Enabling Trust and Privacy Preserving e-KYC System Using Blockchain

Mrs.M. Ashwitha Reddy[1], R Naveen[2], Potlapalli Neeraj Rao[2],K Sree Kalyani[2]
[1]Asst.Professor, Computer Science and Engineering, CMR Engineering College, medchal, T.S, India,
[2]B. Tech,Computer Science and Engineering,CMR Engineering College,medchal, T.S,India

Abstract: The electronic know your customer (e-KYC) system allows financial institutions or identity providers to set up a procedure for reliant parties to verify a client's identification. The majority of banks operate their e-KYC system on the cloud because to the efficient resource usage and high degree of accessibility and availability of cloud computing. In essence, the important problem becomes the security and privacy of e-KYC-related data kept in the cloud. Strong authentication and conventional encryption are often used by existing e-KYC systems to satisfy their security and privacy requirements[1]. According to this paradigm, the file is encrypted using the host's key and uploaded to the cloud by the owner of the KYC system. This approach results in communication, key management, and encryption dependence overheads. In this research, we present the e-KYC TrustBlock, a unique blockchain-based e-KYC scheme that binds client consent enforcement with the ciphertext policy attribute based encryption (CP-ABE) technique to achieve compliance in terms of trust, security, and privacy.

Additionally, we introduce attribute-based encryption to make it possible for sensitive transactions stored in the blockchain to be accessed with great precision while maintaining privacy[2]. Finally, we run tests to demonstrate the practical scalability and efficiency of our system.

1. INTRODUCTION

Electronic-Know Your Customer (e-KYC) is a service that banks or financial institutions (FIs) provide to their clients as part of a virtual banking operation including identity identification and verification online in order to increase cost effectiveness and customer satisfaction. FIs may electronically verify their customers' identities and access KYC information for both individual and corporate clients using the e-KYC system. Financial institutions may either use pre-made e-KYC software that has all essential features, or they can create their own. They may then choose to install the system as a cloud-based or on-

premise solution. The majority of businesses have chosen the cloud as their preferred platform for storing their systems and data due to the trend of the outsourcing model.

When compared to host-based e-KYC authentication, which requires that documents be verified through a centralised host, a cloud-based e-KYC system offers a more effective and adaptable authentication method[3]. As a result, there is a single point of failure and a bottleneck in the flow. Due to the provider's complete control over all system transactions, the traceability of the validated transaction is also restricted. But many potential businesses worry about the security and privacy issues with cloud-based solutions. This is due to the fact that any public cloud tenant, including cloud service providers (CSPs), may examine client data documents stored in the e-KYC system on the cloud[4]. Most banks and FIs must install an encryption method in addition to the strong authentication capability offered by the CSPs in order to handle this issue.In order to do this, banks and FIs using the e-KYC system must encrypt the e-KYC data files before uploading them to the cloud. When one of the relying parties requests verification, the host party has two options: either it can decrypt the file and confirm the results of the verification to the requestor, or it can send the requestor a copy of the encrypted files along with the decryption key.

A Description Of The Project: By providing a safe and effective blockchain-based eKYC documents registration and verification procedure using lightweight key cryptography protocols operated in the cloud Interplanetary File System (IPFS), we hope to fill such research gaps in this work. We create a smart contract to produce and enforce the user's consent that must be digitally signed in order to satisfy the fundamental privacy need surrounding the user's consent gathering.The consents will be consistently saved in a blockchain with tamper-proof functionality that is advantageous for auditing.In order to address the problem of data privacy, we provide an improved cryptographic protocol that uses symmetric encryption with public key encryption to encrypt client credential files and ciphertext policy attribute-based encryption (CP-ABE) to encrypt blockchain transactions.Due to the one-to-many encryption and fine-grained access control that CP-ABE offers, it enables several FIs to access shared encrypted transactional data on the blockchain of the same client depending on the established access policy. To allow effective reencryption based on a simpler policy tree structure, we specifically developed the policy update method.

