Modeling Effective Information Security in Mobile Banking System

Ikemelu Chinelo Rose-Keziah[1]., Agbakwuru. A. Onyekachi[2] & Amanze Bethran Chibuike[2]
[1]Department of Computer Science, Nwafor Orizu College of Education Nsugbe, Anambra state.
[2]Department of Computer Science, Imo State University, Owerri, Imo State.
DOI: 10.56201/ijcsmt.vol.11.no5.2025.pg18.33

Abstract
The objective of the study is to develop mobile based application multifactor authentication (MFA) model for effective information security in the mobile banking system that utilizes three (3) tiers of security authentications options; the use of (PIN); (PIN & Finger Print) and (PIN, Finger Print & OTP) for strong authentication that will be difficulty for unauthorized access or cyber criminals to penetrate. This study also applied RSA and AES crytographic algorithm. The motivation of this study is as a result of prevalent and incessant fraud associated with the current single factor (SF) or two factor (2FA) authentication mechanisms in the existing mobile banking system, which is as a result of high demand of mobile devices for mobile banking transactions. The methodologies that were adopted are Object-Oriented Analysis and Design (OOAD) and Agile. Top-down bottom approach in software development was adopted. Software tools include Java, Flutter SDK, Dart programming and Firebase- MySQL. The results of implementation and testing were secured mobile based application MFA model for affective information security in the mobile banking system that utilized three (3) tiers of security authentications; the use of (PIN), (PIN & finger print) and (PIN, finger Print & OTP) for access controls depending on the amount to be transacted, secured device-IMEI of every registered user, redirection of unauthorized access to the honeypot and provision of detailed transaction history of customers. These multi-factor authentications will be difficult for authorized user or any criminal attack such as phishing, impersonation, surfing attacks and man in the middle attack to penetrate the transaction system in mobile banking system.

Keywords: *PIN, RSA, AES, OTP*

Introduction

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, perusal, 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 center (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). These institutions understand that it is necessary to produce some mechanism to protect the confidentiality and detect some intrusions into the network. Danvas (2014) 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 stress 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. As postal services expanded, governments created official organizations to intercept and decipher letters (e.g. the UK secret office and deciphering Branch in 1653).There were rapid advancements in telecommunications, hardware and software, as well as data encryption in the early years of 21st century (Wikipedia, 2016). The availability of similar, more powerful and less expensive computing equipment made electronic data processing come within the reach of small business organizations, big companies, financial institutions (such as banks, saving institutions, credit unions, finance and leasing companies and mortgage companies) and home users. These companies quickly became interconnected through the internet. As a result, the rapid growth and widespread use of electronic data processing and electronic transactions conducted through internet, along with numerous occurrences of international terrorism. This geared the need for effective method of protecting the companies' and financial institution's data (especially, in banking sector) and the information they store, process and transmit from an unauthorized access or user. These institutions must focus beyond hard controls and challenges of ensuring data integrity, accuracy and consistency of data over its entire life cycle. Mcgladery (2013), the academic disciplines of computer security and information assurance emerged along with numerous financial institutions, all sharing the common goals of ensuring the security and reliability of information and information systems. The relevance of any financial institution is to secure, maintain the integrity, confidence and accuracy of information transaction that passes through the network. But one of the major drawbacks of financial institutions' implementation is the problem of integrity engendered by the emerging internet fraud. These seem to be challenged in the banking sector (especially in mobile banking system) which is focus of this research. Across Nigeria, online banking system technological advancement has led to the increase of deployment of ATM systems and use of mobile devices for online and mobile banking systems respectively. Mobile devices such as smart phones (especially Android phones) have paved their way rightly into the routine of human life. As they have a significant role in the daily life. Users feel comfortable and easy to use their phones more than their PC these days (Shaji, 2017). Android phone is a powerful smart phone that runs on the Android operating systems (OS) that is developed by google and is used by majority of mobile phone manufactures. Ferrage et al., (2020). Smartphone sales are the majority of mobile handsets sold worldwide. This is in line with the National Communication Commission (2019), which stated that Nigeria has over 150 million mobile subscribers and it expected that the percentage of this population, considering the government desire for cashless society, would embrace the mobile banking option. Android phones have 84% share of smart phones, tablets, 72%, while apple's iOS –powered by iPhones have only 27%. Mobile internet penetration is forecast to be above 90 % in 2027.More than one

