Plastic Financial Fraud In The Most Populated Black Africa; Nigeria:The Mitigation Based-On One-Time Password

WAZIRI VICTOR ONOMZA
School of Information and Communications Technology
Cyber Security Science Department
School of Information and Communications Technology
Federal University of Technology,
Minna, Niger State, Nigeria

JOHN ALHASSAN
School of Information and Communications Technology
Cyber Security Science Department
School of Information and Communications Technology
Federal University of Technology,
Minna, Niger State, Nigeria

IDRIS ISMAILA
School of Information and Communications Technology
Cyber Security Science Department
School of Information and Communications Technology
Federal University of Technology,
Minna, Niger State, Nigeria

ABDULRAHMAN TUNDE
School of Information and Communications Technology
Cyber Security Science Department
School of Information and Communications Technology
Federal University of Technology,
Minna, Niger State, Nigeria

Abstract : **The increase in the use of plastic payment cards in developing nations would surely lead to more Plastic fraud, Thus, there is a there is a need to develop modern more secure systems that could be used to enhance the security of the inherent plastic cards being used today. This project proposes a system that uses the One-Time Password technology to prevent plastic fraud. The project aims at the risk associated with the current use of plastic card increases. The design and the implementation of the One-Time Password serves as an additional means of authentication to the already in use static PIN. The project also provides recommendation to both banks and customers in other to make the use of plastic payment card more secure, as these cards will become more common with introduction of the cashless economy policy by the Central Bank of Nigeria.**

Keywords: **FinancialFraud, Plastic Card, ONE-TME Password, authentication, Cashless Economy**

INTRODUCTION

The invention and rapid usage of the Internet has led to the emergence of Internet Banking and other online related services that ranges from Instant Messaging, Electronic Mails, to Cloud Computing and other advantages of the Internet.

With all these advantages, the Internet also comes with disadvantages with the major one being “Cyber Crime” or “Internet Crime”. Cyber Crime can be defined as illegal activities that are being carried out on the Internet or on the Cyber Space by exploiting certain loopholes or vulnerabilities on the target system. (Internet crime complaint center (IC3) report 2009)

The emergence of the Internet Banking leads to the Introduction of Plastic payment cards that provide a suitable and secure medium which people conduct a variety of financial transactions. This lessen the burden of carrying a lot of money by individuals, and therefore, the risks of being attacked by armed robbers. It also solves the problem of money laundering.

With the calling for the embracement of the cashless economy by the Central Bank of Nigeria (CBN), the use of Plastic Cards have risen in about two years to 200,000Point of Sales terminal (POS) distributed and more are being surging, aiding the already Automated Machine which are already in used in the country (DailyIndependent News. 2012).

But with this exciting innovation, it has also lead to new crime opportunities called “Plastic Frauds”. Plastic fraud is defined as the use of plastic payment cards such as Debit Card, Credit Card or Master Card information to perform a transaction without the knowledge or the permission of the Owner, or the issuer (Moon et al, 2010). In a more elaborate eloquent, the plastic cards are stolen or acquired by duress through robbery siphon money from the victim’s account.

Criminals have in abundance, effective innovations and adaptive approaches to plastic fraud; thereby, making it hard to curb by the law enforcement agencies. Hence, it has become very important for Financial Institutions to provide ameliorations and proactive methodsto mitigate plastic fraud to the minimal level; as such crimes cannot be wholly eliminated in a very most populated Black Country, Nigeria.

Statistics shows that banks suffered from fraud and forgeries by losing N21.29 billion, with ATM remaining the commonest type. One hundred and sixteen (116) ATM-related cases valued at N17.2

million were reported in the first half of 2011, compared with four hundred and eleven(411)cases amounting to N82.2 million recorded in the second half of 2010. The lost amount to forgeries in 2010 was the lowest since 2008 when the industry reported N53.522 billion loss, representing a 60.22 per cent drop. Also, the number of fraud cases reduced by 13.15 per cent from one thousand, seven hundred and sixty four(1,764) to previous year's one thousand five hundred and thirty two (1,532), just as the report noted that those with very low probability of recovery were minimal(Nigeria Deposit Insurance Corporation (NDIC) annual report in 2012).But Plastic fraud is believed to have risen by almost 60% towards the end of the year 2013, but the fact could not be established as Nigerian Banks now underreport and hide incident of forgeries and frauds whenever they occur to appropriate authorities. Some of these reports are later found out accidentally long after they occurred or later when the truth about the underreported incidents are later been found out, or from customers that complain or social media or through other forms (Nigeria Deposit Insurance Corporation (NDIC) annual report in 2012).

