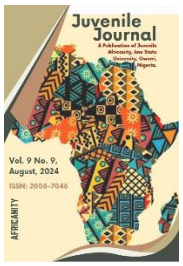


Juvenile Journal
Publication of Juvenile Africanity, Imo State University, Owerri, Nigeria.
ISSN: 2006-7046
Vol.9 No. 9 August 2024
https://mejhpgs.online/index.php/jjja

Multi Security Mobile Banking Application

[1]Iloanya Emmanuel UC
Department of Computer Science
Imo State University, Owerri, Nigeria

[2]Dr C.C.Ibebuogu
Department of Computer Science
Imo State University, Owerri, Nigeria

[3]Dr (Mrs) Ebele Leticia Eleberi
Department of Computer Science
Imo State University, Owerri, Nigeria

Abstract

Multi-Security Mobile Banking Application is a web Based Application that secures transaction by introducing more than one security options. The aim of the study is to develop web based application multi-factor authentication (MFA) model for effective information security in the banking system that utilizes three (3) tiers of security authentication options; (PIN); (PIN & OTP) and (PIN, OTP & Finger Print) for strong authentication that will be difficulty for unauthorized access or cyber criminals to access. The researcher is motivated by prevalent and incessant fraud associated with the current single factor (SF) authentication mechanisms in the existing mobile banking system such as PIN hacking, identity theft,Duplicate Flash Player,Uncontrollable cash transfer by unauthorized user which is as a result of high demand of mobile devices for mobile banking transactions. Object-Oriented Analysis and Design (OOAD) and prototyping would be deployed to carry out the methodology. Software tools to be used include JavaScript, PHP, and MYSQLite for the Database. The expected result would be called Multi - Security Mobile Banking Application (MSMBA) model for affective information security in the mobile banking system that utilized three (3) tiers of security authentication options.

Keywords: Multi, Factor, web-based, Mobile banking, Database double factor security, Software OTP, PIN, Authentication, MFA.

1. Background of the Study

Information security field has grown and evolved in recent years. Information security, sometimes referred to as 'InfoSec', is the practice of securing information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction

(Greig et al., 2019). It is a general term that can be used regardless of the form the data may take either electronic, physical, etc. It is imperative to highlight that the two major aspects of information security are information technology security (IT Security) and information assurance (IA). Information technology security (IT Security) is, sometimes referred to as "computer security". IT security is information security applied to technology, most often some form of computer systems. Its Security specialists are almost always found in many major financial institutions, enterprises, or establishments due to the nature and value of the data within large businesses. They are responsible for keeping all of the technology related to information within the organization and secured them from malicious cyber-attacks that often attempt to breach into critical private information or gain control of financial information transactions or internal systems (upwork.com/resources centre (2021). Information assurance is the act of ensuring that data is not lost when critical issues arise. These issues include, but not limited to, natural disasters, computer/server malfunction, physical theft, or any other instance where data have the potential of being lost

(Committee on National Security Systems, 2017).

Since early days of writing, politicians, diplomats, the military, governments, corporation, hospitals, private businesses and financial institutions process a lot of confidential data about their employees, customers, products, research and financial status. These data are collected, processed into information, stored on electronic computers and transmitted across networks to various computers(Pujitha&Mallu ; 2018. These institutions understand that it is necessary to produce some mechanism to protect the confidentiality and detect some intrusions into the network. (Danvas2014) stated that, Julius Caesar's cipher at 50BC was invented in order to prevent his secret messages from being read in case they get into the hands of wrong users. He further stressed that, the most part protection was achieved through the application of procedural handling controls. Sensitive information was marked on to indicate that it should be protected, transported, by trusted persons, guarded and stored in a secure environment or strong box

This multi-factor authentication will be implemented using the knowledge base factor (PIN, OTP) and biometrics factor (finger-print&facerecognition) for effective security to block the criminal if he/she succeeds in passing the first level of authentication.

What has caused this rise in the criminal activities in the mobile banking system is because of the weakness of the current authentication system in place; the single factor (SFA) and two factor authentication (2FA) mechanisms. This involves the knowledge base and possessive factor (pin or password and ATM card information respectively).Pin or password can no longer be effectively used for security of the information transactions in the banking system network.