hundred and ninety two (192) countries have active 4G mobile networks, which cover almost 50% of the global population.(Garba et al., 2020). Smart phones have greatly used in mobile banking systems. Mobile banking is defined as the services provided by a bank that allows its customers to conduct financial information transaction remotely using a mobile device such as smartphone or tablets. (Bankwithus.in/what-is-mobile-banking, 2022). It can also define as facility which provides banking services such as funds transfer, account statement, bill payment, transaction history, viewing account balances, checking rates, acquiring loan and checking rates via a user's mobile phone (Jayshri *et al*., 2021) Unlike conventional banking transactions, online or mobile is done without the services of human or cashier. As the use of mobile devices increases on daily basis, users of mobile banking continue to increase and this endangers the security of information transaction across the internet. The mobile banking security system has been breached as result of activities of emerging internet fraudsters and intelligent criminals that escalate in daily basis. Today, there are rampant cases of pin hacking, identity theft, re-activation of debit card fraud, stealing of debit card information, authentication attack, shoulder surfing attack, man-in-the-middle (MITM) attack, brute force attack, USSD technology vulnerabilities, denial of service attack, forgery, eavesdropping and phishing various forms of dishonest, being encountered by individuals or users who need the services of online mobile banking transaction service across the internet. These problems increase as a result of the authentication mechanism in place. In the existing banking system in Nigeria almost all the banks make use of SFA (single factor authentication) such as pin or password and 2FA (two factor authentication) that is; the use of personal identification number (PIN and card) just like in the ATM systems. The pin authentication according to Santhi, and Kumar, (2012) has stood the test of time mainly because of its speed and memo ability which are part of metrics, used to access the authentication system (both in ATM and mobile banking services in Nigeria. The second metrics, which is security, has often been compromised. Security can be breached when pin or password is hacked or divulged to an authorized person or card information stolen by an impostor for fraudulent purposes. This is in line with Chris (2019) who stated that mobile banking platform offer convenience to users on the run. But this advantage can be distressed if customers do not feel secure when using the services. They are prone to fraud and offer some elements of risk, because simple passwords are easy to guess by any impostor and difficult one may be snooped using sophisticated techniques". It can be purchased from professional hacks and cyber criminals. It can also be easily give out through social network. Therefore, the pin or password authentication mechanism in the exiting banking systems is no longer secure for effective security of information transactions in the banking system in Nigeria. This view is in line with Rajalakshmi *et al*. (2019) and Sahaji & Soman, (2020). Again, according to the Mohamed, (2014), SFA is well-suited for website or application access, it is not secure for enough for online transactions in the banking system. However, it was based on this argument and aforementioned problems that the idea of adopting mult-factor levels of authentication that will enhance security of transactions came up. Hence, the significance of the study; "Android based Multi-factor Authentication for Effective Information Security in the mobile Banking System." This is a Multi-factor Authentication (MFA) that can provide significant strength in the existing mobile banking system in Nigeria which is the focus of this study. This according to FFIEC (2012) is the use of multi-factor authentication (MFA) which requires the application of two or more authentication factors. Multifactor authentication is achieved by combining the three independent credentials: what the user knows (knowledge-based authentication), what the user has (possessive based authentication-security token or smart card)

and what the user is (biometric verification). Single-factor authentication (SFA), in contrast, requires only the knowledge the user possesses (Guma&Anael,2020). Moreover, MFA also entails the application of MFA in security systems in which more than one form of authentication factor are implemented to satisfy the legitimacy of a transaction (Rahav,2018). The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access online information transaction system. In 2005, in the United States interest in multifactor authentication (MFA) was driven by regulations such as Federal Financial Institutions Examination Council (FFIEC). FFIEC issued guidance for financial institutions, recommending financial institution conduct risk-based assessment, evaluating customer awareness programs, and developing security measures to reliably authenticate customers remotely accessing online financial services. Officially, recommending the use of authentication methods that depend on more than one factor specially, what a user, knows, has and is, to determine the users' identity (FFICE, 2011). In line with this, on August 15^{th,} 2011, the FFIEC also pushed supplemental guidelines which state that, by definition, "a true" multi-factor authentication system must use distinct instances of the three factors of authentication; it has defined and not just used distinct instances of a single factor. The updated guidance outlines for the minimum authentication security control necessary for online banking activities. It directs the financial institutions to formally access their existing authentication methods and implement more secure techniques and enhanced technologies. The update guidance state that, financial institution must use multifactor authentication and also employ multiple layers of authentication that is, they should use different security and access controls at different points in online banking. (FFIEC, 2012), which is in line with this study. The aim of this study is to develop a multi-factor authentication (MFA) model for effective information security in mobile banking system. Moreover, voice recognition and smart card was also suggested by (Deepa, 2014) for security authentication in the mobile banking platform system. This also proved ineffective because two citizens can have the same voice which may be sensitive to error. Again, it can be affected by certain illness or physical conditions. If this occurs, one can easily hack and fraud ones account**.** The review of previous studies suggested by other researchers was based on the use of SFA or 2FA authentication which has some shortcoming as emphasized above. None has focused on the use of MFA that involves three (3) tiers of authentications for security of information transaction in the banking system. This gap therefore has further strengthened the rational for the present study. Thus, the study, modeling Effective Information Security in the Mobile Banking System, involve the deployment of multi-factor authentication (MFA) as more reliable solution to improve authentication in the existing mobile banking system in Nigeria in securing information transactions. This multi-factor authentication will be implementing using the knowledge base factors (PIN, OTP), the possessive factor (Media access –IMEI) and inherence (finger-print) which is in line with the federal financial institution examination council (FFIEC)for effective security in the mobile banking system. Banking institutions are the key target of hackers and cyber criminals as more and more sensitive information transaction is being stored and manipulated online. And the security of this information or transaction needs to be assured. One of the major draw, backs in the existing mobile banking systems is the chronic problem of integrity engendered by the emerging internet fraud as a result of SFA and of 2FA mechanism in place.

