International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Decentralized Cloud Banking: Empowering Security and Efficiency with Blockchain, IPFS, and Smart Card Technology

Ankur Biswas[1, *], Abhishek Roy[2]

Submitted: 22/08/2023 **Revised**: 07/10/2023 **Accepted**: 22/10/2023

Abstract: ICT development has boosted the usage of electronic communications, especially during the COVID-19 epidemic, which has been advantageous for industries including banking, education, government, and healthcare. To safeguard sensitive messages from security risks, privacy, integrity, non-repudiation, and authentication (PINA) requirements must be upheld. Fraudulent financial transactions in the Indian banking industry have brought attention to the need for study into improving dependability and accountability. A safe and integrated electronic banking system using blockchain and IPFS for cloud banking is suggested to address flaws in electronic communication. To effectively evaluate security settings and resource allocation, simulations utilizing Object-Oriented Modelling (OOM) should be run. The importance of maintaining strong security measures in electronic banking and message transmission systems is emphasized in this study.

Keywords: *Blockchain, Cloud Banking, Object-Oriented Modelling, SmartCard*

1. Introduction

The advancement and development of Information and Communication Technology (ICT) have enabled the widespread adoption of electronic communication via the Internet. This digital form of communication offers the ability to transmit messages instantly, eliminating the requirement for physical proximity. As a result, electronic communication has become increasingly popular. Additionally, due to the need for social distancing during the current Coronavirus situation, electronic message communication has gained significant popularity among the masses. In today's era, individuals increasingly opt to carry out crucial transactions, such as banking, education, and healthcare consultations, from the convenience of their own homes, regardless of their distance from urban areas.However, despite the advantages, electronic message communication is susceptible to threats from adversaries, as the Internet is accessible to everyone, including potential adversaries. Ensuring the implementation of rigorous security protocols is essential to uphold a strong level of integrity during electronic transactions. The occurrence of fraudulent banking transactions, which have resulted in the misuse of people's hard-earned money, has highlighted the need for extensive research to address these security vulnerabilities [23][25].

The authors present a proposal for a secure and user-centric Cloud Banking System (CBS) [1]-[4]. A number of electronic services are offered to citizens through the use of a secure interface that allows them to access diverse electronic services using a Multipurpose Electronic Card (MEC). We have integrated two security technologies into this proposed CBS to ensure a robust level of security. Blockchain [17] and IPFS (Interplanetary File System) [13] and [14] are integrated into the proposed Cloud Banking System. To simulate and evaluate the performance of the system, the authors used Object-Oriented Modeling (OOM). In this case, Amazon Web Services (AWS) was utilized to provide the electronic service model as well as MongoDB and NoSQL [31] to communicate with the database.

Section II provides an explanation of the origins of the work undertaken in this paper. There is a detailed discussion of the background and context of how the proposed Cloud Banking System came to be developed and why it was proposed. The Cloud Banking System itself is described in a comprehensive manner in Section III of this document, as you can see in the picture above. It outlines the key features, functionalities, and components of the system, providing a detailed overview of its architecture and operation. In Section IV, we are going to illustrate how the Cloud Banking System has been implemented as an Object-Oriented Model (OOM). It elaborates on the modeling approach used to design and structure the system, highlighting the static structure and organization of its components. In Section V, the paper presents a sample output, showcasing the practical results and outcomes of the proposed Cloud Banking System. This section demonstrates the system in action and provides tangible examples of its functionality.

Finally, Section VI serves as the conclusion of the paper, summarizing the main findings and contributions of the research. It also explores potential future avenues for

[1]*Research Scholar, Dept. of Comp. Sc. & Engg., Adamas University, Kolkata, India.*
[2]*Professor, Dept. of Comp. Sc. & Engg., Adamas University, Kolkata, India.*
Email: ankur2u@gmail.com[1]; dr.aroy@yahoo.com[2]
**Corresponding author. E-mail: ankur2u@gmail.com*

further research and development, highlighting areas where the proposed Cloud Banking System could be enhanced or expanded upon.

1. Origin of work

The purpose of this presentation is to allow you to see the concepts that were presented in [1] through [4] of a card interface that has a variety of functions, its called MEC. It is through this interface that citizens are able to access a number of electronic services directly from the government directly to their homes. A related service offered by the company is electronic governance, including the range of electronic governance functions, including the provision of electronic governance functions [27][28][30][32][33][34], cloud governance functions [4][5], cloud banking functions [21][22][24][26], cloud voting functions [8][9][28], cloud healthcare functions [10], and cloud transportation functions [11]. It is important to note that as a state-sponsored verifier, the government is not involved in the service provisioning process in the same way that it is in its role as a key participant in this electronic service delivery system, and the key participant in this process is the Service Seeker (Citizen). There are several types of service providers in the industry, such as banks, hospitals, and transport companies that provide services on behalf of the customers. There may be times, however, when the government or one of its agencies participates in the provision of services. For example, the government and its agencies may be involved in the Electronic Communication process during the implementation of a Cloud Voting system [8][9]. It clear that as the technology advances, there will be a gradual addition of participants to these new electronic services as the system progresses.

Having the ability to verify the identity of a user is crucial to the effectiveness of this comprehensive electronic service delivery system.

2. Proposed Cloud Banking System

Proposed Cloud Banking System (CBS), three essential participants will assume crucial roles in the process. Users (citizens), governments, and banks will each have a role to play. The government acts as the document verifier, responsible for verifying the identity of citizens. Banks utilize the Public Cloud to connect users to their services. Powered by robust cryptographic protocols, the authors have incorporated Blockchain [15] [16] into their project in order to ensure the security of electronic transactions and user identities. The purpose of this article is to provide a comprehensive explanation of what we propose in terms of (CBS), as shown in Figure 1 so you can have a better understanding of our proposed system.

USER Side: During the initial stage of the process, the user (citizen) inputs the necessary information and transmits it to the framework via a Public Kiosk. The user initiates the electronic transaction by submitting a SERVICE REQUEST, which is the first element in the electronic transaction process.

PUBLIC KIOSK Side: During the second phase, when the public kiosk receives a SERVICE REQUEST that includes the bank details submitted by the user, the government receives the REQUEST.

GOVERNMENT Side: In the third step, the Government utilizes a Firewall to protect Cloud Banking transactions and prevent unauthorized access to the proposed system by malicious code. As illustrated in Figure 1, the Firewall is an important component that is crucial to accepting the SERVICE REQUEST, triggering Phase-I, which is the stage at which the request is accepted.

This process has been made more secure through the use of Intrusion Prevention Systems (IPS) [12] as well as Intrusion Detection Systems (IDS) [19], which are used to ensure the security of all requests during the fourth step. These systems are responsible for detecting and preventing any unauthorized intrusion or malicious activity within the Cloud Banking system.

It is at step 5 that a request for a service is made by the user through the Cloud Banking Interface, which is the 5th step in the process.

As a result of the verification process that is being performed on the user's SERVICE REQUEST in Step 6, the result can be either one of two scenarios, depending on the type of verification process which is being performed.

Scenario 1 (Successful Validation): An illustration shown in Figure 1 shows how a Cloud Banking transaction begins at Step 10 by entering Phase 2 of the process, a step that begins at the beginning of Phase 2.

Scenario 2 (Unsuccessful Validation): As a result of this transaction, Step 7 in the sequence of steps is reached.

During Step 7, the system keeps track of the total number of unsuccessful attempts. Each user is typically allowed a maximum of three (03) attempts.

Step 8: Depending on how the transaction is handled, there are two possible otcomes:

Scenario 3 (Successful Validation): This signifies the beginning of Phase 2 as shown in Figure 1, which signifies the advance from Step 9 to Step 10 of the SERVICE REQUEST process. There is a possibility that the Failed Attempt Counter will be equal to or less than 3in which case STEP 11 will be carried out.

Scenario 4 (Unsuccessful Validation): There is an opportunity for an invalid Service Request if the number of Failed Attempts exceeds the designated maximum limit

of three. If this occurs, the process can move forward to Step 9.

In Step 9, the client will receive a notification via a system timeout that the SERVICE REQUEST has been terminated after three unsuccessful attemptsAs of the moment, the (CBS) is in the process of detecting a failure message within the system as it relates to a failed transaction.

Once the Government has confirmed the identity of the User in Step 10, the SERVICE REQUEST proceeds to this stage of the process. At this point, the Query Optimizer comes into play, enhancing performance by optimizing the query for efficient execution.

In Step 11, the SERVICE REQUESTS flow through the Scheduler, which ensures efficient channelization of the requests, particularly in comparison to concurrent SERVICE REQUESTS from other clients. This helps to optimize the overall processing and handling of the requests.

