ABSTRACT

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. 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

Keywords: *KYC, Blockchain, IPFS, DLT*

Table of Contents

Index of Figures

Index of Tables

CHAPTER 1

INTRODUCTION

1.1 Introduction

The Know your customer (KYC) is a very common term in the banking and financial sector. At this moment, the manual KYC process is outdated and has become a necessity to automate the KYC verification process. Studies around the world have made several attempts to make a better verifi- cation process for KYC. Many academics tried to propose a Blockchain-based solution. Blockchain technology recently draws the attention of the public, as a dispute that leads to the foundation that the trust-free economical transaction is possible with its distinctive method .

The blockchain permits unnamed and secure transactions of virtual currencies (such as Bitcoin, Litecoin, etc) and saves the metadata regarding the transaction details in a database. The database is secured and impede the alteration in the transaction history by cryptography techniques. The legitimate user can write to the file using the private key. In banking, blockchain is safe and can reduce processing/transaction costs considerably. The banks or other financial organizations such as insurance industries maintain diverse policies and require multi-steps processing between parties. Besides, these require a secure transaction, short processing/settlement time. To facilitate these concerns, the researcher has proposed various distributed platforms. Raikwar et al. proposed a blockchain based distributed platform for financial transaction processing in insurance industry. Puthal et al. introduced a decentral- ized framework using blockchain which allows sharing and integration of all distributed actors. This will help industry to analyze the spread and plan further development .

1.2 Overview

A bank generally serves to a large client base in both retail and corporate sector. The ‘Know Your Customer’ process, also known as KYC, which helps the institution to verify identity of client. KYC is a Regulatory and legal requirement that must be fulfilled by the companies or financial institutions for both new and existing clients. The major challenge faced by banking sector is increased regulatory cost of KYC process that has negative impact on business. The aim of this paper is to propose a new approach to the KYC verification process. We introduce a system, based on DLT that proposes a solution to the increased costs of the KYC process and the lack of customer satisfaction. The key reason for using DLT is that it allows us to observe the KYC cost structure at an aggregate level for all the financial institutions operating in a jurisdiction and to tackle the inefficiencies that emerge from the duplicated conduct of similar tasks by all participating institutions (i.e., DLT allows us to render the execution of duplicated tasks completely unnecessary, and this delivers far greater cost savings than would any effort to merely make these duplicated tasks more cost efficient)

The "Know Your Customer" process, also known as KYC, helps organizations verify the identity of their customers. KYC is a regulatory and legal requirement that a business or financial institution must meet for new and existing customers. The main challenge of the banking industry is to control the cost of the KYC process, which negatively affects the business. The purpose of this article is to propose a new KYC verification process. We have developed a DLT-based system that provides a solution to the additional cost of the KYC process and the lack of customer satisfaction. The main reason we use DLT is because it allows us to monitor the KYC fee structure across all financial institutions in the jurisdiction and on a consolidated basis for inefficiencies from similar transactions. In all organizations involved (for example, DLT frees us from doing all the repetitive tasks and saves more money than trying to simplify these repetitive tasks).

KYC is the process by which banks obtain information about the identity and address of the buyer. Due diligence to identify the client is a process followed by regulators. This process ensures that the bank's services are not abused. It is the company's responsibility to complete the KYC process when opening an account. Banks are also required to regularly update customers' KYC information KYC can be manual, time consuming and repetitive in organizations. Sharing KYC information on the blockchain will enable financial institutions to achieve better results, increase efficiency and improve customer experience. The KYC blockchain system provides transparency and immutability, allowing financial institutions to verify the authenticity of available information on DLT platforms. The decentralized KYC process is an easy way for users to access new information securely and quickly.

1.3 Problem Definition

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.

1.4 Motivation

Aims to be accomplished in our project are as follows: “we are intended to do this. We propose a solution based on Blockchain technology, which reduce the traditional KYC verification process cost. The Major addition to it is that the whole verification process is conducted only once for each customer, irrespective of the number of institutionsthey register and thereby increasing the transparency by securely sharing the results through DLT. This approach involves proof of concept (POC) with ethereum. This process reduces cost overhead, improved customer experience and increases transparency. The ‘Know Your Customer’ process, also known as KYC, which helps the institution to verify identity of client. KYC is a Regulatory and legal requirement that must be fulfilled by the companies or financial institutions for both new and existing clients.

1.5 Literature Survey

1 The purpose of project Pervasive Decentralization of Digital Infrastructures: A Framework for Block chain Enabled System and Use Case Analysis and their author is F. Glaser he publish a Social Science Research Network Rochester NY SSRN Scholarly Paper ID 3052165. Is in year of Jan. 2017. And the mean purpose is Block chain technology recently draws the attention of the public, as a dispute that leads to the foundation that the trust - free economical transaction is possible with its distinctive method and it’s more secure.

2 A lightweight multi-tier s-mqtt framework to secure communication between low-end iot nodes and their author is A. Rahman, S. Roy, M. S. Kaiser and M. S. Islam and they publish in the Year of 2018 5th International Conference on Networking Systems and Security . we discuss a detailed analysis of data & devices security issues and present an enhanced security model with a view to improving the security issues and its more complex .

3 A Blockchain Framework for Insurance Processes the author is M. Raikwar, S. Mazumdar, S. Ruj, S. Sengupta, A. Chattopadhyay and K.-Y. Lam they publish in 2018 9th IFIP International Conference on New Technologies Mobility and Security. we focus on the design of an efficient approach for processing insurance related transactions based on a block chain-enabled platform and its less applicable

4 The Blockchain as a Decentralized Security Framework and the author D. Puthal, N. Malik, S. Mohanty, they publish IEEE Consumer Electronics Magazine, in 2018.the overview of this technology for the realization of security across distributed parties in an impregnable and transparent way and it’s more costly. M. Mahmud, M. S. Kaiser, M. M. Rahman, M. A. Rahman, A. Shabut, S. Al-Mamun, etc.

5 This author publish Cognitive Computation, vol. 10 in oct 2018 the TMM utilizes both node behavioral trust and data trust, which are estimated using ANFIS, and weighted additive methods respectively, to assess the nodes trustworthiness and its more time consuming

1.6 Existing System

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.Sharing of confidential KYC data must be authorized by customers, and a bank-customer relationship must be kept secret from network.

1.7 Proposed System

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. sharing of confidential KYC data must be authorized by customers, and a bank-customer relationship must be kept secret from network.

1.7.1 Objectives:

1. To Secure and faster for sharing sensitive information.
2. To allow customer and business institute to verify record customer record.
3. To allow third party verification.
4. More Secure due to block chain.

An important class of applications requires data to be shared selectively among mutually anonymous transacting peers while retaining the tamper-resistant evidentiary and validation features of a blockchain. KYC validations of corporate customers by banks. Economical, swift, secure, and transparent platform for KYC document verification for the Banking system through Interplanetary File System (IPFS) and blockchain technology. 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. we describe the design and implementation of a smart contract for consent-driven and double-blind data sharing on the Hyperledger Fabric blockchain platform. We show how a KYC application was built around this model to address the needs of the banks.

1.7.2. Area of Project:

Computer & Information Security.

1.7.3. Features:

With the current rate of growth of the banking sector, such an approach really has the ability to bring about big improvement and shared gain to all of concerned stakeholder In our proposed system we are sharing KYC documents with blockchain so user document and details keep safe and secure. In above architecture we can see we have created one secure IPFS system so user here kept their documents and details.In Second part when user required to done transaction from one bank to other bank that time our system will help to provide easy KYC to send amount easily and securely.In Diagram we can see there is strong security algorithm so on one side we are doing encryption and other side doing decryption.

CHAPTER 2:

ANALYSIS AND FEASIBILITY

2.1. Analysis

Technological innovation and consequential decentralisation are driving forces in the ongoing evolution and increasing openness of digital infrastructures and services. One of the most discussed and allegedly disruptive innovations is the distributed database technology referred to as blockchain. Although it is still in its technological infancy, experimental adoption and customization seem to be in full progress in various potential fields of application ranging from decentralized grids for computation and storage to global financial services. However, the technology and its path of development still entail a lot of common unknowns for practitioners and researchers alike. Especially regarding the question how the technology could amend or be incorporated into the existing landscape of digital services, processes and infrastructures.

KYC (Know Your Customer) is a process of verifying the identity of customers to prevent fraud and illegal activities. Blockchain and IPFS are two technologies that can be used to improve the KYC process by providing transparency and security. Blockchain is a distributed ledger that allows transactions to be recorded and verified without the need for a central authority, while IPFS is a decentralized storage system that allows files to be stored and retrieved securely. Using blockchain and IPFS for KYC would involve creating a decentralized platform that allows customers to securely share their identity information with banks and financial institutions. However, there are still challenges to overcome, such as ensuring that the platform complies with data protection regulations and addressing the scalability issues of blockchain technology.

The use of blockchain and IPFS for KYC transparency and security in banking is a promising solution that can significantly improve the current process. The benefits of using blockchain and IPFS include transparency, security, immutability, and decentralization. Blockchain is a distributed ledger that enables transactions to be recorded and verified without the need for a central authority, providing transparency to the KYC process. IPFS is a decentralized storage system that allows files to be stored and retrieved securely, providing additional security against data loss. Privacy and data protection concerns can be addressed through cryptography and digital signatures, and the scalability issue of blockchain technology can be addressed through advancements in blockchain technology. Overall, the use of blockchain and IPFS for KYC transparency and security in banking is a promising solution that can significantly improve the current process's efficiency and security, but it is essential to address the challenges of privacy, data protection, and scalability to ensure that the solution is effective and compliant with the regulatory framework.

Blockchain Concept:

A blockchain is a distributed ledger with growing lists of records (blocks) that are securely linked together via cryptographic hashes. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree, where data nodes are represented by leaves). The timestamp proves that the transaction data existed when the block was created. Since each block contains information about the previous block, they effectively form a chain (compare linked list data structure), with each additional block linking to the ones before it. Consequently, blockchain transactions

are irreversible in that, once they are recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.

Blockchains are typically managed by a peer-to-peer (P2P) computer network for use as a public distributed ledger, where nodes collectively adhere to a consensus algorithm protocol to add and validate new transaction blocks. Although blockchain records are not unalterable, since blockchain forks are possible, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. A blockchain was created by a person (or group of people) using the name (or pseudonym) Satoshi Nakamoto in 2008 to serve as the public distributed ledger for bitcoin cryptocurrency transactions, based on previous work by Stuart Haber, W. Scott Stornetta, and Dave Bayer. The implementation of the blockchain within bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications and blockchains that are readable by the public and are widely used by cryptocurrencies. The blockchain may be considered a type of payment rail.

Private blockchains have been proposed for business use. Computerworld called the marketing of such privatized blockchains without a proper security model "snake oil"; however, others have argued that permissioned blockchains, if carefully designed, may be more decentralized and therefore more secure in practice than permissionless ones.

2.2. Feasibility Study

For all new systems, the engineering process should start with the feasibility study. The input to the feasibility study is only description of the system and how it will be used within an organization. The result of the feasibility study should be a report, which recommends whether or not it is worth carrying with the requirement engineering and the system development process. Feasibility study considerations are.

2.2.1 Technical Feasibility

The technical feasibility involves financial considerations to accommodate the technical enhancements, with the existing provision of computerization; the work can be completed efficiently. The project is implemented in Netbean 8, Apache Tomacat 8.0 & MySQL 5.0, Android Studio which is user friendly, Freeware, efficient and error free. The Windows 7 or higher windows operating system as well as any OS in which the project was implemented made time much less as we are already familiar with windows environment.

The computerized material planning process is to be developed in any database management tool, which can be ported to any pc based platform. However, for optimum functionality and ease of use for users a network of one central active hub running the program with several passive nodes is recommended.

To handle back end we are implementing database solution using MYSQL which having inbuilt data backup & restore facility. MYSQL run on all windows platform so it is quite feasible

2.2.2. Economic Feasibility

Economic analysis is the most frequently used method for evaluating the effectiveness of the system. It is more commonly known as cost analysis procedure to determine the benefits and saving that are expected from ‘NFC based Passport System’ the labor expense is reduced .The cost for the development of ‘NFC based Passport System’ is very less.

The cost of Net bean 8, Android Studio & MySQL software’s for management is at present economical because they available in free of cost. The benefits in turn reduce a lot of manual paper work. The development cost in future will be putting the system on its extension. In short software’s Net beans 8 & MySQL which are used for designing this system are easily available at free cost.

2.2.3 Operational Feasibility

Under this category of service we conduct a study to analysis and determine whether our system need can be fulfilled by using a proposed system. The result of our operational feasibility will clearly that the solution proposed for your system is operationally workable and conventionally solves users problem's under consideration after proposal is implemented.

As system divided into different modules each modules having user friendly GUI. Admin, User of those outline particular are the users that are involved in this 'NFC based Passport System'. They have to login and register. After proper login and registration they will get an access to the control panel which is iconize with their technologies. Hence user interface is highly user friendly as per specifications of Admin and teachers also having modules as per their requirement which are easy to understand. So its operational feasibility is clean and clear. To enhance the success ratio user must have basic knowledge of computer & and Internet. In case of live web based system user must be having access to the Internet.

CHAPTER 3

PROJECT REQUIREMENTS

3.1 About Proposed Project

We have proposed a system that can help the banking system for security purpose how bank to bank transfer also check kyc if amount greater than 1 lakh. An important class of applications requires data to be shared selectively among mutually anonymous transacting peers while retaining the tamper-resistant evidentiary and validation features of a blockchain. KYC validations of corporate customers by banks. Economical, swift, secure, and transparent platform for KYC document verification for the Banking system through Interplanetary File System (IPFS) and blockchain technology. 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. we describe the design and implementation of a smart contract for consent-driven and double-blind data sharing on the Hyperledger Fabric blockchain platform. We show how a KYC application was built around this model to address the needs of the banks

3.2. Area of implementation

In this project, we used Data Mining as an area of implementation for the 'KYC Transparency and Security for Banking using Block Chain and IPFS.'

3.3. Functional Requirements

Sr. no	Functions	Input	process	Output
1	Collecting Data	Email-ID, Account No, Mobiles No. Aadhar no, pan card no, Driving license, etc.	When customer applies for KYC then he must insert all the basic information related to transaction like email Id, Account number, mobile number, Aadhar number and pan card number.	Data Stored Successfully.
2	Distribution of data	-	After collecting all the data from user, the specified algorithm distributes the user credentials to the multiple servers	Data successfully distributed into multiples blocks.
3	Fetching of data	User request for data	Whenever user demands, bank management verifies data or customer wants to update it at that scenarios all the information which is distributed to multiple servers get invoked at a single point and customer or bank can access it for further operations	Data successfully fetched from multiples blocks/ server.
4	Multiple data access	User requirement	When user wants a service of another bank the second bank accesses the system and confirms the user identity for secure transaction.	Multiple banks access data successfully.

Table 3.1 Function Requirements

3.4. Non-Functional Requirements

3.4.1 Performance Requirements

Performance is measured in terms of the output provided by the application.Requirement specification plays an important part in the analysis of a system. Only when the requirement specifications are properly given, it is possible to design a system, which will fit into required environment. It rests largely in the part of the users of the existing system to give the requirement specifications because they are the people who finally use the system. This is because the requirements have to be known during the initial stages so that the system can be designed according to those requirements. It is very difficult to change the system once it has been designed and on the other hand designing a system, which does not cater to the requirements of the user, is of no use.

The requirement specification for any system can be broadly stated as given below:

- The system should be able to interface with the existing system
- The system should be accurate
- The system should be better than the existing system

The existing system is completely dependent on the user to perform all the duties.

3.4.2 Security Requirements

The software system defined in this SRS must follow industry recommended practices forsecure software development. At a minimum, the software development must practice the principle of least privilege for defining access-level requirements of the software system and its associated services. The production-release version of the software system must pass an
automated dynamic application security testing tool (e.g., HP WEBINSPECT).

