Enabling Trust and Privacy Preserving E-Kyc System Using Blockchain

Veera Sabari Shree.J , Sharulatha .N.S, Sowmiya .K, Sherine.A

Department of computer science and Engineering

PSNA College of Engineering and Technology (Autonomous)-Dindigul

1.ABSTRACT

A cloud-based e-KYC system provides a more efficient and flexible authentication method compared to the host based e-KYC authentication method where documents need to be validated via the centralized host. Essentially, the security and privacy of e-KYC related documents stored in the cloud becomes the crucial issue. Existing e-KYC platforms generally rely on strong authentication and apply traditional encryption to support their security and privacy requirement. In this model, the KYC system owner encrypts the file with their host's key and uploads it to the cloud. This method induces encryption dependency and communication and key management overheads. In this paper, we introduce a novel blockchain-based e-KYC scheme called e-KYC Trust Block based on the ciphertext policy attribute based encryption (CP-ABE) method binding with the client consent enforcement to deliver trust, security and privacy compliance.

2.INTRODUCTION

Electronic-Know Your customer (e-KYC) is a service that banks or financial institutions (FIs) provide virtual banking operation related to authentication and verification of identity electronically to their customers for improving cost efficiency and customer satisfaction. The e-KYC system enables FIs to electronically verify their customer identity and retrieve KYC data for both individual and corporate clients. To implement the e-KYC system, financial institutions either employ off the-shelf e-KYC software fully equipped with necessary functions or develop their own. Then, they can deploy the system as an on-premise or a cloud-based model. Due to the trend of the outsourcing model, most enterprises have adopted the cloud as the preferred platform for housing their system and data. A cloud-based e-KYC system provides a more efficient and flexible authentication method compared to the hostbased e-KYC authentication method where documents need The associate editor coordinating the review of this manuscript and approving it for publication was Mansoor Ahmed . to be validated via the centralized host. This causes a traffic bottleneck and single point of failure problem. Also, the traceability of the verified transaction is limited since all transactions occurring in the system are entirely managed by the provider. Nevertheless, the security and privacy issue of a cloud-based solution is a concern for many potential enterprises. This is because e-KYC system located on the cloud store customer data documents and it might be viewed by any public cloud tenants or even the cloud service providers (CSPs). To address this concern, most banks and FIs need to implement an encryption mechanism in addition to the strong authentication feature provided by the CSPs. To this end, banks and FIs possessing the e-KYC system need to encrypt the e-KYC data files before they are uploaded to the cloud. When the relying parties request for verification, the host party can either perform the verification by either decrypting the file and sending back the confirmation of the verification result to the requestor or transmitting the copy of encrypted files along with the decryption key to the requestor. This first approach introduces the overheads related to the verification process, communication, and centralized decryption while the latter approach needs to handle key management especially secure key sharing. Specifically, key revocation and key re-generation in the cloud e-KYC environment have not been addressed by any research works. If the client would like to withdraw his consent from any banks or FIs, they have no right to store the client's identity data anymore. Accordingly, the data should be completely deleted and the decryption key needs to be revoked. Any banks or FIs sharing the revoked key need to regenerate a key to fully guarantee that unauthorized banks or FIs cannot access the client's data stored in the cloud. In addition to the aforementioned problems, exiting cloud e-KYC platforms do not provide shared information for the transaction occurring in the e-KYC verification available for traceability. Recently, blockchain technology has attracted huge interest by a number of enterprises in many industries including the banking and financial sector. There is a growing interest in using e-KYC platforms that use blockchain and cloud system. Blockchain technology truly promotes the decentralized system enabling transparency, agility, trustworthiness, and cost effectiveness for transaction processing and management in multi-user and multi-provider environment. In the blockchain system, a smart contract which is a self-executing program that can be implemented on the blockchain enables the automated execution of system logics or functions efficiently. This empowers the usability and programmability of any systems running on the blockchain network. For years, a number of research works related to blockchain-based KYC have proposed to deliver the decentralized authentication and verification process. However, there are shortcomings that have not been fully solved by existing works. First, there are no works that provide electronic client's consent function with the solid nonrepudiation property which is an essential requirement of privacy regulations such as General Data Protection Act (GDPR) in the KYC registration process. Second, most existing works overlook the privacy of transaction stored in the smart contract and blockchain. In addition to the identity or credential documents that are encrypted on the cloud storage, the privacy of all e-KYC processing transactions such as transaction status sharing, data origin authentication, and smart contract that contains personal data stored in the blockchain should be preserved. Finally, most works have a limited feature to allow the customers to access and update their credentials located on the cloud service paid by the FI. In this paper, we aim to address such research gaps by introducing a secure and efficient blockchain-based e-KYC documents registration and verification process with lightweight key cryptographic protocols run in the cloud Interplanetary File System (IPFS). To facilitate the foundational privacy requirement regarding the user's consent collection, we develop a smart contract to generate and enforce the consent to be digitally signed by the customer. The consents will be systematically stored in a blockchain having tamper-proof property which is useful for auditing. Regarding the data privacy issue, we propose an optimized cryptographic protocol by applying symmetric encryption with public key encryption to encrypt the customers' credential files and employ the ciphertext policy attribute-based encryption (CP-ABE) to encrypt the blockchain transactions. Since CP-ABE provides a one-to-many encryption with fine-grained access control, it allows several FIs to access common encrypted transactional data in the blockchain of the same client based on the access policy defined. Specifically, we devise the policy update algorithm to enable efficient re-encryption based on a less complicated policy tree structure. Finally, our system allows users to update their e-KYC data with any banks or FIs engaging in the blockchain. The updated e-KYC data is broadcasted in the ledger and the synchronization of the updated data is done by the responsible smart contract.