Finally, users can update their e-KYC information with any banks or FIs using the blockchain using our system. The relevant smart contract synchronises the new data when the revised e-KYC data has been published in the ledger.

2. LITERATURE SURVEY

2.1 Existing System

Smart contracts and blockchain technology are now being used in a wide variety of applications. Numerous works have specifically suggested a blockchain-based framework for identification and authentication [5], and it has been shown that a blockchain is effective for managing identification and authentication. However, the e-KYC procedure is much more involved than a straightforward authentication task. Instead, it requires numerous FIs, a specialised blockchain platform, secure credential registration, KYC document management, secure and lightweight client verification. Additionally, the KYC system needs to be protected against new types of remote and spoofing attacks [6]. Recent studies on blockchain-based e-KYC have concentrated on developing a framework for safe user identity management and credentials verification as well as minimising communication costs when financial institutions engage.

A proof-of-concept (PoC) method for blockchain-based KYC was put up by Shabair et al. suggested method was tested on the Grid'5000, a large distributed platform, in private blockchain scenarios. In [7], Norvill et al. introduced a method that streamlines the KYC process by enabling automated and permissioned document distribution via the blockchain. A Hyperledger Fabric network for KYC optimisation was suggested by Allah et al. in . This concept gives customers complete ownership of the smart contracts that keep their client KYC data in the distributed ledger database. However, the security and key management issues surrounding the KYC process were not addressed in these works. In [8], Kapsoulis et al. suggested leveraging IPFS and smart contracts to construct an e- KYC system. In this work, the collection of smart contacts is used to perform KYC document actions such as creation, reading, updating, and deletion. The IPFS and private contract methods are used to store the KYC papers. By specific blockchain nodes with administrator privileges, the security of the KYC transaction is managed. To safeguard the KYC data, however, there is no

encryption used.Several research works have focused on CP-ABE as a privacy-preserving technique used to secure blockchain databases [9]. According to a distributed attribute-based encryption (BDABE) system described by Bramm et al. suggested attributes may be dynamically added to or removed at any moment by a blockchain transaction. To assign the characteristics to the users, the suggested approach provides mapping between several attribute authorities. It provides the adaptability to allow reliable and effective maintenance of user characteristics in the blockchain system. Using blockchain technology and CP-ABE, Fan et al. presented a traceable data exchange mechanism in . The CP-ABE technique is used to encrypt data in this scheme, and a secret key may be produced using the system settings found in the private blockchain. The blockchain enables data owners to identify data consumers and manage data sharing based on a preset access policy.A CP-ABE methodology was used by Yuan et al. [10] and Wu et al. to offer data privacy protection and fine-grained sharing in the blockchain system. These systems handle the various access rights by enforcing the access rules and recording any data changes on the blockchain. The system offers audit trails to facilitate the traceability of cryptographic operations and transaction activities in the event that there is any key abuse scenario brought about by any malevolent users or authorities.A traceable attribute-based encryption with dynamic access control (TABE-DAC) method based on the CP-ABE based linear secret sharing scheme (LSSS) and blockchain was suggested by Guo et al. The suggested approach enables flexible policy updating, tracing of users' private key leakage, and fine-grained sharing of encrypted private data on cloud. To lower the calculation cost of such procedures, the authors added a hash function to the key and ciphertext creation process. Gao et al. suggested a blockchain, secure ciphertext policy, attribute concealing access control mechanism.The data kept on the blockchain is secured using the CP-ABE. However, this scheme implements crypto using composite order groups, which results in high computation costs.

