



IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 7, July 2023

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379



9940 572 462



6381 907 438



ijircce@gmail.com



www.ijircce.com

Secured Privacy-Preserving and Sharing KYC documents for Banking System Using Blockchain Technology.

Rohini S, Prof. Dr. Gunavathi H S

M.Tech Student, Department of Computer Science and Engineering, Bangalore Institute of Technology, Bangalore, Karnataka, India

Assistant Professor, Department of Computer Science and Engineering, Bangalore Institute of Technology, Bangalore, Karnataka, India

ABSTRACT: The process of document verification is an essential step that involves evaluating the papers provided by end users and ensuring that they are trustworthy. Digital documents are susceptible to problems such as duplication, loss, data theft, and forgeries as a result of developments in technology. Traditional systems suffer from a lack of privacy and transparency, in addition to having high costs and latencies. Decentralized systems like blockchain are being presented as a solution to both the need for faster processing and increased security. In our proposed system the entire verification process is carried out only once for each customer, regardless of the number of institutions they register with, and the KYC documents are securely saved in IPFS of Blockchain, where the KYC documents can be accessed by bank through encryption and decryption process. AES (Advanced Encryption Standard) is used to encrypt and protect electronic data. It is a symmetric encryption which enable the privacy preserving and fine-grained access of sensitive transactions stored in the blockchain.

KEYWORDS: KYC, Block Chain, authentication, verification, encryption, decryption, decentralized system.

I. INTRODUCTION

Electronic-Know Your Customer, abbreviated as "e-KYC," is a service that banks and other financial institutions (FIs) provide their clients in the form of a virtual banking operation that is connected to the identification and verification of identity electronically. This is done with the goal of increasing both cost efficiency and customer satisfaction [4]. Through the use of the e-KYC system, financial institutions are able to electronically verify the identification of their customers and get KYC data for individual customers as well as corporate customers. Either off-the-shelf e-KYC software that is fully equipped with the essential functionalities or custom-built e-KYC software is used by financial institutions in order to successfully deploy the e-KYC system [1]. After that, customers have the option of deploying the system in either an on-premise or cloud-based configuration. The majority of businesses have switched to utilising the cloud as their primary platform for storing their information and systems in response to the growing popularity of outsourcing models. When opposed to the host-based e-KYC authentication approach, in which documents must be physically present, the cloud-based e-KYC system offers an authentication method that is both more efficient and versatile in order for it to be checked by the centralised host. This creates a bottleneck in the flow of traffic and a single point of failure in the system [2]. Additionally, the traceability of the confirmed transaction is restricted due to the fact that the provider is responsible for managing each and every transaction that takes place inside the system. However, the problem of security and privacy associated with cloud-based solutions is a worry for a significant number of prospective businesses. This is due to the fact that e-KYC systems that are hosted in the cloud are able to store client data documents, and these documents may be read by any public cloud tenants or even cloud service providers (CSPs) [3]. In order to overcome this issue, the majority of financial institutions, including banks, will need to deploy an encryption system in addition to the robust authentication function offered by CSPs. To this aim, financial institutions (FIs) and banks that are in possession of the e-KYC system are required to encrypt the e-KYC data files prior to uploading them to the cloud [5]. When relying parties make a request for verification, the host party has two options for carrying it out: either it can decrypt the file and send the confirmation of the verification result back to the party that made the request, or it can send the copy of encrypted files along with the decryption key to the party that made the request. To ensure the safety of financial transactions and to conduct the KYC process in a more streamlined and secure manner, a Blockchain-based security management device is being developed [6]. Blockchain technology is

a novel method of decentralised data storage that uses mathematical, cryptographic, and economic principles to record and verify transactions across many users. It's a tamper-obvious, secure distributed database where the events inside a transaction may be used to prove the transaction's legitimacy. As a public distributed ledger, blockchains are often controlled by a decentralised network of computers called nodes, which work together to follow a consensus procedure for recording and verifying transactions. All Blockchains are an example of a distributed computing system with strong Byzantine fault tolerance and may be deemed safe by design despite the fact that blockchain facts are not unalterable due to the possibility of blockchain forks. Know The Know Your Client (KYC) techniques that banks use to their customers are pointless, unwieldy, and expensive [7]. Therefore, a tool is recommended to automate routine tasks and facilitate the exchange of information necessary for Know Your Customer checks. The general block diagram for the e-kyc is as shown in the below figure,

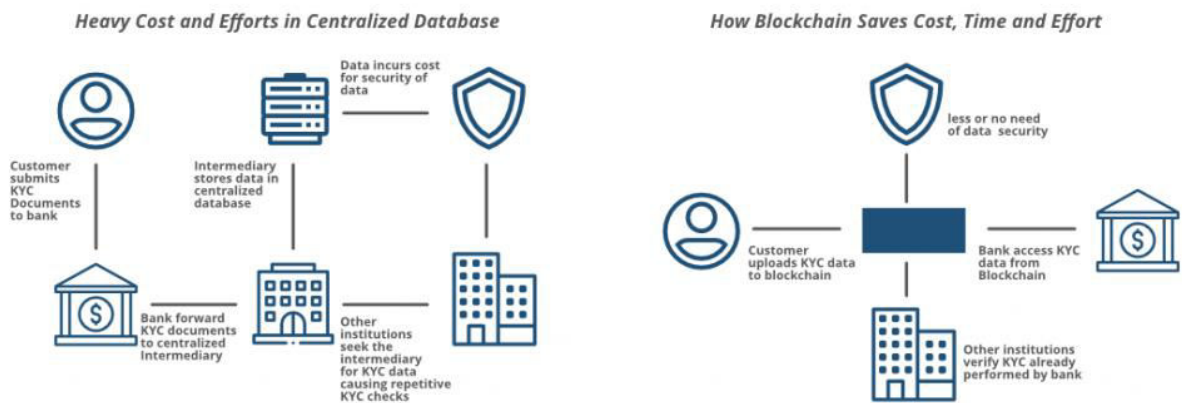


Figure 1: The general block diagram for the e-KYC process [21].