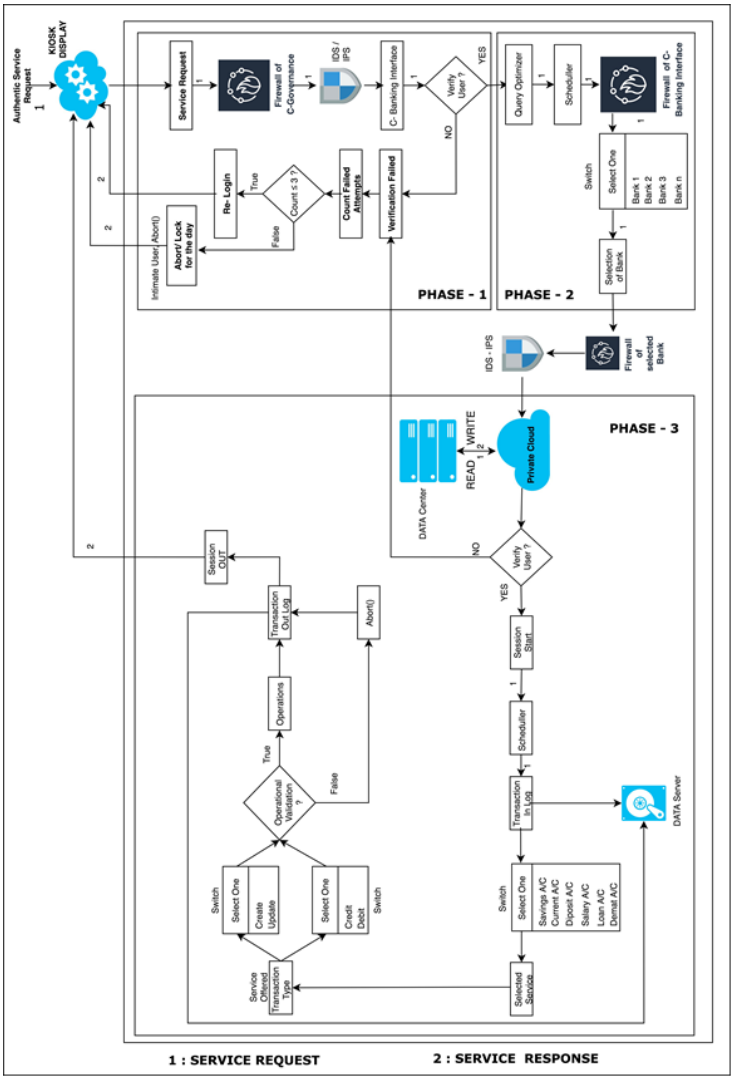

Fig. 1: proposed cloud banking system

The FIREWALL assumes a vital role in accomplishing one of the primary objectives of the Government, which is to safeguard the security of Cloud Banking Transactions. This is described in step 12 of the report. It acts as a protective barrier, preventing unauthorized access and safeguarding the integrity and confidentiality of the transactions

BANK Side: A user's SERVICE REQUEST is advanced in Step 13 to establish a connection between their preferred bank and their Service Request. This step enables the User to establish a secure and reliable communication channel with the chosen Bank for carrying out the desired banking transactions.

Step 14: The SERVICE REQUEST undergoes processing through the Firewall of the Bank. This stage serves as a crucial defense mechanism against any malicious attempts by adversaries, ensuring their prevention and safeguarding the transaction's integrity.

Step 15: There are two Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) that are part of the Cloud Banking System and are designed to detect and prevent malicious intrusions that are in the process of being processed. These systems work together to identify and prevent any unauthorized intrusions or malicious activities, ensuring the security and integrity of the SERVICE REQUEST.

With the start of Step 16 of the Bank's Private Cloud project, the Bank's Private Cloud has entered Phase 3 with the response to the End User's SERVICE REQUEST. As depicted in Figure 1, the service request is used to initiate Phase 3 of the project. In order to ensure comprehensive records of its financial transactions, the Bank must establish a connection between the Data Center and the Private Cloud to enable seamless data transfer and storage. The Data Center is capable of performing both READ and WRITE operations.

Step 17: As a result of the security protocol implemented by the Bank, the electronic transaction can proceed in accordance with the guidelines and procedures prescribed by the Bank and can take following paths.

Scenario 5 (Validation Success): It is at Step 18 of the transaction's sequence that the transaction advances.

Scenario 6 (Validation Failure): A maximum of three attempts are allowed for the User to complete the transaction before the transaction loops back to Step 7.

Step 18: Following the successful completion of the security protocols, the Bank commences the execution of the SERVICE REQUEST session, which signifies the beginning of banking transactions.

Step 19: The Scheduler aids in expediting the transaction.

Step 20: A Transaction In Log is generated and maintained on the Data server.

step 21: Using the Bank's web page, the User is provided with an overview of the accounts available for him to transact with.

In Step 22 of the process, the User chooses one of the financial services that are available on the Bank's list of available services.

Depending on the type of transaction the User selects in step 23 of the process, a SERVICE REQUEST will create either of the two scenarios below.

Scenario 7 (Status: SUCCESS): There is a step 24 in the process in which the SERVICE REQUEST proceeds.

Scenario 8 (Status: FAILURE): By invoking the abort () function, the SERVICE REQUEST is redirected to Step 24, facilitating the progression of the banking transaction.

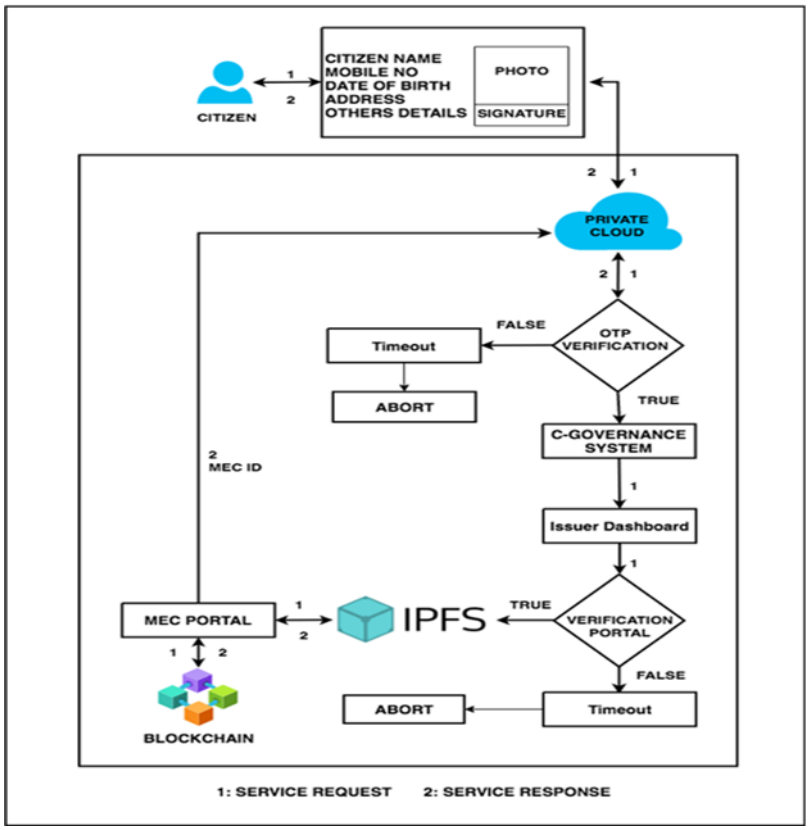

Fig. 2: Visual representation for registration and verification of MEC during Phase I of banking transaction

As part of the transaction monitoring process, a Transaction Out Log is maintained on the designated data

server of the Bank, as depicted in step 24. This serves as a record of both successful and unsuccessful transactions, and it is used in the monitoring process.

PUBLIC KIOSK Side: It is only when the Bank has successfully verified the Customer's identity at Step 25 will the session be terminated, and the User will be provided with a SERVICE RESPONSE via the Public Kiosk, after the Bank has successfully verified the Customer's identity.

USER Side: At the conclusion of Step 27 in the process, a successful Cloud Banking Transaction is indicated by the SERVICE RESPONSE, which is returned to the User. This signifies the successful completion of the transaction. There are two major phases to the Cloud Banking System, and they are as follows: Phase I and Phase II. A multipurpose electronic card (MEC) can be registered and verified in Phase I, whereas the actual banking transactions will take place in Phase II, which is where the real action begins.

It is shown in Figure 2 that during the first phase of the banking transaction, which is Phase I, the Multipurpose Electronic Card (MEC) will be registered and verified by the Cloud Governance System after the User sends a SERVICE REQUEST to the Cloud Governance System, the registration will be completed. In order to verify the user's identity, one-time passwords (OTPs) are used [20]. Following the System Timeout, the abort () function will be called if the command fails. A SERVICE REQUEST will proceed to the verification portal once the One Time Password (OTP) [18] has been verified successfully. In order to generate a hash and store it on the blockchain, the use of IPFS is required. The verification portal generates the hash, which is then stored on the blockchainThere are two main components of the MEC system.

Figure 3 shows the steps that follow the successful registration of the User as part of Phase I of the banking transaction, which illustrates the subsequent steps of Phase II of the banking transaction that follow the successful registration of the User. Upon registering for the Cloud-Governance Interface and using the Multipurpose Electronic Card (MEC) that the user has been provided, the user then uses the Public Kiosk to initiate a SERVICE REQUEST to contact the Cloud-Governance Interface. A reply will be generated by the Cloud-Service Server after receiving the SERVICE REQUEST from the client and is verified via Blockchain. This response will then be delivered to the customer via the Blockchain. It is possible to invoke the abort () function whenever the verification fails [6], [7]. In order to access the Cloud-Service Server, a SERVICE REQUEST must go through this firewall to pass through it, ensuring that any unwanted traffic entering the data center is filtered out before it reaches it. Therefore, as a result of the SERVICE REQUEST progressing through the private cloud to the desired Bank Server, the SERVICE REPLY can be retrieved via the Bank Server.

There is widespread recognition that Object-Oriented Modeling (OOM), as well as other approaches used based upon it, can be useful in simulating the operational aspects of a Cloud Banking System (CBS) before it is invested with substantial resources in its actual deployment. The author demonstrates for the proposed CBS a practical demonstration of OOM in the section that follows as an example to illustrate his point.