2.2Proposed System

In this study, we provide a lightweight key cryptographic protocol-based blockchain-based electronic KYC document registration and verification procedure that is operated in the cloud Interplanetary File System (IPFS) to solve such research gaps. We create a smart contract to produce and enforce the user's consent that must be digitally signed in order to satisfy the fundamental privacy need surrounding the user's consent gathering. The consents will be consistently kept on a blockchain with tamper-proof capabilities that is advantageous for

auditing.In order to address the problem of data privacy, we provide an improved cryptographic protocol that uses symmetric encryption with public key encryption to encrypt client credential files and ciphertext policy attribute-based encryption (CP-ABE) to encrypt blockchain transactions. Due to the one-to-many encryption and fine-grained access control that CP-ABE offers, it enables several FIs to access shared encrypted transactional data on the blockchain of the same client depending on the established access policy. To allow effective reencryption based on a simpler policy tree structure, we specifically developed the policy update method. Finally, users can update their e-KYC information with any banks or FIs using the blockchain using our system. The relevant smart contract synchronises the new e-KYC data when the revised data has been published in the ledger.

2.2IDENTITY MANAGEMENT SYSTEM USING BLOCKCHAIN

A decentralised database powered by blockchain technology connects several nodes through a communication network. Blockchains, which enable decentralised transaction management and many parties to verify, execute, and store data, are built using cryptographic mechanisms, data storage, networking, and incentive systems. In particular, the blockchain maintains information about transactions, and each finished block is given a cryptographic ID called a hash value. Since 2009, Satoshi has been introducing the blockchain-based BitCoin concept.As a result, it gained recognition as a tested technology that makes safe and distributed cryptocurrency possible.With "smart contracts," blockchain technology can enhance its technical use and implementation flexibility in addition to the decentralised storage and sharing of transactional data. Smart contracts are self-executing programmes that impose predetermined actions when a certain set of circumstances are satisfied . Blockchain is currently used in various application domains, including KYC platform, because to its advantages of decentralised model, transparency, traceability, and immutability.

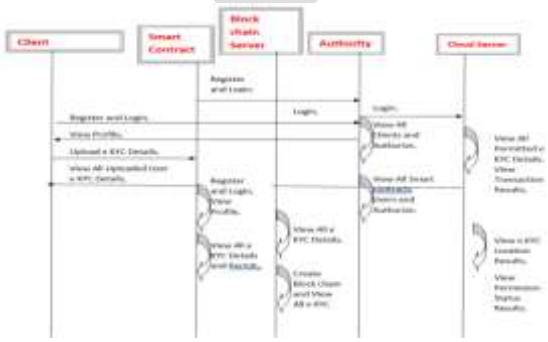

Fig 1: System Flow

3. SYSTEM ANALYSIS&DESIGN

3.1SYSTEM OVERVIEW

The following entities make up the system model: an authority, customers, financial institutions, IPFS, a blockchain, and three smart contracts.

• Authority: The authority creates the system's master private key MSK as well as the public parameter PK.

The authority releases PK and keeps the MSK a secret from subscribers. Each financial institution (FI) receives a secret key that was created by the authority using the CP-ABE procedure.

• Clients are the people who join the blockchain-based KYC at financial institutions. Each client's key pair is used to encrypt and decode the information related to their credentials. The FI must get the client's digitally signed permission before allowing the credentials to be stored in any FI's database or in the cloud system.

• IPFS is a cloud database that houses KYC documents that are encrypted and linked to each user account. It is used to create cryptocurrency transactions using the user's credentials. It keeps the address of the hash value of the client credential files, which are encrypted in the IPFS storage, in a distributed hash table (DHT).

• The transactions of all KYC-related activities are stored on a blockchain. Clients' important transactions are all encrypted. Based on hash values and encryption, the data on the blockchain is impenetrable, which also deters certain illicit acts.

• All KYC procedures are managed and automated by smart contracts. In our system, there are three smart contracts: (1) Register contract, which authenticates users, registers new users, and uploads encrypted credentials to IPFS; (2) Master contract, which manages client

profiles, maintains the hash value of every client's citizen ID for interacting with IPFS, and generates e-consent; and (3) Verify contract, which performs KYC verification.

3.3 System Architecture: By sending a read command to FB, any user may get details on the network architecture. The latter replies with the whole transcript of B. The users that share a payment channel keep a local copy of the current value rather than publishing it. Each user is aware of the PCN payment costs that other users have set. The public keys of each node are known to one another.