The Banks feared reporting the incidents because they believe revealing this fact will lead to their losing customers as Nigerians are known to always become panic when information like these are revealed. This tendency phenomenon of withdrawal is a general norm all over world for customers to withdraw their resources from perceived lack of security by the commercial institutions.This, notwithstanding, the crime must be controlled, and that is why the banks must adopt preventive and proactive measures with proficient countermeasures incombating the crimeby employing various security technological toolsin this undesirable battle.

1.1One Time Password (OTP)

(A one-time password (OTP) is a password that isvalid for only one login session or transaction.OTPs avoid a number of shortcomings that areassociated with the traditional (static) passwords. Themost important shortcoming that is addressed byOTPs is that, in contrast to static passwords, theyare not vulnerable to replay attacks. This meansthat a potential intruder who manages to record anOTP that was already used to log into a service orto conduct a transaction will not be able to abuseit, since it will be no longer be validated. On the downside,OTPs are difficult for human beings to memorize.Therefore they require additional technology to work(en.wikipedia.org/wiki/one-time_password)

OTP can be generated by random algorithms typically whichproducepseudo-random numbers within polynomial time. This process makes the OTPs algorithms more hard and secure within provable security probabilistic polynomial time (PPT) This becomesnecessary; otherwise, it would be easy topredict future OTPs by observing previous ones.Concrete OTP algorithms vary greatly in theirdetails. Various approaches for the generation ofOTPs are listed below:

Based on **time-synchronization** between theauthentication server and the client providing thepassword (OTPs are valid only for a momentarilyperiodof time) but can be broken by theoretically PPT.

Using a mathematical algorithm to generate anew password based on the previous password (OTPs are effectively a chain and must be used in apredefined order).Using a mathematical algorithm where the newpassword is based on a challenge (e.g., a randomnumber chosen by the authentication server ortransaction details) and/or a counter.

(There are also different ways to make the useraware of the next OTP to use. Some systems use special electronic security tokens that the usercarries and that generate OTPs and show themusing a small display. Other systems consist ofsoftware that runs on the user's mobile phone. Yetother systems generate OTPs on the server-sideand send them to the user using an out-of-bandchannel such as SMS messaging. Finally, in somesystems, OTPs are printed on paper that the user isrequired to carry the initialization process) (en.wikipedia.org/wiki/One-time_password).

1.2 Motivation

With the increase in fraud cybercrimes globally(Nigeria being a particular case in our approach) which are targeted against the banks in the countries, there has been a rising need for this crime to be combated in order toameliorate the rate of cybercrime in the country. One of the major challenges facing the financial institutions in this country is identity theft which mostly leads to plastic fraud

With these and other unreported crimes, we are motivated by this paper write up to work on the Prevention of Plastic fraud as it can go a long way in securing the economic and political stability future of the country and also to enlighten the general public on how to use Plastic Cards more securely.

In this wise,the paper designs design a simulating system for preventing plastic fraud in the financial institutions in Nigeria or elsewhere.

RELATED WORKS

This paper reviews some major frauds incidences around the globe based plastic cards.

Plastic fraud is defined as the use of plastic payment cards such as Debit Card, Credit Card or ATM (VISA) Card information to perform a transaction and or withdraw money without the knowledge or the permission of the Owner, or the issuer. (Moon et al, ibid).

To prevent Plastic Payment Card Fraud, attention must be paid to different areas and these include the technical and non-technical methods that can be adopted. Varieties of researches have been conducted in the field of detection and prevention of Plastic Payment Card Fraud. Other security techniques have been proposed to preventing Plastic Fraud; also the One Time Password Technology has been implemented on other areas to ensure security in various organizations. One-Time pad has played the central roles in military dissemination of information to forestall enemies eavesdropping, most especially during the Second World War (War II).One-Time Pad plays the central of the symmetric keys that Shannon Claude proved to perfectly secure. One-Time Pad is the only Provably Secure Key use in Symmetric encryption.

Wada and Odulaja, (2012**)** carried out a study on Nigeria plastic cards and their study revealed that (E-banking is still at its infant level with most of the banks having mainly information sites and providing little Internet transactional services. However, most studies in these areas revealed that there has been a very steady move away from cash as transactions are now being automated.Crime and corruption represent a major concern for business executives not only in Nigeria but also in other parts of Africa. In Nigeria, the most serious problem to economic activities and business are financial crimes and corruption in higher officesthat averages to 75% and 71% respectively)(Business Survey on Crime & Corruption and Awareness of EFCC in Nigeria, Summary Report, 2009-2010).