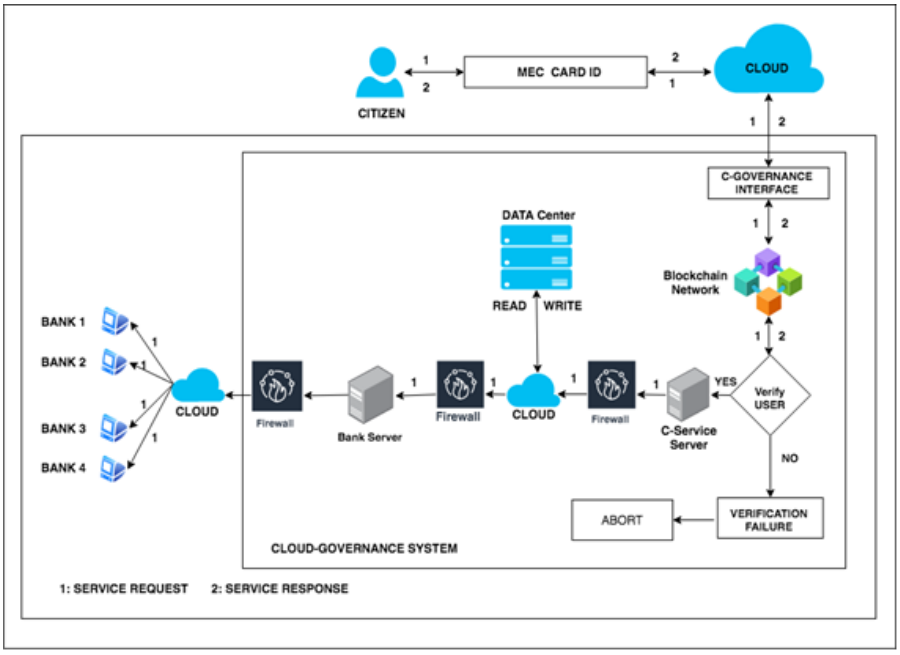

Fig. 3: Visual representation of Phase II of banking transaction.

3. Object-Oriented Modelling of Cloud Banking System

The idea behind Object-Oriented Modeling (OOM) is to provide a visual representation of the interconnections among various objects within an application. The OOM methodology combines application development with database management in order to create an integrated language framework and a cohesive data model. OOM facilitates the identification of objects and the interaction with them in order to retrieve data for retrieval purposes. Our proposed Cloud Banking System (CBS) is portrayed in the following Class Diagrams, which give a clear view of how it is structured in terms of its static structure.

a. Class Diagram of Cloud Banking Systems

As shown in Figure 4, there are a number of attributes associated with a User Class, including:

1. Private attributes:

a) password: This attribute represents the confidential password of the User.

2. Protected attributes:

a) This attribute is utilized to indicate the User's mobile phone number, which will be utilized to initiate the login process at the public kiosk once the User's mobile phone number is provided.

b) email: This attribute denotes the User's email ID.

c) name: This attribute signifies the User's name.

d) A date of birth is an attribute of this object that indicates the date of a user's birth (DOB).

e) A Multipurpose Electronic Card ID (MEC ID) contains a date attribute that represents the date on which the MEC ID was issued.

f) The father's name the User identifies how they were raised. The name of their father is indicated by this attribute.

g) A user's mother's name is indicated by this attribute, which indicates the name of the user's mother.

h) address: This attribute represents the address of the User.

i) transactions: This attribute serves as a crucial parameter for facilitating the implementation of secure Cloud Banking transactions based on Blockchain technology.

j) mecId: The mecId attribute represents the unique identifier of the User's Multipurpose Electronic Card (MEC). The MEC plays a pivotal role in uniquely identifying the User and serves as a comprehensive interface for conducting various electronic transactions in a single-window manner.

k) photo: The photo attribute stores the User's uploaded photograph, serving as a visual representation of the User's identity.

l) signature: The signature attribute stores the User's uploaded signature, serving as a unique identifier and verification method.

m) services: This attribute defines a schema-type object for services, encompassing the diverse range of service types available to users from the provided list.

n) documents: This attribute establishes a schema-type object for documents, encompassing the collection of uploaded documents associated with the User.

o) It is possible to use the LoginLogs attribute to create a schema-type object that contains the list of logs generated by the User for tracking their login activities, which contains the list of logs generated by the User.

3. Public methods:

a) A new account is created by using the signup () function.

b) A short description of a user's account can be retrieved from a form using the formNoOne user details () method, it is possible to retrieve the user's gender and date of birth as well as their email address.

c) FormNoTwo user details (): The purpose of this function is to retrieve the current address and permanent address of the user from their profile in the form of a single string.

d) By using this function, we are able to retrieve information about the Parents of the User and also information about the User themselves from the database.

e) It is possible to infer detailed information about a user from the formNoFour () function. A photo and a signature of the user are obtained by this function.

f) As a part of the UploadOtherDetails () method, the user is able to upload additional documents to support his request.

g) The GetDocs () method refers to the user's uploaded documents that are associated with the account.

h) The CheckMecIdExists () parameter is used when a particular user attempts to log in through the public kiosk during the process of logging in a specific user.

i) An example of this is the function login (), which describes how the user logs into the application.

j) GetUser (): This function returns information about a user, such as his or her name and email address.

k) It offers a variety of electronic services through a single interface by allowing the user to login using a kiosk (), allowing them to access many electronic services.

l) A function called getvalidateDetails () performs a validation on the User's details in order to determine if they are eligible for any of the provided services.

Fig. 4: Class Diagram Of User

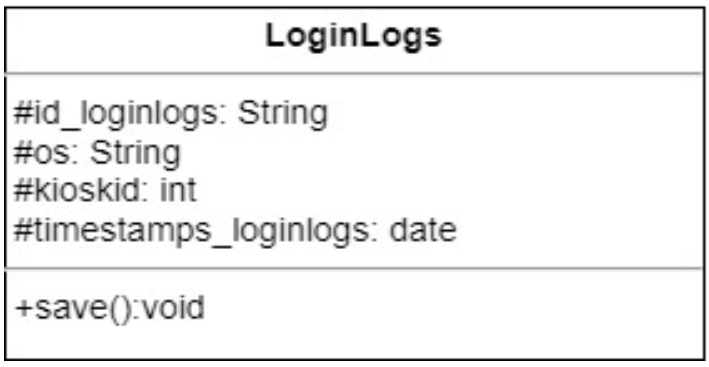

Fig. 5: Class Diagram Of Login Log

The attributes of the LoginLogs Class, as depicted in Fig. - 5, are as follows:

1.Protected attributes:

a) The attribute id_loginlogs represents the primary ID of the LoginLogs, ensuring its uniqueness.

b) Kiosks use an operating system called OS which corresponds to the version of the OS the Kiosk is using.

c) Kiosks are identified by their unique identifiers (IDs) and this attribute indicates that the kiosk is unique.

d) In the timestamp_loginlogs attribute, the date and time information of the login log transactions is stored in the date and time field of the log records and is stored in the timestamps_loginlogs attribute.

2.Public methods:

a) It is this function that performs the saving of the data to the Datacenter for persistent storage that is invoked by the save () function.

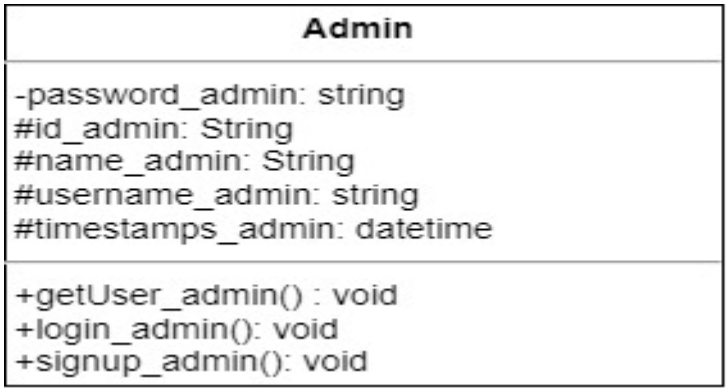

Fig. 6: Class Diagram Of Admin.

As shown in Figure 6, the following attributes are attributes of the Admin Class:

1. Private attributes:

a) The attribute "password_admin" represents the confidential password of the administrator.

2. Protected attributes:

a) A primary identifier for the Admin class is represented by the attribute "id_admin".

b) A name for the administrator is represented by the attribute "name_admin".

c) The username_admin is used for logging into the admin dashboard, which can be accessed via the admin login page, and is the username used by the admin to login to the administrator's account.

d) It keeps a record of the date and time details of each transaction that is processed by timestamps_admin.

3. Public methods:

a) The getUser_admin() function is responsible for obtaining the information about the admin user.

b) As a user, you can log in to your account as an administrator through the login_admin() function.

c) Signup_admin(): This function is responsible for registering an administrator on the site when they register for it.

It is evident from Figure 7 that there are a number of attributes associated with the Issuer Class, which include:

1. Private attributes:

a) The attribute "password_issuer" represents the confidential password of the Issuer.

2. Protected attributes:

a) The attribute "name_issuer" represents the name of the issuer.

b) An attribute with the name "username_issuer" represents the username that will be used for the issuer's dashboard login, and it will display the username of the issuer.

c) 'unit' refers to a unit's name, which is denoted by its attribute.

3**. Public methods:**

a) The function "getUser_issuer()" provide details of the Issuer.

b) The function "login_issuer()" represents the login process for the Issuer.

c) The function "signup_issuer()" signifies the process of registering an Issuer.

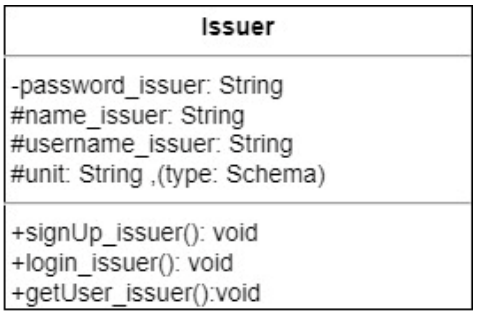

Fig. 7: CLASS DIAGRAM OF ISSUER.

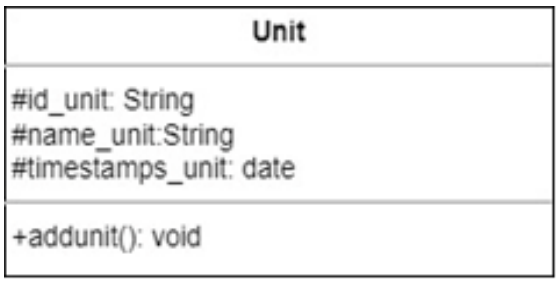

Fig. 8: CLASS DIAGRAM OF UNIT.

