the banking industry.
.

III. PROPOSED SYSTEM

The know-your-customer (KYC) procedure is used by banks to confirm the identity of their clients and stop criminals from exploiting them to launder money. The manual KYC procedure that is in use today is antiquated, laborious, and dangerous. The distributed, immutable, and secure nature of blockchain-based KYC verification makes it possible to overcome these limitations.[9] To improve security, blockchain also includes the CPABE algorithm. Blockchain technology is frequently used by organizations to protect sensitive data and carry out financial transactions. Financial organizations can validate KYC data by using the CPABE algorithm and blockchain technology. By using a blockchain system, the goal is to completely transform the KYC verification procedure for financial organizations. The technology would rectify the deficiencies in the current KYC procedure and lower the dangers connected to financial offenses.

3.1 Blockchain-Based KYC Authentication

To develop a decentralized ledger that securely maintains client data and verification details, the suggested approach entails integrating blockchain technology into the current KYC verification process. The immutability of blockchain technology can be utilized to maintain the integrity and permanence of data by guaranteeing that KYC information records are not altered. [10] By putting smart contracts into place, several parts of the KYC process can be automated. Particular conditions and regulations for customer data verification can be established, and actions can be carried out based on predetermined standards. This all-encompassing strategy aims to improve the KYC process's security and transparency while increasing its efficiency, which will eventually help to stop fraudulent activity and protect consumer data. This proposal aims to modernize the KYC verification process, enhancing its security, transparency, and efficiency while effectively combating financial crimes and improving customer data protection.

3.2 Pillars of Intensified KYC Measures

The incorporation of the Ciphertext-Policy Attribute-Based Encryption (CPABE)[11] method strengthens security by improving access control and precisely encrypting confidential KYC papers. Decentralizing the KYC verification process among blockchain

network nodes reduces dependency on a central authority and enhances security in general. The installation of encryption and access control measures enabled by CPABE ensures tight data confidentiality and limited access to client data. Meticulous attention is paid to compliance with pertinent financial regulations, and data protection legislation, including GDPR[14] and local privacy requirements. This all-encompassing strategy helps to ensure the privacy and regulatory compliance that are essential to contemporary financial operations, while also bolstering the security of the KYC process.

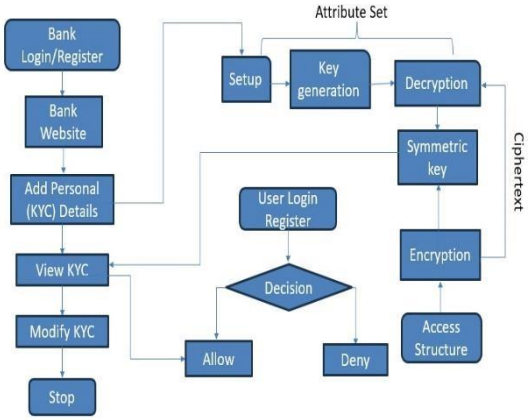

Fig2. The Architecture of the proposed system

Enhanced security measures are provided by integrating a blockchain-based system with CPABE, protecting sensitive data and thwarting illegal access.[19] Ensuring the confidentiality and proper treatment of client information is a top priority, and compliance with privacy legislation is no exception. Additionally, implementing this system allows for increased scalability and efficiency, which facilitates streamlined operations and future expansion. Furthermore, the use of cloud technology creates an adaptable and user-friendly platform that lessens the difficulties involved with key management and promotes easy access to and management of data.

IV. RESULT

Banks use KYC to stop illegal activity, but the manual procedure that was once used is laborious and antiquated. Decentralization, immutability, and increased security are provided via blockchainbased KYC, which is further reinforced by the CPABE algorithm. With this technology, financial institutions may verify KYC papers quickly and effectively.

Fig3. Account creation.

For KYC, choose the account based on accurate customer identification and documentation to comply with regulations and prevent fraudulent activities.