We avoid talking about other network issues like blocked nodes and specific channel congestion.

These problems are not related to the one this study is trying to solve. Concurrent payment issues may be solved using the recommendations made in [22].

We take into account the paradigm of bounded synchronous communication [35]. The number of entries in B, represented by the symbol |B|, correlates to time in this model. Rounds of fixed communication are used to split the time. It is expected that within a finite number of execution steps, every message a user sends in a round will reach the designated recipient. A user's lack of communication is shown by the absence of a message in a round.

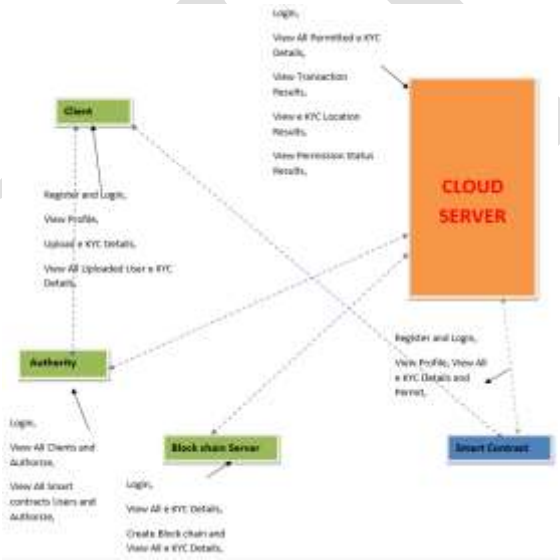

Fig 2 : System Architecture

3.4 Data Flow Diagram : Whenever a new system is developed, user training is required to educate them about the working of the system so that it can be put to efficient use by those

for whom the system has been primarily designed. For this purpose the normal working of the project was demonstrated to the prospective users. Its working is easily understandable and since the expected users are people who have good knowledge of computers, the use of this system is very easy.

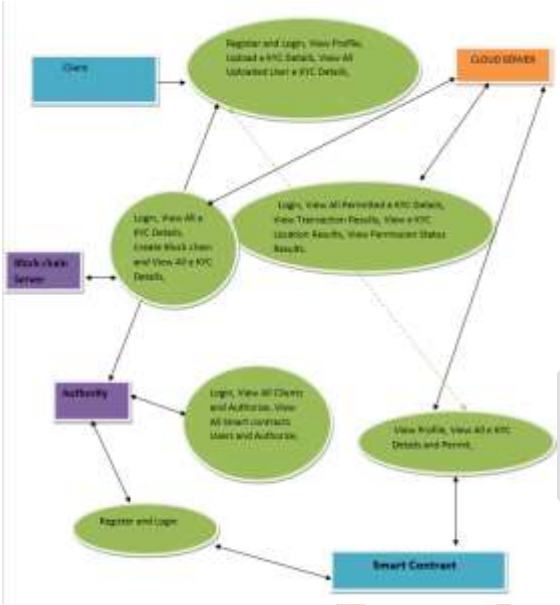

Fig 3: Data Flow Diagram

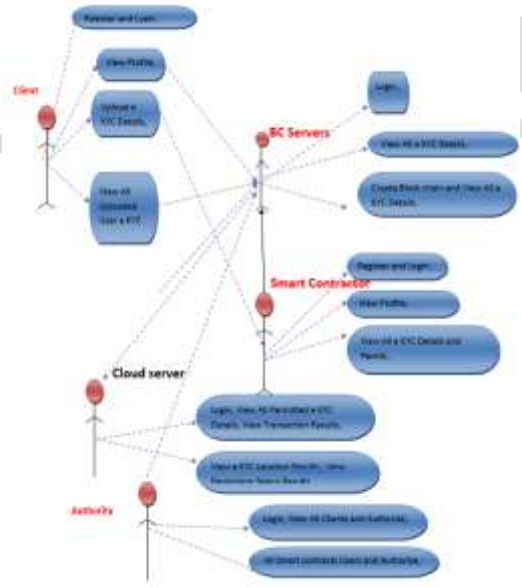

Fig 4 Use Case UML Diagrams

4. CONCLUSION

We have outlined the blockchain-based, privacy-preserving e-KYC solution. Our suggested solution offers user consent enforcement together with secure, decentralised authentication and verification of the e-KYC procedure. In our system, symmetric key and public key encryption ensure the privacy of both customers' identity documents stored in the cloud, while symmetric key encryption and CP-ABE encrypt sensitive transaction data stored in the blockchain. Our system also enables the consumer or the data owner to change the KYC information.