According to Figure 8, the following are the characteristics of a Unit Class, which are shown in the following table:

1. Protected attributes:

a) A prominent attribute of the "id_unit" attribute is an indicator of the primary ID associated with the Unit Class, as shown in Figure 8.

b) Figure 8 depicts the name of the unit within the Unit Class as indicated by the attribute "name_unit" in the unit class, as portrayed in Figure 8.

c) In this attribute, we have the date and time information for each transaction within the Unit Class. As you can see in Figure 8, the "timestamp_unit" attribute is responsible for storing the date and time information of each transaction.

2. Public methods:

a) The "addunit()" function is implemented to facilitate the creation of a new unit within the system

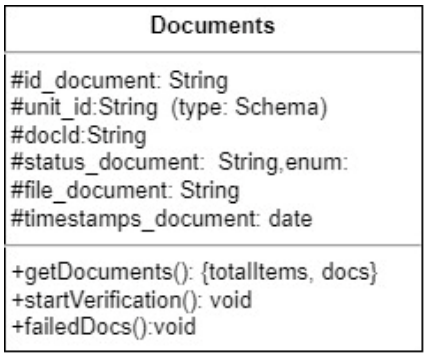

Fig. 9: CLASS DIAGRAM OF DOCUMENTS.

As shown in Figure 9, the following are some of the attributes that relate to Document Classes:

1. Protected attributes:

a) A document's primary identifier is represented by the attribute id_document, which can be found in the attribute table.

b) The attribute unit_id represents the identifier of the unit.

c) The attribute docId signifies the unique identifier assigned to each document, allowing for individual document identification.

d) The attribute status_document indicates the current status of the document. The initial value of this field is set to "Pending". The potential values for this field include "Pending", "Verified", and "Fail".

e) The attribute file_document denotes the Interplanetary File System (IPFS) hash of the file.

f) It provides a record of when each transaction took place with the timestamp_document attribute.

2. Public methods:

a) There is a function called getDocuments() that retrieves information and details about all the documents that have been uploaded.

b) In order to start the document verification process, the start verification() function is called by the document verifying software.

c) FailureDocs() is used in order to indicate whether the unit verifier marked a document "Fail" by using the failedDocs() parameter.

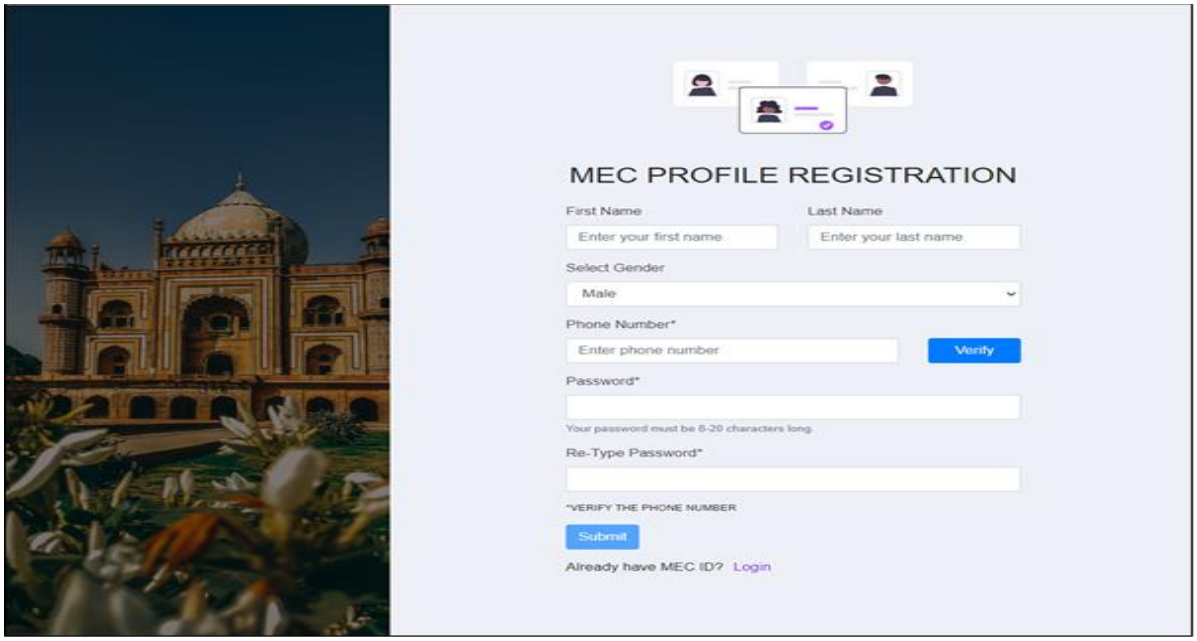

Fig. 10: MEC Profile Registration.

4. Sample Outputs

In this section, we will focus on discussing a sample output generated by the proposed Cloud Banking System (CBS).

Figure 10 illustrates the MEC PROFILE REGISTRATION process, where users are required to complete the MEC Portal registration form by providing their First Name, Last Name, Gender, Phone Number, and choosing a password. To ensure two-step authentication

during registration, a One-Time Password (OTP) is sent to the user's mobile phone, as shown in Figure 11. The user's enrollment in the MEC.

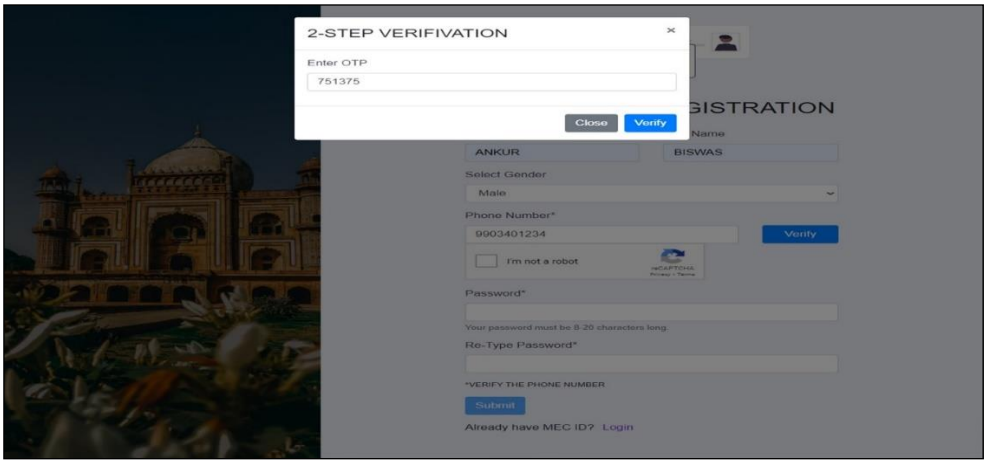

Fig. 11: MEC Profile Registration using OTP.

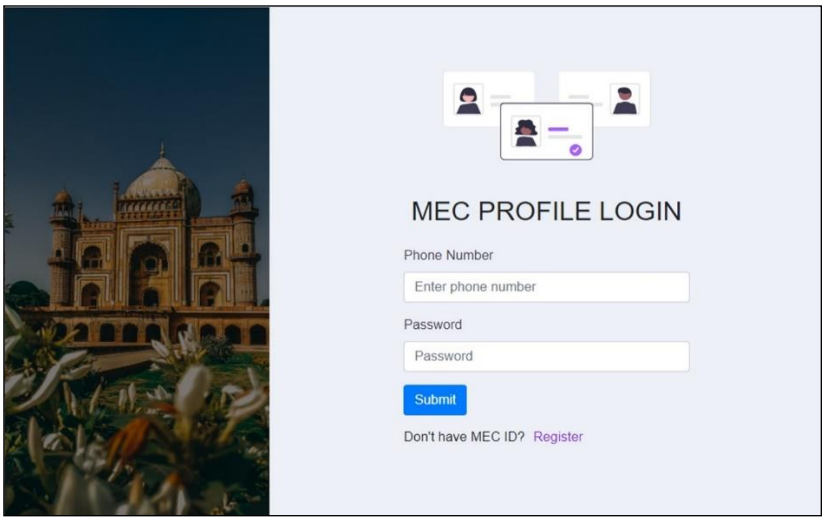

Fig. 12: MEC Profile Login.

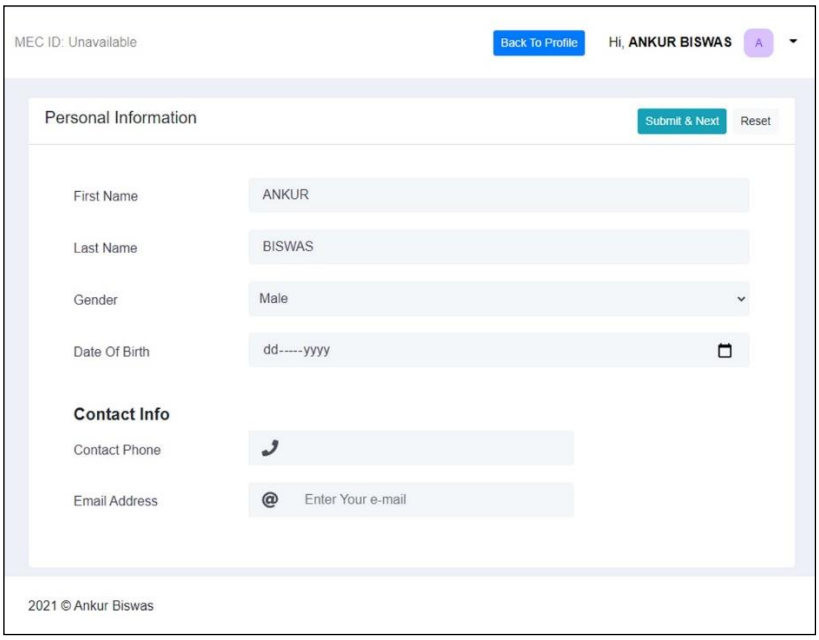

Fig. 13: MEC Profile personal details.