II. RELATED WORK

At the moment, the blockchain technology as well as smart contracts are being used in a variety of different application domains. Specifically, several publications [1, 2], [7], [8], [12], [15] have presented a blockchain-based identity and authentication framework, and it has been proved that a blockchain is effective for the administration of identification and authentication. Nevertheless, the e-KYC procedure is a great deal more involved than a straightforward authentication activity. Rather, it entails safe credential registration, maintenance of KYC documents, a safe and lightweight verification procedure between customers, numerous FIs, and a blockchain platform that is only devoted to this purpose, and it is all encrypted. In addition, there are newly developed forms of spoofing and remote attacks on the KYC system that need to be defended against [4]. Recent research studies connected to a blockchain-based e-KYC have focused on the development of a framework for the safe storage and verification of user credentials as well as the optimisation of the communication overhead involved in the interaction between various financial institutions. The authors of [3] presented a proposal for a KYC document verification process that would use the IPFS system in conjunction with blockchain technology. This strategy involves the consumers registering their identification information with the bank, after which their credentials are hashed and encrypted with the help of the encryption application gpg4win. Nevertheless, the confidentiality of transactions on blockchains and their ability to be traced are not topics that are addressed in this study. In the article [5], Shabair et al. suggested a proof-of-concept (PoC) method for a blockchain-based know your customer (KYC) system. The suggested system was tested in private blockchain settings, which were run on top of a large-scale distributed platform called Grid'5000. In the paper [6], Norvill et al. described a solution that streamlines the Know Your Customer (KYC) process by enabling automated and permissioned document distribution via the blockchain. The Hyperledger project was suggested by Allah et al. in [9].

The authors of this article have provided a short overview of how the use of blockchain technology to store and track data might have an effect on the contemporary banking business, namely the KYC document verification procedure. On paper, which is an outmoded technique, the Know Your Customer procedures used in banking today are quite reliable. The usage of blockchain technology in the know your customer (KYC) procedure would significantly cut down on the number of intermediaries required by the proposed system. As a consequence of this, fraud should be reduced as much as possible throughout the process of integrating client documents into the bank database [10]. This may be accomplished by improving customer experience, reducing costs, boosting efficiency, and enhancing transparency. The new system will operate in a manner that is similar to the KYC system that was previously in place. This study intends to address some of the limitations of the existing system and suggest the addition of new elements in

order to develop a system that is both more secure and more comprehensive. Customers and corporate institutions would be able to check and record client KYC papers in the distributed ledger technology (DLT) if the suggested system is implemented. IPFS will be used in the system that is being suggested, which will result in a large efficiency boost for DLT storage [11]. By leveraging blockchain technology, the suggested action resulted in an improvement to the pre-existing KYC system. The removal of the need for third parties is a characteristic of DLT that is fairly well-known, and we make advantage of smart contracts to construct the logic behind data mobility. The blockchain technology uses a variety of cryptographic security protocols in order to provide a more secure environment for the processing of transactions that take place over an unsecured channel. By integrating distributed ledger technology (DLT), encryption, and the consensus mechanism of blockchains, the suggested KYC process has the potential to improve security, transparency, and privacy while simultaneously optimising data storage, updating, sharing, and accessing processes. Additionally, it enhances the overall experience of the client and boosts the customer's sense of ownership [12]. IPFS is being utilised for the new KYC document management system that has been suggested. using the Inter Planetary File System (IPFS) and the Technology Behind Blockchain. We propose a platform that utilises these technologies and aims to be cost-effective, quick, privacy-conscious, secure, and transparent. It will be used in the financial system to verify KYC documents. Users are unable to submit their KYC papers to the Blockchain network since doing so is too expensive. As a stand-in solution, the Know Your Customer (KYC) papers may be uploaded to the IPFS and subsequently dispersed utilising the Blockchain Network. Users are able to upload their transaction history as well as their hashes to the IPFS network, where they may be stored safely until they are required by the Blockchain network. This technique will result in a size reduction of the blockchain data that is substantially smaller [13]. We offer a solution based on Blockchain technology that will reduce the costs associated with the traditional KYC verification method. The most significant distinction is that the whole verification process is carried out just once for each user, regardless of the number of institutions they register. This improves transparency by allowing users to safely share the findings using distributed ledger technology (DLT). In this method, a proof of concept (POC) using Ethereum is carried out. This method not only lowers expenses but also boosts customer satisfaction and makes operations more open and transparent [14]. In this paper, a novel trust management platform is presented. This platform is self-sovereign and decentralises the Know-Your-Customer (DKYC) model. It does this by improving customer security and privacy through consent-based access, incorporating regulator governance, and assisting banks in using trusted and accurate customer data while lowering customer acquisition costs [15].

III. PROPOSED ALGORITHM

We propose a solution-based system for safe and privacy-preserving KYC sharing that makes use of blockchain technology. This system will allow consumers to send their KYC papers to financial institutions without compromising the customers' privacy or security in the process. It is the responsibility of the system to restrict access to the information to just those individuals who have been granted permission to see it. The fact that the whole verification procedure is carried out just once for each client, regardless of the number of institutions they register for, is the most significant improvement that has been made to it. This has significantly increased the level of transparency achieved by safely disclosing the findings.

The proposed architecture is as shown in the below figure, when the customer of the banks applies the applications, it has been sent to the financial institutions or the organization for the checking the details are right or not by considering the block chain methodology.