1.2 METHODOLOGY

In existing system, blockchain-based identification and authentication framework have been proposed and it has been demonstrated that a blockchain is efficient for identification and authentication management. However, the process of e-KYC is much more complicated than simple authentication task. Rather, it involves secure credential registration, KYC document management, secure and lightweight verification process between clients, multiple FIs**,** and a dedicated blockchain platform. In addition, new kinds of remote and spoofing attack to the KYC system need to be countered. Recent research works related to a blockchain-based e-KYC focus on devising a framework for secure user identity management and credentials verification as well as optimizing the communication overhead of the interaction among financial institutes.

1.1 2023 OBJECTIVE

Electronic-Know Your customer (E-KYC) is a service that banks or financial institutions (FIs) provide virtual banking operation related to authentication and verification of identity electronically to their customers for improving cost efficiency and customer satisfaction.

1.2 SCOPE

The E -KYC system enables FIs to electronically verify their customer identity and retrieve KYC data for both individual and corporate clients. To implement the e -KYC system, financial institutions either employ of the -shelf e -KYC software fully equipped with necessary functions or develop their own. A cloud -based e -KYC system provides a more efficient and flexible authentication method compared to the hostbased E -KYC authentication method where documents need.

1.3 BENEFITS

- Easier to communicate between applications.
- Easier to distribute information to more consumers.
- Rapid development.
- Web services make it easier to communicate between different applications.
- They also make it possible for developers to reuse existing web services.
- Instead of writing new ones.

1.4 BACKGROUND

This section describes the concept of blockchain used to support identity and access management system. Then, we provide the basic theory of CP-ABE.

2.LITERAT2URE SURVEY

1.Enabling Trust and Privacy-Preserving e-KYC System Using Blockchain S. Fugkeaw, "Enabling Trust and Privacy-Preserving e-KYC System Using Blockchain," in IEEE Access, vol. 10, pp. 49028-49039, 2022, doi: 10.1109/ACCESS.2022.3172973. In this model, the KYC system owner encrypts the file with their host's key and uploads it to the cloud. This method induces encryption 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 attribute-based encryption (CP-ABE) method binding with the client consent enforcement to deliver trust, security and privacy compliance. The electronic know your customer (e-KYC) is a system for the banking or identity provider to establish a customer identity data verification process between relying parties. Due to the efficient resource consumption and the high degree of accessibility and availability of cloud computing, most banks implement their e-KYC system on the cloud. Essentially, the security and privacy of e-KYC related documents stored in the cloud becomes the crucial issue.