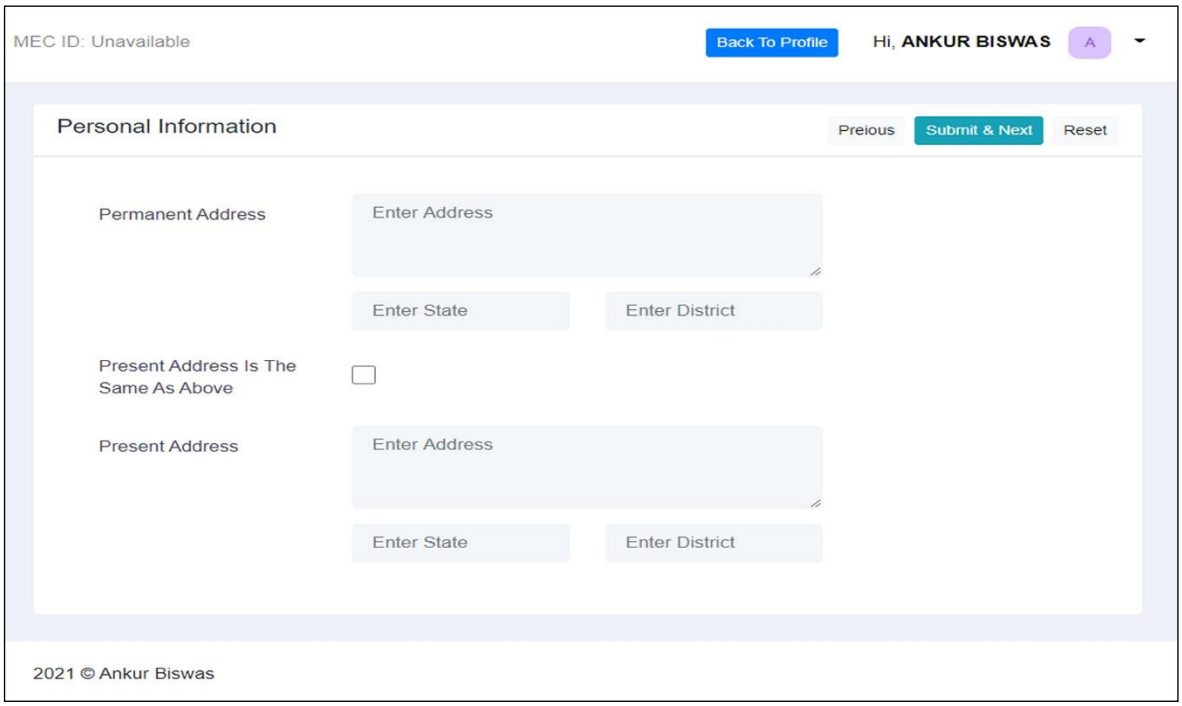

Fig. 14: MEC Profile personal address details.

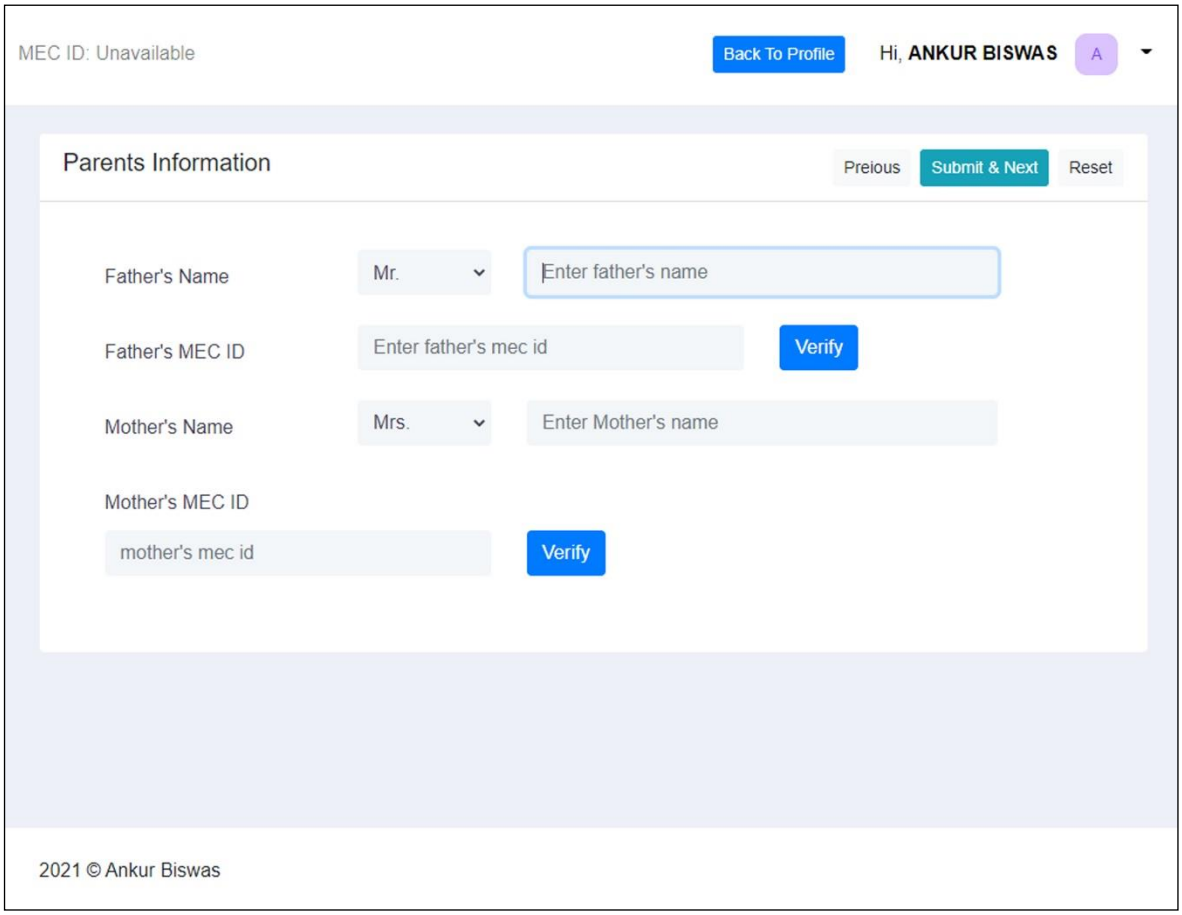

Fig. 15: Parent details update in MEC Profile

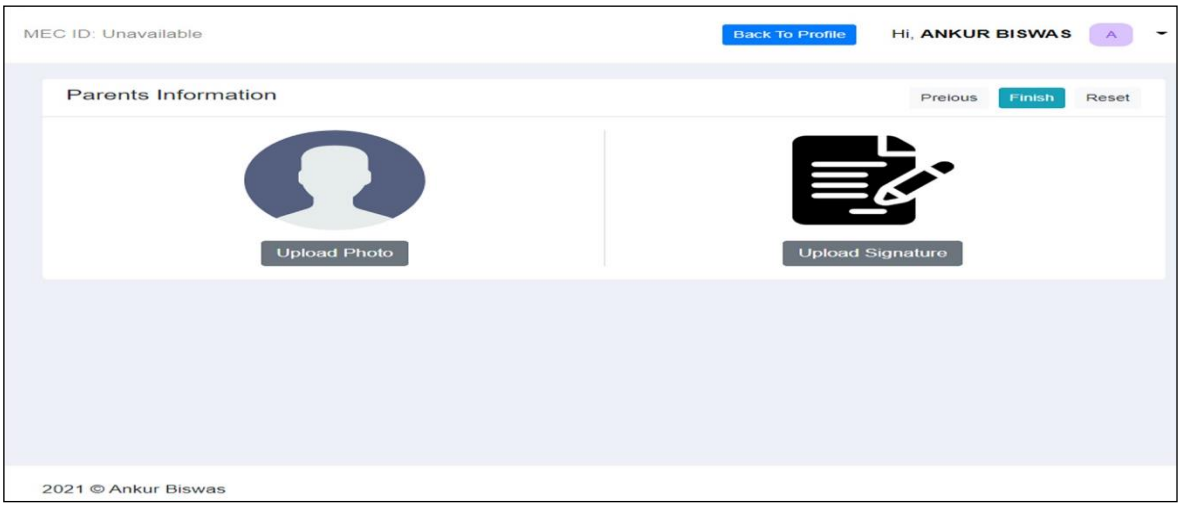

Fig. 16: Upload image and signature of a user in MEC Profile.

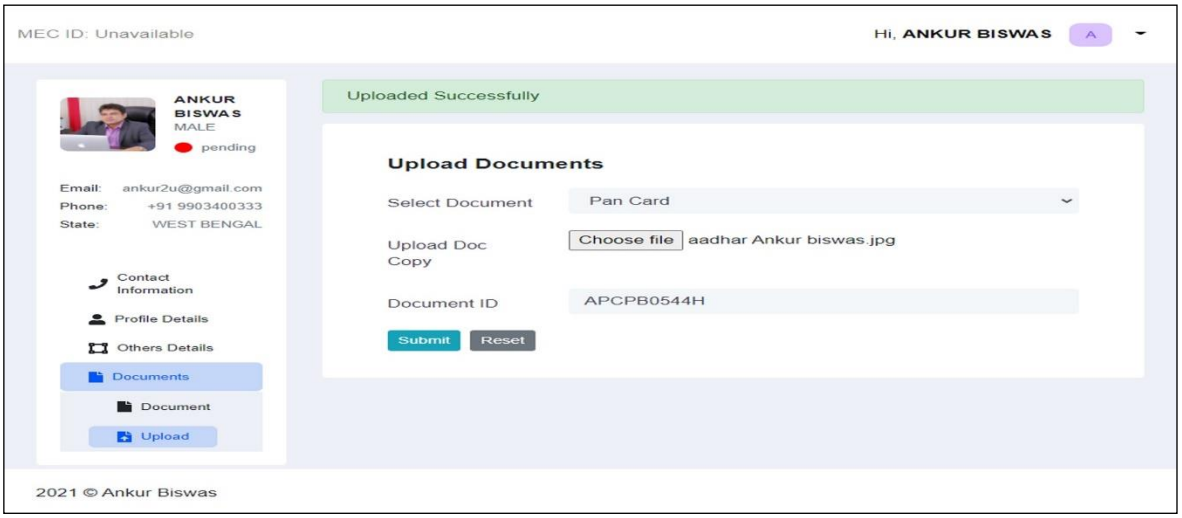

Fig. 17: Upload documents of a user in MEC Profile.