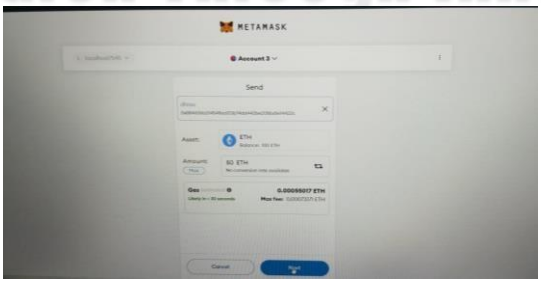

Fig4. Select the account for the transaction

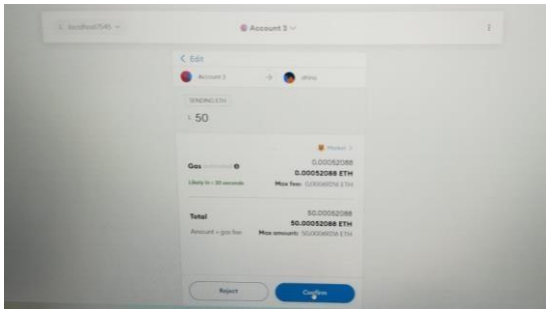

Figure 5. transaction account confirm

Figure 6. After the transaction completed

V. CONCLUSION

For banks to verify their customers and stop illicit activities like money laundering and terrorism, Know Your Customer (KYC) is essential. A more effective solution is required because the current KYC procedure is inefficient and less safe. With the use of the CPABE algorithm, blockchain-based KYC verification provides increased security, immutability, and decentralization. Secure client data verification and storage are guaranteed by this integration. Financial institutions are using blockchain for effective KYC document validation, and many other companies are using it for safe transactions and data protection. Blockchain technology offers safe and transparent recordkeeping, addressing the drawbacks of traditional KYC processes. Businesses can safely keep and exchange consumer data by implementing a decentralized identity verification system. Blockchain technology reduces vulnerabilities to cyber threats and data breaches by guaranteeing data security and privacy through sophisticated cryptographic mechanisms. The Malicious actors find it far more difficult to manipulate data thanks to the decentralized structure of blockchain. By streamlining data management and enhancing security, integrating blockchain technology into the KYC procedure ensures a more secure and trustworthy verification process.

REFERENCES

[1] Rajput, Venkatesh U. "Research on know your customer (KYC)." International Journal of Scientific and Research Publications 3, no. 7 (2013): 541-546.

[2] Kapsoulis, Nikolaos, Alexandros Psychas, Georgios Palaiokrassas, Achilleas Marinakis, Antonios Litke, and Theodora Varvarigou. "Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture." Future Internet 12, no. 2 (2020): 41.

[3] Yadav, Piyush, and Raj Chandak. "Transforming the know your customer (KYC) process using blockchain." In 2019 International Conference on Advances in Computing, Communication and Control (ICAC3), pp. 1-5. IEEE, 2019.

[4] Mondal, Prakash Chandra, Rupam Deb, and Mohammad Nurul Huda. "Know your customer (KYC) based authentication method for financial services through the internet." In 2016 19th International Conference on Computer and Information Technology (ICCIT), pp. 535-540. IEEE, 2016.

[5] Mondal, Prakash Chandra, Rupam Deb, and Mohammad Nurul Huda. "Transaction authorization from Know Your Customer (KYC) information in online banking." In 2016 9th international conference on electrical and computer engineering (ICECE), pp. 523-526. IEEE, 2016.

[6] Soni, Anuraj, and Reena Duggal. "Reducing risk in KYC (know your customer) for large Indian banks using big data analytics." International Journal of Computer Applications 97, no. 9 (2014).

[7] George, Denson, Anand Wani, and Ashutosh Bhatia. "A blockchain based solution to know your customer (kyc) dilemma." In 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1-6. IEEE, 2019.

[8] Yadav, Piyush, and Raj Chandak. "Transforming the know your customer (KYC) process using blockchain." In 2019 International Conference on Advances in Computing, Communication and Control (ICAC3), pp. 1-5. IEEE, 2019.

[9] Eduardo Demarco, André. "Analysing blockchain/distributed ledger technology in capital markets and know your customer process." Journal of Securities Operations & Custody 12, no. 1 (2020): 58-71.

[10] Drgon, Matus. "Know Your Customer using Distributed Ledger Technology."

[11] Ratnawat, Niraj, Saujanya Pandey, Rudresh Paradkar, and Soumi Banerjee. "Optimizing the KYC Process using a Blockchain based approach." In ITM Web of Conferences, vol. 44, p. 03039. EDP Sciences, 2022.

[12] 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.

[13] Malhotra, Diksha, Poonam Saini, and Awadhesh Kumar Singh. "How blockchain can automate KYC: systematic review." Wireless Personal Communications 122, no. 2 (2022): 19872021.

[14] Thavanathan, Jenitha. "Process Innovation with Blockchain in Banking-A case study of how Blockchain can change the KYC process in banks." Master's thesis, NTNU, 2017.

[15] Choi, Nakhoon, and Heeyoul Kim. "A Blockchain-based user authentication model using MetaMask." Journal of Internet Computing and Services 20, no. 6 (2019): 119-127.

[16] Choi, Nakhoon, and Heeyoul Kim. "A Blockchain-based user authentication model using MetaMask." Journal of Internet Computing and Services 20, no. 6 (2019): 119-127.

[17] Nagendra, Chandini. "A decentralized service for personal data privacy protection." PhD diss., California State University, Sacramento, 2020.

[18] Sundareswaran, N., S. Sasirekha, I. Joe Louis Paul, S. Balakrishnan, and G. Swaminathan. "Optimised KYC blockchain system." In 2020 International Conference on Innovative Trends in Information Technology (ICITIIT), pp. 1-6. IEEE, 2020.

[19] Zhang, Yichen, Jiguo Li, and Hao Yan. "Constant size ciphertext distributed CP-ABE scheme with privacy protection and fully hiding access structure." IEEE Access 7 (2019): 4798247990.

[20] Li, Chunhua, Jinbiao He, Cheng Lei, Chan Guo, and Ke Zhou. "Achieving privacy-preserving CPABE access control with multi-cloud." In 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom), pp. 801-808. IEEE, 2018.