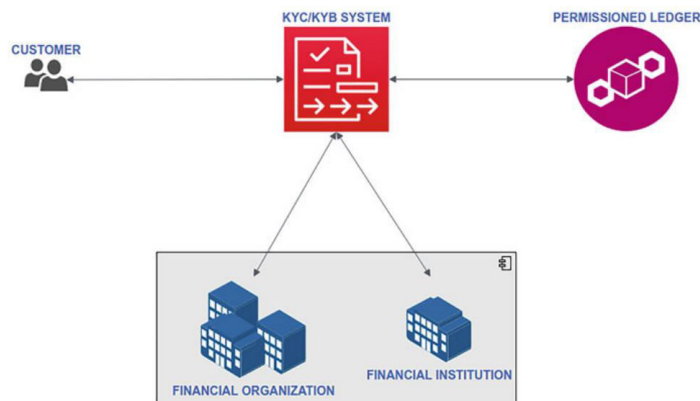


Figure 2: Proposed Architecture.

The details of the applications and the interactions between the bank and the applications are provided in the below figure,

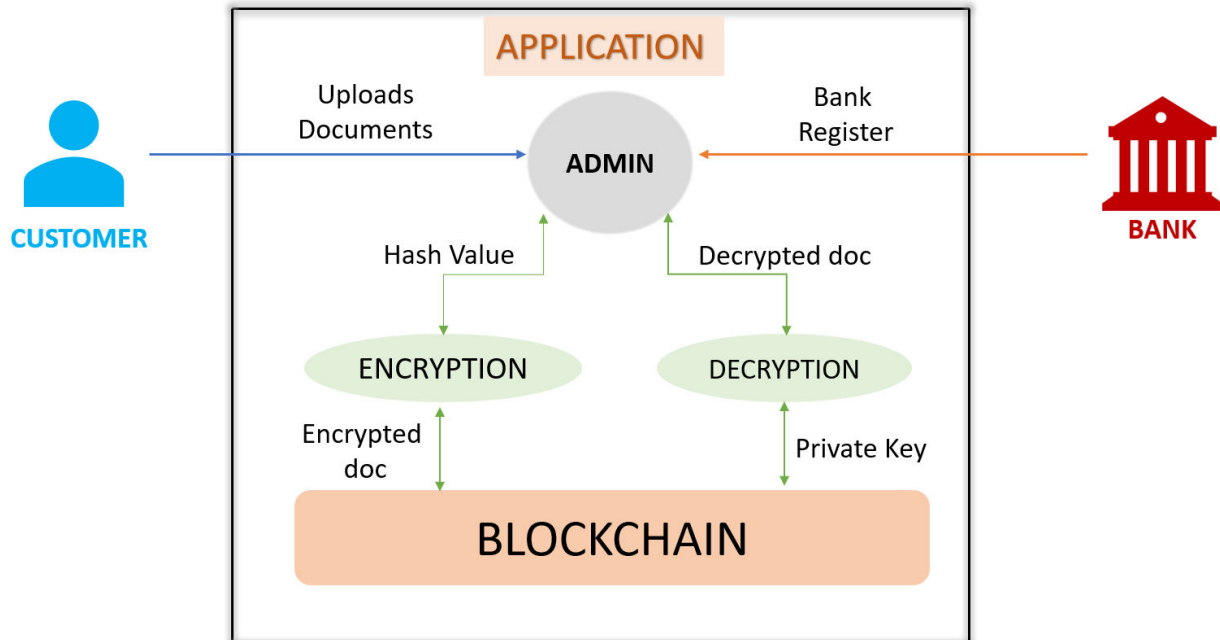


Figure 3: Process of verification of application from bank using blockchain.

A. Identified modes in the model:

1. Authentication module
2. Data handling module
3. Security module
4. Block chain module

The details of the models are provided in this sub-section,

Authentication Module:

The authentication module is responsible for user signup and login. It verifies the user's registration status and then lets them log in using their existing details. There is an option to sign up for a new account if the user is not already registered. Once the user has been verified, the module will load the appropriate application pages for their privilege level.

Data Handling Module:

The data management component is in charge of setting up and processing the users' KYC (Know Your Customer) information. By potentially evaluating and validating the data to ensure its completeness and accuracy, it guarantees that the bare minimum of KYC standards is satisfied. The financial sector is only one of several that uses know your customer procedures to safeguard against fraud.

Security Module:

The encryption and decryption mechanisms make up the security module. The data of users will be more protected and private according to this module. Personal information and other user input is encrypted before being stored. Using cryptographic techniques, encryption converts the plaintext into an unreadable code called ciphertext. The server then stores this information in an encrypted form. When the information is required, the ciphertext is retrieved from storage and decrypted using the proper method. This makes it so that administrators and other people who shouldn't have access to the plain text data can't read it, keeping important information safe.

Blockchain Module:

The blockchain component ensures the safe and distributed storage of information. After the information has been encrypted, it is sent to the blockchain, a decentralised and unalterable record. Due to its distributed structure, blockchain technology distributes data over a network of computers, making it more resistant to loss or alteration. The blockchain is a distributed ledger in which each "block" is linked to the one before it by a hash (a cryptographic hash value). This safeguards the genuineness and reliability of the information kept on the blockchain.

By integrating these features, the platform can provide users a safe space to store and manage their information while still protecting their privacy. The use of blockchain technology also improves the application's data storage and administration in terms of both security and openness.

B. AES algorithm

Due to the growing usage of the Web for the transmission of confidential documents mostly on a professional & private level, online protection has emerged a cause of worry. Information security requires cryptography to protect information against unauthorized entry. The encrypting key's magnitude determines the robustness. The very same key is utilized in both encoding & decoding in the symmetrical crypto algorithm known as AES (Advanced Encryption System). The working of AES Algorithm. The steps followed in AES is given below,

Step 1: Pre-processing

- Convert the input data (message) into a binary representation (bytes). If the data is a string, use UTF-8 encoding to convert it to bytes.
- Append a '1' bit to the end of the data. This ensures that the data is one bit longer than a multiple of 512 bits (the block size for SHA-256).
- Append '0' bits until the data length is 64 bits less than a multiple of 512 (i.e., the data length is 64 bits shy of a multiple of 512).
- Append the original data length as a 64-bit big-endian integer. This ensures the final block size is exactly a multiple of 512 bits.