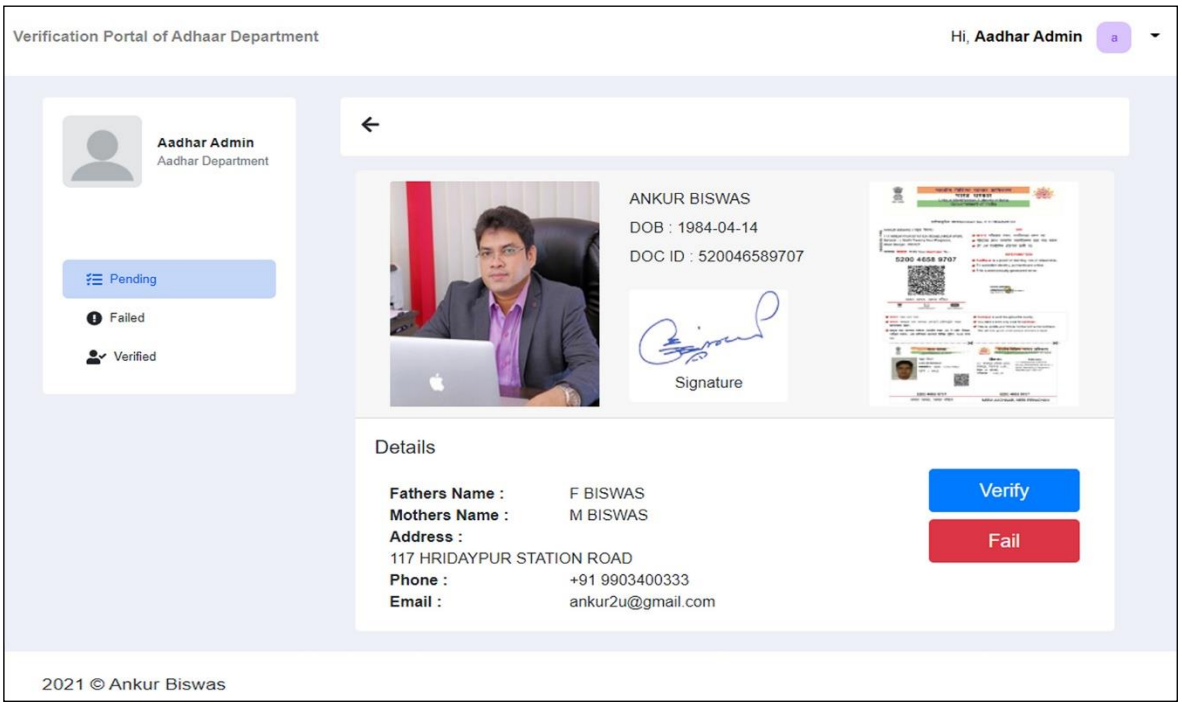

Fig. 18: Document issuer verification portal.

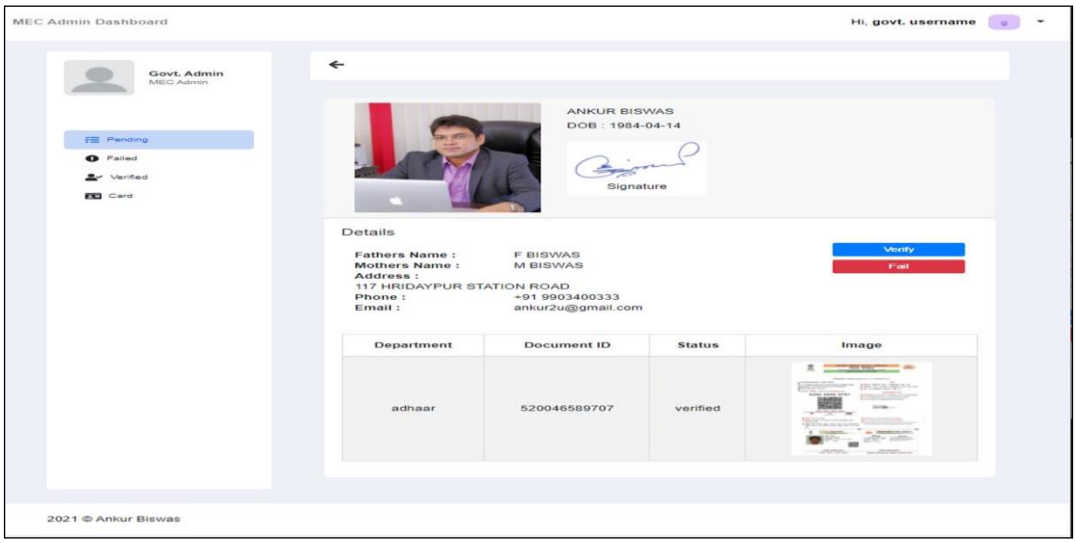

Fig. 19: MEC Admin portal.

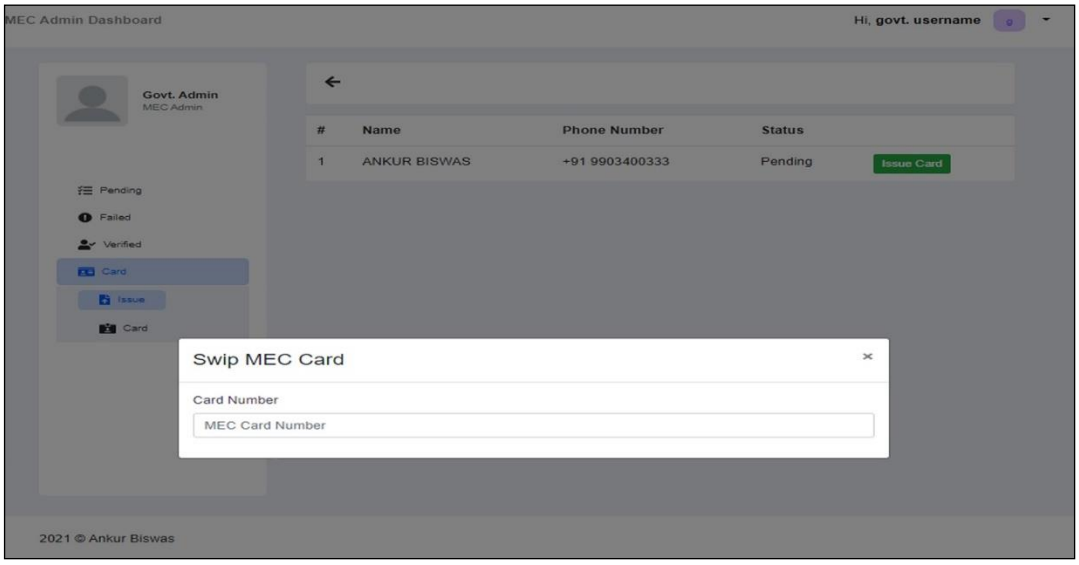

Fig. 20: MEC card issue in MEC Admin portal.

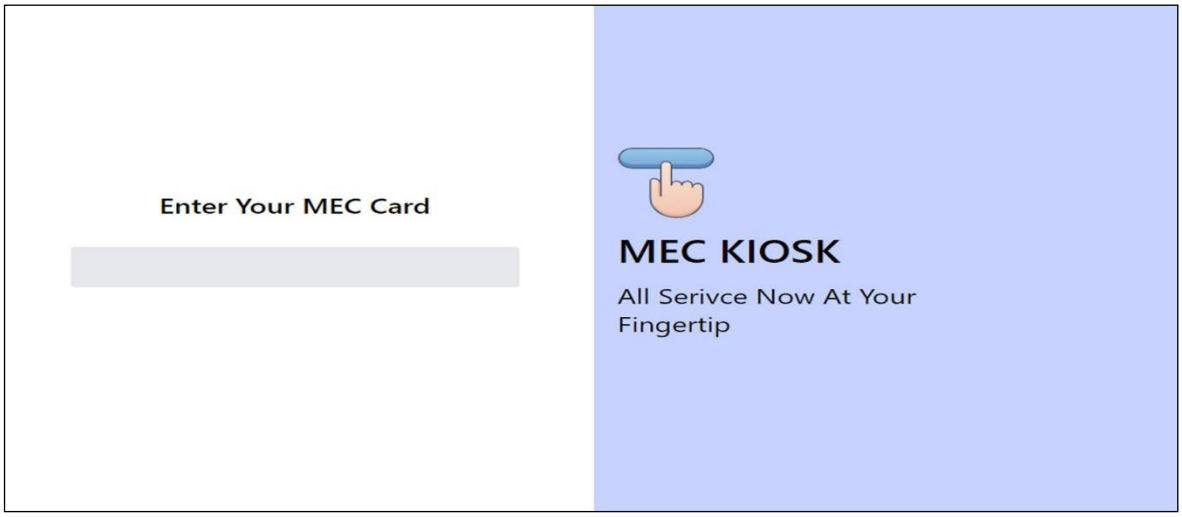

Fig. 21: Kiosk Login Portal.