3.4.3 Software Quality Attributes

1. **Reliability**

XYZO should provide reliable and relevant search results 100% of times. The checkout operation should end reliably within 5 seconds

2. **Availability**

XYZO should be available 99.999% of times throughout US region. All software upgrades, patches and fixes should be done without shutting down the application. There should be disaster recovery environment to handle natural disasters.

3. **Security**

Following security standards should be followed,
Login operation should be performed using transport layer security (HTTPS)

3.5. Hardware Requirements:

For development:

S. No.	Hardware	Specifications
1)	Processor	Intel Core i3
2)	RAM	1 GB
3)	Storage	256 GB SSD

Table 3.2 Hardware Requirements

For Use:

S. No.	Hardware	Specifications
1)	Processor	Intel Core i3 or above
2)	RAM	1 GB or above
3)	Storage	More than 256 GB or more
4)	Other Hardware	Network Interface Card (NIC) mouse, keyboard and monitor, etc

Table 3.3 Minimum Requirements

3.6. Software Requirements

- **Software Requirement for Development of Project:**

S. No.	Software	Operation
1)	XAMPP Server	1.8.2
2)	Net beans 7.2 or 8.0	7.2 or 8.0
3)	Operating System	Windows OS

Table 3.4 Software Requirements

- **Project Operation**

S. No.	Software	Operation
1)	Browser	Any Web browser
2)	Operating System	Windows OS or above

Table 3.5 Project Operation Requirements

CHAPTER 4

PROJECT DESIGN AND IMPLEMENTATION

4.1 Design Concept

Year planner chart is also called as time line chart. Time line chart is use for proper scheduling of project. A timeline chart can be developing for entire project. Alternately separate time line chart is developing for each function. A time line chart enables what task will be conducted at given point of time. The task set that is selected is collection of software engineering work task, milestone and deliverable that must be to complete a particular project. In timeline chart all project task are listed in left-hand column. The horizontal bar indicates duration of each task. When multiple bars occur at the same time, task concurrency is implied. The diamond indicates milestones. Time line chart help to determine how each task is initiated in addition it gives the understanding of priority and criticality of each task. When force with serve deadline pressures, a project scheduling technique called Time-Boxing is used. Time line plan is use for correct setting up of project. A timeline chart can be rising for entire project. Alternately divide time line chart is on the rise for each function. Year Planner enables you to create a structured and renewed Year Plan of your project. It is designed to help you identify the project's goals and outlines the analysis, strategies and planning required for these goals to be achieved. The Year Planner allows you to create a yearly plan for your project. Here you are able to outline what you want your project to achieve during the year ahead. Therefore, you are able to stay focused on the big picture and will not get lost in the detailed day-to-day planning. It also reduces risks and increases the chances of success for your project

4.2. System Diagram

1.In Second part when user required to done transaction from one bank to other bank that time our system will help to provide easy KYC to send amount easily and securely.

2.In Diagram we can see there is strong security algorithm so on one side we are doing encryption and other side doing decryption.

1. Register

-Here user can register and user info will be encrypting using blockchain here on portal.

2. Login

-Login Here

3. Upload Documents.

-User Can Upload documents in IPFS with encrypt.

4. Bank to Bank Transfer

-Show bank to bank transfer also check kyc if amount greater than 1 lakh

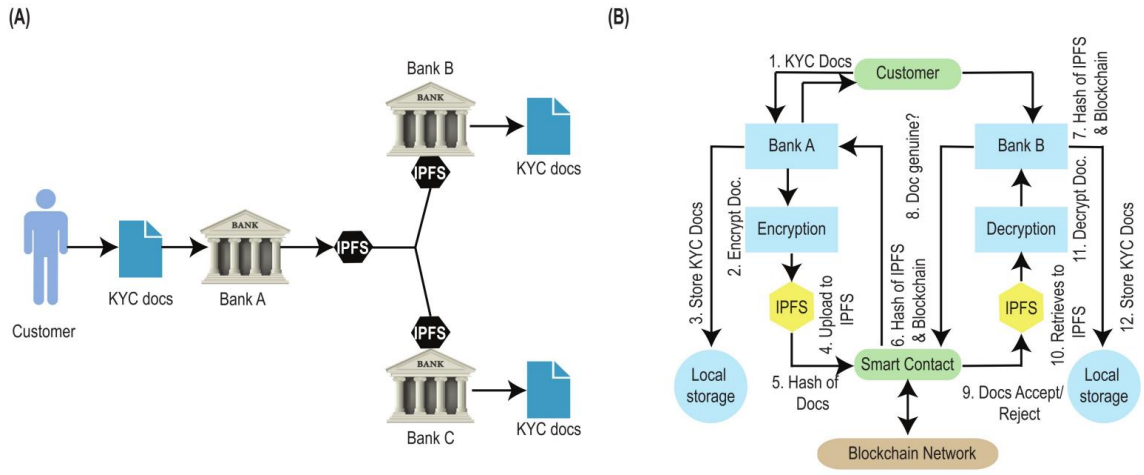


Fig No 4.1 System Diagram

4.3. DFD Diagram:

A data flow diagram is a graphical representation of data through an information system, modelling its process aspects. A data flow diagram is primary step to create an overview of the system. A DFD shows what kind of information will be input to an output from the system, where the data will come from and go to, and where the data will be stored.

User submits KYC information to the system.

The system stores the KYC information on IPFS, a decentralized storage platform, and records the IPFS hash on the blockchain for secure and transparent record-keeping.

Upon verification, the user's KYC status is updated on the blockchain.

Authorized parties can access the user's KYC information on IPFS using the recorded hash.

The system periodically reviews and updates the user's KYC information as necessary.

If the user's KYC status changes, the system updates the blockchain record accordingly.

Note that the specific DFD for such a system would depend on many factors, such as the specific design of the blockchain and IPFS components, the types of users and authorized parties, and the particular KYC requirements and processes involved.

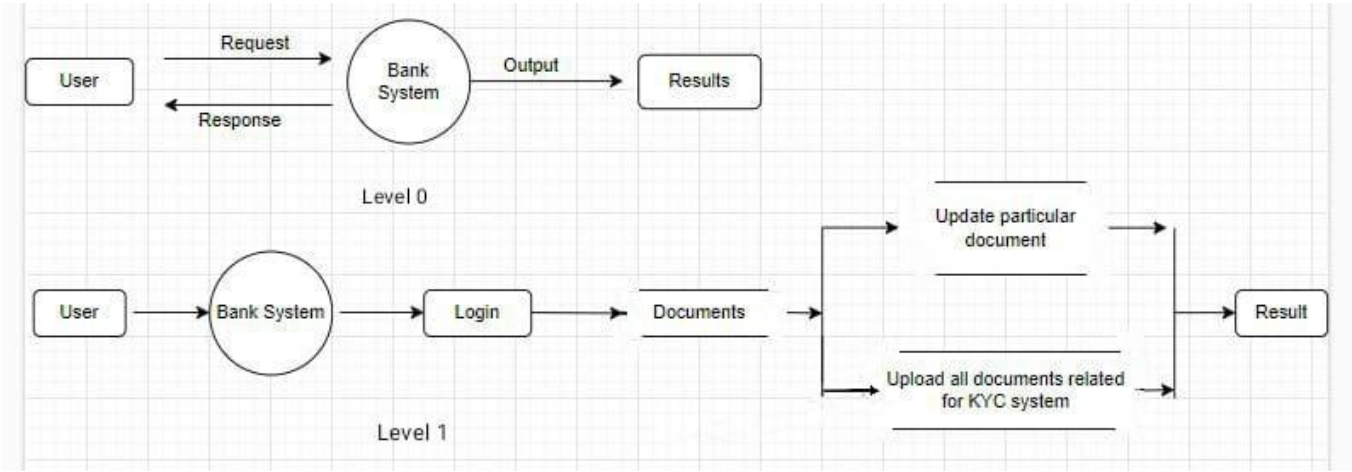


Fig No 4.2.: DFD Level 0 ,1,2

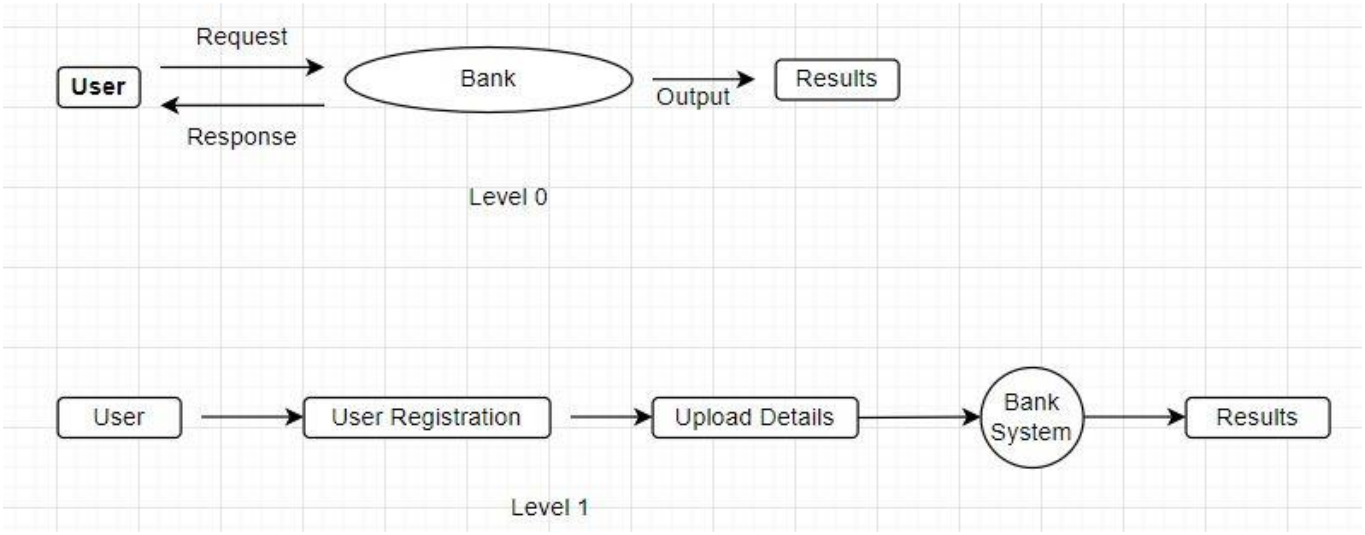


Fig No 4.3: DFD Level 0,1,2 bank Module

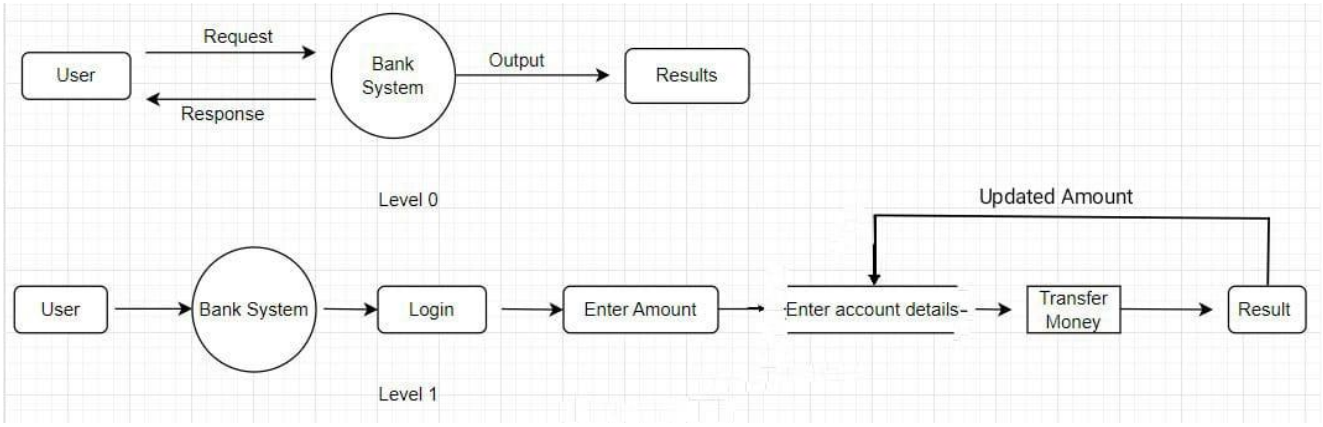
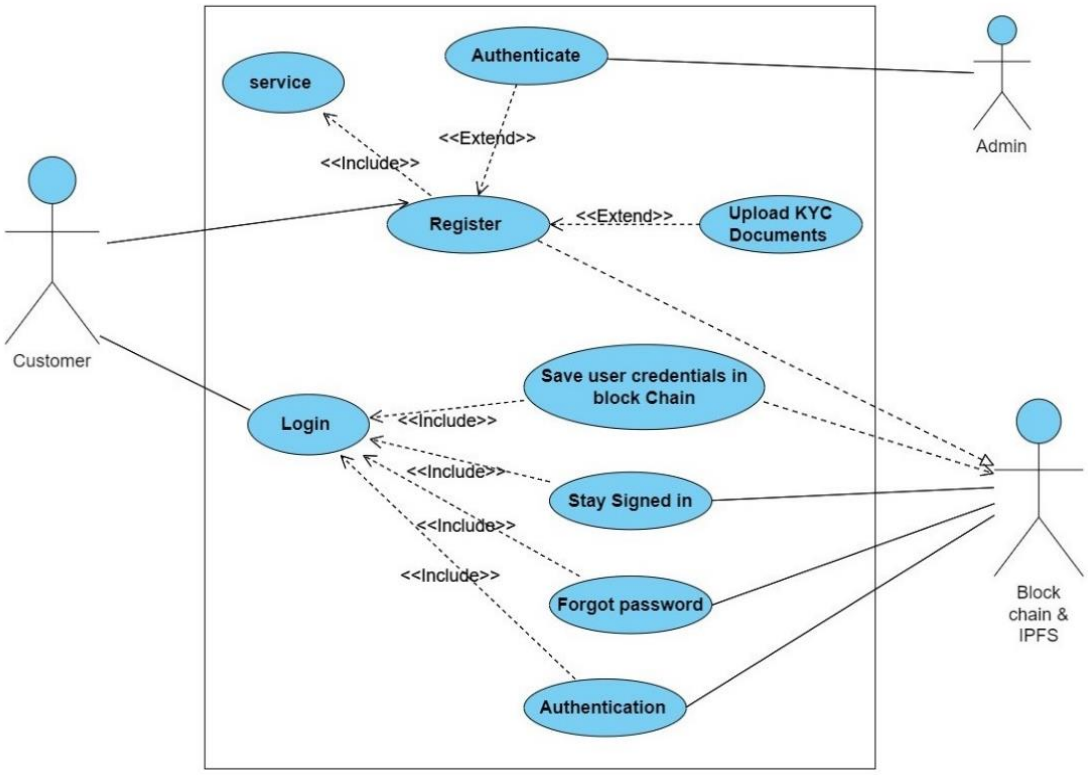
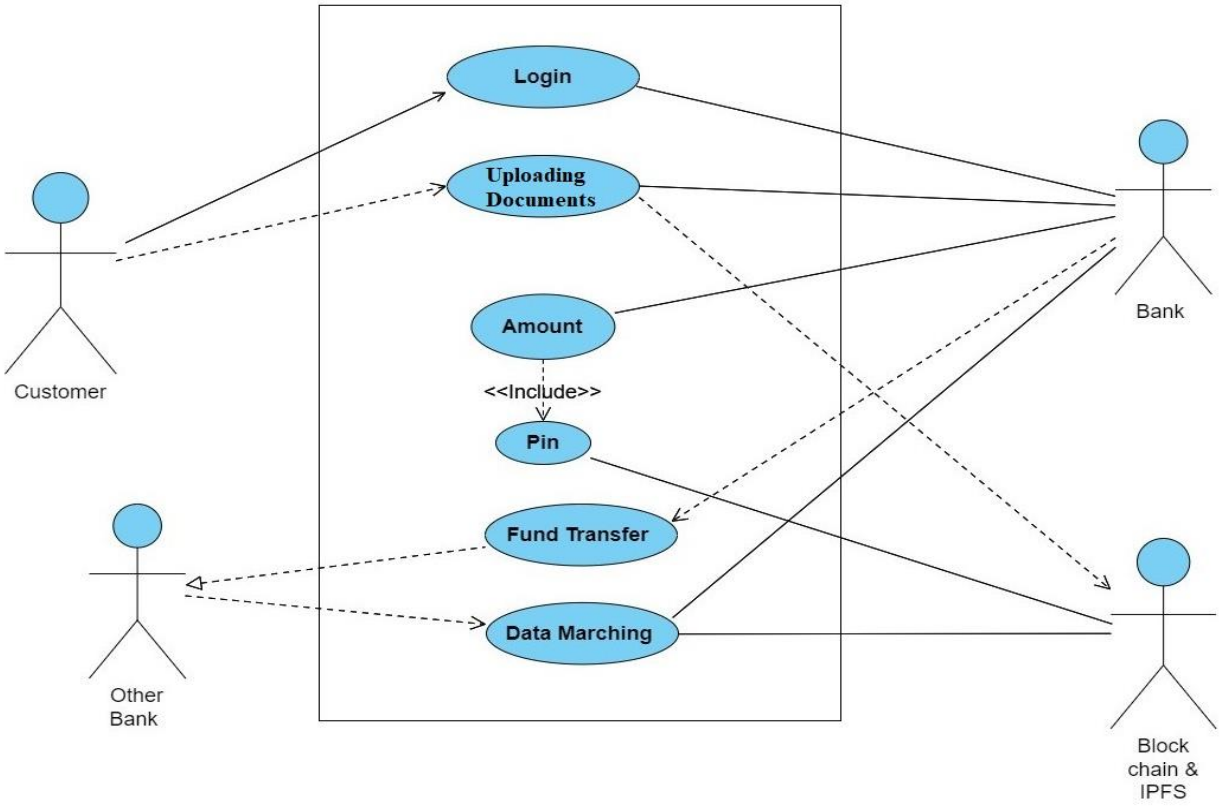


Fig No 4.4 : level 0,1 User module.