Step 2: Initialize the hash values

- The SHA-256 algorithm uses eight 32-bit integers (A, B, C, D, E, F, G, H) as its initial hash values.
- These initial hash values (also known as " H_0 " or "state") are generated using specific constants derived from the square roots of the first eight prime numbers.

Step 3: Process the message in 512-bit blocks

Divide the pre-processed data into 512-bit blocks (16 words of 32 bits each).

- Process each block sequentially, updating the state variables (A, B, C, D, E, F, G, H) as follows:
- Prepare 64 words (W0 to W63) by expanding the 16 words of the block.
- Use a loop to perform 64 rounds of processing, updating the state variables in each round.
- Each round involves bitwise operations such as AND, OR, XOR, logical right shifts, and addition modulo 2^{32} .

Step 4: Finalize the hash

- Concatenate the eight 32-bit state variables (A, B, C, D, E, F, G, H) to get a 256-bit hash value.
- Represent the hash value as a hexadecimal string.

The below figure shows the procedure for generating the hash messages to encrypt the information.

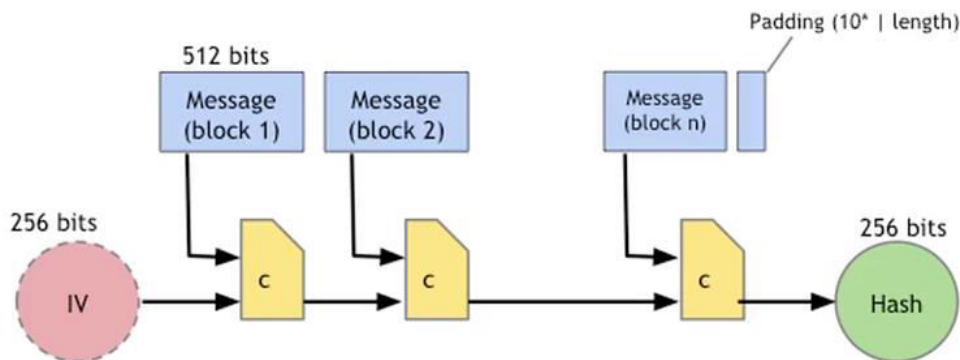


Figure 4: Hash generation

Encryption process

We present a two layer encryption scheme comprising symmetric key encrypts and CP-ABE encryption.

The below steps explains the process of encryption, every files undergoes the encryption by following below steps

- Encrypts message M the algorithm is run by register contract. It takes symmetric key to encrypt data M. The algorithm produces the cipher text C_{tm} and stores in IPGS
- Encrypt sym key : The algorithm takes as inputs authority public key Pk_k , access control policy used to encrypt data in blockchain ACPid and sym key. HTen the encrypted sym key CT_k is produces and it is stored in block chain

Decryption process

It is the phase performed by the financial institute and the admin,

The below two steps formalizes the decryption process

- Decrypt CT_k : The algorithm takes as the input as $FISK_{Fiid}$ (secret key generated by the authority based on CP_ABE method and used to financial institute) and CT_k . The output is a symmetric key symkey
- Decrypt CT_n (An encrypt data in blockchain): The algorithm then takes as input symkey and CTM.

IV. SIMULATION RESULTS

This section provides the details about the implementation carried out and the snapshots of the website, the website is hoisted in the local server and the it is as shown in the below figure,

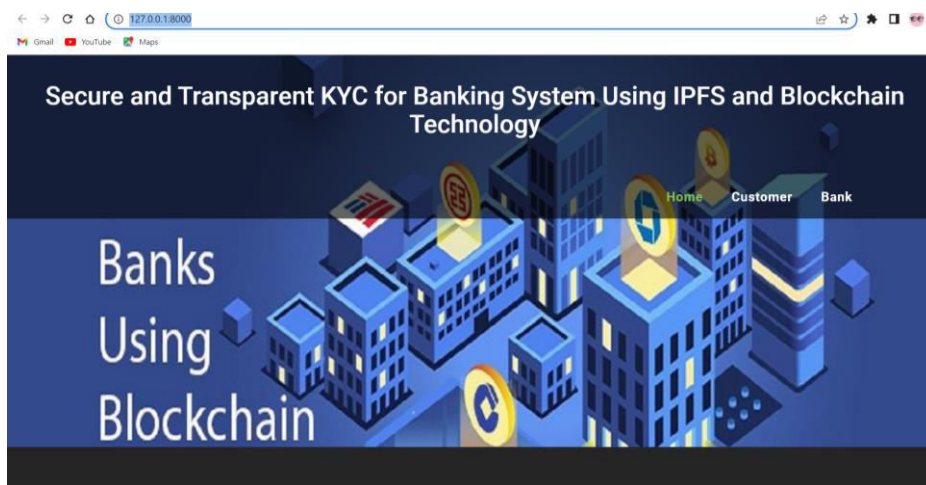
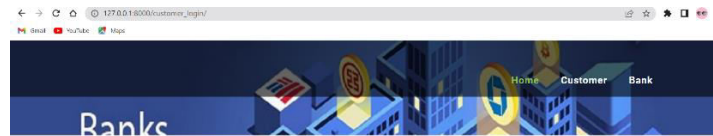


Figure 5: Home page for the website.