In response to the guidance, the United States (US) financial institutions went and deployed additional knowledge-based authentication methods, such as shared secrets or challenge questions, only to discover later that such methods do not satisfy the regulatory definition of true multifactor authentication because they could not give the true security desired. As a result, the supplemental regulatory guidelines and structure enforcement are now beginning to force the abandonment of knowledge-based methods in favor of "true multifactor authentication''. The FFIEC (2021) Further stated that the Financial Institution should adopt an effective authentication and access risk management principles and practice for digital banking services and information systems.

Based on the apparent failure of the existing system, multifactor (MFA) authentication has been proposed in this research work as a more reliable solution to improve authentication in the current system. This multi-factor authentication (MFA) system has a three (3) tier authentication options depending on the amount of money to be transacted. The authentication factors include PIN, NIN and additional multi modal biometrics (finger-print, face, and iris recognition) and OTP security to block the criminal if he/she succeeds in passing the first level. If the current system is redesigned and implemented with MFA mechanism, it will prevent fraudsters from easily penetrating the financial system. This will also improve security of information transaction and reduces challenges and vulnerability of hackers and cyber criminals in mobile banking system particular in Nigeria and the world at large.

2. Statement of the Problem

i) Today, there are rampant cases of such as PIN hacking, password theft, identity theft, re-activation of debit card information fraud. In the SF mechanism, the pin can be easily hacked by an attacker who may penetrate someone's account and steal huge amounts of money. It can also be purchased from professional cyber criminals.

ii) Uncontrollable transfer of cash by unauthorized user. Most times, when we use only pin to access our mobile App this grants access to the user to carry out transactions as desired and the criminal can go as far as emptying the account. Multifactor security will help to control the withdrawal limit because each security category has withdrawal limit you can perform. (Ndunagu et al., 2019).

iii) Duplicate Flash Player is a video application which is either installed via an infected SMS or predatory E-Mail that contains some malicious download link. Once the mobile device users install the app over a smartphone, it requests the mobile phone administrator rights via permission prompt. After this, the malware of the app creates a dummy login screen that gets visible when the user opens it next time. Once the user enters the user credentials or bank login credentials, the malware copies it and sends the data into the database of the malicious users that it can use later on.

3. Aim and Objectives of Study

i. To develop web based application MFA model with (3 tiers) options for effective security of transaction in banking system.

ii. To develop a model that will control transaction limit by introducing a security measure depending on the amount a customer tends to transact.

iii. To block criminal and unauthorized users from

committing fraud to the banking system using the customer's pin.

iv. To provide a model that can prevent customer's transaction form been accessed by unauthorized person.

v. To create authentications multi options for customers in the mobile web banking system for accessing their account.

4. Significance of the Study

i. Increase the reliability, accuracy, efficiency and security in service delivery in banking system.

ii. Prevent or block the cyber-criminal or unauthorized user that commit fraud in the financial institution.

iii. Boost the integrity and be of high benefits to the banking institutions.

iv. It alsoignites an urgent action for the federal government innovative plan for the training of adequate computer or IT professionals on the development of software security programs and maintenance of MFA authentication mechanisms.

v. Again, it will bring about the need for government to train computer forensic professionals for crime detention.

vi. Moreover, this research is significant because treating security issues with kid gloves can bring down the economy of the country with great consequences such as poverty, loss of employment, increase in crime etc. It is, therefore, crucial that a scientific solution like this should be adopted to avert this challenge.

vii. Furthermore, this work is very importance because the model will be highly applied in the banking sector and other financial institutions. It will also be beneficial to the mobile banking users for trust, confidence and easy mobile transactions.

5. The Scope of Study

This work will focus on the development of web based mobile banking application MFA model for banking system which will authenticate users that are remotely

accessing the banking system based on different levels of access controls for security of their transactions while using the mobile App.

6. Limitation of Study

The limitation of this study is difficulty in collecting information from the bank. The bank staff and manager find it difficult to release some important information during the interview at the initial stage. It is not easy for the researcher despite subsequent visit. The Cost of execution may be little high because the MFA mechanism application will be incorporated on the smart phone (Android phone) that has the features of smart biometrics. Although many users can afford android phones because of the technology innovation on the use of mobile devices for easy self-mobile banking system. Another limitation is the cost of disseminating information and data gathering.