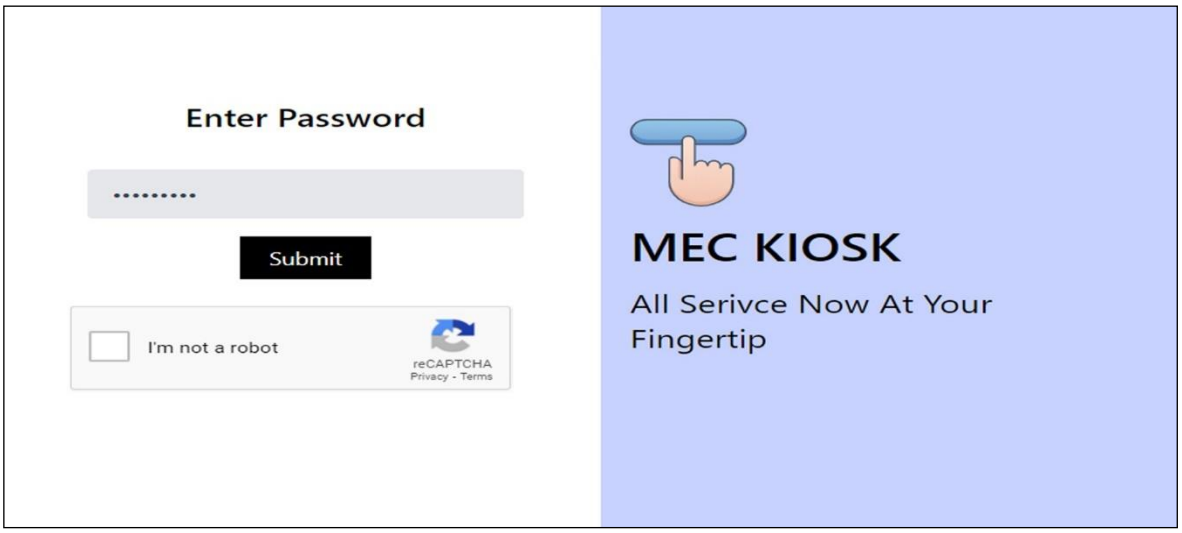

Fig. 22: Kiosk Login with Password.

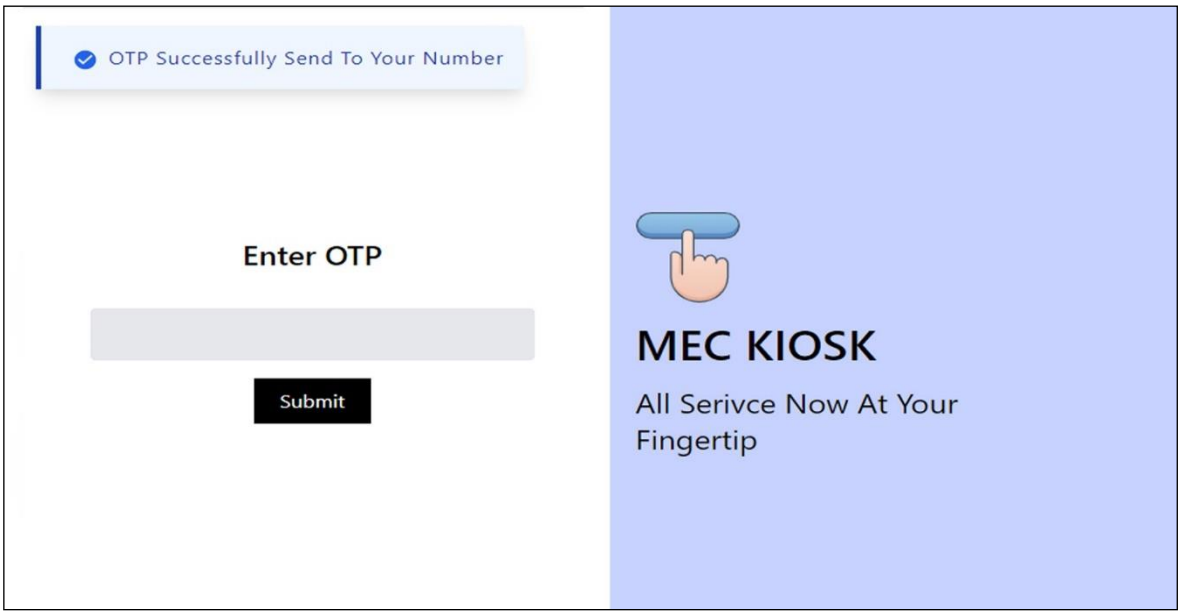

Fig. 23. Kiosk Login with OTP verification.

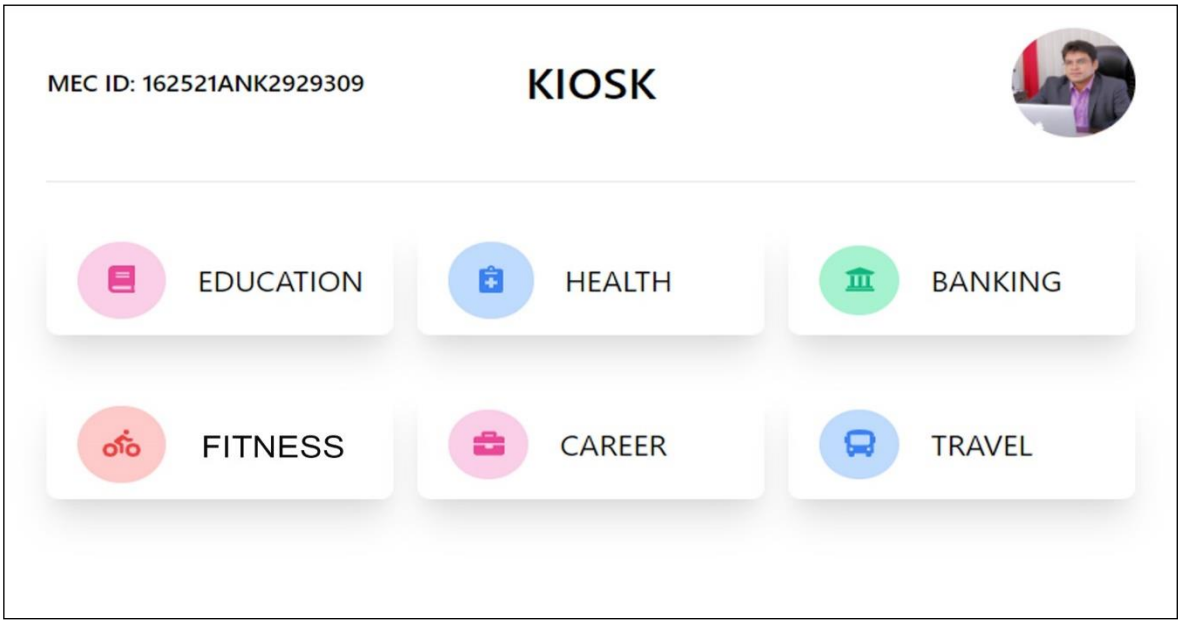

Fig. 24: KIOSK.

portal is confirmed after successful verification using the OTP. Figure 12 presents the MEC profile login page, where users need to enter their registered mobile number and password to access their MEC profile. Additionally, in Figure 13, you can see an example of the MEC portal's ability to capture personal information such as the date of birth (DOB) and email address. In a similar way, in Figure 14, the User is able to input their address information. Last but not least, in Figure 15, we can see that. In order to register, the user must provide their Father Name, Mother Name, and their MEC ID to proceed with the registration process. Figure 16 showcases the user's upload of an image and signature as part of the registration process. In Figure 17, the user uploads a document and specifies the document number. Once the document is uploaded, Figure 18 demonstrates that the relevant unit receives the details within their dedicated portal. Upon successful document verification by the unit, as shown in Figure 19, the user's information is updated in the MEC Admin Dashboard. The MEC Admin then proceeds with the verification process to complete the user's registration. Once the verification is successfully completed, the MEC Admin assigns a unique MEC Card Number to the user. Figure 20 represents the issuance of a new card to the user through a swipe process. The Kiosk Login Portal is displayed in Figure 21, allowing the user to swipe their MEC card and enter the password, as illustrated in Figure 22. To ensure the security of users' accounts, the portal immediately sends a One-Time Password (OTP) to the user's mobile phone after they enter their password. Figure 23 shows the user inputting the OTP. In the case of a successful login, as shown in Figure 24, Upon entering the Kiosk page, the user has access to the page where the desired service can be accessed, from where the user can take advantage of it.

5. Conclusions

In recent times, there has been a rise in fraudulent economic transactions due to insufficient user identification in an integrated manner. This concern has led to extensive research on integrating banking systems with user identification involving multiple parties, including the user (citizen), government, and bank. By engaging multiple parties, this collaborative approach ensures the identification of genuine users and effectively mitigates the risk of fraudulent transactions, thus safeguarding the financial assets of citizens. It has been proposed that a single-window-based user interface could be implemented as a further enhancement to this integrated banking system. The authors of this paper have successfully addressed this objective through the introduction of a Cloud Banking System that leverages a versatile electronic card interface. This system enables unique user identification through a dedicated identification number assigned to the electronic card. Additionally, the electronic interface facilitates diverse electronic transactions via a cloud platform. A robust mechanism known as PINA, it establishes privacy, integrity, non-repudiation, and authentication of the data within the cloud banking system. By integrating Blockchain and InterPlanetary File System (IPFS), the authors were able to strengthen the security of this system. Before committing huge amounts of energy and resources to the deployment of the proposed model in the field, it is prudent to perform simulations of the proposed model. To achieve this, Object-Oriented Modeling (OOM) was utilized, resulting in a Class Diagram that elucidates the relationships among the key entities and highlights the static structure of the proposed model.