2. Literature Review

Nduagu *et al*., (2019) developed a system named development of an enhanced mobile banking security: multifactor authentication approach using two android phones and pin. In this case,

mobile app will be installed in one android phone while the PIN and OTP transaction token to be generated by the users alternate number installed in another android phone. This type of authentication is not secure because the pin is prone to shoulder surfing or can gets into the hands of authorized user for fraudulent purposes in the mobile banking. The use of two android phones can be cumbersome for the mobile banking user. It is very expensive and also prone to deft by an authorize user. The multifactor authentication for bank using mobile phones proposed by the jayshri et al., (2021) using OTP (one time passwords) generated by the mobile phone for authentication purposes. Unlike the traditional method of generating and delivery of OTP for authentication through the web, the proposed system overcomes the problems with utilizing OTPs with SMS cost and delays, along with international roaming restrictions. The procedure also adopted hashing function of SH256 and MD5 encryption technique. The technique used cannot be termed as multifactor authentication. Rohit et al., (2016) proposed smart authentication system for android smart phone using only face recognition for authentication in the mobile banking system. In this case only face recognition cannot be termed multi-factor authentication and if the face is hacked the authentication will be breached. Security of multifactor authentication model to improve authentication system was developed by Tamara Mohamed (2014) using ear biometric for security. This biometric may have problem during the capturing process because not all the inner features of ear will be captured and this may result inaccuracy and may waste time during authentication process. Adeoye, (2012) carried out a study on mobile banking, infrastructure, and mobile banking trends. He used what the customer has (a digital device) and what they know (PIN) for authentication purposes in the mobile banking. He also showed that two-factor authentication is better than one-factor authentication; it also found out that the 2FA was porous. The study recommended customer education should be used to educate the users on skimming techniques and that banking providers should not offer cost against PIN credit and debit card losses. The study, however, failed to show that adding another layer of authentication will decrease the porosity of two-factor authentication. A biometric based mobile banking on android device was proposed by (Belkhede *et al.*, 2012). They proposed a system that captures the fingerprint of a client with the use of his / her smart phone camera. The solution involves the use of biometric authentication mechanism. a payment application would be installed onto an android device, for authentication finger print is taken at run time. The finger print template would be captured by the phone and compared against a stored template or a database server. The fingerprint template is encrypted by using the RSA algorithms and sends it to the host server (i.e., bank). Fingerprint is used for login purpose for the bank application on mobile (Belkhede *et al*., 2012) mobile device act as a client and the bank website act as a server (host server). Once finger print is taken as a login, it is sent to the server for matching as request, and server send reply message. If matched then login will be successful and user can do the transaction. In the client server module for providing the enhanced security authors use the encryption technique so the wireless transmission cannot be hacked to reveal the fingerprint template. This technique cannot be termed as multifactor authentication. A new secured Application mobile banking model for Nigeria was proposed by Faisal (2017) that utilizes three levels of authentication mechanism: such as (Bank Verification Number (BVN), mobile phone's Media Access Control (MAC) and biometric factor, fingerprints and finger vein multimodal biometric data) to enhance security in the mobile banking. Biometric Kerberos Authentication Protocol (BKAP) proposed by (Han *et al.*, 2013) was also adopted for authentication of biometric factor at the server. The voice recognition and smart card developed by Deeper (2014) for security authentication in online banking system. This is proved ineffective