CUSTOMER LOGIN

Username

Password

LOGIN

[User Register Here](#)



Figure 6: Customer Login page



CUSTOMER REGISTER

Fullname

Email

Mobile

Location

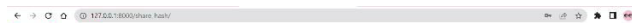
Username

Password

SUBMIT



Figure 7: Customer registration page



CUSTOMER OPEN A ACCOUNT

Select Bank

Select Bank

Select Location

Select Location

Fullname

Email



Figure 8: Upload KYC documents



BANK LOGIN

Username

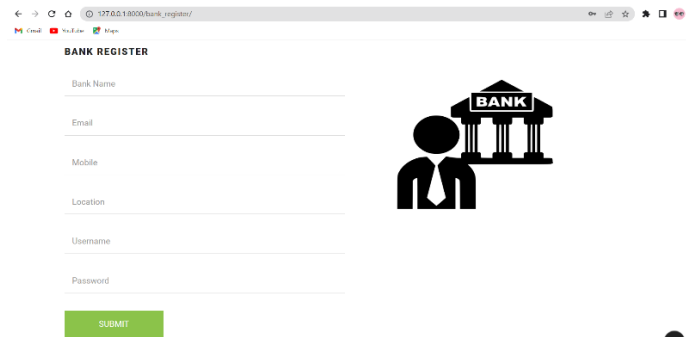
Password

LOGIN

[User Register Here](#)

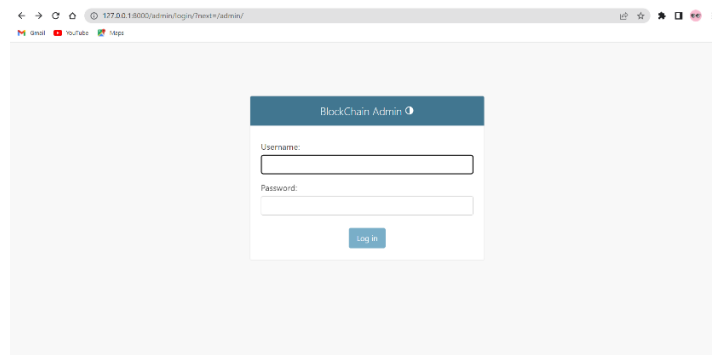


Figure 9: Bank login page



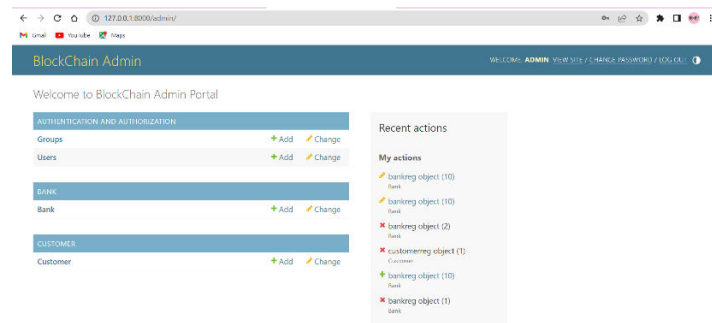
The screenshot shows a web browser window with the URL 127.0.0.1:8000/bank_register/. The page is titled "BANK REGISTER" and contains a registration form with the following fields: Bank Name, Email, Mobile, Location, Username, and Password. A green "SUBMIT" button is located at the bottom of the form. To the right of the form is an icon of a person in a suit standing in front of a building labeled "BANK".

Figure 10: Bank Registration page



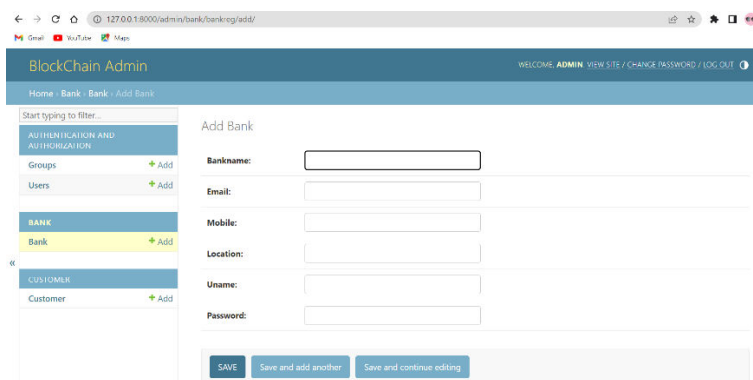
The screenshot shows a web browser window with the URL 127.0.0.1:8000/admin/login/?next=/admin/. The page is titled "BlockChain Admin" and features a login form with fields for "Username:" and "Password:". A blue "log in" button is positioned below the password field.

Figure 11: Admin login page



The screenshot shows the "BlockChain Admin" portal. The header includes the text "BlockChain Admin" and "WELCOME: ADMIN VIEW SITE / CHANGE PASSWORD / LOG OUT". Below the header, there is a "Welcome to BlockChain Admin Portal" message. The main content area is divided into two sections: "AUTHENTICATION AND AUTHORIZATION" and "Recent actions". The "AUTHENTICATION AND AUTHORIZATION" section contains three categories: "Groups" (with "Add" and "Change" buttons), "Users" (with "Add" and "Change" buttons), "BANK" (with "Add" and "Change" buttons), and "CUSTOMER" (with "Add" and "Change" buttons). The "Recent actions" section, titled "My actions", lists several actions with status indicators: "bankreg object (10) bank" (success), "bankreg object (10) bank" (success), "bankreg object (2) bank" (error), "customerreg object (1) Customer" (success), "bankreg object (10) bank" (success), and "bankreg object (1) bank" (error).

Figure 12: Admin portal page



The screenshot shows the "BlockChain Admin" portal with the "Add Bank" form. The breadcrumb trail is "Home > Bank > Add Bank". The form has a search bar at the top left. The "Add Bank" form includes fields for "Bankname:", "Email:", "Mobile:", "Location:", "Uname:", and "Password:". At the bottom of the form, there are three buttons: "SAVE", "Save and add another", and "Save and continue editing".