4.4. UML Diagram (Use Case)

The Use Case Diagram shows the actual functionality of system, and how the users are inter-connected with each other. This diagram gives the exact working of the system. In this system Admin can update information, documents and notification. The Voter varies the updated data of schemes and can view the Ward information Use case for kyc transparency and security using blockchain and ipfs A possible use case for KYC (Know Your Customer) transparency and security using blockchain and IPFS (Interplanetary File System) is in the financial industry, particularly for anti-money laundering (AML) and counter-terrorism financing (CTF) compliance. In this use case, customer identity information is stored on a blockchain, which is a decentralized and tamper-evident ledger. The customer can grant permission for authorized parties, such as financial institutions and regulators, to access their KYC data on the blockchain. The use of a blockchain ensures that the data is secure, transparent, and cannot be altered without the knowledge of all parties. IPFS can be used to store the actual KYC documents, such as passports and identification cards. By using IPFS, the documents can be stored in a decentralized manner, reducing the risk of a single point of failure and improving data availability. The use of IPFS also enables easy access to the KYC documents from anywhere in the world, further enhancing transparency and reducing the potential for fraud or corruption.Overall, the combination of blockchain and IPFS can provide a secure and transparent solution for KYC compliance in the financial industry, while also ensuring customer privacy and control over their own data.


Authenticate
service
Admin
<<Extend>>
<<Include>>
Register
<<Extend>>
Upload KYC Documents
Customer
Save user credentials in block Chain
Login
<<Include>>
<<Include>>
Stay Signed in
<<Include>>
<<Include>>
Forgot password
Block chain & IPFS
Authentication


Login
Uploading Documents
Customer
Bank
Amount
<<Include>>
Pin
Fund Transfer
Data Marching
Other Bank
Block chain & IPFS

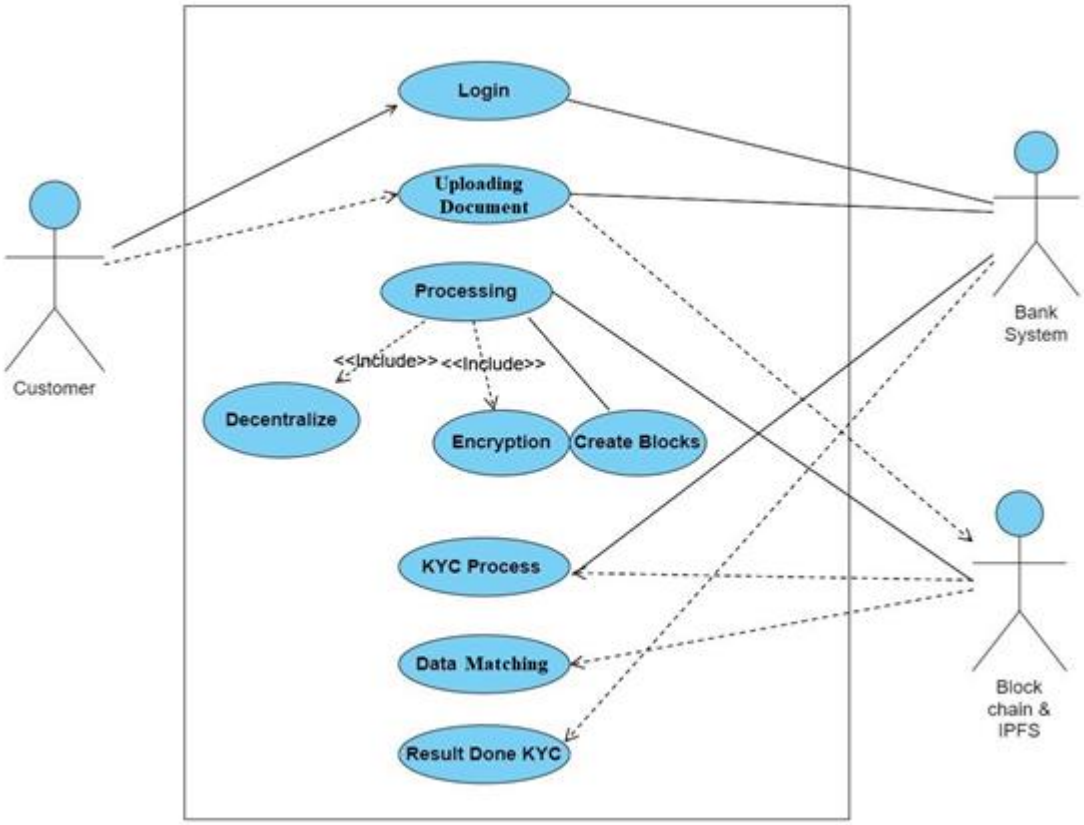


Fig No 4.5: UML Diagram

4.5. Activity Case Diagram

This activity diagram shows how the activity is performed and changed as per the condition.The activity performed by the user and activity performed by system are clearly shown in this diagram. This diagram helps in easy decision in implementation phase.

In this activity diagram, the process begins with starting the KYC process. Then, the KYC data is collected from the customer. Once the KYC data is collected, it is hashed to ensure the security of the data. The hashed KYC data is then added to IPFS, which stores the hash securely. Additionally, the hash is also added to the blockchain to ensure transparency and immutability.

After the hash is added to both IPFS and the blockchain, the KYC data is verified. If the KYC data is approved, the process ends with the KYC being approved.

This activity diagram shows how blockchain and IPFS can be used together to ensure the transparency and security of KYC processes.

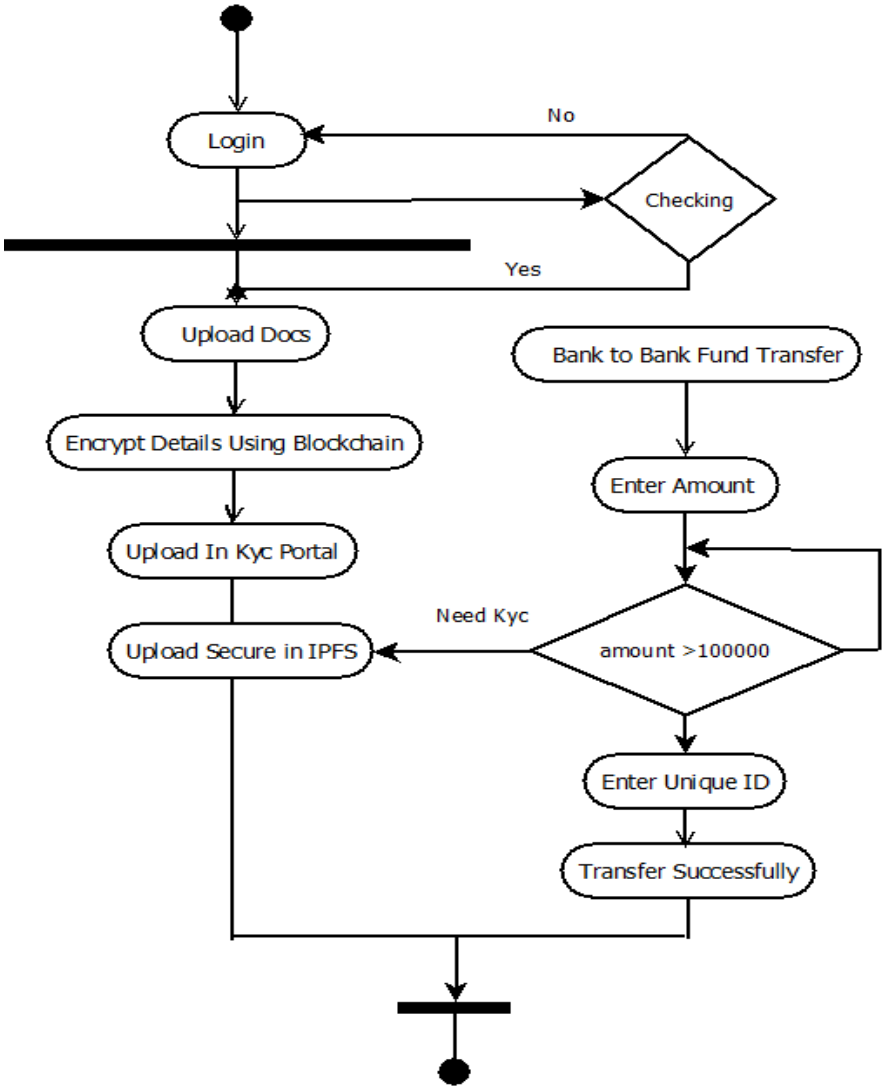


Fig No 4.6. Activity Case Diagram

4.6 Class Diagram

Class Diagram is a static structure diagram that describes the structure of a system by showing the system classes, their attributes, operations and relationships.In this diagram, there are three classes: KYC Record, Blockchain, and IPFS. KYCRecord class represents a single KYC record with the attributes customer ID, customer Data, and docHashes. Customer ID is the unique identifier of the customer, customer Data contains the personal data of the customer, and docHashes contains the hashes of the customer's documents. Blockchain class represents the blockchain technology. It contains methods for adding blocks to the blockchain (add Block ()), verifying blocks (verifyBlock ()), getting blocks (getBlocks ()), and getting the latest hash (getLatestHash ()). IPFS class represents the IPFS technology. It contains methods for adding files to IPFS (addFile()), verifying files (verifyFile()), getting files (getFile()), and deleting files from IPFS (deleteFile()). The associations between the classes indicate that a KYCRecord object can have multiple docHashes, a Blockchain object can have multiple KYCRecord objects, and an IPFS object can have multiple KYCRecord objects.Overall, this class diagram shows how blockchain and IPFS can be used together to ensure transparency and security in KYC processes.

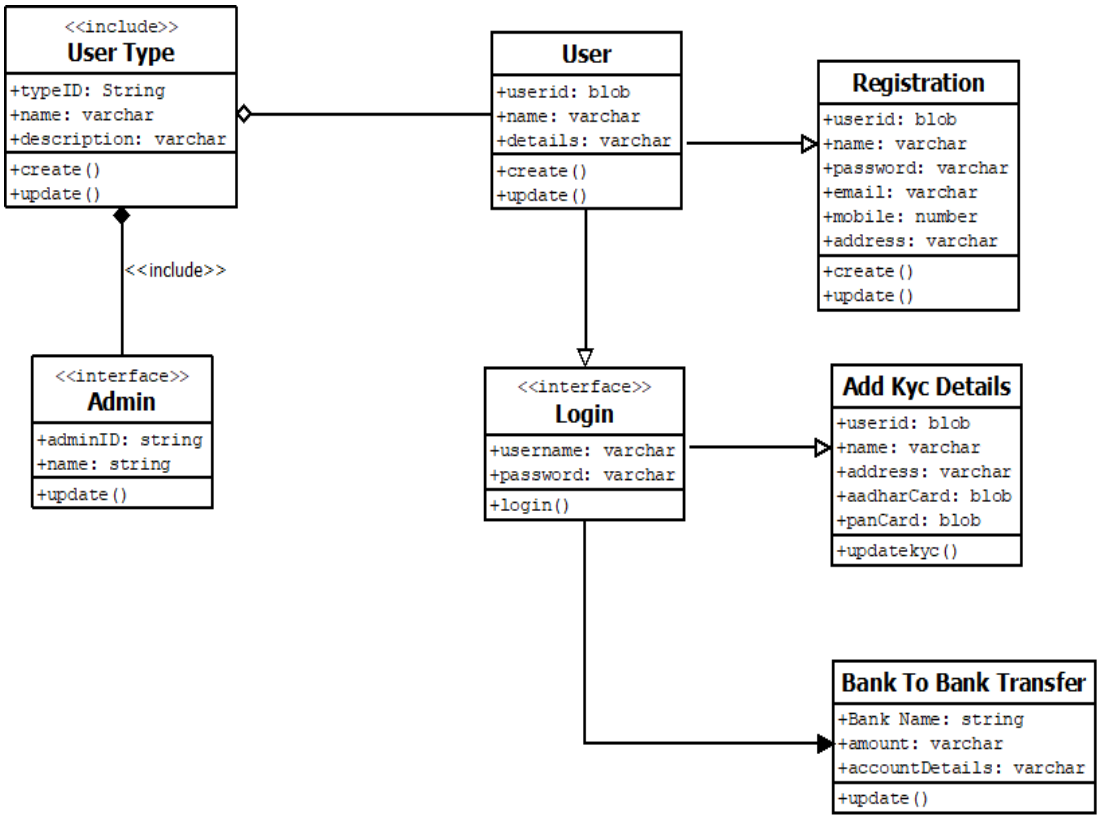


Fig No 4.7. Class Diagram

4.7. Collaboration diagram

A Collaboration diagram is a type of visual presentation that shows how various software objects interact with each other within an overall architecture and how users can bene t from this collaboration. In this collaboration diagram, there are five classes: KYCRecord, Blockchain, IPFS, KYC Process, and KYC Approval. The KYCRecord, Blockchain, and IPFS classes are the same as in the previous diagrams. The KYC Process class is responsible for starting and managing the KYC process. It contains methods for starting the KYC process (startKYC()), collecting the KYC data from the customer (collectData()), hashing the KYC data (hashData()), adding the hash to the blockchain and IPFS (addHash()), and verifying the KYC data (verifyData()). The KYC Approval class is responsible for approving the KYC data. It contains a method for approving the KYC data (approveKYC()).The collaboration diagram shows that the KYC Process class interacts with the KYCRecord, Blockchain, and IPFS classes to ensure the transparency and security of the KYC process. Additionally, the KYC Approval class interacts with the KYC Process class to approve the KYC data.Overall, this collaboration diagram shows how the different classes collaborate to ensure the transparency and security of the KYC process using blockchain and IPFS technology.