because two citizens can have the same voice which may be sensitive to error. Again it can be affected by certain illness in physical conditions. If this occurs one can easily fraud ones account for fraudulent (Deeper, 2014). Finger print and GSM were proposed by Muhammad *et al*., (2015) for security authentication in online banking system. This authentication is worrisome because the user cannot be carrying out the finger scanning device with mobile device any time he or she wants to carry out transaction online. A biometric based mobile banking on android device was proposed by Bankhead *et al*. (2012). The finger template was capture by the smart phone. The finger print was used for login purpose in to the mobile banking application and not for an authentication. Sasidevi et al., (2015) developed application that run on a smart phone device and communicate with remote service providers such as one when a smart phone user needs to check his bank account or make some transactions remotely. One uses three authentication schemes: A user chosen two passwords (one is known to bank representative and the other are anonymous) and bank generated OTP. This approach is a two-factor authentication and does not explore the use of biometrics as well as it relies on what the user knows and not the other factors – what the user has or is**.** A biometric based mobile banking has been proposed by (Bilal *et al.*, 2011). Their proposal works thus: Registered users will directly go to login form while new users will go to registration form. They proposed scanner that utilizes radio frequency (RF) scanning. Their reason is that with RF scanning, it is possible to differentiate between living cells and dead or copied cells. After the verification of data, the customer will be able to access the database through web server. If the finger print matches with that of the database, then customer will be able to start mobile banking services through mobile handset. Cha *et al.*, (2015) proposed security enhancement of micro-payment systems with the user based knowledge based authentication and using a smart watch to have possession-based authentication. The study fails to show how that implementation can be done to increase the security of information in the mobile banking system. Biometric based mobile banking has been proposed by (Bilal *et al*., 2011). Their proposal work thus: Registered users will directly go to login form while new users will go to registration form. They proposed scanner that utilizes Radio Frequency (RF) scanning. Their reason is that with RF scanning, it is possible to differentiate between living cells and dead or copied cells. After the verification of data, the customer will be able to access the database through web server. If the finger print matches with that of the database then customer will be able to start mobile banking services through mobile handset. For additional security Lightweight Directory Access Protocol (LDAP) server is used. If first finger prints authentication is not found in database then it will be checked in LDAP server for more verification. New users are required to register any three finger print in database and also need to fill in a registration form. If the finger print of the bank customer is registered successfully then customer will be able to use mobile bank services. For secure authentication purposes they proposed finger print scanner device. Mobile manufacturing companies will make the biometric scanner device with mobile hand set. The mobile customer will used it for authentication purposes. After capturing finger print, the data will be transmitted through internet. And the data can be accessed through bank server. The finger print scanner device can be attached to mobile phone though a port. They narrated that the process which statistically gives the best possible template is called consolidation. Consolidation of three finger template produce high quality enrolled template according to Statistical Research, they reported. With the help of the finger scanner device, mobile handset gets three samples as shown in the figure. These samples are stored in bank server with appropriate account holder. In case of cut, burn, damage of one finger the other finger print data will still serve as a unique identifier they claimed. Finger print is present for matching in the

database record. Every time new finger print is compared to the stored finger print. For authentication purposes and to secure customer data at server end additional server known as Server LDAP authentication is used. In LDAP, the client sends the query packet through TCP/IP to the server. The server confirms the identifier on LDAP Directory Information Tree (DIT) which is stored on LDAP server. When the result is found, it is sent back to client. In case of result not found then query will be sent to another LDAP server. This LDAP verify the data in tree model structure method. They claimed that LDAP authentication has many advantages like centralized usage, privileges, management, and storage of user information and user accounts (Bilal *et al*., 2011). The Rohit *et al.*, (2016) proposes a Smart Authentication System for android Smart phones where he provide face recognition & detection for android mobile & android smart phones. He matched the persons face into mobile database stored face template of the person/user. If user face is not same or not matched with original face template then user gets email or location of unauthorized user. In this mail he get unauthorized people face image snapshot or his GPS location. Also he provides two services. In 1st service he can delete mobile private information from mobile and in the 2nd service the mobile tracker system. In mobile tracker system he can tracks the mobile phone, if the user loss his or her smart phones then he can track last location of mobile on Google map and last location seen through website.

