Blockchain for Enhancing Trust and Privacy in Electronic Know Your Customer

ABSTRACT

This paper presents e-KYC Trust Block, a blockchain-based electronic Know Your Customer (e-KYC) system that enhances trust, security, and privacy in identity verification. Traditional e-KYC systems rely on cloud storage and conventional encryption, leading to key management complexities and security vulnerabilities. To address these challenges, e-KYC Trust Block integrates Ciphertext Policy Attribute-Based Encryption (CP-ABE) for fine-grained access control and Interplanetary File System (IPFS) for secure document storage. Additionally, it employs smart contracts to enforce client consent and ensure auditability. By combining symmetric and public-key encryption, the system minimizes communication overhead while maintaining data confidentiality. Experimental results validate its efficiency, scalability, and security, making it a robust solution for privacy-preserving e-KYC processes.

EXISTING SYSTEM

At present, blockchain technology and smart contracts have been leveraged in many application areas. Particularly, blockchain-based identification and authentication framework have been proposed by many works [1], [2], [7], [8], [12], [15] 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 [4]. 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.

In [5], Shabair *et al.* proposed a blockchain-based KYC in the form of proof-of-concept (PoC) system. The proposed system was conducted in private blockchain environments over the Grid'5000 a large-scale distributed platform. In [6], Norvill *et al.* presented a system that allows automation and permissioned document sharing over the blockchain to reduce the KYC process. In [9], Allah *et al.* proposed a Hyperledger Fabric network for KYC optimization model. In this model, the customer has full right to own the smart contracts in which customer KYC data is stored in the distributed ledger database. However, these works did not address the security and key management issue of KYC process.

In [10], Kapsoulis *et al.* proposed a way to implement e- KYC system using smart contracts and IPFS. In this work, KYC document operations such as create, read, update and delete are done through the set of smart contacts. The KYC documents are stored in the IPFS and through the private contract method. The security of the KYC transaction is managed by specific nodes in the blockchain with administrator privileges. However, there are no encryption used to protect the KYC data.

Regarding the privacy preserving technique applied for securing blockchain database, CP-ABE has received the attention of several research works [17]_[21], [24], [26], [27]. In [17], Bramm *et al.* proposed a Blockchain-based Distributed Attribute-Based Encryption (BDABE) scheme allows the attributes to be created and deleted dynamically at any time by a transaction on the blockchain. The proposed scheme supports mapping between multiple attribute authorities to assign the attributes to the users. It offers the flexibility for supporting secure and efficient user attributes management in the blockchain system.

In [18], Fan *et al.* proposed a traceable data sharing scheme using blockchain and CP-ABE. In this scheme, data is encrypted by a CP-ABE method and a secret key can be generated based on the system parameters available in the private blockchain. In the blockchain, the data owner can obtain the identity of data consumer and control data sharing based on the predefined access policy.

Yuan *et al.* [19] and Wu *et al.* [20] employed a CP-ABE approach to support data privacy protection and _ne-grained sharing in the blockchain system. In these schemes, any changes to the data are recorded on the blockchain and the access policy is enforced to manage the different permissions of access. If there is any

key abuse case initiated by any malicious users or authorities, the system provides audit trails to support the traceability of cryptographic operations and transaction activities.

Guo *et al.* [21] proposed a traceable attribute-based encryption with dynamic access control (TABE-DAC) scheme based on the combination of CP-ABE based linear secret sharing scheme (LSSS) and blockchain. The proposed scheme achieves fine-grained sharing of encrypted private data on cloud, traceability of users' private key leakage, and flexible policy update. The authors also introduced a hash function in the key and ciphertext generation to reduce the computation cost of such operations. In [24], Gao *et al.* proposed a secure ciphertext-policy and attribute hiding access control scheme and blockchain.The CP-ABE is used to protect the data stored in the blockchain. However, this scheme uses composite order groups for their crypto implementation which results in expensive computation cost.

Disadvantages

1. An existing methodology doesn’t implement PRIVACY-PRESERVATION OF SENSITIVE DATA IN BLOCKCHAIN.
2. The system not implemented Privacy-preserving e-KYC credentials with client consent..

Proposed System

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 reencryption 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.

Advantages

1. The advantage of having CIPHERTEXT POLICY ATTRIBUTE-BASED ENCRYPTION(CP-APE) is to protect the data from external attacker.

2. The system is very safe and secure since it is implemented with BLOCKCHAIN IN IDENTITY MANAGEMENT SYSTEM.

System Requirements

H/W System Configuration

Processor	- i5
RAM	- 4 GB (min)
Hard Disk	- 20 GB
Key Board	- Standard Windows Keyboard
Mouse	- Two or Three Button Mouse
Monitor	- SVGA

Software Requirements

Operating System	- Windows
Language	- Java 8 or JDK 1.8
Server	- Apache Tomcat9.0
IDE’s	- Notepad , Eclipse. • Database Connection - JDBC
Database	- Mysql / WorkBench
Coding Language	- Java/J2EE(JSP,Servlet)