By definition; cybercrime may be referred to as any form of misconduct in cyber space. It is simply defined as the criminal use of the Internet. Cybercrime is believed to have started in the 1960’s in the form of hacking.This was followed by privacy violations, telephone tapping, trespassing and distribution of illegal materials in the 1970s. The 1980s witnessed the introduction of viruses. The fast pace of development of ICT from the 1990s till today has added to the list of criminal exploits in cyber space. Today, the Internet is used for espionage and as a medium to commit terrorism and transnational crimes). (Olasunkanmi.O. 2010).

With (E-banking gaining ground in Nigeria and other parts of Sub-Sahara Africa, customers and online buyers are facing great risk of unknowingly passing on their information to fraudsters. "Hackers” get information of those who have made purchases through websites and then make fake cards, which they use with less detection. Absence of a law specifically dealing with card-related crimes in Nigeria may be giving malicious individuals a loophole to operate freely without being apprehended.

Finally, the authors provided positive insights into how cybercrime impacts on E-banking from a Nigerian perspective using social theories to explain causation with a view to guiding policy makers on behavioral issues that should be considered when formulating policies to address cyber-criminal activities in Nigeria.(Wada and Odulaja).

(Ehimen and Bola 2009)defined(computer crime as “any criminal activities involving an information technology infrastructure: including illegal access or unauthorized access, illegal interception that involves technical means of non-public transmissions of computer data to, from or within a computer system; data interference that include unauthorized damaging, deletion, deterioration, alteration or suppression of computer data; systems interference that is interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data; misuse of devices, forgery (ID theft), and electronic fraud))”.

The authors categorized(cybercrime in Nigeria into two, Crimes that target computer network or devices directly and Crimes facilitated by computer network.)

(ibid, 2009) conducted an investigation and review criminal laws in Nigeria. They further investigated cybercrime and it’s socio-economic consequences and the damages on the image of Nigeria, they analyzed the activities of internet fraudsters also known as “Yahoo Yahoo boys” in Nigeria who uses false pretense to extort money from unsuspected victims with males transmuting to the female gender in reverent love but abstractive affairs. The authorsfurther highlighted the point that (as the time of writing the paper) there is no specific law in the country to combat cybercrime, which makes the country a safe haven for the criminal to operate freely. Nonetheless, this crime-free law just observed is no longer in existence as the Nigeria National Assembly has constituted laws that reflect various castigatory terms recently.

In another research development, Bhasin(2007)identified that businesses are subjected to crime with the advent of computers especially the internet. He noted that cybercriminal uses information technological tools to perpetrate the crimes.Furthermore, he highlighted that the banking sector comprises of both public and private sector and also foreign banks not to forget small or regional and co-operative banks. All these banks use various Information Technology resources e.g. ATM, phone banking etc. with these cybercrime present a high risk to the financial institutions.He further discussed the commonly high-tech crimes perpetrated against banks as he outlined Phishing, Identity Theft, Worms and Trojan horses, Spyware, Internet search engines, Blackmail and Denial of Service (DOS) or Distributed Denial of Service.)

He further explained Phishing as (masquerading an illegitimate website to make it look like the website the victim is banking with to collect or steal customer details. He identify Identity Theft as another major problem which is also related to phishing giving the definition as “Manipulating or improper accessing another person’s identity information” in other to fraudulently establish a claim over the account benefit.)

According to the author,(Worms and Trojan are significant threats to banks, he defines worms as “a program (or algorithm) that replicates itself over a computer network and usually performs a malicious action, such as using up the computer’s resources and possibly shutting the system down”. He relates the activities of worm to that of a computer virus, but Trojan on the other end doesn’t replicate but can be destructive also, Trojan conceal virus and also spywares like key logger.)

The author describes spyware as “Any software that covertly gathers user information through the user’s Internet connection without his or her knowledge, usually for advertising purposes” and they range from harmless pop-up to ability to record any activity on a computer and transmit it remotely to the hacker.

Internet search engines such as Google can be used to pull out sensitive information out a website e.g. credit card details, admin login pages etc.

Finally, he talked about the risk of (Denial of service attack against online banking, Denial of service does harm by bringing down computer or the network. Distributed Denial of service occurs when the attack is launched simultaneously with various innocent client computers against a computer system or network.He emphasized that there is no other option banks can do to curb cybercrime than to be proactive; more than thirty (30) percent of successful hacks are committed by employees or in-house worker.)

He recommended that the first line of defense should start with senior management not the Information Technology because implement policies would not be a cure at all. Then categorized a comprehensive approach to physical, technical and administrative security control as follows; preventive, detective, determent, recovery.