3. ANALYSIS OF 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). The system enhances the current authentication system in the mobile banking system in Nigeria based on the combining of three factors of authentication; the knowledge, possessive, and the inherence factor (FFIEC, 2021). Specifically the proposed system classifying under three factors of authentication based on the FFIEC thus; the knowledge factor the use of (PIN, OTP), the possessive factor (IMEI of the device) and the inherence factor (finger print recognition) for security authentications depending on the amount to be accessed. That is, authentication using these factors depends on the amount of money to be transferred. The used of IMEI number of the mobile device which is more standard to uniquely identify the users' device, will also enhance security. The use of biometric fingerprint will add more security since it is unique feature to every individual which will be captured using device biometric feature incorporated on it. This expectation has been fulfilled in today's manufactures of smart phones like android phones which have powerful biometric features for security authentications. It will also use Android as a platform, which is the most popular mobile operating system for effective implementations. The PIN and OTP generated will be encrypted using AES-256 bit algorithm. The AES-256 bits algorithm that was used will make it difficult to hack by hackers. AES-256 bit algorithm that will be used also has the least encryption and decryption time. 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 the basic bio 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. Balance inquiry function send money
d. Help function
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(six digits number)and proceed;
9. You will be ask to provide and submit a valid means of identification, such as user names , NIN,BVN, voter'scard, password and setting PIN & finger for authentication .Ensure that the ID is clear before submitting. IMEI of the device will be automatically captured by the software at the backend.
10. The mobile banking application will prompt you to link your bank account for seamless fund transfers transactions and other financial services.

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 for login using email and password (6 digits number) on the mobile banking application platform.
b. 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, & Finger Print):

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.

f. Next the mobile client application using smart device biometric features will require the user to scan of his finger for authentication. The biometric scanning device that would be incorporated on the smart mobile device should utilize radio frequency (RF) of high resolution. The reason is that with RF scanning, it is possible to differentiate between living cells and dead or copied cells. (Faisal et al., 2017).

g. This will cross match with fingers template stored on the central database server of the bank, if it matches after the successful verification, the user will carry out transactions successfully or otherwise will start afresh or retry again.

3rd Tier: If transaction is greater than <#500,000 &above: Authenticate via (PIN, Finger printer& OTP):

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

h. 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.

i. Next the mobile client application smart-device incorporated with biometric features will require the user to scan of his or her finger print for authentication. If the finger print matches with stored template in the bank server database is correct.

j. Next the server will automatically generate 4 digit OTP (One Time Password) which is send to the user's registered user phone number and this will have a life span of 30 seconds to terminate. The user has to enter the valid OTP else the entire transaction will be terminated. If the user enters the OTP before the time line.

k. The transaction will be granted. Note the mobile application client, transmits the device IMEI (the IMEI of the primary SIM in case of a dual SIM phone), and phone number to the bank server for verification too, during authentication.

l. The OTP serves as a transaction confirmation number, which he/she must input to confirm the transaction. OTP is encrypted using an AES 256 bit-Encryption algorithm.

m. If the customer selects "Log-out" on the menu, the mobile application is closed automatically, signaling the end of operation.

The system used multiple factor authentication (MFA) options for payment transactions as have been described above. That is, authentication options depend on the amount of money to be transacted. Here OTP will be encrypted using AES-256 bit algorithm which makes it difficult for criminals to hack. Also, AES-256 has the least encryption and decryption time.

Additional Security in the System

a. The proposed system also integrated the development of a honey pot environment in the mobile banking system which served as a controlled environment for redirecting and monitoring attackers. That is for storing fake or intentionally vulnerable credentials and to detect and alert an unauthorized access attempts to the management.
b. The mobile media access control of the phone (MAC) address, IMEI is integrated for security of the mobile device and to ensure that only registered devices are allowed to complete a particular transaction.
c. Altogether, the proposed system developed will give a strong and effective security of information transaction in the mobile banking system unlike what is obtainable in the existing system. Below depicts the architectural high level model design of the proposed system.

MOBILE USER

Registration

Registration details correct?