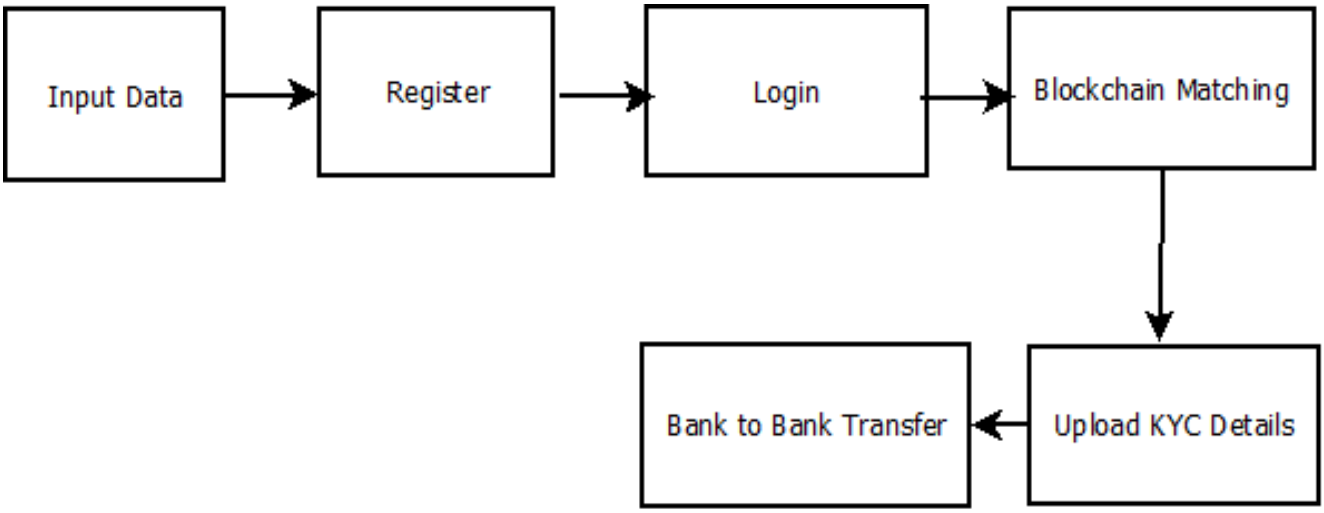


Fig No 4.8.Collaboration diagram

4.8. Deployment diagram

A Deployment diagram Unified Modelling Language models the physical deployment of artefact on nodes. The deployment diagram shows what the hardware component, what the software component run on each node and how the different pieces are connected.

A Deployment diagram Unified Modelling Language models the physical deployment of artefact on nodes. The deployment diagram shows what the hardware component, what the software component run on each node and how the different pieces are connected.

A Deployment diagram Unified Modelling Language models the physical deployment of artefact on nodes. The deployment diagram shows what the hardware component, what the software component run on each node and how the different pieces are connected.

A Deployment diagram Unified Modelling Language models the physical deployment of artefact on nodes. The deployment diagram shows what the hardware component, what the software component run on each node and how the different pieces are connected.

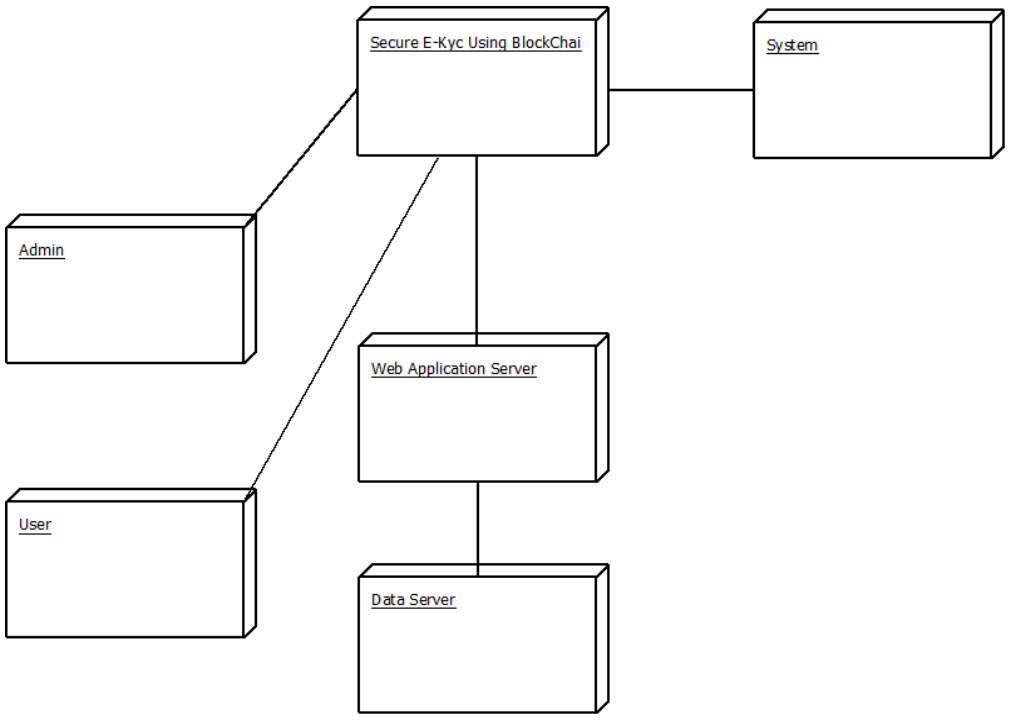


Fig No 4.9. Deployment diagram

4.9 Sequence diagram

A Sequence diagram is a interaction diagram that shows how processes operate with one another and in what order. It is a construct of a message sequence chart. A sequence diagram shows object interaction arrange in time sequence. The sequence of messages exchange between the objects needed to carry out the functionality of the scenario**.**

Sequence Diagram

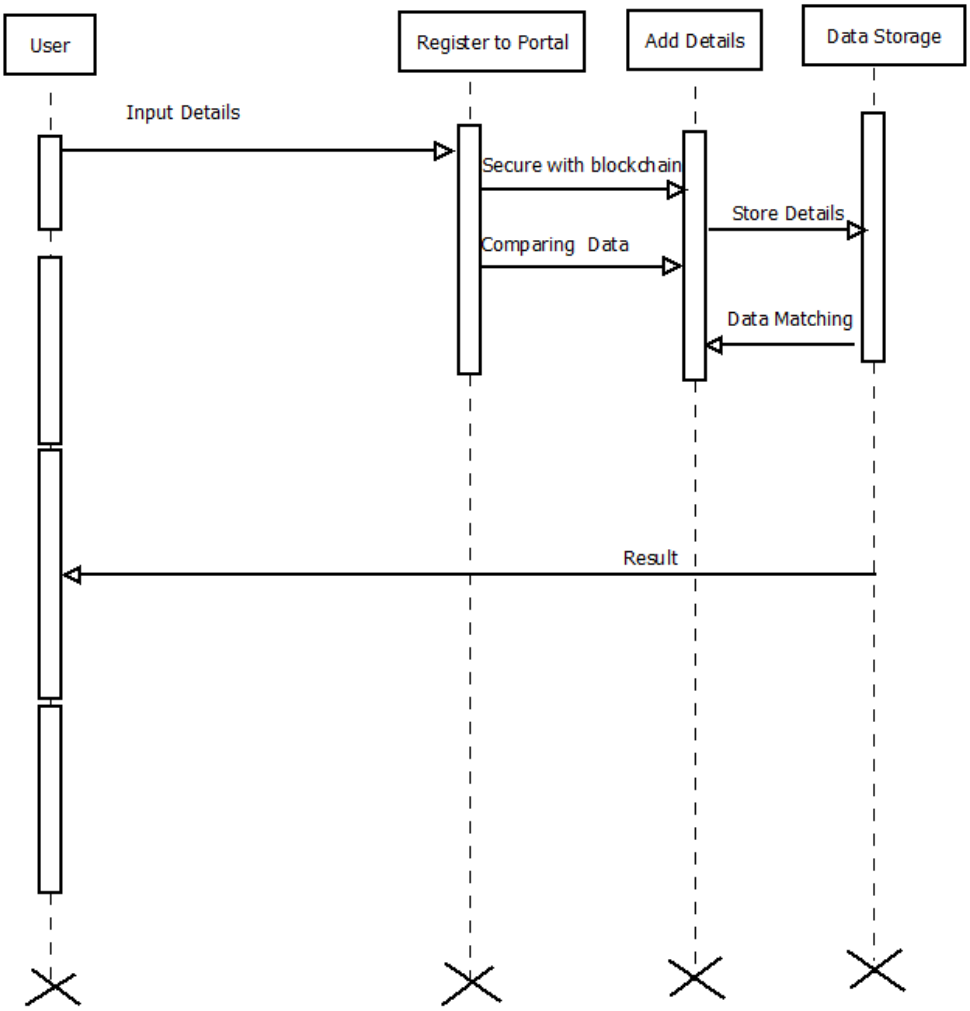


Fig No 4.10. Sequence Diagram for Voter

4.10 Module Analysis

4.10.1 Modules

1. **Register**
2. **Login**
3. **Upload KYC**
4. **Fund Transfer**
5. **Bank Login**
6. **Create Account**
7. **Verify KYC**
8. **View Account**

4.10.2 Purpose of Module:

1. **Register:**

This is the first module in our project through which customer need to done his registration for getting the benefits of the other modules for doing the KYC through our portal.

For doing the registration user need to enter his first name, last name, appropriate email address, his/ her contact number and the password as pan card number. After filling all the registration details we user clicks on submit button the all the details get inserted into the database.

Now, user is able to use the KYC facility after doing login into the portal from login tab.

2. **Login:**

For getting into the KYC portal user need enter his/her contact number and the password when he/she enter while doing the registration.

After doing login, the user is permit access the other modules of the system like Upload KYC, Fund Transfer, Create Account, Verify KYC.

3. **Upload KYC :**

This module is the core module of our system through which user need to put his Aadhar card number, pan card number also need to upload original copy of the Aadhar and Pan cards.

When user enters the details then after submitting it, the data is stored into database

4. **Fund Transfer:**

After completing the upload KYC task then customer is allowed to transfer the fund to any other account. For doing the fund transfer customer need to enter the account holder's name, accurate account number, IFSC code of the respective bank and the amount greater than 1 lakh. By completing all the process customer can successfully transfer money to any one

5. **Bank Login:**

This tab allow bank authorize person to perform the verification process of the customer's KYC details at the bank side. For doing this, bank to login into their side by entering the bank's username and password.

6. **Create Account:**

After doing the bank login, bank should create customer account into our portal by using the create account tab. For creating the account into our portal, bank need to enter his name, contact number, email address and his own permanent address. After entering all the details, the details of user get added into the database.

7. **Verify KYC:**

After creating the account of the customer at bank side, then bank has right to verify the KYC of the customer by entering the Unique id or the files of the Aadhar and Pan card. If the verification is done then details of the customer is visible on the screen .

8. **View Account :**

This also one tab which is accessible to the bank side which holds the details like Account number, Contact number, Email Address and the Address of the customer of all the Users who create their account on our portal.

4.10.3 Algorithm

Step 1: Collect customer data from various sources, including government-issued identification documents, proof of address, and other relevant information.

```
D = collect_customer_data()
```

Step 2: Encrypt the data using a strong encryption algorithm to ensure the privacy and security of the customer's personal information.

```
E = encrypt(D)
```

Step 3: Generate a unique hash value for the encrypted data using a secure hashing algorithm. This hash value will serve as a unique identifier for the customer's KYC information.

```
H = hash(E)
```

Step 4: Upload the encrypted data to the IPFS network, which provides a decentralized and tamper-proof system that ensures the data cannot be lost or tampered with.

```
ipfs_hash = IPFS.upload(E)
```

Step 5: Store the hash value on the blockchain, which provides an immutable record of the customer's KYC information.

```
blockchain_tx = Blockchain.store(H)
```

Step 6: Implement access controls to ensure that only authorized personnel can access the customer's KYC information.

```
authorized_users = get_authorized_users()
if user in authorized_users:
    // Access customer data
    customer_data = IPFS.get(ipfs_hash)
else:
    // Raise unauthorized access exception
```

Step 7: Record all transactions related to the customer's KYC information on the blockchain, including who accessed it and when, to provide an audit trail and increase transparency.

```
transaction_log = []
transaction_log.append((E, H, timestamp, user))
Blockchain.record(transaction_log)
```

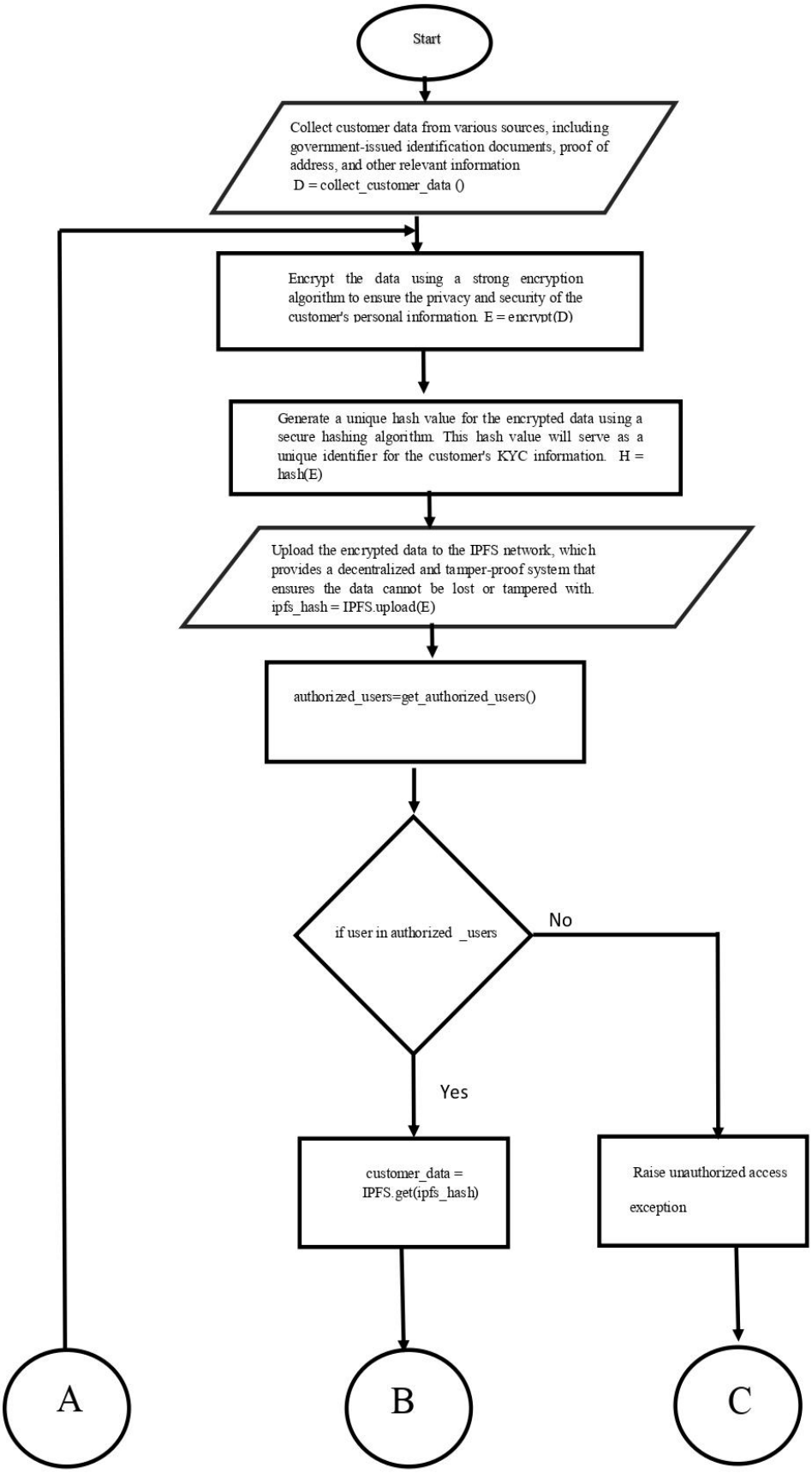
Step 8: When a customer's KYC information is updated, repeat steps 2 to 7, but using the same hash value generated in step 3. This ensures that the customer's KYC information remains linked to the same identifier and that the old information is not lost.

```
D_new = update_customer_data(D)
```

```
E_new = encrypt(D_new)

H_new = H

ipfs_hash_new = IPFS.upload(E_new)

 if H_new != hash(E_new):

      H_new = hash(E_new)

      blockchain_tx_new = Blockchain.store(H_new)

      transaction_log_new = []

      transaction_log_new.append((E_new, H_new, timestamp, user))

      Blockchain.record(transaction_log_new)
```

4.10.4 Flowcharts

Flowcharts are nothing but the graphical representation of the data or the algorithm for a better understanding of the code visually. It displays stepby-step solutions to a problem, algorithm, or process. It is a pictorial way of representing steps that are preferred by most beginner-level programmers to understand algorithms of computer science, thus it contributes to troubleshooting the issues in the algorithm. A flowchart is a picture of boxes that indicates the process flow in a sequential manner. Since a flowchart is a pictorial representation of a process or algorithm, it's easy to interpret and understand the process. To draw a flowchart, certain rules need to be followed which are followed by all professionals to draw a flowchart and is widely accepted all over the countries.