2. Distributed blockchain-based authentication and authorization protocol for smart grid Y. Zhong, M. Zhou, J. Li, J. Chen, Y. Liu, Y. Zhao, et al., "Distributed blockchain-based authentication and authorization protocol for smart grid", Wireless Commun. Mobile Comput., vol. 2021, pp. 1-15, Apr. 2021. Meanwhile, considering the additional interference torque generated by the afterbody to the vehicle in the separation process, a control system for interference suppression of the booster separation is designed. Simulation results verify that the designed control system can rapidly suppress the booster separation interference when the dynamic pressure is about 150 kPa and the vehicle has the static instability of 5%, thereby realizing the stable attitude of the vehicle. A method of variable structure switching-based control is proposed in this paper for rapid suppression on hypersonic vehicle booster separation interference. Switching control systems in real time according to state changes caused by flow field interference, the method can keep the attitude stability of hypersonic vehicle booster separation under the high dynamic pressure of static instability.

3. Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology A. A. Mamun, A. Al Mamun, S. R. Hasan, S. R. Hasan, M. S. Bhuiyan, M. S. Bhuiyan, et al., "Secure and transparent KYC for banking system using IPFS and blockchain technology", Proc. IEEE Region Symp. (TENSYMP), pp. 348-351, Jun. 2020. The proposed system allows a customer to open an account at one Bank, complete the KYC process there, and generate a hash value using the IPFS network and share it using the blockchain technique. Upon receiving the private key, any Bank/financial organization can retrieve, store customer data (i.e., KYC) securely using IPFS network if the customer wishes to open another account in that Bank/financial organization. The proposed system can save time, money, and repetitive work during the KYC process when someone tries to open an account at multiple Banks. The know your customer or know your client (KYC) is a guideline for the banking system to validate a customer using identity, appropriateness, risk assessment in establishing a banking relationship. With the growing concern of security, the KYC process is complex and involves a high cost for completing for a single customer. In this work, we propose an economical, swift, secure, and transparent platform for KYC document verification for the Banking system through InterPlanetary File System (IPFS) and blockchain technology.

3. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

In existing system, blockchain-based identification and authentication framework have been 2023 proposed and it has been demonstrated that a blockchain is efficient for identification and authentication management. However, the process of e-KYC is much more complicated than simple authentication task. Rather, it involves secure credential registration, KYC document management, secure and lightweight verification process between clients, multiple FIs, and a dedicated blockchain platform. In addition, new kinds of remote and spoofing attack to the KYC system need to be countered. Recent research works related to a blockchain-based e-KYC focus on devising a framework for secure user identity management and credentials verification as well as optimizing the communication overhead of the interaction among financial institutes.

3.2 PROPOSED SYSTEM

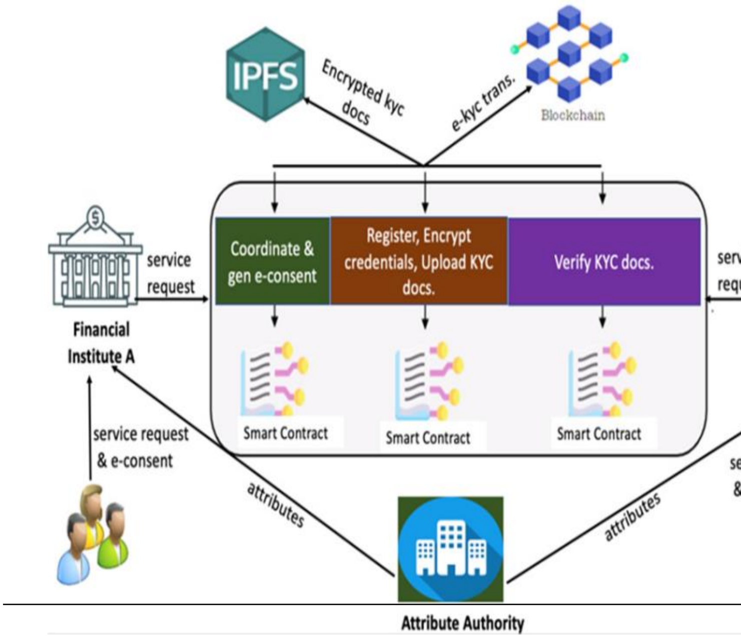
In proposed system, we provide the first attempt applying CP-ABE for a blockchain-based KYC management with the user-controlled capability for protecting sensitive data contained in the blockchain. Existing schemes focus on protecting data files shared in cloud while the privacy of transaction data in the blockchain is overlooked. In addition, none of the above research has addressed the practical security and privacy issue with the aim of achieving both efficient security and privacy management compliance related to customer consent using digital signature in the e-KYC system.

