Extended Identity Based Aggregation Scheme (Idbas) For Banking Application For Detecting And Preventing Using Mitigate Attacks

Mrs.J.Roselin Lourd[1], Dhakshayani.S[2], Abirami.K[3], Jothi.M[4]
[1]Head, Dept of CSE
[2, 3, 4]Dept of Computer Science
[1, 2, 3, 4] RAAK college of Engineering and technology Puducherry
[2, 3, 4]Pondicherry university Puducherry

Abstract- *The paper presents the online banking application process,it secure analysis of online banking systems. Several models are evolving and being applied to many banking applications systems to preventing and detecting online banking fraudsters.It is a financial sector and it is a part of the companies that consists of institutions that provides financial services to commercial and retailed customers.It includes a wide range of industries, including banks, investments or insurance companied. This financial institutions are they exposed to cyber-security attacks. Many banks places where money available and cyber criminals attacking banks offer a variety of ways to profit through national governments and financial support for hackers.*

I. INTRODUCTION

Nowadays, millions of websites are hosted on the web in the Internet era. A stack of servers is needed to maintain the hosted site, which is very costly. The servers' traffic rates must be steady and must be regularly checked and maintained. Need to hire more people to organize and maintain the servers. All of the data will be stored in data centers. As a result, continual attempts to maintain the server issue and the workers may detract from our ability to meet our business objectives using "Cloud Computing" to prevent time-consuming upkeep. "Cloud computing is a practice of employing a network of remote servers to store, manage, and process data from anywhere within the world." it's utilized in place of a local server or a personal computer. The service like storing data and applications is delivered to the organization's devices through the internet. Cloud computing provides many benefits through the services combining the data centers, resources, and servers through the internet. Cloud Services are based on pay-per-use regulations. The services are accessible from

II. BANKING APPLICATIOBUSING MITIGATATE ATTACKS

A.KYC PRIVACY AND SECURITY COMPLIANCE

Based on the thorough review of a survey of KYC regulations done by Price Waterhouse and Coopers [28], Technical Standard for Digital Identification Systems published by World Bank Group [29],and the report on existing remote on-boarding solutions in the banking sector by EU commissions [30], the security and privacy-related compliance regulated by financial institutions around the globe take customer due diligence as the core consideration and emphasize the following four common requirements for digital identification including KYC compliance.

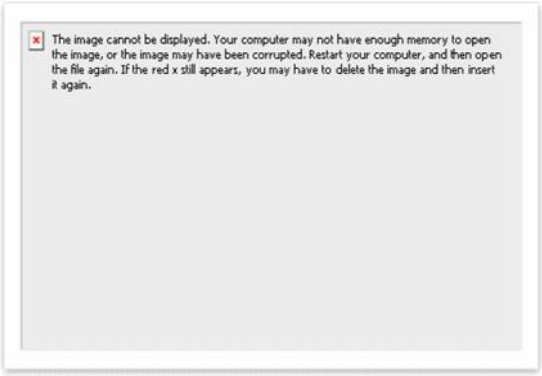
B.BLOCKCHAIN IN IDENTITY MANAGEMENT SYSTEM

Blockchain technology delivers a decentralized database where multiple nodes are linked to one another by the communication network. Blockchains are constructed from cryptographic mechanism, data storage, networking, and incentive schemes to support decentralized transaction

management where multiple parties can check, execute, and store the

C.CIPHER TEXT POLICY ATTIBUTE-BASED ENCRYPTION(CP-APE)

A cipher text policy attribute based encryption scheme consists of four fundamental algorithms it has they are key generation, encryption, decryption and setup algorithm.The setup algorithm it takes no input other than implicit security paramater. It outputs the public parameter and the master key.



III. PROBLEM DEFINITION

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. 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 addition to the strong authentication

IV. PROPESD SYSTEM

The rapid growth of security incidents and data recently had risen concerns on the internet banking security issues. The existing internet banking authentication mechanism that primarily relies on the conventional password-only authentication cannot effeciently resist to recent password guesssing and password cracking attacks. To address this problem, this project proposed an IDBAS scheme by adding an additional protection mechanism on the existing user authentication mechanism. When the malicious user attempts to unauthorized access to the online bank account by entering his guessed password, instead of rejecting the access and preventing them for using the application and keeping theain, and three smart contracts.

Authority: The authority generates the public parameter PK and the master private key MSK of the system. The authority keeps the MSK secret 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 (FI).

Clients: They are the customers of financial institutes who join the blockchain-based

KYC. Each customer has her 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.

IPES:IPFS 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 (DHT) keeping the address of the hash value of the clients' credential files which are encrypted in the IPFS storage Blockchain: 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 tamper proof bas on hash value and cryptography mechanism, which also prevents some illegal activities.

Smart contracts: They are used to control and automate all KYC processes. In our system, there are three smart contracts including (1) Register contract is responsible for authenticating users, enrolling new users, and uploading the encrypted credentials to the IPFS, (2)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 (3) Verify contract is responsible for KYC verification.

V. 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. 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

REFERENCES

[1] A. Akavia, S. Goldwasser, and V. Vaikuntanathan, "Simultaneous hardcore bits and cryptography against memory attacks," in Proc. 6th Theory Cryptography Conf., 2021, pp. 474–495

[2] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in Proc. 9th Int. Conf. Theory Appl. Cryptol., 2022, pp. 452–473.

[3] M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen, "Certificate based (linkable) ring signature," in Proc. Inf. Security Practice Experience Conf., 2021, pp. 79–92

[4] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang, "Malicious KGC attacks in certificateless cryptography," in Proc. 2nd ACM Symp. Inf., Computer. Communication. Security, 2020, pp. 302–311.

[5] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. Int. Conf. Theory Appl. Cryptographic Techniques., 2021, pp. 127–144.

[6] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. ACM Conf. Computer. Communication. Security, 2020, pp. 417–426.

[7] D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control of security capabilities," ACM Trans. Internet Techniques., vol. 4, no. 1, pp. 60– 82, 2019.