Start
Collect customer data from various sources, including government-issued identification documents, proof of address, and other relevant information
D = collect_customer_data ()
Encrypt the data using a strong encryption algorithm to ensure the privacy and security of the customer's personal information. E = encrypt(D)
Generate a unique hash value for the encrypted data using a secure hashing algorithm. This hash value will serve as a unique identifier for the customer's KYC information. H = hash(E)
Upload the encrypted data to the IPFS network, which provides a decentralized and tamper-proof system that ensures the data cannot be lost or tampered with.
ipfs_hash = IPFS.upload(E)
authorized_users=get_authorized_users()
if user in authorized _users
No
Yes
customer_data = IPFS.get(ipfs_hash)
Raise unauthorized access exception
A
B
C

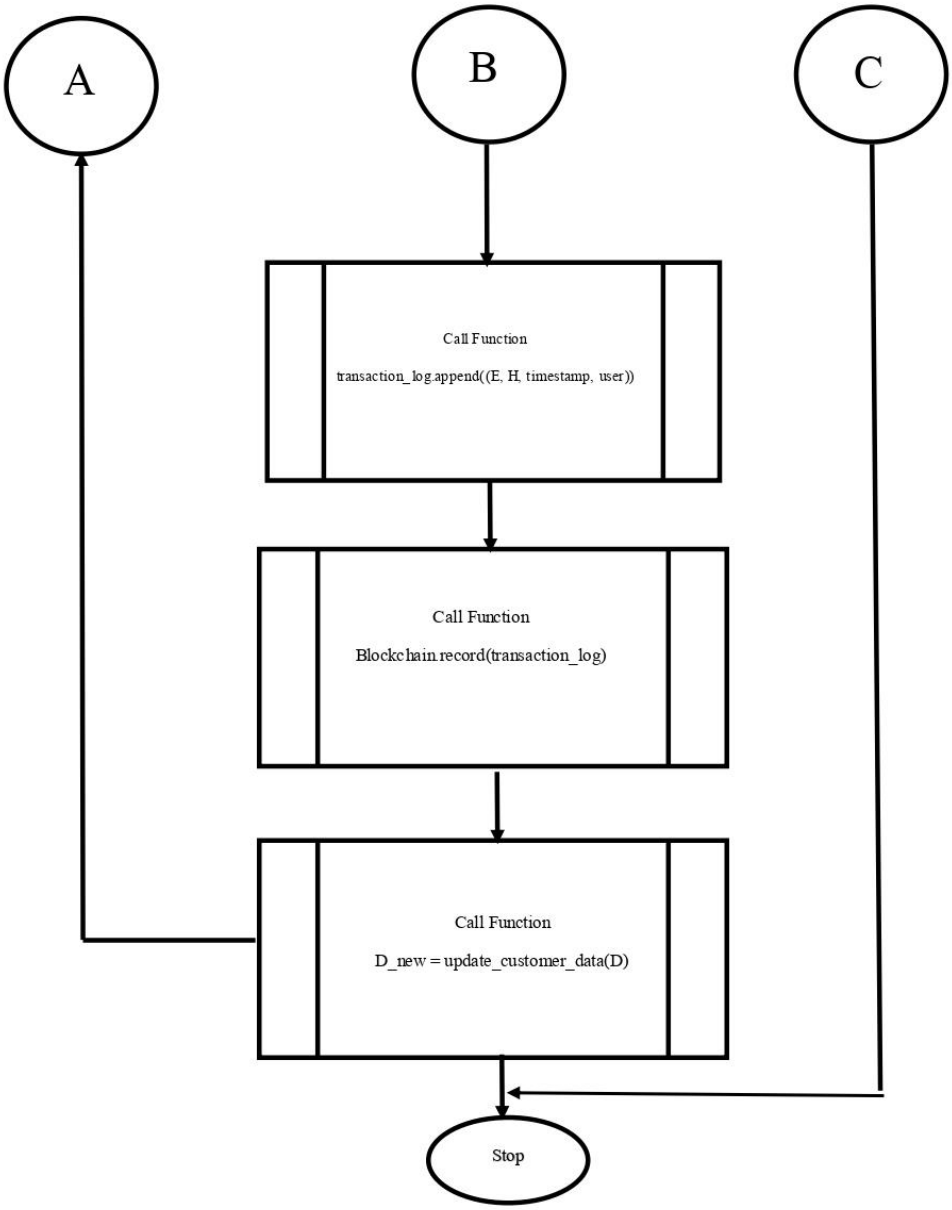


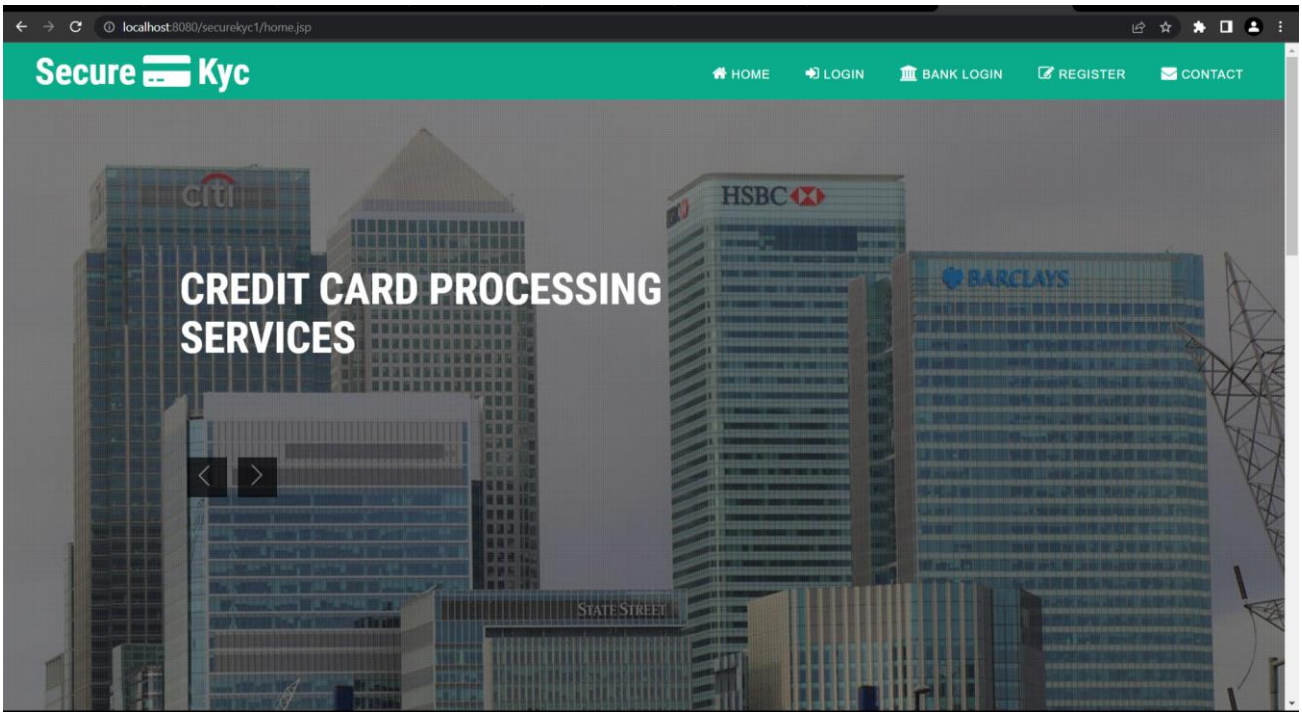
Fig No 4.5.1. flow chart

CHAPTER 5

RESULTS AND SCREENSHOTS WITH EXPLANATION

1 Home Page

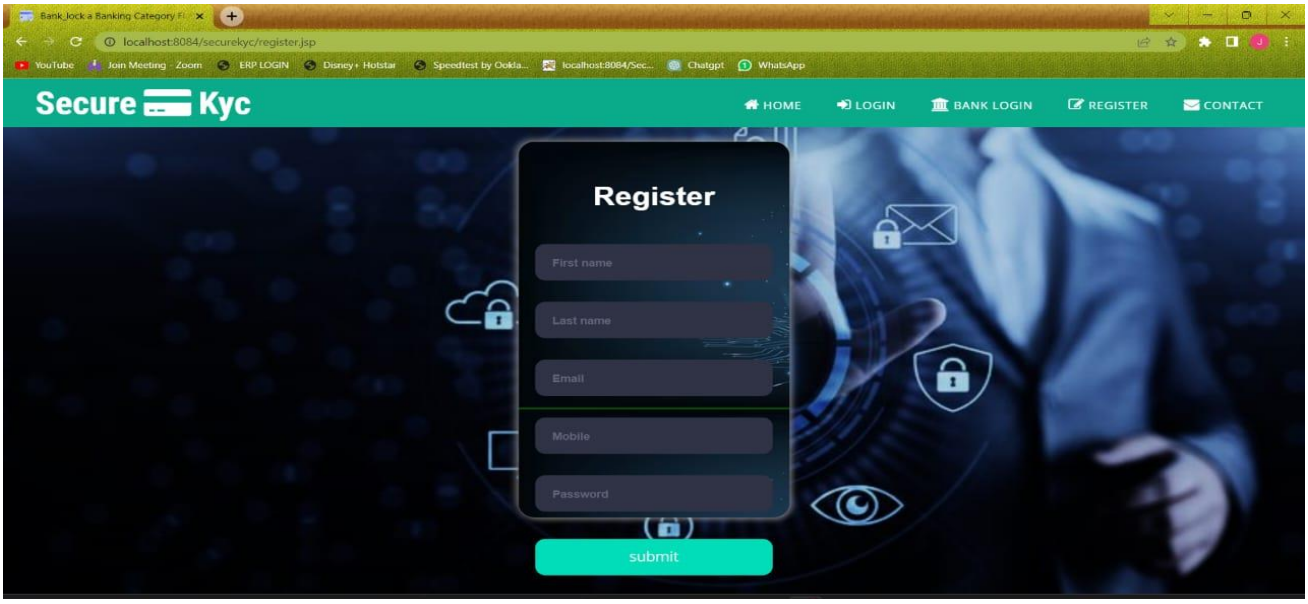
It is the first page of our website. In this top of the side Various action can be perform by clicking on different option such as Customer Login , Bank Login , User Registration , Contact us.



2 Registration Page

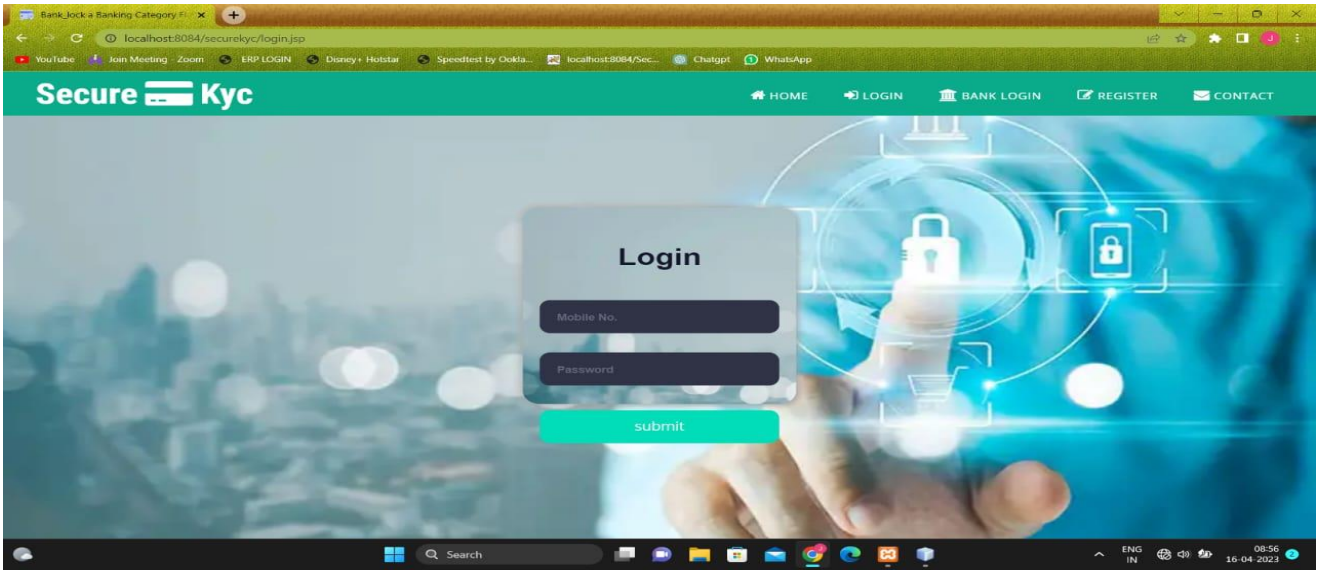
The registration module is a component that allows users to sign up and create an account on a website. It typically includes a form where users can enter their personal information, which is then saved in a database for future use. The registration module is a critical component of any online service that requires user authentication and authorization. On this Mobule , various fields are listed, such as first name, last name, email, mobile number, and password, are used in the registration module.

- First name: This is the user's given name, which may or may not include a middle name or initial. It's often used to personalize communications with the user.
- Last name: This is the user's family name or surname. Like the first name, it's often used to personalize communications with the user.
- Email: This is the user's email address, which is used for communication and as a unique identifier for their account.
- Mobile number: This is the user's phone number, which may be used for verification purposes or for sending text messages related to their account.
- Password: This is a secret code chosen by the user that is used to authenticate their identity and protect their account from unauthorized access.