7. Methodology

This chapter dwells on how the multi-factor authentication system would be developed. The process includes; research design, software development method, system development, and implementation. Before going into details in this chapter, it is pertinent to look briefly at the concept of the software development method or model and research design methodology. Software development model or methodology or system development methodology in software engineering is a framework that is used to structure, plan, and control the process of developing an information system. A wide variety of such frameworks have evolved over the years, each with its own recognized strengths and weaknesses.

Methodology is a road map of how a meaningful research is to be conducted. Methodology properties include: Data gathering instrument, Data extraction and sources of data. A Software design methodology is a set of procedure that one can follow to accomplish a software development process from the beginning to its completion.

The problem is formulated, user requirements are identified, and then a model is built based upon real–

world objects. The analysis produces models on how the proposed system should function and how it must be developed such as:

1. User Functional Input Requirements:

Functional Requirement describes the use cases and actors that are found in the new System "Modelling Effective Information Security in the Mobile Banking System". Each user case is described in details with diagrams and tables in their respective module section. These user case diagrams model the desired behaviour of the system. The Functional requirement is categorized in two (2) main modules:

1. Public Users
2. Banks/Financial Industries

Public User Requirement Module

Every adult within any civilized country have the right to mobile phones which could enable them download and install the application of their choice depending the uses. On this case, adequate security of people's funds is very crucial as they need to enrol themselves by using the mobile application which could guarantee adequate security of their financial transactions which are stated below and shown in figure 3.1.

- NIN (National Identification Number)
- Voters card
- Driver's license
- NEPA bill
- Passport
- BVN (bank verification number) for identification.

8. Reasons for Adopting the OOADM

The reasons for adopting the OOADM in the proposed system are as the result of the following advantages:

i) **Improved modularity:** OOAD encourages the creation of small, reusable objects that can be combined to create more complex systems, improving the modularity and maintainability of the software.

ii) **Better abstraction:** OOAD provides a high-level, abstract representation of a software system, making it easier to understand and maintain.

iii) **Improved reuse:** OOAD encourages the reuse of objects and object-oriented design patterns, reducing the amount of code that needs to be written and improving the quality and consistency of the software.

iv) **Improved communication:** OOAD provides a common vocabulary and methodology for software developers, improving communication and collaboration within teams.

v) **Reusability:** OOAD emphasizes the use of reusable components and design patterns, which can save time and effort in software development by reducing the need to create new code from scratch.

vi) **Scalability:** OOAD can help developers design software systems that are scalable and can handle changes in user demand and banking requirements over time.

vii) **Maintainability:** OOAD emphasizes modular design and can help developers create software systems that are easier to maintain and update over time.

viii) **Flexibility:** OOAD can help developers design software systems that are flexible and can adapt to changing banking requirements over time.

ix) **Improved software quality:** OOAD emphasizes the use of encapsulation, inheritance, and polymorphism, which can lead to software systems that are more reliable, secure, and efficient.

Modus Operandi of Authentication in the Existing Mobile Banking System in Nigeria: The modus of operandi of authentication here is that, before an intending mobile user is illegible to access mobile banking transaction services he/ she must register with the bank. The requirement for registering and using mobile banking may vary among different banks; however, some requirements are basic to all banks statement.

In the existing system, before a mobile banking user gets to the stage of authentication he or she needs to undergo two phases: the enrolment and the registration phase.

1. **The enrolment phase:** The enrolment phase involves obtaining user's details bio data. This involves the first name, middle name and last name. The bank will also request for the following NIN (National Identification Number), voters card, driver's license, or NEPA bill, passport and BVN (bank verification number) for identification. These bio data will enable the bank to generate an account number of the user which will be sent to the registered phone number of the user stored in the SIM card (subscriber's identity module).The SIM information will be stored in the bank database server for identification and authentication purposes.
2. **Registering and using mobile banking**: After the internet mobile banking user must has been enrolled by the bank. An intending user having been enrolled must have an account with the bank, online user ID (Internet Banking ID) a payment card such as Debit/ATM Card, credit card from the bank. These will enable the user to proceed for registration or sign up on the bank mobile application. The Steps for Registering or Activating Mobile system