Acknowledgement:

I would like to begin by expressing my heartfelt gratitude to my Co-Authors Abhishek Roy for their constant guidance and support without which I could not have completed this dissertation. I consider myself to be extremely privileged to have been working under his guidance.

Author Contribution:

In this research, Ankur Biswas and Abhishek Roy collaborated on the conceptualization and validation of the study. Ankur Biswas developed the methodology, performed formal analysis, and curated the data. Additionally, Ankur Biswas took the lead in writing the original draft and managing project administration. Both authors contributed to software development, investigation, writing review, and editing, as well as data visualization. Abhishek Roy provided supervision and secured funding for the research.

Data Avaliablity:

The data that supports the findings of this study are available upon reasonable request.

Competing Interest:

The authors declare no competing interests related to this work.

Declaration

Conflict of Interest:

It is also declared that there is no conflict of interest regarding the content of this research paper.

Funding:.

There is no funding.

References

[1] A. Biswas and A. Roy, "Multilevel User Verification in Cloud Banking System", *Lecture Notes on Data Engineering and Communications Technologies*, pp.

527-537, 2021. https://doi.org/10.1007/978-981-33-4968-1_41.

[2] A. Biswas and A. Roy, "Blockchain-Based User Authentication in Cloud Governance Model", *Intelligent Sustainable Systems*, pp. 815-825, 2021. https://doi.org/10.1007/978-981-16-2422-3_64.

[3] A. Biswas, R. Sil and A. Roy, "A Study on Application of Interplanetary File System", *Communication and Intelligent Systems,* pp. 1017-1025, 2021. https://doi.org/10.1007/978-981-16-1089-9_79

[4] A. Roy, "Object-Oriented Modeling of Multifaceted Service Delivery System Using Connected Governance", *Services and Business Process Reengineering*, pp. 1-25, 2020. https://doi.org/10.1007/978-981-15-2455-4_1.

[5] A. Roy, "Smart delivery of multifaceted services through connected governance", *3rd International Conference on Computing Methodologies and Communication (ICCMC)*, 2019. https://doi.org/10.1109/iccmc.2019.8819851.

[6] A. Biswas and A. Roy, "A study on Dynamic ID based user authentication system using smart card", *AJCT*, vol. 5, no. 2, Nov. 2019. http://www.asianssr.org/index.php/ajct/ article/ view/871.

[7] A. Roy and S. Karforma, "Uml Based Modeling of ECDSA for Secured and Smart E-Governance System", *Computer Science and Information Technology (CS and IT)*. 2013..https://doi.org/10.5121/csit.2013.3219.

[8] R. Purkayastha and A. Roy, "Static Structure of Smart Card based Cloud Voting System," in *Proc. 2nd Global Conference for Advancement in Technology (GCAT)*, pp. 1-9, 2021. doi: 10.1109/GCAT52182.2021.9587878.

[9] R. Purkayastha and A. Roy, "Object Oriented Modelling of Cloud Voting System," in *Proc. Asian Conference on Innovation in Technology (ASIANCON)*, 2021, pp. 1-7, doi: 10.1109/ASIANCON51346.2021.9544953.

[10] S. Mohapatra, K. Paul, A. Roy, "Object-Oriented Modeling of Cloud Healthcare System Through Connected Environment", Applications *of Internet of Things*, 151-164, 2020. https://doi.org/10.1007/978-981-15-6198-6 14.

[11] G. Mobin and A. Roy, "A literature review on cloud based smart transport system", *5th International Conference on Trends in Electronics and Informatics (ICOEI)*, 2021. https://doi.org/10.1109/icoei51242.2021.9452884.

[12] S. Biswas, A. Roy, "An Intrusion Detection System Based Secured Electronic Ser-vice Delivery Model." *3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, India, pp. 1316-1321, 2019.

[13] N. Singhal, M. Sharma, S. Samant, P. Goswami, Y. Reddy, "Smart KYC using blockchain and IPFS", *Lecture Notes in Electrical Engineering*, pp 77–84, 2020. https://doi.org/10.1007/978-981-15-3125-5-9.

[14] S. Muralidharan, H. Ko, "An InterPlanetary file system (IPFS) based IoT framework", *IEEE international conference on consumer electronics (ICCE)*, pp 1–2, 2019. https://doi.org/10.1109/ICCE.2019.8662002

[15] N. Tapas, G. Merlino, F. Longo, "Blockchain-based IoT-cloud authorization and delegation", *IEEE international conference on smart computing (SMARTCOMP)*, Taormina, pp 411–416, 2018.

[16] V. Odelu, "IMBUA: identity management on blockchain for biometrics-based user authentication", *Advances in intelligent systems and computing*, pp 1–10, 2019. https://doi.org/10.1007/978-3-030-23813-1-1

[17] N. Nizamuddin, H. Hasan, K. Salah, "IPFS-Blockchain-Based Authenticity of Online Publications", *Lecture Notes in Computer Science*, pp 199–212, 2018. https://doi.org/10.1007/978-3-319-94478-4_14.

[18] N. Ying, Z. Yao, Z. Hua, "The study of multi-level authentication-based single sign-on system*", 2nd IEEE international conference on broadband network and multimedia technology*, pp 448–452, 2009.

[19] P. Lotfallahtabrizi and Y. Morgan, "A novel host intrusion detect ion system using neural network", in *Proc. IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, pp.124-130, 2018.

[20] I. Gordin, A.Graur, A. Potorac, "Two-factor authentication framework for private cloud", in *Proc. 23rd International Conference on System Theory, Control and Computing (ICSTCC)*, pp. 255–259, 2019.

[21] A. Mahalle, J. Yong, X. Tao, "Protecting privacy in digital era on cloud architecture for banking and financial services industry", in *Proc. 6th International Conference on Behavioral, Economic and Socio-Cultural Computing (BESC)*, pp. 1–6 , 2019.

[22] A. Mahalle, J. Yong, X. Tao, "Ethics of IT security team for cloud architecture infrastructure in banking

and financial services industry", in *Proc. IEEE 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pp. 506–511, 2019. https://doi.org/10.1109/CSCWD.2019.8791928

[23] S. Nagaraju and L. Parthiban, "Trusted framework for online banking in public cloud using multifactor authentication and privacy protection gateway"' *J. Cloud Comp. pp* 4-22, 2015. https://doi.org/10.1186/s13677-015-0046-4.

[24] S. P. Tripathi, A. Kumar, R. Astya, "Study on secured framework for cloud based online banking", in *Proc. International Conference on Computing, Communication and Automation (ICCCA*), pp. 853–858, 2017. https://doi.org/10.1109/CCAA.2017.8229915

[25] L. Sangavarapu, S. Mishra, A. Williams, G. R. Gangadharan, "The Indian banking community cloud", *IT Professional*, vol. 16, no. 6, pp. 25–32, 2014. https://doi.org/10.1109/ MITP.2014. 97.

[26] M. Singh, K. S. Tanwar, V. M. Srivastava, "Cloud computing adoption challenges in the banking industry", in *Proc. International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, pp. 1–5, 2018. https://doi.org/10.1109/ICABCD.2018.84 65412.

[27] A. Ghosh, T. Das, S. Majumder and A. Roy, "Authentication of userin connected governance model", International Conference on Recent Developments in Science Engineering and Technology, pp. 110-122, 2019.

[28] R. Khatun, T. Bandopadhyay and A. Roy, "Data modeling for e-voting system using smart card-based e-governance system", International Journal of Information Engineering and Electronic Business, vol. 9, no. 2, pp. 45, 2017.

[29] S. Mohapatra and A. Roy, "A Study on Mediclaim Processing in Connected Healthcare System", *Lecture Notes in Electrical Engineering*, pp. 363-374, 2021. https://doi.org/10.1007/978-981-33-6393-9_37.

[30] S. Paul, K. Bandyopadhyay and A. Roy, "A study on integrated cloud education system*", Advances in Electrical and Computer Technologies: Select Proceedings of ICAECT* 2020, pp. 289, 2020.

[31] A. Biswas and A. Roy, "A Study of Identifying and Discussing Cloud Com Puter Threats and Attacks with Mitigation," Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 11, no. 1, pp. 723–729, Apr. 2020. https://turcomat.org/index.php/turkbilmat/article/view/12780.

[32] A. Biswas, R. S. Deol, B. K. Jha, G. Jakka, M. R. Suguna and B. I. Thomson, "Automated Banking Fraud Detection for Identification and Restriction of Unauthorised Access in Financial Sector," 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), 2022, pp. 809-814, doi: 10.1109/ICOSEC54921.2022. 9951931..

[33] Biswas, A., Roy, A. and Nandy, D. (2023) 'Smart card-based secured cloud banking system using smart contracts', International Journal of Computer Information Systems and Industrial Management Applications, Volume 15, pp. 512–521.

[34] Biswas, A. and Roy, A. (2023) 'Enhancing Privacy and Security in Banking through Dynamic ID-based User Authentication System', European Chemical Bulletin, 12(10), pp. 3991–3998. doi:10.48047/ecb/2023.12.10.2792023.

[35] Wanjiku, M., Ben-David, Y., Costa, R., Joo-young, L., & Yamamoto, T. Automated Speech Recognition using Deep Learning Techniques. Kuwait Journal of Machine Learning, 1(3). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/135

[36] Uppal, A. ., Naruka, M. S. ., & Tewari, G. . (2023). Image Processing based Plant Disease Detection and Classification . International Journal on Recent and Innovation Trends in Computing and Communication, 11(1s), 52–56. https://doi.org/10.17762/ijritcc.v11i1s.5993

[37] Nagendram, S., Singh, A., Harish Babu, G., Joshi, R., Pande, S.D., Ahammad, S.K.H., Dhabliya, D., Bisht, A. Stochastic gradient descent optimisation for convolutional neural network for medical image segmentation (2023) Open Life Sciences, 18 (1), art. no. 20220665, .