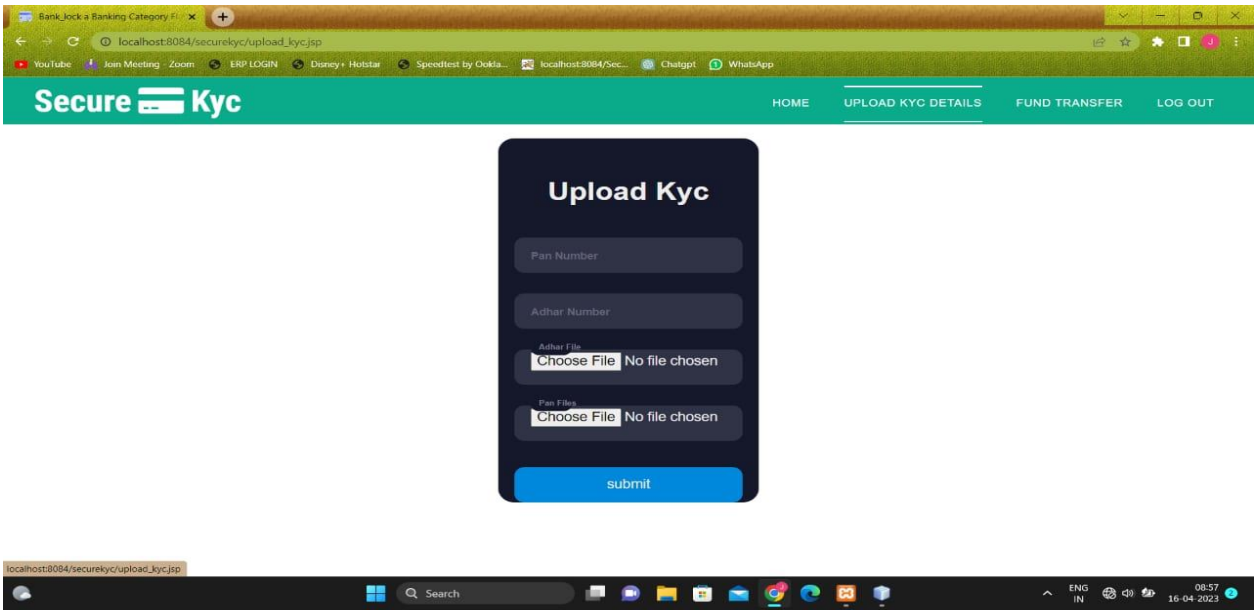
3 Login Page

For getting into the KYC portal user need enter his/her contact number and the password when he/she enter while doing the registration. After doing login, the user is permit access the other modules of the system like Upload KYC, Fund Transfer, Create Account, Verify KYC



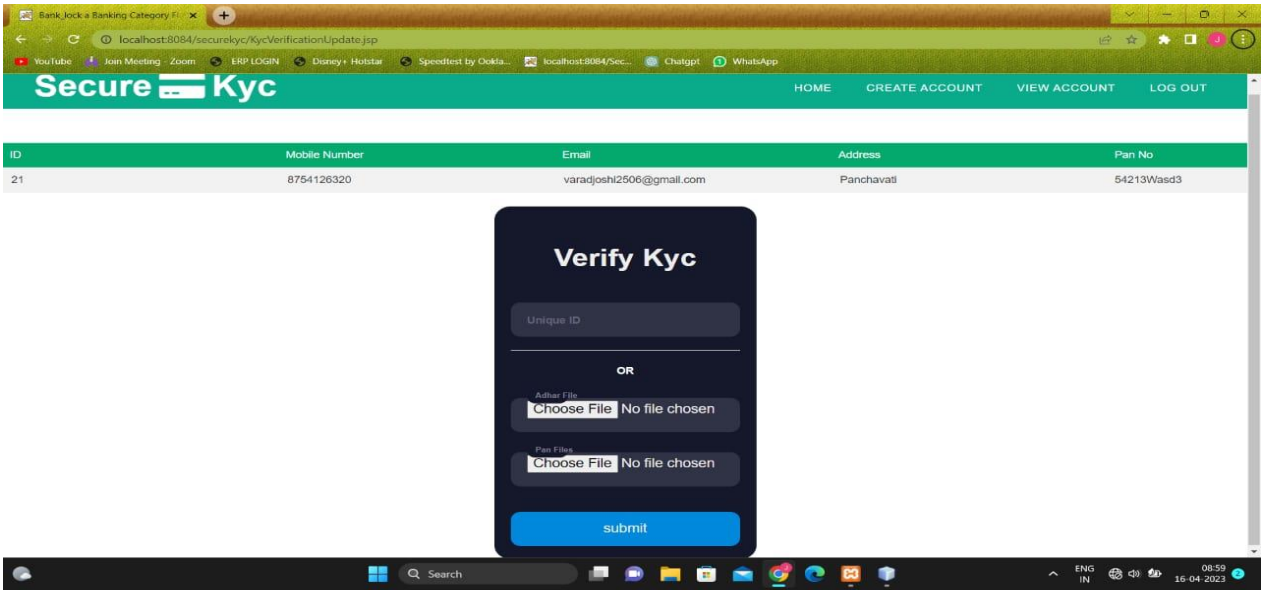
4 Upload KYC

This module is the core module of our system through which user need to put his Aadhar card number, pan card number also need to upload original copy of the Aadhar and Pan cards.
When user enters the details then after submitting it, the data is stored into database



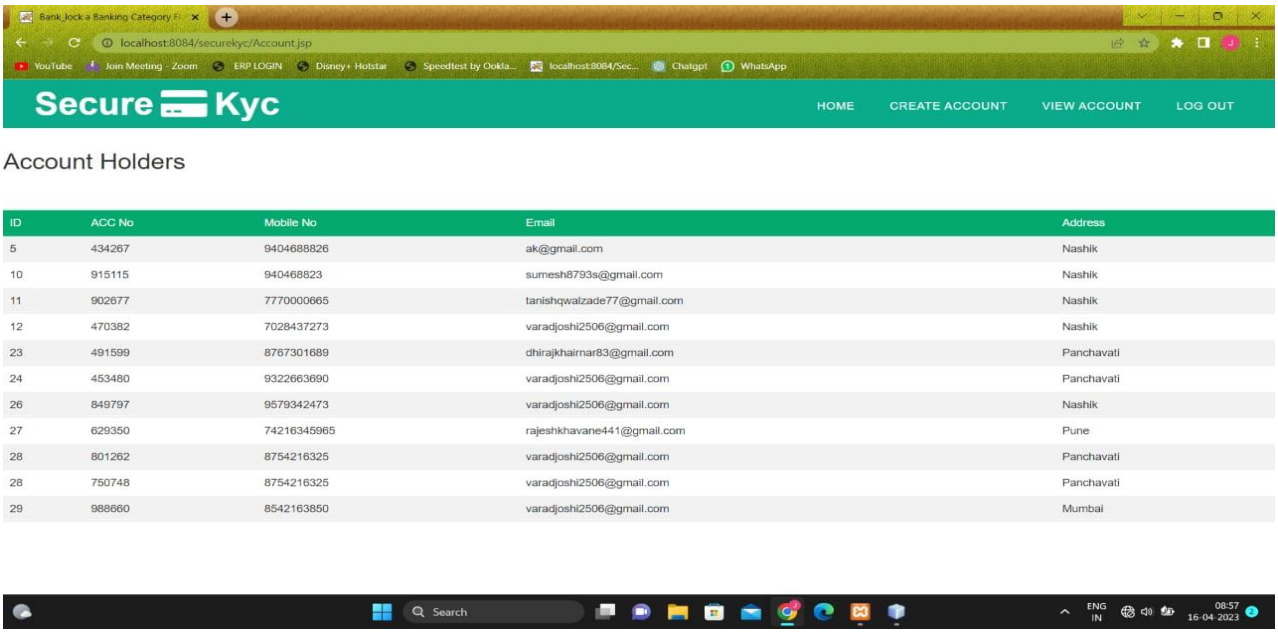
5 Verify KYC

After creating the account of the customer at bank side, then bank has right to verify the KYC of the customer by entering the Unique id or the files of the Aadhar and Pan card. If the verification is done then details of the customer is visible on the screen .



6 Account Holders

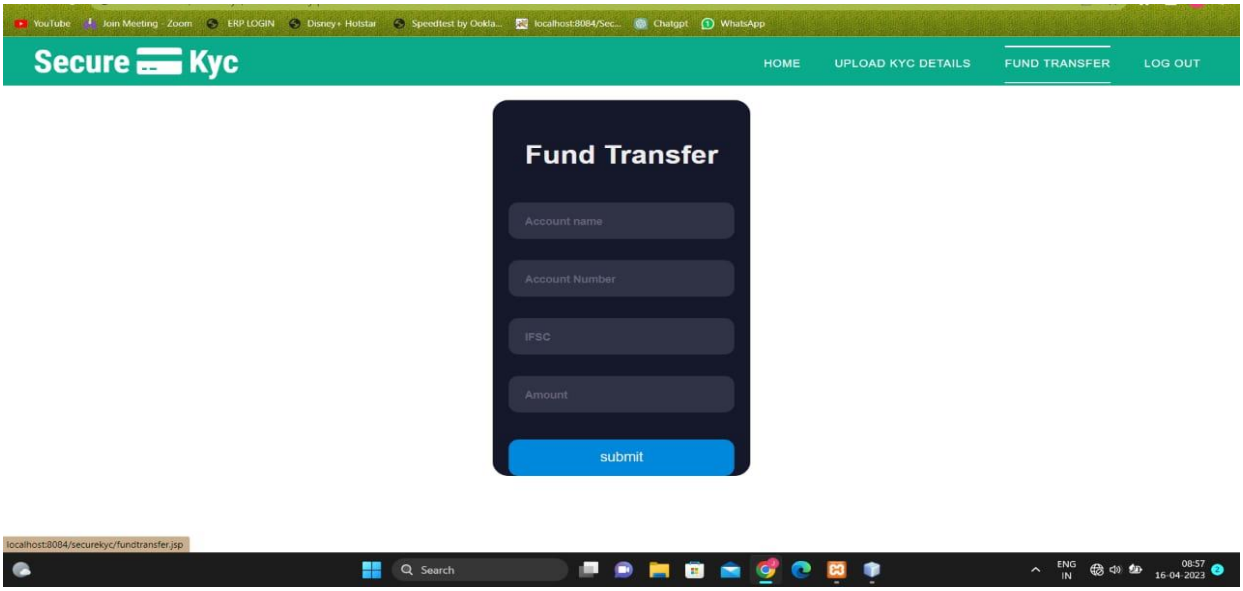
This also one tab which is accessible to the bank side which holds the details like Account number, Contact number, Email Address and the Address of the customer of all the Users who create their account on our portal.



ID	ACC No	Mobile No	Email	Address
5	434267	9404688826	ak@gmail.com	Nashik
10	915115	940468823	sumesh8793s@gmail.com	Nashik
11	902677	7770000665	tanishqwalzade77@gmail.com	Nashik
12	470382	7028437273	varadjoshi2506@gmail.com	Nashik
23	491599	8767301689	dhirajkhairnar83@gmail.com	Panchavati
24	453480	9322663690	varadjoshi2506@gmail.com	Panchavati
26	849797	9579342473	varadjoshi2506@gmail.com	Nashik
27	629350	74216345965	rajeshkhavane441@gmail.com	Pune
28	801262	8754216325	varadjoshi2506@gmail.com	Panchavati
28	750748	8754216325	varadjoshi2506@gmail.com	Panchavati
29	988660	8542163850	varadjoshi2506@gmail.com	Mumbai

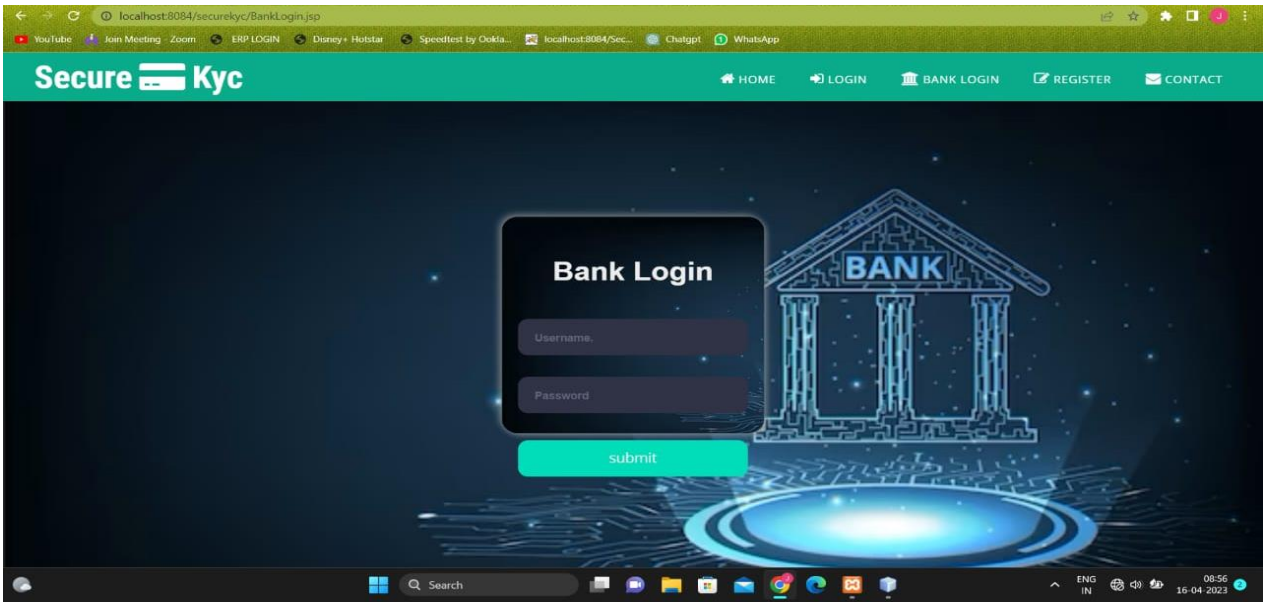
7 Fund Transfer.

After completing the upload KYC task then customer is allowed to transfer the fund to any other account. For doing the fund transfer customer need to enter the account holder's name, accurate account number, IFSC code of the respective bank and the amount greater than 1 lakh. By completing all the process customer can successfully transfer money to any one



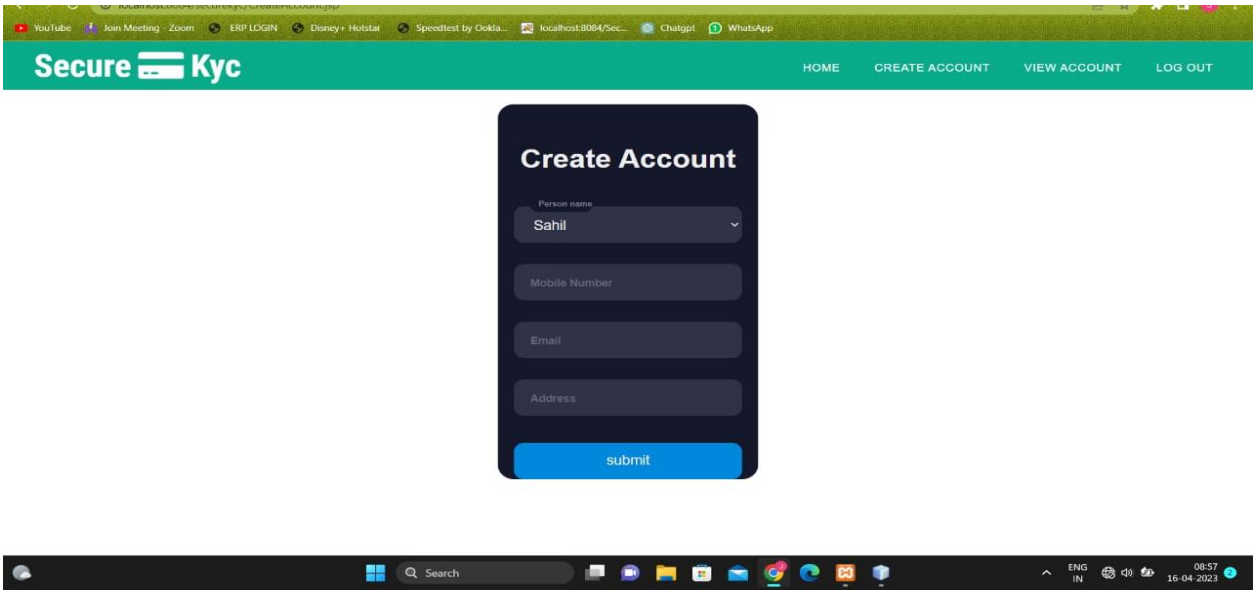
8 Bank Login

This page allow bank authorize person to perform the verification process of the customer's KYC details at the bank side. For doing this, bank to login into their side by entering the bank's username and password.



9 Create Account

After doing the bank login, bank should create customer account into our portal by using the create account option. For creating the account into our portal, bank need to enter his name, contact number, email address and his own permanent address. After entering all the details, the details of user get added into the database.



CHAPTER 6

TESTING

6.1 Introduction

Information Processing has undergone major improvements in the past two decades in both hardware and software. Hardware has decreased in size and price, while providing more and faster processing power. Software has become easier to use, while providing increased capabilities. There is an abundance of products available to assist both end-users and software developers in their work. Software testing, however, has not progressed significantly. It is still largely a manual process conducted as an art rather than a methodology. It is almost an accepted practice to release software that contains defects.