a) Firstly, the mobile banking user has to download the mobile application (Mobile APP) from the APP Store.
b) Click on the register menu, then
c) Select the debit card option
d) Enter the account number or phone number
e) Enter the last 6 digits on the debit card
f) Enter the card PIN

g) A 4 digits registration/verification code will automatically generated and sent to the user's phone

h) The user will input a 4 digit registration code sent to the phone number

i) Upon receiving a successful prompt

j) Choose a password (not less than a 6 digit) which will enable the user to access the mobile banking platform at any time. Reconfirm the password.

k) Choose or create 4-digit PIN for transactions, reconfirm the PIN.

l) Select confirm

Having concluded the registration, the mobile banking user will be illegible to log in with password and account number to the mobile banking platform anytime for banking transaction. The existing system mobile banking application enable mobile banking user to access the following services, such as transfer funds within and across other banks, check account balance, view SMS based on transaction history, payment of bills, purchase of airtime and flight tickets etc.

9. The Modus Operandi of the system

The proposed system is the Modelling of effective information security in the mobile banking system. This is involving the development of mobile base MFA application banking model to enhance security in the existing system. This multifactor will be in conformity with the updated guideline of federal financial institution examination council (FFIEC) directives for banks to start using multifactor or multilayered authentication for access controls for strong security in the banking systems (FFIEC; 2021).

10. Operation of Multi-Factor Authentication in the new System (Mobile Banking)

In the proposed system, before a mobile banking user gets to the stage of multi-factor authentication he or

she needs to undergo two phases: **the enrolment phase** (where we obtain data of the user) and **the registration phase** where the user create an account to make him or her eligible to use the mobile banking application.

A The Enrolment Phase

The enrolment phase involves obtaining the users details, including bio data(the first name, middle name and last name), phone number , finger print, , BVN (bank verification number),National Identification Number (NIN) of the national ID, or valid passport, voter's card and IMEI device and other information at the time of account creation in the bank. These bio data will enable the bank to generate an account number of the user which will be sent to the registered phone number of the user stored in the SIM card (subscriber's identity module).The SIM information will be stored in the bank database server for identification and authentication purposes.

B. The Mobile Application's Platform Functions: The Mobile Application's Platforms developed will have the following functions:

a. Sign up / Registration function

b. Sign in /Log in and authentication options function

c. Transfer

d. Services

e. Transaction history function

C. Sign-Up / Registration Function Phase

For the user to sign up or register in the new system he or she has to undergo the following process:

1. The mobile based application for the proposed system will be lunch to the Google play store or Apple App store after software development. The mobile client application will run on android phone or in iphone operating system.
2. The user has to download the application from Google play store or apple app store on his or her mobile device ;

3. Open the mobile client application on your phone and click ‘’ register ’’
4. Select your preferred language from the options provided;
5. Enter your phone number and click “next”;
6. A verification code will be sent to your number. Input and click ‘’next’ ’to verify your phone number;
7. Provide your personal information; fill in the required fields with accurate personal information, including bio data.‘Click Next’’;
8. Choose a secure and unique password for your account. The password will be alphanumeric or numeric and proceed;
9. The mobile banking application will prompt you to link your bank account for seamless fund transfers and other financial transactions; and
10. You will be ask to provide to submit a valid means of identification, such as PIN, finger ,face , iris NIN, BVN , voters card, IMEI and ensure that the ID is clear before submitting .

D Authentication Phase

In this stage, for an authentication to take place in the new system

a. New user will be prompted to register first, while registered users will directly go to login for using the mobile banking application.
b. Mobile client application prompts the user to scan his or her finger print with mobile device and password to log-in to the mobile banking application platform. From the login page the user is directed to the payment page.
c. The payment page will ask for the payee details and the amount to be transferred, if the amount exceeds the account balance, the transaction fails, otherwise proceed. Now for the

1st tier: If the transaction is (less than) < #100,000: Authenticate via (PIN):

d. Next the mobile client application will require the user to enter his or her PIN. If the PIN cross matched with the PIN template stored in the central

database of the bank server after the successful verification, the user will carry out transactions successfully or otherwise will start afresh and have only three chances to retry again.