4.SYSTEM ARCHITECTURE

4.1.SYSTEM ARCHITECTURE

A system architecture or systems architecture is the computational design that defines the structure and/or behavior of a system.

An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system. It defines the system components or building blocks and provides a plan from which products can be procured, and systems developed , that will work together to implement the overall system.



4.2 CIPHERTEXT POLICY ATTRIBUTE-BASED ENCRYPTION (CP-APE)

Bethencourt et al. [11] originally proposed the formal concept of ciphertext policy attribute-based encryption in 2007. Technically, the core construct of CP-ABE construct is relied on bilinear maps where its mathematical formulation is shown below. Bilinear Map: Let G0 and G1 be two multiplicative cyclic groups of prime order p and e be a bilinear map e : G0×G0 → G1. Let g be a generator of G0. Let H : {0, 1} ∗ → G0 be a hash function that the security model is in random oracle. The bilinear map e has the following properties: 1. Bilinearity: for all u, v ∈ G1 and a, b ∈ Zp, e(ua , v b) = e(u, v)ab 2. Non-degeneracy: e(g, g) 6= 1. Definition 1: Let a set {P1, P2, . . . , Pn} be given. A collection A ⊂ 2 {P1,P2,... ,Pn} is monotone if ∈ ∀B,C : if B ∈ A and B ⊂ C −→ CA. An access structure is a monotone collection A of nonempty subsets of {P1, P2, . . . , Pn}, i.e. A ⊂ 2 {P1,P2,... ,Pn }/∅. Definition2 (Access Tree T [11]): Let T be a tree representing an access structure. Each non-leaf node of the tree represents a threshold gate, described by its children and a threshold value. If numx is the number of children of a node x and kx is its threshold value, then 0 <

kx ≤ numx . When kx = 1, the threshold gate is an OR gate and when kx = numx , it is an AND gate. Each leaf node x of the tree is described by an attribute and a threshold value kx = 1. The kofn threshold gate is also allowed in T, in this case kx = k where k is the threshold value determined in the kofn gate.

Algorithm 1 Register

Procedure

struct AESData{bytes encryptedKey;}

function registerIdentity (clientAddress, userId, clientName, country, Image, PassportID, userAccount) Userstorage client= clients[userAddress];

//to check that the client did not already exist require(! client.set);

//store the client users

[userAddress] = Client({ id: clientId, name: clientName, publickey: publicKey, Image: CrendenFile }); emit EncryptFiles(Image, AESKey);

EncryptKey(AESKey, PubKeyclient_ID)

//Store a collected image and encrypted key ESK into IPFS distributed system with a hash of CredenFileID FileID = StoreImage(EncCrenden) *//Transform the ID and other personal info (e.g., PassportID to a new hash value)*

h = TransformData(CredenFileID, userId) ContractAddress = Deploy(clientId, clientAddress, clientAccount, h) } function deleteIdentity(clientAddress) external;

functionstoreClientDataHash(cientId, dataHash)

public { clientDataHashes[clientId] = dataHash;

end procedure

Algorithm 2 Create e-Consent

Input: Parameter P = (pu1 , . . . , pun)

where p is the purpose for processing personal e-KYC credentials Creden, parameter CP denotes the consent process which can be the consent used for registration stage (InReg) or the consent used for verification stage (InVer), DS is the data subject or the client, FI is the financial institute, S is the sensitivity level which can be Low, Medium, High or Critical