Figure 13: Admin access to Add Bank or edit bank

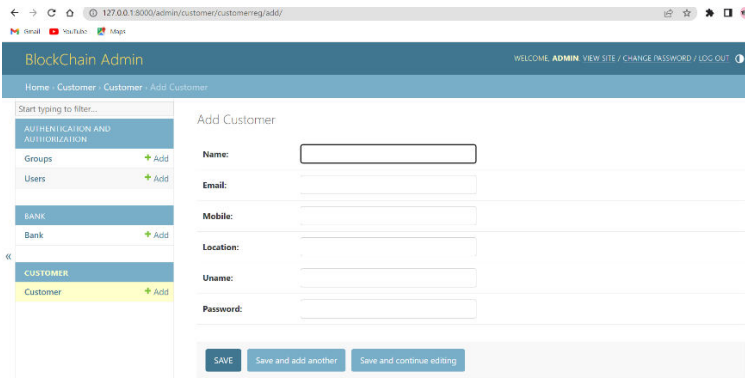


Figure 14: Admin has access to add new customer or edit customer

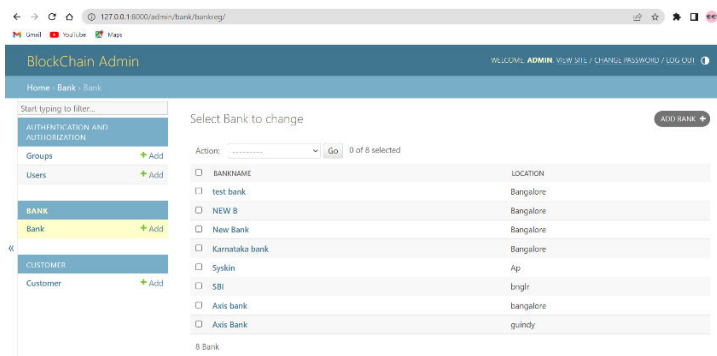


Figure 15: Admin has access to view list of banks and has authority to delete bank

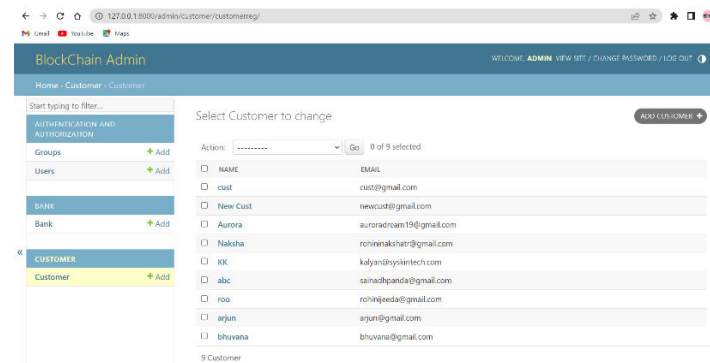
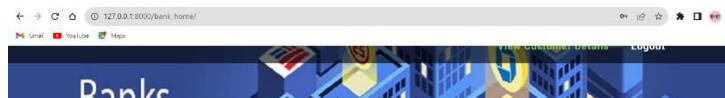


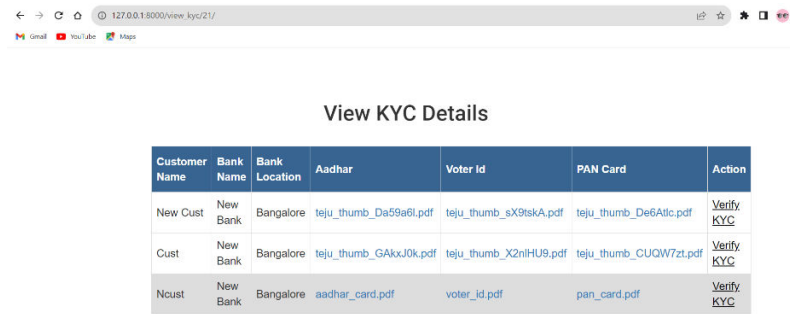
Figure 16: Admin has access to view list of customers and has authority to delete any customer



Bank Customer Details

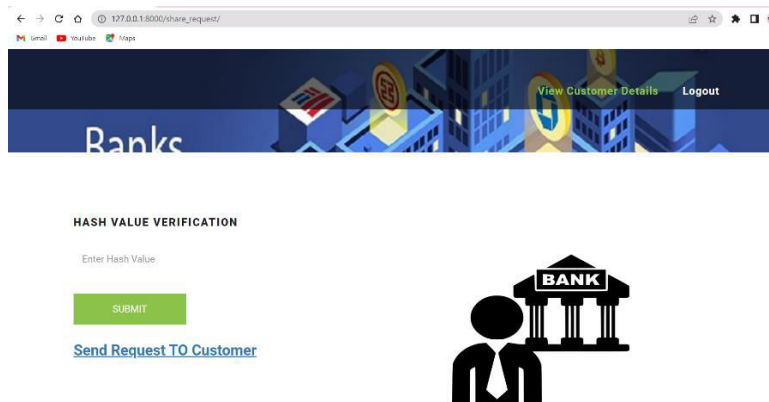
Customer Name	Email	Mobile	Gender	Address	Location	Action
New Cust	newcust@gmail.com	1234567890	female	no 33 , 2nd main	Bangalore	View KYC
cust	cust@gmail.com	8008997364	female	no 33 , 2nd main	Bangalore	View KYC
Noust	ncust@gmail.com	34567887643	female	44, 3rd main	bangalore	View KYC

Figure 17: Bank views list of customer



Customer Name	Bank Name	Bank Location	Aadhar	Voter Id	PAN Card	Action
New Cust	New Bank	Bangalore	teju_thumb_Da59a6f.pdf	teju_thumb_sX9tskA.pdf	teju_thumb_De6A1tc.pdf	Verify KYC
Cust	New Bank	Bangalore	teju_thumb_GAkxJ0k.pdf	teju_thumb_X2niHU9.pdf	teju_thumb_CUQW7zt.pdf	Verify KYC
Ncust	New Bank	Bangalore	aadhar_card.pdf	voter_id.pdf	pan_card.pdf	Verify KYC