2nd Tier: If transaction is from #100,000 to #500,000: Authenticate via (PIN, &OTP):

e. For a payment transaction from #100,000 to #500,000, here after the user has authenticated with PIN, he or she will be directed to the next interface for OTP. (**Faisal, et al., 2017**).

3rd Tier: If transaction is greater than >=500,000 &above: Authenticate via (PIN, OTP, and Finger Print):

In the 3rd tier, If the user enters amount greater than 500,000 naira and above the 3rd tier security authentication will pop out to authenticate the user via (PIN,OTP, Finger).

f. Next the mobile client application will require the user to enter his or her PIN. If the PIN cross matched with the PIN template stored in the central database server of the bank, after the successful verification.

g. Next the mobile client application smart device incorporated with biometric features will require the user to thumb print for authentication. If the finger print matches with stored template in the bank server database is correct.

h. Next the server will automatically generate OTP (One Time Password) which is sent to the user's registered user email and which is used once. The user has to enter the valid OTP else the entire transaction will be terminated.

i. The OTP serves as a transaction confirmation number, which he/she must input to confirm the transaction.

The proposed system used multiple factor authentication (MFA) options for payment transactions as have been described above. That is, authentication options depend on the amount of to be transacted.

11. Algorithm

Lunching the APP Algorithm

- ✓ Step 1: Program start;
- ✓ Step 2: User enter username and password combination;
- ✓ Step 3: If(username==user && password==pass){
- ✓ Step 4: Display Login Successful;
- ✓ Step 5: Launch Dashboard;