Output:e-Consent C C ← e-Consent() for each purpose

P ∈ (p1, . . . , pn) ^consent process CP do P,

CP ←pu, CP{InReg, InVer}

S ← SensitivityLevel(Low, Medium, High, Critical)

CD=ConsentData(Creden, FI,DS)

return C ← Consent (CD, P, CP)

The above algorithm is used to create e-consent where the purpose such as storing, disclosing, transferring, and exporting credential data of the data subject or client is specified for the registration or verification processing transaction. The output is an e-consent generated to ask the client to digitally sign. Below is the function for enforcing e-consent to the client.

Algorithm 3 Enforce e-Consent

Procedure Function enforce_e-consent(clientId)

if (msg.sender!= owner) {throw; }

let privateKey = new clientId(accounts[selectedAccountIndex].key, 'hex')

ifconsent==true then

registerIdentity sign = registerIdentity(PrivKClient_id)

```
end if
if consent==false {throw;}
}
end procedure
```

Algorithm 4 Verification Procedure

```
VerifyProcess(requestID, citizenID)
emit DecryptFile(h, privatekey);
FileEnc = GetImage(h)
DecryptAESKey= (ESK, PrivKClient_id )
DecryptImg = TransformData(EncCredenFile, AESKey)
currentClient=Verify(citizenID)
match=compare(h, currentUser)
if match == true then
Address = ContractAddress(h)
clientEncCreden = Address.IPFS.getFile(h.FileID)
e-consent(h.userID)
CredentFile = DecryptFile(h, privateKey)
end if SaveToLocal(CredentFile)
end procedure
```

.

5. SYSTEM IMPLEMENTATION

Implementation is the stage in the project where the theoretical design is turned into a working system. The most critical stage is achieving a successful system and in giving confidence on the new system for the users, what it will work efficient and effectively. It involves careful planning, investing of the current system, and its constraints on implementation, design of methods to achieve the change over methods.The implementation process begins with preparing a plan for the implementation of the system. According to this plan, the activities are to be carried out in these plans; discussion has been made regarding the equipment, resources and how to test activities.The coding step translates a detail design representation into a programming language realization. Programming languages are vehicles for communication between human and computers programming language characteristics and coding style can profoundly affect software quality and maintainability. The coding is done with the following characteristics in mind.

- Ease of design to code translation.
- Code efficiency.
- Memory efficiency.
- Maintainability.

The user should be very careful while implementing a project to ensure what they have planned is properly implemented. The user should not change the purpose of project while implementing. The user should not go in a roundabout way to achieve a solution; it should be direct, crisp and clear and up to the point.Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

5.1 Modules

5.1 Cloud Authority

The authority generates the public parameter PK and the master private key of the system. The authority keeps the master secret key and publishes PK available for the subscribers. The authority also generates a secret key generated based on the CP-

ABE method and that key is issued to each financial institution. Authority can also view the finance institute request to get knowledge the customer who are registered in the cloud.

5.2 Clients

By using this module, client can enroll their information such as personal and sensitive information into the cloud. Then only they are considered as authorized users to access this application. Clients are the customers of financial institutes who join the blockchain-based KYC. Each customer has his own key pair used to encrypt and decrypt her credential data. To allow the credentials to be stored in any FI's database or in the cloud system, the FI must get the consent digitally signed by the client.

5.3 Storing Sensitive Data

After client has logged successfully, they can store and upload their KYC details in inter-planetary file system. inter-planetary is a cloud database that stores encrypted documents of KYC bound to each user account. It serves for user's credentials to generate transaction for cryptocurrency. It houses distributed hash table keeping the address of the hash value of the clients' credential files which are encrypted in the IPFS storage.