Figure 18: Bank can verify the uploaded documents



HASH VALUE VERIFICATION

Enter Hash Value

[Send Request TO Customer](#)


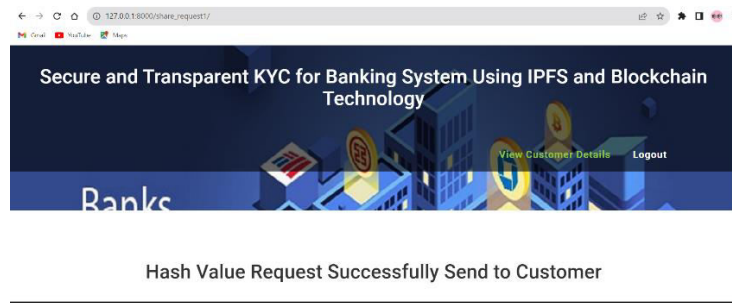


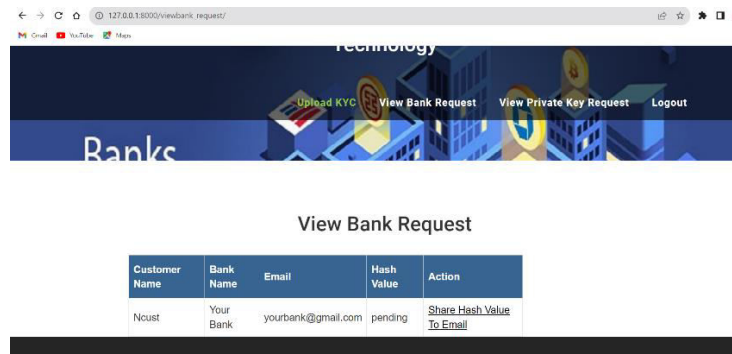
Figure 19: Request for hash value



Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology

Hash Value Request Successfully Send to Customer

Figure 20: To view documents bank send request to customer to share customer details



View Bank Request

Customer Name	Bank Name	Email	Hash Value	Action
Ncust	Your Bank	yourbank@gmail.com	pending	Share Hash Value To Email

Figure 21: customer views bank request to share hash value

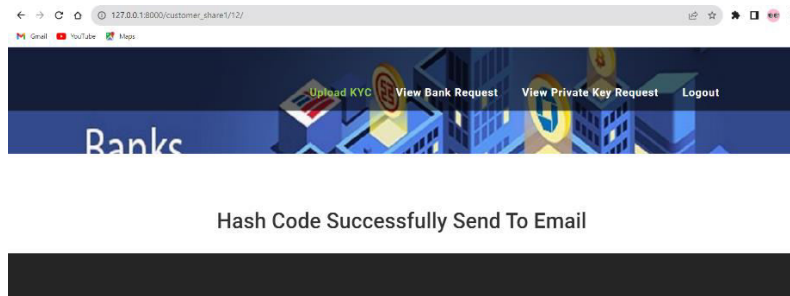


Figure 22: Hash value successfully sent to email

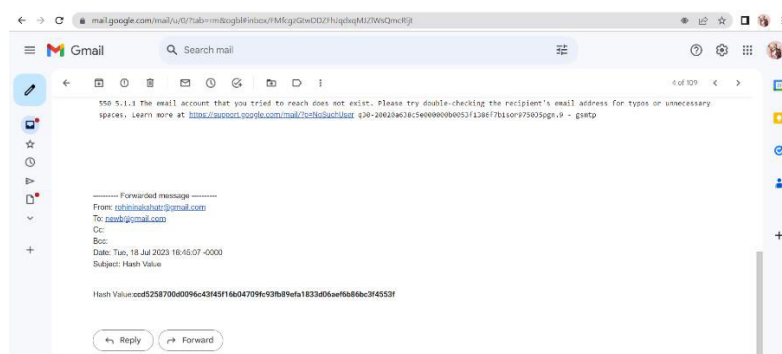


Figure 23: hash value sent to mail



Figure 24: Conversion of encrypted file to decrypted file

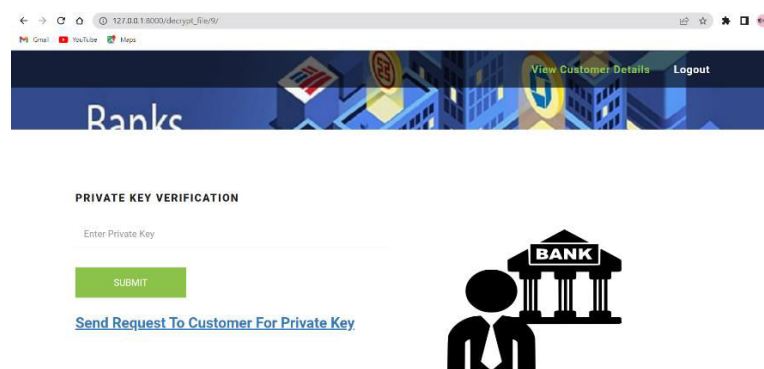
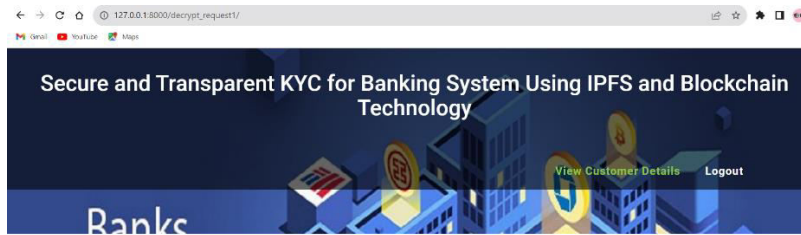
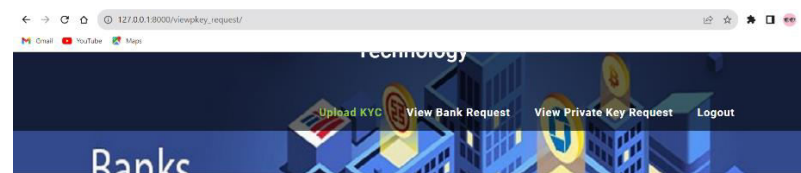