- ✓ };
- ✓ Step 6: end if;
- ✓
- ✓ Step 6: exit

Flow Chat Diagram of the Proposed Mobile Banking system

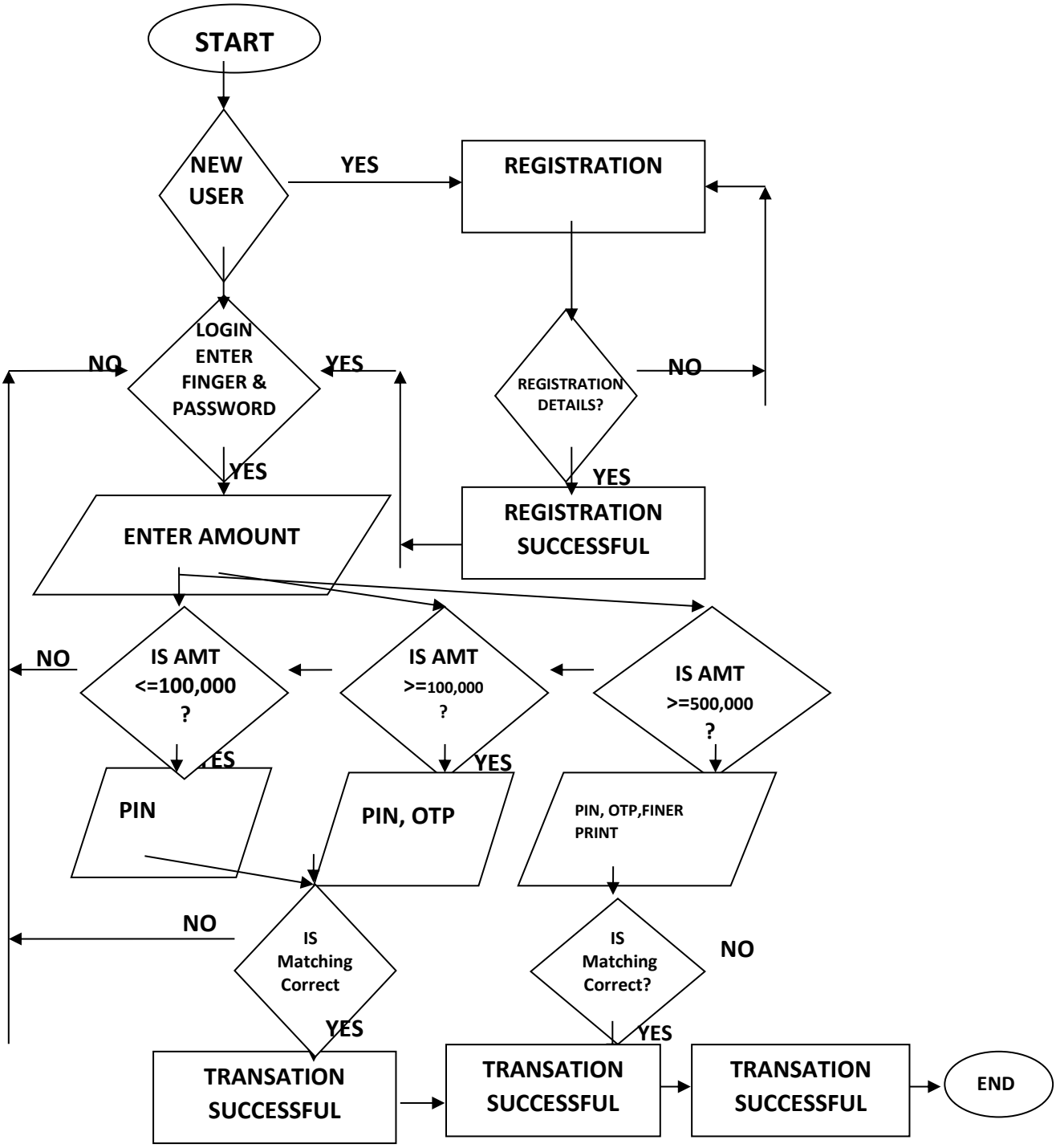


Figure 3.5Flow Chat Diagram of the new Mobile Banking System.

12. Advantages of the New System

1 Robust security is assured on the proposed system by using MFA authentications; PIN, fingerprint, facial recognition, voter's card, OTP and QR depending on the amount to withdraw. (A criminal can easily copy or crack pin or clone ATM card of the user in the case of online ATM). However, a criminal cannot easily clone the face or change the finger print features of the user because of its non-transferable and uniqueness. Even if it involves twins, their fingerprints never match. (Senthil et al., 2015).

2 The development of a honey pot environment will serve as a controlled environment for redirecting and monitoring attackers for decision making.

3 The disadvantages of using only SF or 2FA in the existing system are overcome, lending to increasing reliability on the authentication process of the proposed system.

4 If the fingerprint is faked with those of dead people, liveliness can be developed to stop the fraud in the proposed system.

5 The proposed system will increase customer's confidence in the use of mobile banking transaction system and other financial institutions across the globe.

6 Different levels of authentications on the certain amount to withdraw ensure will make it more difficult for an intruder to penetrate the transaction system.

7 The proposed system authentication security will also enhance banks integrity and more user acceptability on mobile banking system for transaction.

8 The proposed system will prevent criminal or unauthorized access from committing fraud to the banking system if the user's phone is stolen.

9 The proposed system authentication will help to prevent

the user's mobile device from theft.

13. High Level Model of the Proposed System

The development of high level model (HLM) of the proposed system shows proposed high level of multi-factor authentication in the mobile banking system involving PIN, multimodal biometrics (fingerprint, face recognitions & Iris) ,OTP It also shows the relationship among and between the various components in the system. The high level model with the aid of data flow diagrams show how the input data is transformed to output results through a sequence of operations in the propose system. The high level model of the proposed system is illustrated below.