YES

No

LOGIN REQUEST

Enter Email /password

TRANSACTION INTERFACE

Register Successfully

Fund Transfer

ENTER SELECT/AMOUNT

RECHARGE

AUTHENTICATION OPTIONS BASED ON THE AMOUNT

Balance Enquiry

1ST

2ND TIRE

3RD TIRE

ENTER PIN

ENTE R PIN

ENTER PIN

Pay Bills

Dstv/Got

Transaction History

OTP/ IMEI

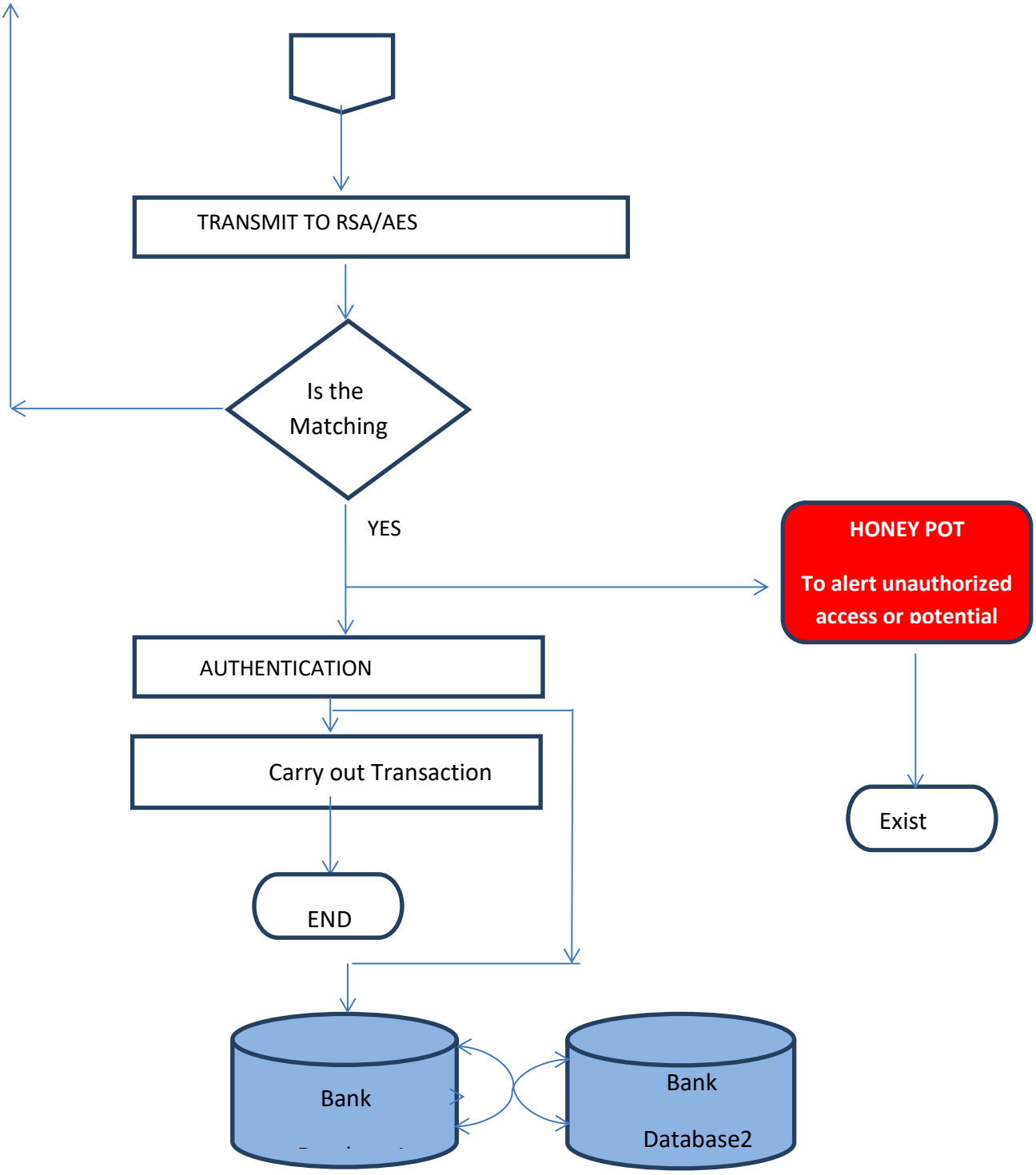

Figure 1 Architectural design of the System

Flowchart Au… …f the System Mobile Banking System

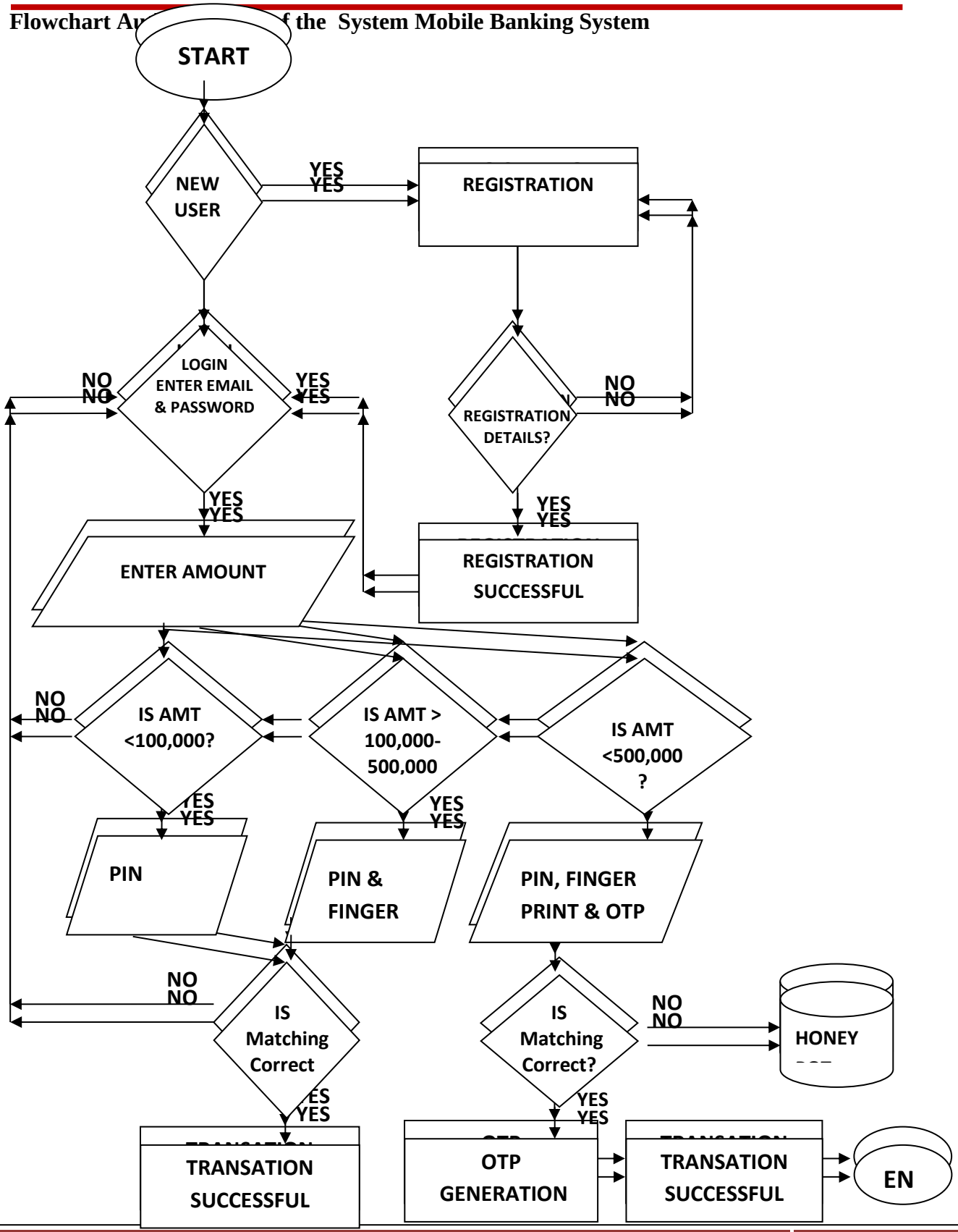

Figure 2: Flowchart diagram of Authentication in the System Mobile Banking System.

Summary

The use of SFA and 2FA for security of transaction in the existing mobile banking system has stood the test of time mainly because of its speed and memorability. Moreover, many banks accepted SFA because it is simple and user-friendly. These authentication mechanisms are no longer secure for effective security of information transaction because of its vulnerable to shoulder surfing attacks, brute force attacks, social engineering attacks, and impersonation attacks and phishing attack. The development of multifactor level security authentication in the proposed system for effective information security in the mobile banking system that have three (3) tiers of security authentication options in place; the use of (PIN), (PIN & Finger) and (PIN, Finger print & OTP) for access controls depending on the amount to be transacted would provide a robust security at different tier that will be difficult for Impersonation, shoulder surfing attacks, brute force attacks, social engineering attacks, and phishing attack. If hackers happened to breach the first level authentication unlike in the existing system it will be difficult for them to breach in the new system. Moreover, the integration of device IMEI in the new system for access control boosted the security of the device and breach unauthorized access in the banking system unlike what is not obtainable on the existing system. Moreover, the new system also used the RSA and AES to encrypt transaction information. The IMEI of the device, OTP generated and other user credentials are encrypted using AES-256 bits algorithm which makes it difficult to hack. Also, AES-256 has the least encryption and decryption time. The RSA-4096bits algorithm was used for card payment encryption. Furthermore, the integration of the honey pot environment in the proposed system also enhance security because it serves as a controlled environment for redirecting and monitoring attackers attempting to breach the real system. Their activities are documented for decision marking to the management. Thus, the proposed system altogether designed to be more secured as well as time efficient and can be implemented in real time. Also the proposed multilevel application ensures effective security that will be difficulty for unauthorized access to penetrate the banking transaction server thereby ensuring confidentiality and integrity of information transaction in the mobile banking system.

References

Greig et al., (2019) Andrews, Karen Renaud, and Stephen Flower day (2015).An ethnographic study to assess the enactment of information security culture in a retail store. World Congress on Internet Security (WorldCIS). IEEE, .chicago. Retrived, 12th Aug., 2020.