Figure 25: Request customer to share private key for decryption of files



Private Key Request Successfully Send to Customer

Figure 26: PK request sent successfully



View Private Key Request

Customer Name	Bank Name	Email	Private Key	Action
Ncust	Your Bank	yourbank@gmail.com	pending	Share Private Key To Email

Figure 27: Customer gets request to share PK

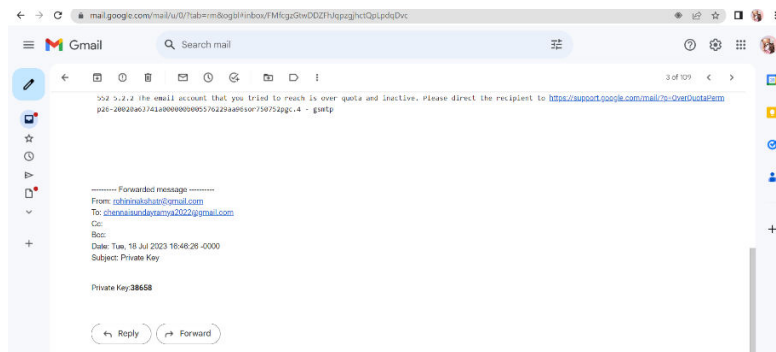
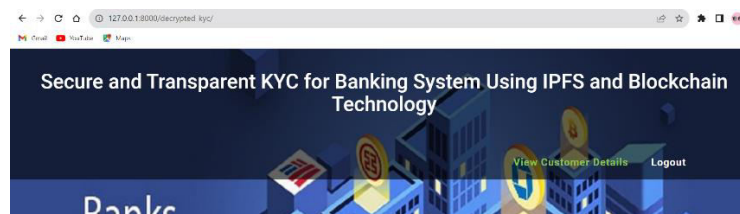


Figure 28: PK sent to mail



View Decrypted KYC Details

Customer Name	AAdhar Card	Pan Card	Voter Id
Ncust	aadhar_card.pdf	voter_id.pdf	pan_card.pdf

Figure 29: Bank can view the decrypted KYC documents.

V. CONCLUSION AND FUTURE WORK

We have presented the secured privacy-preserving and sharing e-KYC documents based on the blockchain. Our scheme delivers secure and decentralized authentication and verification of the e-KYC process with the user's consent enforcement feature. The KYC documents uploaded by the customer will be stored in IPFS of Blockchain. The sensitive transaction data stored in the blockchain is encrypted by symmetric key encryption and AES. The hash value is generated once the documents are stored. Customer opens an account in bank and for the verification of the documents, the bank needs to request customer to view E-KYC documents where the encryption and decryption takes place by sharing hash value and private key to bank. Our proposed scheme is the integration of blockchain technology in the KYC process is a transformative solution that combines enhanced security, privacy preservation, and seamless sharing, offering a new paradigm for the banking system to flourish in the digital age while safeguarding the interests of both banks and their customers.

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] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F. Ang, and R. Ismail, "Blockchain technology the identity management and authentication service disruptor: A survey," *Int. J. Adv. Sci. Eng. Inf. Tech.*, vol. 8, pp. 1735–1745, Sep. 2018.
- [3] 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, and M. A. Yousuf, "Secure and transparent KYC for banking system using IPFS and blockchain technology," in *Proc. IEEE Region Symp.(TENSYP)*, Jun. 2020, pp. 348–351.
- [4] M. Pic, G. Mahfoudi, and A. Trabelsi, "Remote KYC: Attacks and countermeasures," in *Proc. Eur. Intell. Secur. Informat. Conf. (EISIC)*, Nov. 2019, pp. 126–129.
- [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] N. Ullah, K. A. Al-Dhlan, and W. M. Al-Rahmi, "KYC optimization by blockchain based hyperledger fabric network," in *Proc. 4th Int. Conf. Adv. Electron. Mater., Comput. Softw. Eng. (AEMCSE)*, Mar. 2021, pp. 1294–1299.
- [9] N. Kapsoulis, A. Psychas, G. Palaiokrassas, A. Marinakis, A. Litke, and T. Varvarigou, "Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture," *Future Internet*, vol. 12, no. 41, pp. 1–13, 2020.
- [10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Secur. Privacy*, Oakland, CA, USA, May 2007, pp. 321–334.
- [11] I. Gutierrez-Aguero, S. Anguita, X. Larrucea, A. Gomez-Goiri, and B. Urquiza, "Burnable pseudo-identity: A non-binding anonymous identity method for ethereum," *IEEE Access*, vol. 9, pp. 108912–108923, 2021.
- [12] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Accessed: Jan. 8, 2022. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [13] J. P. Moyano and O. Ross, "KYC optimization using distributed ledger technology," *Bus. Inf. Syst. Eng.*, vol. 59, no. 6, pp. 411–423, Dec. 2017.
- [14] A. Chowdhary, S. Agrawal, and B. Rudra, "Blockchain based framework for Student identity and educational certificate verification," in *Proc. 2nd Int. Conf. Electron. Sustain. Commun. Syst. (ICESC)*, Aug. 2021, pp. 916–921.
- [15] GDPREuropeanUnionGuidelines. Accessed: Aug. 12, 2021. [Online]. Available: <https://gdprinfo.eu/>
- [16] G. Bramm, M. Gall, and J. Schütte, "BDABE-blockchain-based distributed attribute based encryption," in *Proc. 15th Int. Conf. e-Bus. Telecommun.*, 2018, pp. 99–110.



Impact Factor: 8.379



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details