**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 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 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 \_les 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 \_le and sending back the confirmation of the verification result to the requestor or transmitting the copy of encrypted \_les 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 trace ability.

Recently, block chain 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 block chain and cloud system. Block chain 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 block chain system, a smart contract which is a self-executing program that can be implemented on the block chain enables the automated execution of system logics or functions efficiently. This empowers the usability and programmability of any systems running on the block chain network.

For years, a number of research works related to block chain-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 non repudiation property which is an essential requirement of privacy regulations such as General Data Protection Act (GDPR) [18] in the KYC registration process. Second, most existing works overlook the privacy of transaction stored in the smart contract and block chain. 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 block chain 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 block chain-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 block chain 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 \_les and employ the cipher text policy attribute-based encryption (CP-ABE) to encrypt the block chain transactions. Since CP-ABE provides a one-to-many encryption with \_ne-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 block chain. The updated e-KYC data is broadcasted in the ledger and the synchronization of the updated data is done by the responsible smart contract.

This paper is structured as follows. Section 2 presents related works. Section 3 explains the theoretical background used in our proposed approach. Section 4 presents our proposed system model. Section 5 provides the security analysis of our scheme. Section 6 provides the evaluation analysis and experiments. Section 7 gives conclusion and future work.