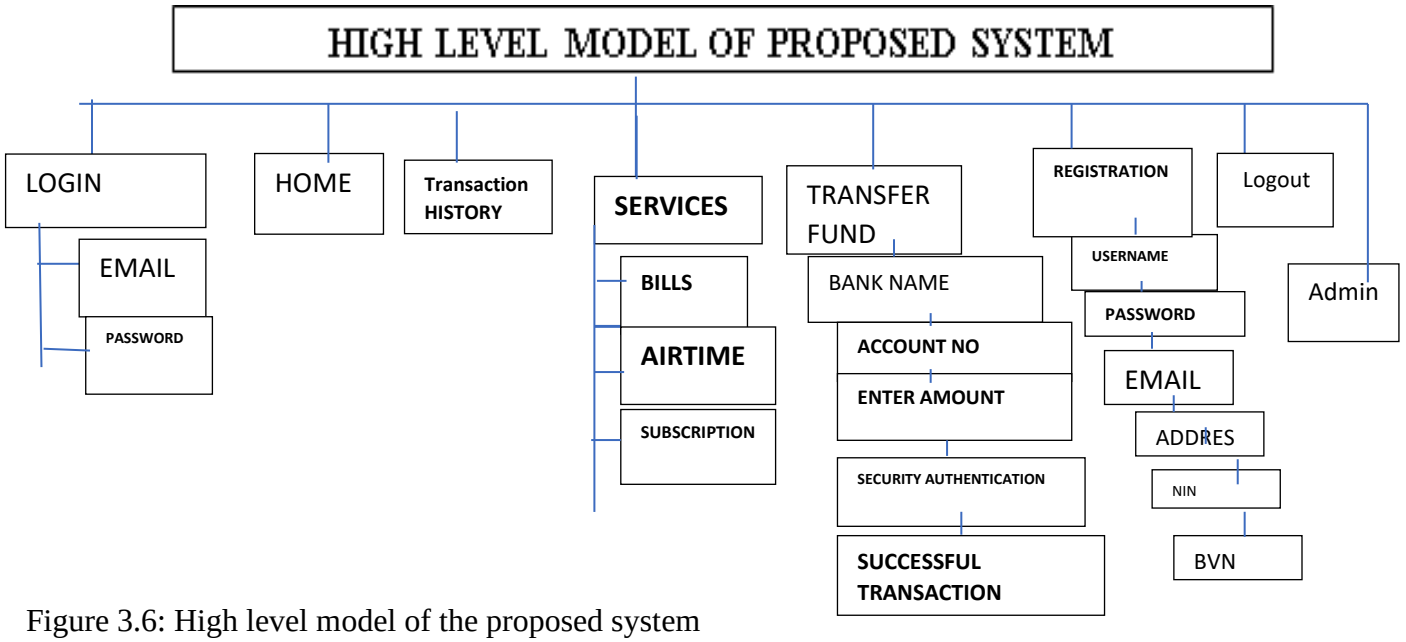


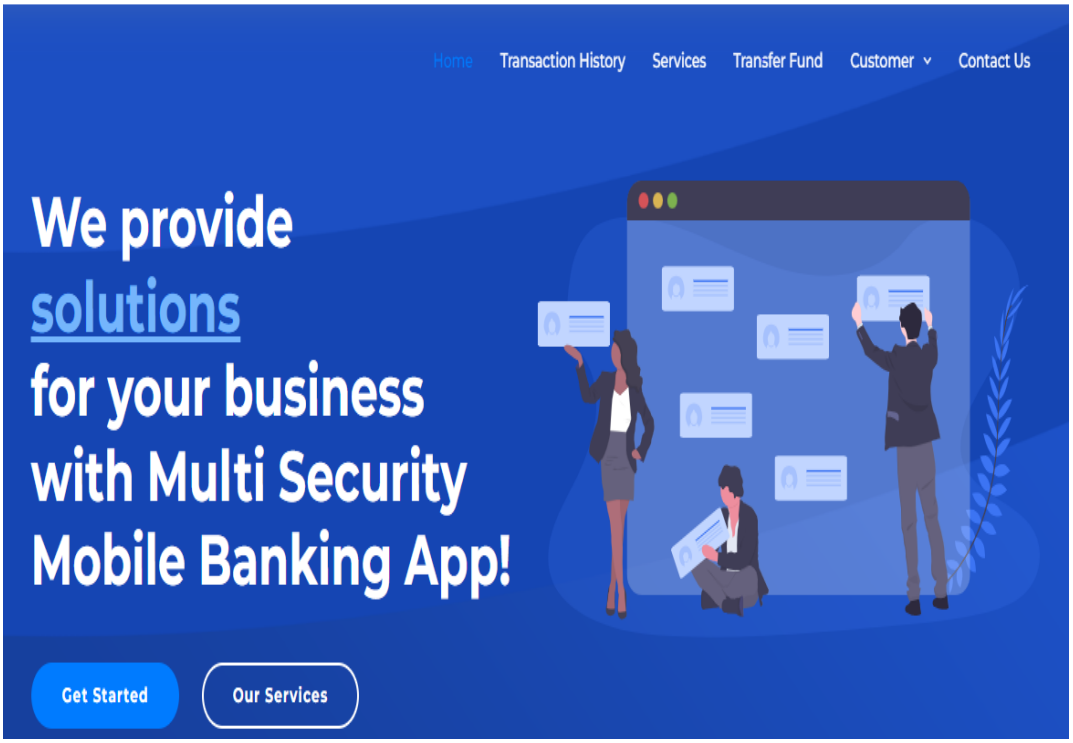
Figure 3.6: High level model of the proposed system