In order to provide dynamic access authorisation, we also created an access policy updating algorithm. In order to assess our scheme's performance, we conducted a comparison with relevant works in terms of computation cost, communication cost, and performance. According to the trial findings, our scheme performs better than other schemes in terms of performance, complete KYC compliance features, and scalable access control.

5. FUTURE SCOPE

In our next research, we'll examine a bigger sample of data in a genuine cloud environment and gauge the system's capacity to handle a significant volume of e-KYC registration and verification requests. Additionally, we will research a method that uses the blockchain's searchable encryption feature to enable batch verification of e-KYC transactions.

6. REFERENCES

[1] Y. Zhong, M. Zhou, J. Li, J. Chen, Y. Liu, Y. Zhao, and M. Hu, ‘‘Distributed blockchain-based authentication and authorization protocol for smart grid,’’ Wireless Commun. Mobile Comput., vol. 2021, pp. 1–15, Apr. 2021, doi: 10.1155/2021/5560621.

[2] RR Kodipaka, S Polepaka, M Rafeeq

International Journal of Computer Applications 125 (15), Design of sentiment analysis system using polarity classification technique.

[3] Mrutyunjaya S Yalawar, Rakesh Kumar Saini, K Vijaya Babu, Sheo Kumar, Smart Farming Using Internet of Things (IoT) Technologies, 2022/5/16, ICCCE 2021: Proceedings of the 4th International Conference on Communications and Cyber Physical Engineering, 115-122, Springer Nature Singapore

[4] Suriya Begum, Farooq Ahmed Siddique, Rajesh Tiwari, "A Study for Predicting Heart Disease using Machine Learning", Turkish Journal of Computer and Mathematics Education, Vol. 12, Issue 10, 2021, pp 4584-4592, e-ISSN: 1309-4653.

[5] W. Shbair, M. Steichen, and J. François, ''Blockchain orchestration and experimentation framework: A case study of KYC,'' in Proc. 1st IEEE/IFIP Int. Workshop Manag. Managed Blockchain (Man Block), Jeju Island, South Korea, Aug. 2018, pp. 23–25.

[6] R. Norvill, M. Steichen, W. M. Shbair, and R. State, ''Demo: Blockchain for the simplification and automation of KYC result sharing,'' in Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC), May 2019, pp. 9–10, doi: 10.1109/BLOC.2019.8751480.

[7] T. Mikula and R. H. Jacobsen, ''Identity and access management with blockchain in electronic healthcare records,'' in Proc. 21st Euromicro Conf. Digit. Syst. Design (DSD), Prague, Czech Republic, Aug. 2018, pp. 699–706.

[8] M Rafeeq, CS Kumar, NS Chandra
International Journal of Simulation--Systems, Science & Technology 19 (4) A Novel Framework for Road Transportation Systems using Cloud Computing.

[9]. A New Approach For Secure Login Method And Forestall Cyber Bulling In Social Media.In: K Vijaya Babu, Mrutyunjaya S Yalawar Shantala S Yalawar International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878,Volume-8, Issue 1C2, May 2019

[10] D Palanivel Rajan, CN Ravi, Desa Uma Vishweshwar, Edem Sureshbabu, A Review on Various Cloud-Based Electronic Health Record Maintenance System for COVID-19 Patients, 2023/3/9, Advances in Cognitive Science and Communications: Selected Articles from the 5th International Conference on Communications and Cyber-Physical Engineering (ICCCE 2022), Hyderabad, India, 151.Springer Nature.