Software that is not thoroughly tested is released for production. This is true for both off-the-shelf software products and custom applications. Software vendor and in-house systems developers release an initial system and then deliver fixes to the code. They continue delivering fixes until they create a new system and stop supporting the old one. The user is then forced to convert to the new system, which again will require fixes.

In-house systems developers generally do not provide any better level of support. They require the users to submit Incident Reports specifying the system defects. The Incident Reports are then assigned a priority and the defects are fixed as time and budgets permit.

6.2 Importance of Testing

Testing is difficult. It requires knowledge of the application and the system architecture. The majority of the preparation work is tedious. The test conditions, test data, and expected results are generally created manually. System testing is also one of the final activities before the system is released for production. There is always pressure to complete systems testing promptly to meet the deadline. Nevertheless, systems testing are important.

In mainframe when the system is distributed to multiple sites, any errors or omissions in the system will affect several groups of users. Any savings realized in downsizing the application will be negated by costs to correct software errors and reprocess information.

Software developers must deliver reliable and secure systems that satisfy the user's requirements. A key item in successful systems testing is developing a testing methodology rather than relying on individual style of the test practitioner. The systems testing effort must follow a defined strategy. It must have an objective, a scope, and an approach. Testing is not an art; it is a skill that can be taught.

Testing is generally associated with the execution of programs. The emphasis is on the outcome of the testing, rather than what is tested and how it's tested. Testing is not a one-step activity; execute the test. It requires planning and design. The tests should be reviewed prior to execution to verify their accuracy and completeness. They must be documented and saved for reuse.

System testing is the most extensive testing of the system. It requires more manpower and machine processing time than any other testing level. It is therefore the most expensive testing level. It is critical process in the system development. It verifies that the system performs the business requirements accurately, completely, and within the required performance limits. It must be thorough, controlled and managed.

6.3 Testing Definitions

Software development has several levels of testing.

- Unit Testing
- Systems Testing
- Acceptance Testing

6.3.1 Unit Testing

The first level of testing is called unit testing which is done during the development of the system. Unit testing is essential for verification of the code produced during the coding phase. Errors were been noted down and corrected immediately. It is performed by the programmer. It uses the program specifications and the program itself as its source. Thus, our modules are individually tested here. There is no formal documentation required for unit-testing program.

6.3.2 Integration Testing

The second level of testing includes integration testing. Here different dependent modules are assembled and tested for any bugs that may surface due to the integration of modules. Thus, the administrator module and various visa immigration modules are tested here.

6.3.3 Systems Testing

The third level of testing includes systems testing. Systems testing verify that the system performs the business functions while meeting the specified performance requirements. It is performed by a team consisting of software technicians and users. It uses the Systems Requirements document, the System Architectural Design and Detailed Design Documents, and the Information Systems Department standards as its sources. Documentation is recorded and saved for systems testing.

6.3.4 Acceptance Testing

The final level of testing is the acceptance testing. Acceptance testing provides the users with assurance that the system is ready for production use; it is performed by the users. It uses the System Requirements document as its source. There is no formal documentation required for acceptance testing.

Systems testing are the major testing effort of the project. It is the functional testing of the application and is concerned with following,

1. Quality/standards compliance
2. Business requirements
3. Performance capabilities
4. Operational capabilities

Below are defined a few test cases which have been implemented for the various screens. The outputs have been registered and the required changes have been incorporated.

6.4 Test Cases

Test Cases for Admin Login

Module Name: Admin Module **Testing Type:** Unit Testing **Test Objective:** To check GUI working of all the functionalities **Test Performed by:**				
Test Case ID	**Description**	**Expected Result**	**Actual Result**	**Status**
TC-1	Enter the ID and password	Admin should get logged into the System	Admin login successful	Pass
TC-2	View Login panel	Admin Login dashboard should be displayed	Admin Dashboard displayed	Pass

Table 6.1 Admin Modules test cases.

Test Cases for Add Kyc Module

Module Name: Add Kyc Module **Testing Type:** Unit Testing **Test Objective:** To check GUI working of all the functionalities **Test Performed by:**				
Test Case ID	**Description**	**Expected Result**	**Actual Result**	**Status**
TC-1	Add Kyc Details	Adhar,Pan, Name, Added	Data Updated Successfully	Pass
TC-2	View Kyc	Details Should be View	View Successfully	Pass

Table 6.2 kyc module test cases .

6.4.1 Functional testing

1. login Module

TEST CASE ID	DESCRIPTION	TEST DATA	STEPS	EXPECTED RESULT	ACTUAL RESULT	PASS/ FAIL
TC_1	To verify when user enters only username without password and press login button	Bhushan @12	Step 1: Open browser Step 2: Enter url of kyc portal Step 3: Enter username Step 4: Press login button Step 5: Stop	Please enter password	Please enter password	Pass
TC_2	To verify when user press login button without entering username and password	-	Step 1: Open browser Step 2: Enter url of kyc portal Step 3: Press login button Step 4: Stop	Please enter username and password	Please enter username and password	Pass
TC_3	To verify when user enters password only	Bhushan 1234	Step 1: Open browser Step 2: Enter url of kyc portal Step 3: Enter password Step 4: Press login button Step 5: Stop	Please enter username	Please enter username	Pass
TC_4	To check whether user enters correct password and incorrect password	Username: Bhushan @12 Password: bhushan @11	Step 1: Open browser Step 2: Enter url of kyc portal Step 3: Enter username and password	Password is invalid	Password is invalid	Pass

			Step 4: Press login button Step 5: Stop			
TC_5	To check whether user enters incorrect username and correct password	Username: Bhushan Password: Bhushan@1234	Step 1: Open browser Step 2: Enter url of kyc portal Step 3: Enter username and password Step 4: Press login button Step 5: Stop	Username is incorrect	Username is incorrect	Pass
TC_6	To verify when user enters incorrect username and password	Username: Bhushan Password: Bhushan@12	Step 1: Open browser Step 2: Enter url of kyc portal Step 3: Enter username and password Step 4: Press login button Step 5: Stop	Username and password is incorrect	Username and password Is incorrect	Pass
TC_7	To verify when user enter correct username and password	Username: Bhushan@12 Password: Bhushan@1234	Step 1: Open browser Step 2: Enter url of kyc portal Step 3: Enter username and password Step 4: Press login button Step 5: Stop	Login successful	Login successful	Pass
TC_8	To verify when user enters correct username and password but captcha field is blank	Username: Bhushan@12 Password:	Step 1: Open browser Step 2: Enter url of kyc portal	Please enter captcha	Please enter captcha	Pass

		Bhushan @1234	Step 3: Enter username and password Step 4: Enter captcha Step 5: Press login button Step 6: Stop			
TC_9	To verify when user enters correct username and password but incorrect captcha	Captcha: 736543	Step 1: Open browser Step 2: Enter url of kyc portal Step 3: Enter username and password Step 4: Enter captcha Step 5: Press login button Step 6: Stop	Invalid captcha	Invalid captcha	Pass
TC_10	To verify when user enters correct username password and captcha	Username: Bhushan @12 Password: Bhushan @1234 Captcha: Ki98DK	Step 1: Open browser Step 2: Enter url of kyc portal Step 3: Enter username and password Step 4: Enter captcha Step 5: Press login button Step 6: Stop	Login successful	Login successful	Pass

Table 6.3 Function testing

6.4.2 Non - Functional testing

TEST CASE ID	DESCRIPTION	STEPS	EXPECTED RESULT	ACTUAL RESULT	PASS/FAIL
TC_1	To check whether websites is compatible with other browsers or not	Step 1: Open different browsers Step 2: Enter url of kyc system in each browser Step 3: Stop	Website is compatible with all the web browsers	Website is compatible with all the web browsers	Pass
TC_2	To check whether all the controls are available on webpage or not	Step 1: Open browser Step 2: Enter url of kyc system Step 3: Stop	All controls are available	All controls are available	Pass
TC_3	To check the response of website	Step 1: Open browser Step 2: Enter url of kyc system Step 3: Stop	Webpage loads within 10 seconds	Webpage takes more time than 10 seconds	Fail
TC_4	To check whether the GUI of webpage is user friendly or not	Step 1: Open browser Step 2: Enter url of kyc system Step 3: Observe the webpage Step 4: Stop	GUI of webpage is very easy to operate	GUI of webpage is very easy to operate	Pass
TC_5	To check whether webpage fetches record from all the servers in sequential manner or not	Step 1: Open browser Step 2: Enter url of kyc system Step 3: Request for fetching the data Step 3: Stop	Record fetched in sequential manner	Record fetch in sequential manner	Pass

Table 6.4 Non Functional testing .

CHAPTER 7

COST ESTIMATION

7.1 Project Cost Estimation.

Step 1: Measure the size in terms of the amount of functionality in a system. Function points are computed by first calculating an unadjusted function point count (UFC).

Sno.	Function points	Number	Description
1	User inputs	5	User Login, upload kyc details , fund transfer , Bank Login , Create Account
2	User outputs	3	Verify KYC , Unique id , KYC uploaded
3	User requests	2	Unique id , upload KYC
4	Internal Files	1	Database
5	External interfaces	1	KYC uploaded.

Step 2: Multiply each number by a weight factor according to complexity of the parameter, associated with that number.

Complexity considered is average.

Sno.	Function points	Number	Weight Factor	Multiplication
1	User inputs	5	8	40
2	User outputs	3	6	18
3	User requests	2	4	8
4	External interfaces	1	10	10
5	Internal files	1	4	4

Step 3: Calculate the total UFP (Unadjusted function points) by adding the multiplication column in above table

UFP = 40+18+8+10+4

= 80

Step 4: Calculate the total TCF (Technical Complexity Factor) by giving a value between 0 and 5

Sr no.	Technical Complexity Factor	Value
1	Data communication	5
2	Distributed Data Processing	5
3	Performance criteria	4
4	Heavily Utilized Hardware	1
5	High Transaction Rates	2
6	Online Data Entry	5
7	Online Updating	4
8	End user efficiency	4
9	Complex Computations	2
10	Reusability	4
11	Ease of Installation	5
12	Ease of Operation	5
13	Portability	3
14	Maintainability	4

Step 5: Sum the resulting numbers to obtain DI (degree of influence) by adding the value column in above table

DI = **53**

Step 6: TCF (Technical Complexity Factor) by given formula

TCF = 0.65+0.01*DI

= 0.65+0.01*53

= **1.18**

Step 7: Calculate FP (Function Points) using the given formula

FP = UFP*TCF

= 80*1.18

= **94.4**

Step 8: To find KLOC (Lines of code) using language factor and FP

Language factor of JSP = 53

KLOC= Language factor * FP

= 53*94.4 = **5.00**

Step 9: To calculate the effort and nominal development time using given formula and constants

Effort = $a_1*(KLOC)^{a_2}$ PM

Tdev =$b_1*(Effort)^{b_2}$ Months

Development mode considered is Organic.

Values of the constants in the Organic Development mode:

a_1=2.4 a_2=1.05 b_1=2.5 b_2=0.38

Effort = 2.4*(5.00)^$^{1.05}$

= **13.00 PM**

Tdev =2.5*(13.00)^$^{0.38}$

= **6.62 Months**

Step 10: Calculate the cost required to develop product by multiplying development time and average salary of engineers

Average salary is 2400

Cost required to develop the product = 6.62 * 2400

= **15,888**

Hence the total cost required to develop the product is ₹ 15,888 /-

CHAPTER 8

APPLICATIONS

1. Access control system for digital contents distribution.

Blockchain can be used to create a secure access control system for digital content distribution, such as music, movies, or ebooks. This system can allow content owners to track and control the distribution of their content, while ensuring that only authorized users can access it. Blockchain's decentralized and immutable nature can prevent unauthorized modifications or tampering of the distribution records.

2. Media Database Systems.

can be used to create a decentralized and transparent media database system that allows creators to protect their intellectual property rights and get compensated for their work. For example, musicians can register their songs on a blockchain-based platform that automatically tracks their usage and ensures they receive appropriate royalties. This can help eliminate intermediaries and reduce transaction costs.

3. Can be used to hide a secret chemical formula or plans for a new invention.

Blockchain can be used to store and protect confidential information, such as a secret chemical formula or plans for a new invention, Government database and Military database. The information can be encrypted and stored on a blockchain, with access restricted to authorized parties through a secure key. The decentralized and immutable nature of blockchain can prevent unauthorized modifications or tampering of the information.

4. Though attempts have been made to provide privacy for cryptocurrency and some types of smart contracts and Preserving digital evidences

Blockchain can provide privacy for certain types of transactions and smart contracts by using techniques such as zero-knowledge proofs or homomorphic encryption. These techniques can allow parties to prove that certain conditions have been met without revealing the actual details of the transaction or contract.

And the tamper-proof and transparent record of digital evidence, such as legal documents, contracts, or digital identity. This can help prevent fraud and disputes by ensuring that the evidence is authentic, unalterable, and easily accessible. Blockchain can also help automate and streamline the process of collecting and verifying digital evidence, reducing the time and cost involved.

5. Pervasive Decentralization of Digital Infrastructures: A Framework for Blockchain Enabled System and Use Case Analysis :

Technological innovation and consequential decentralisation are driving forces in the ongoing evolution and increasing openness of digital infrastructures and services. One of the most discussed and allegedly disruptive innovations is the distributed database technology referred to as blockchain. Although it is still in its technological infancy, experimental adoption and customization seem to be in full progress in various potential fields of application ranging from decentralized grids for computation and storage to global financial services. However, the technology and its path of development still entail a lot of common unknowns for practitioners and researchers alike. Especially regarding the question how the technology could amend or be incorporated into the existing landscape of digital services, processes and infrastructures.

6.A Lightweight Multi-tier S-MQTT Framework to Secure Communication between low-end IoT Nodes

The evolution and expansion of networking technologies have managed to create large scale connectivity among versatile devices and applications that led to the jargon internet of things (IoT). IoT has evolved due to the convergence of wireless sensor networks (WSN) and internet technologies with a view to approaching towards smart city prospects. In IoT, for maintaining device to device communication, HTTP protocol has been used for remote monitoring and analysis of data from large number of sensing elements but it consumes more power, have comparatively lesser efficiency of transmission and cannot utilize system bandwidth efficiently as well. Thus the protocols MQTT (Message Queuing Telemetry Transport), AMQP and CoAP are quite capable of handling wireless sensor traffic under very low bandwidth and constrained network conditions. Security is also another major concern as IoT applications collect private data and allow access to various control functions over the internet.

7.The Blockchain as a Decentralized Security Framework

The blockchain is emerging as one of the most propitious and ingenious technologies of cybersecurity. In its germinal state itself, the technology has successfully replaced economic transaction systems in various organizations and has the potential to revamp heterogeneous business models in different industries. Although it promises a secure distributed framework to facilitate sharing, exchanging and integration of information across all the users and third parties, it is important for the planners and decision-makers to analyse it in-depth for its suitability in their industry and business applications. The blockchain should be deployed only if it is applicable and provides security with better opportunities in obtaining increased revenue and reductions in cost. This article presents an overview of this technology for realization of security across distributed parties in an impregnable and transparent way.

8.A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience Applications

Rapid advancement of Internet of Things (IoT) and cloud computing enables neuroscientists to collect multilevel andmultichannel brain data to better understand brain functions, diagnose diseases, and devise treatments. To ensure secure andreliable data communication between end-to-end (E2E) devices supported by current IoT and cloud infrastructures, trustmanagement is needed at the IoT and user ends. This paper introduces an adaptive neuro-fuzzy inference system (ANFIS)brain-inspired trust management model (TMM) to secure IoT devices and relay nodes, and to ensure data reliability. Theproposed TMM utilizes both node behavioral trust and data trust, which are estimated using ANFIS, and weighted additivemethods respectively, to assess the nodes trustworthiness. In contrast to existing fuzzy based TMMs, simulation resultsconfirm the robustness and accuracy of our proposed TMM in identifying malicious nodes in the communication network.With growing usage of cloud based IoT frameworks in Neuroscience research, integrating the proposed TMM into existinginfrastructure will assure secure and reliable data communication among E2E devices

CHAPTER 9

FUTURE SCOPE

With the current rate of growth of the banking sector, such an approach really has the ability to bring about big improvement and shared gain to all of concerned stakeholder.