Danvas, M. and Ngugi, K. (2014): Determinants Influencing Adoption of Radio

Mcgladery, P. (2013). Information Security and Information Assurance: The Discussion about the Meaning, Scope and Goals. In: Organizational, Legal, and Technological Dimensions of Information System Administrator. Retrieved, 13th June, 2022.

Sahaji&S.Soman(2020).security improvement mobile banking using hybrid Authentication. Processing in of 3rd international conference in Artificial Intelligence . Istanbul, turkey , Retrieved, January ,2023.198-201.

Ferrage, M.A et al (2020) .Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues. 1-32 Retrieved, 12th August 2022

Jayshri, S.,Jagrutisonar, S.&Komal, S.(2021).Multifactor authentication for bank using mobile phones. *International research journal of engineering and technology (IRJET).* Retrived , 10th November,2022.

Santhi, B. and Kumar, K. (2012), Novel Hybrid Technology in ATM Security Using Biometrics. *Journal of Theoretical and Applied Information* Technology. Retrieved, Apirl 2012. Vol.37(2).217-221.

Chris, E.M. (2019) Atm Machine Security: Bank Atm Security Device . Http// www. Crime doctor .com/business htm. Retrieved, 15th October, 2022,2-4.

Rajalakshmi,P. sangeetha,R.vanathi, b. shanmugam, K . , Sindhya S.(2019). *International Journal of Engineering Development and Research (IJEDR*) chennai, india(www.ijedr.org) Retrieved, 29th March, 2023.1-9

Sahaji&S.Soman(2020).security improvement mobile banking using hybrid Authentication. Processing in of 3rd international conference in Artificial Intelligence . Istanbul, turkey , Retrieved, January ,2023.198-201.

Mohamed, Tamara .S. (2014) Security of Multifactor Authentication Model to Improve Authentication Systems Information and Knowledge Management Vol 4 No 6. Retrieved, 13th June, 2022

Guma,A. M,A.&Anael, E.S.(2020).Two factor authentication scheme for mobile money review of threat models and countermeasures. Future internet.www.mdpi./com/journal/furture internet. Retrieved ,12th Septermeer,20231-3

Rahav,A.(2018).The secret security wiki.(http://doulbleoctopus.com/security-wiki/authentication/single-factor-authentication. Retrieved ,6th November ,2022.1-3

Rahav,(2018) (A. The Secret Security Wiki: https://doubleoctopus.com/security-wiki/ *authentication/single-factor-authentication/* .Retrieved on 4 February 2023.

Deepa, Malviya (2014).Face Recognition Technique: Enhanced Safety Approach for ATM .*International Journal of Scientific and Research Publications,* Vol. 4, no. 12, www.ijsrp.org. Retrieved, April 4th, 2022 ,. 1-4.

Ndunagu J.N. et al.,(2019). Development of mobile banking security: Multifactor Authentication Approach. J*ournal of electrical and telecommunication system research* Retrieved 10, Sept., 2022.

Jayshri, S.,Jagrutisonar, S.&Komal, S.(2021).Multifactor authentication for bank using mobile phones. *International research journal of engineering and technology (IRJET)*. Retrived , 10th November,2022.

RohitNarkede et al (2016). International conference on research entertainment and advancements in technology and engineering http://www.ijerom.org. Retrieved, January 8th, 2024.1-5.

Mohamed, Tamara .S. (2014) Security of Multifactor Authentication Model to Improve Authentication Systems. *Journal of Information and Knowledge Management.* Vol 4 , 6. *www.ijste.org.*Retrieved, 4th August, 2022.81.

Adeoye, O. S. (2012). Evaluating the performance of two-factor authentication solution in the banking sector. *International Journal of Computer Science Issues*, 9(4), 457–462.

Mo hammad, B.L. Alhassan M.E. and Ganiyu, S.O. (2015). An Enhanced Atm Security System Using Second-Level Authentication**.** *International Journal of Computer Applications.* Vol.111(5)Retrieved February 2015.1-6.

Sasidevi, J., Sugumar, R., &Priya, P. S. (2015). New-Multi-Phase Distribution Network Intrusion Detection, 5(3), 1277–1280.

Bilal, M., &Sankar, G. (2011). Trust & Security Issues in Mobile Banking and it's Effect on Customers. Karlskroma: Blekinge Institute of Technology.16- 20 .

Cha, B., Lee, S., Park, S., &Ji, G. L. Y. (2015). Design of Micro-payment to Strengthen Security by 2 Factor Authentication with Mobile & Wearable Devices, 109, 28–32

RohitNarkede et al (2016). International conference on research entertainment and advancements in technology and engineering http://www.ijerom.org. Retrieved, January 8th, 2024.1-5.