14. Contributions To Knowledge

The study has contributed in the area of security of user banking transactions by using three factor security measures namely: PIN, Finger-Print and OTP. It has brought an idea to the banking sector to know that three security measures could be integrated in the banking sector to control access and indeed capture fraudsters on real-time basis. The study presented the developed system source

code to improve and contribute in knowledge discovery by researchers, students and instructors in the area of mobile phone development and security systems. The study has created awareness about the importance of mobile banking security; it has provided guideline for future researchers to improve the system.

MULTIL FACTOR MOBILE BANKING APP



Reference

Akomea, et al; (2019): mobile banking applications authentication are poorly protected, thus giving opportunity for the attackers to hack them.

Ali, et al (2020): mobile money crime where fraudsters masquerade as employees of the bank by calling or sending SMS messages to mobile money users and agents to reveal their data including PINs for an update".

Bankwithus.in/what-is-mobile-banking, (2022); facility which provides banking services, such as; funds transfer, account statement, bill payment, transaction history, viewing account balances, checking rates.

Buku&Mazer ; (2017): Mobile banking system platform (MBSP) of the user's bank.

Chinta, et al. (2016,): social engineering techniques to evade mobile banking's 2FA scheme, compromise user

accounts, and avoid fraud detection technologies.

Chen. (2021): illegally or unauthorized access of the financial details of legitimate mobile user to perform illicit transactions

Dasgupta, D. Roy, A.; Nag.A.(2016) Toward the design of adaptive selection strategies for multi-factor authentication. Computer Security. 2016, 63, 85-116.

Danvas (2014): mechanism to protect the confidentiality and detect some intrusions into the network.

Deepa, (2014): voice recognition and smart card; for security authentication in the mobile banking platform system.

Eman. T. A., Daniyal, A. (2019) Two Factor Authentication Framework Using OTP-SMS Based onBlockchain. Department of Information System, Faculty of Computing and information technology, King Abdulaziz University, Jeddah, Saudi Arabia.

Edureka; (2023): cryptography as a construction and analyzing protocols that prevent third parties or the public from reading private messages.

FFICE, (2011): use of authentication methods that depend on more than one factor specially.

Ferraget, etal (2020); Smartphone sales are the majority of mobile handsets sold worldwide.

Fahmida, (2019): The disadvantage of pattern base authentication.

Faisal (2020): the push notification services offered by modern mobile platforms, such as; phone's APNS and Android cloud to device messaging, is used to provide a real-time challenge/response mechanism on a mobile device.

Greig et al (2019) 'InfoSec', the practice of securing information from unauthorized access, use, disclosure, disruption, modification.

Gunson, N. Marshall, D.: Morton, H.; Jack, M. (2011) User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. ComputerSecurity. 2011, 30, 205-220

Garba et al., (2020); Mobile internet penetration is forecast to be above 90 % in 2027.

Guma&Anael; 2020: Single-factor authentication (SFA), in contrast, requires only the knowledge the user possesses

Global crime survey (2014): economic crime as the major concern for organizations across all regions and worst hit is the financial sector of about 37% of global crime in (2020).

Greek; (2023): decryption reverse process and conversion of a secret message into a plain text message.

Grundmann, (2018): USSD interface and Telecommunication Company.

Gwahula, R.; (2016): mobile banking accounts and perform fraudulent transactions, or. change of PIN.

Harini, N.; Padmanabhan.T. (2013) others. 2CAuth: A new two factor authentication scheme using QR-code. Im J. Eng. Technol. 2013, 5, 1087-1094.