5

5.4 Finance Depository

In this module, finance institute can register their information in cloud. After finance institute logged successfully, they can request to the customer to get knowledge of the customer who are created an account in respective finance institute. After that, the client submits the request for the e-KYC verification by using her citizen id to the FI. The requesting FI calculates the hash value and transfers it to the Verify contract. Hence FI request to the cloud to check and verify the details customer whether the given information or legitimate or fake details.

5.5 Blockchain Technique

It is used to store the transactions of all KYC related activities. All sensitive transactions of the clients are encrypted. The data on the blockchain is tamperproof based on hash value and cryptography mechanism, which also prevents some illegal activities.In which smart contracts are used to control and automate all KYC processes. In our system, there are three smart contracts including Register contract is responsible for authenticating users, enrolling new users, and uploading the encrypted credentials to the IPFS, Master contract is responsible for controlling client profiles, keeping hash value of the citizen ID of all clients for interacting with IPFS, and e-consent generation, and Verify contract is responsible for KYC verification.

6. REFERENCES:

References Made From:

1.Y. Zhong, M. Zhou, J. Li, J. Chen, Y. Liu, Y. Zhao, and M. Hu,``Distributed blockchain-based authentication and authorization protocolfor smart grid,'' Wireless Commun. Mobile Comput., vol. 2021, pp. 115,Apr. 2021, doi: 10.1155/2021/5560621

2. A. A. Mamun, A. Al Mamun, S. R. Hasan, S. R. Hasan, M. S. Bhuiyan,M. S. Bhuiyan, M. S. Kaiser, M. S. Kaiser, M. A. Yousuf, andM. A. Yousuf, ``Secure and transparent KYC for banking systemusing IPFS and blockchain technology,'' in Proc. IEEE Region Symp.(TENSYMP), Jun. 2020, pp. 348351.

3. N. Ullah, K. A. Al-Dhlan, and W. M. Al-Rahmi, ``KYC optimizationby blockchain based hyperledger fabric network,'' in Proc. 4th Int.Conf. Adv. Electron. Mater., Comput. Softw. Eng. (AEMCSE), Mar. 2021,pp. 12941299.

4. N. Kapsoulis, A. Psychas, G. Palaiokrassas, A. Marinakis, A. Litke,and T. Varvarigou, ``Know your customer (KYC) implementation withsmart contracts

on a privacy-oriented decentralized architecture," FutureInternet, vol. 12, no. 41, pp. 113, 2020.

5. M. Pic, G. Mahfoudi, and A. Trabelsi, ``Remote KYC: Attacks and countermeasures," in Proc. Eur. Intell. Secur. Informat. Conf. (EISIC), Nov. 2019,pp. 126129.

.Sites Referred:

http://www.sourcefordgde.com

http://www.networkcomputing.com/

http://www.almaden.ibm.com/software/quest/Resources/

http://www.computer.org/publications/dlib/

7. CONCLUSION

We have presented the privacy-preserving e-KYC approach based on the blockchain. Our proposed scheme delivers secure and decentralized authentication and verification of the e-KYC process with the user's consent enforcement feature. In our scheme, the privacy of both customers' identity documents stored in the cloud is guaranteed by the symmetric key and public key encryption while the sensitive transaction data stored in the blockchain is encrypted by symmetric key encryption and CP-ABE. Our scheme also allows the KYC data to be updated by the data owner or the customer. In addition, we devised an access policy update algorithm to enable dynamic access authorization. For the evaluation, we performed comparative analysis between our scheme and related works in terms of the computation cost, the communication cost, and performance. The experimental results showed that our scheme outperforms existing schemes in terms of performance, comprehensive KYC compliance features, and the scalable access control mechanism.

FUTURE ENHANCEMENT

For future works, we will test a larger sample of data in the real cloud environment and measure the throughput of the system in accommodating high number of e-KYC registration and verification requests. In addition, we will investigate the technique to enable batch verification of e-KYC transactions stored in the blockchain with the searchable encryption feature.