In the future, blockchain-based KYC utilities will help bring cost savings to any industry that relies on identity verification. This is because the technology will allow banks and other financial institution to rely on a more secure organized unified model of data handling.

Blockchain technology in banking revolutionizes the system by building a decentralized database of digital and unique assets. Through a distributed ledger, it becomes easier to transfer the assets through tokens that represent the assets “off-chain”.

Blockchain is chain of blocks which contains the information of transactions. In this paper we have discussed about some mining techniques and architecture of blockchain. We have also discussed use for algorithms and its limitations. Nowadays Blockchain is growing faster but it still has many limitations such as redundancy, complexity, energy and resource consumption, security flaws etc. One of the limitations of blockchain is storage issue. The future research direction would be solution for storage issue of blockchain. What will happen if blockchain is combined with cloud technology? How it will affect the storage and security issue of blockchain.

CHAPTER 10

CONCLUSION

Blockchains represent the future of transactions and are beginning to transform entire industries. Consequently, there is considerable interest in exploring blockchains for various industry use cases. They are particularly useful in supporting multi-party business transactions where the entities need not trust each other. The immutable, cryptographically secured, and replicated, ledger, consensus to validate transactions, and permissioned access are all attractive salient attributes for enterprises to consider blockchains as the future transaction network.

CHAPTER 11

REFERENCES

11.1 REFERENCES

1]Implementation of Least Significant Bit Image Steganography with Advanced Encryption Standard Adit Pabbi;Rakshit Malhotra;K Manikandan 2021 International Conference on Emerging Smart Computing and Informatics (ESCI) [2021]

2] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," IEEE Symposium on Security and Privacy, 2016,pp 839-858. "Consumer Digital Identity: Leveraging Distributed Privacy Enhancing Technology," (White Paper: Secure Key):https://securekey.com/resources/consumer-digital-identity/

[3] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin," IEEE Symposium on Security & Privacy (Oakland) 2014,pp 459-474, IEEE, 2014.

[4] C. Garman, M. Green, and I. Miers, "Accountable privacy for decentralized anonymous payments", International Conference on Financial Cryptography and Data Security (Barbados), pp. 81-98,2016.

[5] A. M. Antonopoulos, "Mastering Bitcoin: Unlocking Digital CryptoCurrencies" (1st ed.). O'Reilly Media, Inc., 2014.

[6] "A Next-Generation Smart Contract and Decentralized Application Platform" (Whitepaper):https://github.com/ethereum/wiki/wiki/White-Paper

[7] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance", In Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI '99). USENIX Association, Berkeley, CA,USA, 173-186, 1999.

[8] N. Garg, "Apache Kafka. Packt Publishing", 2013.

11.2 Web Reference:

- https://www.**ibm**.com/developerworks/opensource/top-**projects**/php/
- www.research.**ibm**.com/labs/africa/**project**-lucy.shtml
- www.idc.**iit**b.ac.in/**projects**/student/**project**-areas.html
- www.**iit**r.ac.in/departments/ECE/pages/Academics+BTech_**Projects**.html
- www.**nic**.in/**projects**/government-eprocurement-solution-**nic**-gep**nic**-20

CHAPTER 12

LIST OF PUBLISHED/PRESENTED PAPERS/ COMPETITION

Sr.No	Title	Level	Date of publication	Venue	Award Won
Paper Presented					
1	KYC Transparency and Security for banking using Block chain and IPFS.	National	11/04/2023	Sanjivani K,B, P ,Polytechnic Kopargoan	participation
Project Competition					
2	KYC Transparency and Security for banking using Block chain and IPFS.	National	31/03/2023	Loknete Gopinathji Munde institute of engineering eduction and research nashik	participation
Paper Publish					
3	KYC Transparency and Security for banking using Block chain and IPFS.	International	30/04/2023	International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)	participation

Table 12.1: List of Published/Presented papers/ Competition

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

KYC Transparency and Security for Banking using Block Chain and IPFS

Dhanraj Kadam, Varad Joshi, Dhiraj Khairnar, Gayatri Kolhe
Department of Computer Technology
K.K Wagh Polytechnic, Nashik, Maharashtra, India

Abstract: *Know Your Customer or Know Your Customer (KYC) is a financial institution's guideline for identifying customers using identity, compliance and risk assessment to build relationships in banking. With security concerns, the KYC process has become difficult and costly for a client. In this work, we propose an efficient, fast, secure and transparent platform for KYC authentication for banking institutions through the Interplanetary File System (IPFS) and blockchain technology output. The application process allows customers to open an account at a bank, complete the KYC process there, and use the IPFS network to generate a hash and distribute it using blockchain technology. After obtaining the private key, any bank/financial institution can obtain the customer's information (eg.For example KYC) If a customer wants to open another account with a bank/financial institution, use IPFS network for security. A planned process can save time, money and redundancies in the KYC process when trying to open accounts at multiple banks.*

Keywords: KYC, Blockchain, IPFS , SHA , DLT etc

I. INTRODUCTION

Banks often serve large customers in retail and commercial establishments. The "Know Your Customer" process, also known as KYC, helps organizations verify the identity of their customers. KYC is a regulatory and legal requirement that a business or financial institution must meet for new and existing customers. The main challenge of the banking industry is to control the cost of the KYC process, which negatively affects the business. The purpose of this article is to propose a new KYC verification process.

We have developed a DLT-based system that provides a solution to the additional cost of the KYC process and the lack of customer satisfaction. The main reason we use DLT is because it allows us to monitor the KYC fee structure across all financial institutions in the jurisdiction and on a consolidated basis for inefficiencies from similar transactions. In all organizations involved (for example, DLT frees us from doing all the repetitive tasks and saves more money than trying to simplify these repetitive tasks).

KYC is the process by which banks obtain information about the identity and address of the buyer. Due diligence to identify the client is a process followed by regulators. This process ensures that the bank's services are not abused. It is the company's responsibility to complete the KYC process when opening an account. Banks are also required to regularly update customers' KYC information.

KYC can be manual, time consuming and repetitive in organizations. Sharing KYC information on the blockchain will enable financial institutions to achieve better results, increase efficiency and improve customer experience. The KYC blockchain system provides transparency and immutability, allowing financial institutions to verify the authenticity of available information on DLT platforms. The decentralized KYC process is an easy way for users to access new information securely and quickly.)

II. SYSTEM ARCHITECTURE

In our proposed system, we share kyc documents with the blockchain so that documents and user details remain secure. In the above architecture, we can see that we have created a secure IPFS system, so users keep their documents and details here. In the second part, when a user needs to make a transaction from one bank to another, our system will help to provide simple KYC to send the amount easily and securely. In the image we can see that there is a strong security algorithm, so we encrypt on the one hand and decrypt on the other.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

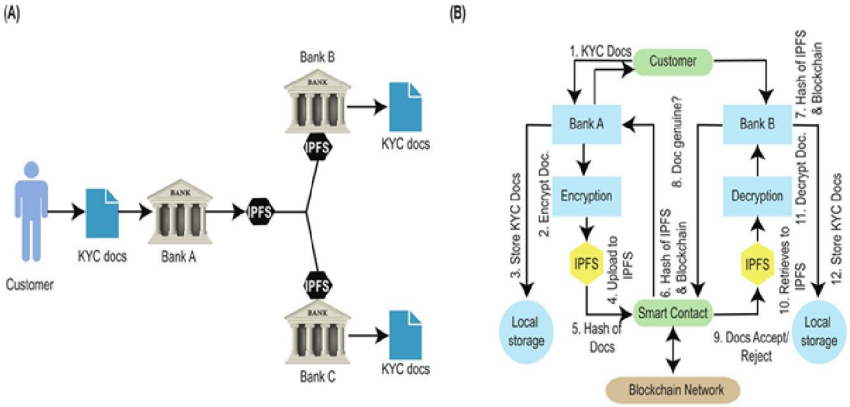
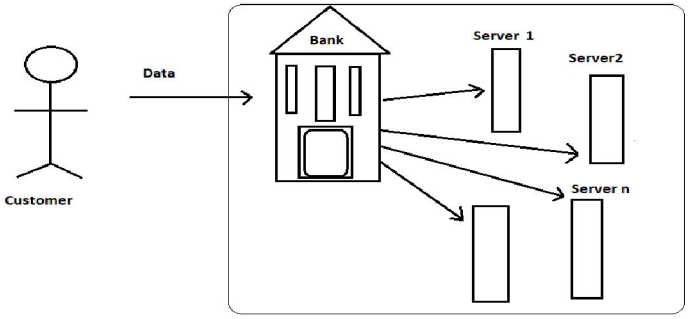


Figure 1.1: System Architecture.

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. sharing of confidential KYC data must be authorized by customers, and a bank-customer relationship must be kept secret from network



III. LITERATURE SURVEY

The purpose of project Pervasive Decentralization of Digital Infrastructures: A Framework for Block chain Enabled System and Use Case Analysis and their author is F. Glaser he publishes a Social Science Research Network Rochester NY SSRN Scholarly Paper ID 3052165. Is in year of Jan. 2017. And the mean purpose is Block chain technology recently draws the attention of the public, as a dispute that leads to the foundation that the trust - free economical transaction is possible with its distinctive method and it's more secure.

A lightweight multi-tier s-mqtt framework to secure communication between low-end IOT nodes and their author is A. Rahman, S. Roy, M. S. Kaiser and M. S. Islam and they publish in the

Year of 2018 5th International Conference on Networking Systems and Security. we discuss a detailed analysis of data & devices security issues and present an enhanced security model with a view to improving the security issues and its more complex

A Blockchain Framework for Insurance Processes the author is M. Raikwar, S. Mazumdar, S. Ruj, S. Sengupta, A. Chattopadhyay and K.-Y. Lam they publish in 2018 9th IFIP International Conference on New Technologies Mobility and Security. we focus on the design of an efficient approach for processing insurance related transactions based on a block chain-enabled platform and its less applicable

The Blockchain as a Decentralized Security Framework and the author D. Puthal, N. Malik, S. Mohanty, they publish IEEE Consumer Electronics Magazine, in 2018.the overview of this technology for the realization of security across distributed parties in an impregnable and transparent way and it's more costly. M. Mahmud, M. S. Kaiser, M. M. Rahman, M. A. Rahman, A. Shabut, S. Al-Mamun, et al.

This author publishes Cognitive Computation, vol. 10 in oct 2018 the TMM utilizes both node behavioral trust and data trust, which are estimated using ANFIS, and weighted additive methods respectively, to assess the nodes trustworthiness and its more time consuming

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

1. Continuous Decentralization of Digital Infrastructure :
A Blockchain-Enabled System Framework and Use Case Analysis:
Technological innovation and resulting decentralization are drivers of continuous development and increasing openness digital infrastructure and services. One of the most discussed and arguably most disruptive innovations is the distributed database technology known as blockchain. Although still in its technological infancy, experimental adoption and adaptation appears well advanced in several potential application areas, ranging from distributed computing and storage networks to global financial services. However, the technology and its development path still involve unknowns common to many practitioners and researchers.
In particular, questions about how to modify the technology or integrate it into existing digital services, processes and infrastructure.

2. Lightweight multi-layer S-MQTT framework to secure communications between low-end IoT nodes.
Internet of Things (IoT). Due to the convergence of Wireless Sensor Networks (WSN) and Internet technologies, the Internet of Things has evolved to come closer to the vision of smart cities. In the Internet of Things, in order to maintain device-to-device communication, the HTTP protocol has been used for remote monitoring and data analysis of a large number of sensing elements, but the consumption of 'energy is large, the transmission efficiency is relatively low, and it cannot be effectively used system bandwidth.
Therefore, MQTT (Message Queuing Telemetry Transport), AMQP and CoAP protocols are quite capable of handling wireless sensor traffic under very low bandwidth and limited network conditions. Security is also another major concern as IoT applications collect private data and provide access to various control functions over the internet.

3. Blockchain as a decentralized security framework :
Blockchain is becoming one of the most popular and unique cybersecurity technologies. The technology itself is in its infancy, has successfully replaced economic transaction systems in various organizations, and has the potential to revolutionize heterogeneous business models across different industries.
Although it promises to provide a secure distributed framework to facilitate the sharing, exchange and integration of information between all users and third parties, it is important that planners and decision makers thoroughly analyze its applicability in their industrial and commercial applications. Sex is important. Blockchain should only be deployed when it is applicable and offers security a better chance of increasing revenue and reducing costs. This paper describes the technique to provide security between distributed parts in an untouchable and transparent manner (IoT) and cloud computing enable neuroscientists to collect multi-layered and multi-channel brain data to better understand brain function, diagnose diseases and design treatments. To ensure secure and reliable data communication between end-to-end (E2E) devices supported by today's IoT and cloud infrastructures, trust management at the IoT and user level is required.

IV. PROPOSED SYSTEM

In our proposed system, we share KYC documents with the blockchain so that documents and user details remain safe. In the above architecture, we can see that we have created a secure IPFS system, so users keep their documents and details here. In the second part, when a user needs to make a transaction from one bank to another, our system will help with easy KYC to send the amount easily and securely. In the image we can see that there is a strong security algorithm, so we encrypt on the one hand and decrypt on the other.

V. PROBLEM DEFINITION

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.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

VI. ANALYSIS

Technological development and distribution benefits are the driving forces behind the continued development and increased openness of digital infrastructure and services. One of the most discussed and allegedly disruptive innovations is the distributed ledger technology known as blockchain. While the technology is still in its infancy, testing and implementation appears to be progressing in applications ranging from distributed networks to computing and storage for international financial services. However, technology and its development still have many unknowns for doctors and scientists. In particular, the question of how technology can adapt to or join the existing field of digital services, processes and procedures.

VII. CONCLUSION

Blockchains represent the future of transactions and are beginning to transform entire industries. Consequently, there is considerable interest in exploring blockchains for various industry use cases. They are particularly useful in supporting multi-party business transactions where the entities need not trust each other. The immutable, cryptographically secured, and replicated, ledger, consensus to validate transactions, and permissioned access are all attractive salient attributes for enterprises to consider blockchains as the future transaction network.

REFERENCES

[1]. Implementation of Least Significant Bit Image Steganography with Advanced Encryption Standard Adit Pabbi;Rakshit Malhotra;K Manikandan 2021 International Conference on Emerging Smart Computing and Informatics (ESCI) [2021]

[2]. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," IEEE Symposium on Security and Privacy, 2016, pp 839-858. "Consumer Digital Identity: Leveraging Distributed Privacy Enhancing Technology," (White Paper: Secure Key): https://securekey.com/resources/consumer-digital-identity/

[3]. E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin," IEEE Symposium on Security & Privacy (Oakland) 2014,pp 459-474, IEEE, 2014.

[4]. Garman, M. Green, and I. Miers, "Accountable privacy for decentralized anonymous payments", International Conference on Financial Cryptography and Data Security (Barbados), pp. 81-98,2016.

[5]. "Zero-knowledge Security Layer to be Added to Quorum Blockchain Platform", Press Release: https://z.cash/blog/zsl-quorum.html

[6]. A. M. Antonopoulos, "Mastering Bitcoin: Unlocking Digital Crypto Currencies" (1st ed.). O'Reilly Media, Inc., 2014.

[7]. https://www.ibm.com/developerworks/opensource/top-projects/php/

[8]. www.research.ibm.com/labs/africa/project-lucy.shtml

[9]. www.idc.iitb.ac.in/projects/student/project-areas.html

[10]. www.iitr.ac.in/departments/ECE/pages/Academics+BTech_Projects.html

[11]. www.nic.in/projects/government-eprocurement-solution-nic-gepnic-20