The author identified Risk assessment as to direct the rest of action and lead to effectiveness if properly carried out, implement prevention techniques, policies and tool. Also have a sound business recovery plan in policies and procedures in case of successful attack.

And lastly he also recommended that banks should develop incident response plan as part of policies then educate employees through training and seminars. Lastly bank should use specific Information Technology system to countermeasure and help mitigate crimes e.g. Fraud Detection System.

Ayofe, and Oluwaseyifunmitan(2009) in their paper titled “Towards Ameliorating Cybercrime and Cyber Security” The methodology employed by the authors in performing the research was collection of data which include the use of questionnaire, personal interviews, Observation and so on. They analyzed the gathered information and make some recommendation towards making the cyberspace a safer place.

The authors describe (cybercrime as wreaking havoc on computer data or networks through interception, or destruction of such data. It also involves committing crime with the use of computer system or against them. They categorized cybercrime into three; Cybercrime against person/individual, Cybercrime against property and Cybercrime against government.

They outline the causes of these crimes which include the sake of been recognized, another reason is the zeal to make quick money by the hacker and also using cybercrime to fight for a cause in which the hacker believes in.)

They suggest (cybercrime can be eradicated by first identifying the challenges of already existing system; they suggest investment in education and harmonization of international cooperation and law and encourage coordination and cooperation between national law enforcement agencies.)

The authors further identify the type of people who are involved in cybercrime as Idealist who are young people between the ages of 13-21 and their motivation is just to be in the spotlight of the media.

The other type of people involve in cybercrime are the Greed Motivated hackers, who are very dangerous because they are ready to commit any crime so far it will mean making money; and the last set as the Cyber terrorist, the most dangerous and their aim is not just money but to stand for what they believe is just. Their main target is mainly government.

They concluded by alerting that cybercrime and cyber security must be a great concern to all government in the world and countries who neglect or fail to tackle it swiftly will suffer great consequences.

Adeoti J.O, (2011)in his paper entitled “Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out” emphasize the objectives of the paper as to (scrutinize various ATM frauds in the country and to provide solutions to mitigate the fraud in the banking industry, the methodology that is been used to carry out the research was sampling 5 banks randomly from the 25 banks. The sampled banks are First Bank, UBA, Union Bank, Guarantee Trust Bank, and Zenith Bank. Questionnaires were distributed to 50 customers per sampled banks in Ilorin Kwara State. A Scale of 5-points was used to measure the level of agreement or disagreement by the respondents. Frequency distribution was used to analyze the data collected and examined the pattern of response to each variable under investigation the study seeks to investigate the dimensions of ATM frauds in Nigeria, the frequency counts and percentages were used to capture the responses of the respondents. From the above gender distribution of respondents, 52% of the respondents were males, while 48% were females. From the respondents' age classification, 40.8% of the respondents were within the age bracket of 31-40 years while 31.2% of the respondents were within the age bracket of 41-50 years. In other words 72% of the respondents were youths whose ages range between 31 and 50 years. This is an indication of the level of literacy of the respondents. 56% of the respondents were married, 28% were single and 10% and 6% were divorcee and widows / widowers respectively. Students, civil servants and self-employed business men and women fall into the categories of the singles and the married which constitutes about 84%. The level of education of the customer in all the 5 sampled banks are as follows: 46% of the sampled customers have tertiary education, 36% have secondary education while 10% had primary education. 8% of the sampled customers were illiterate three dimensions featured prominently in thelevel of agreement and disagreement on dimensions of ATM frauds in banks. The three prominent dimensions are ranked in the Dimensions that are 20% and above are card jamming, shoulder surfing and stolen ATM cards. The three constitute about 65.2% of ATMs fraud cases in Nigeria, 80 respondents (32%) favored video surveillance as a method of checkmating the ATM frauds, 50 respondents (20%) supported setting withdrawal limit while 40 respondents amounting to 16% supported remote monitoring. 14% of the respondents believed that customers' awareness is very central to checkmating ATM frauds. Many customers have received text messages from hackers asking them to send their pin codes. He concluded by noting that every nation has a peculiar ATM fraud that is common to it. The e-banking has great possibilities but that would be dependent on the extent to which the ATM frauds are controlled. There are many other products that are ATM related that have been developed in developed countries. For such products to have a hold in Nigeria, the ATM fraud-related problems must be solved. Such products are electronic fund transfer at the point of sale and electronic card products. Recommendations were made to both banks and customers to curb this crime.)

Jenifer R.S (2012) in his paper entitled “A Five Way Fuzzy Authentication for secured banking” proposed to combine the use of Pin Number along Keypad ID, RFID Tag, Fingerprint. Image, One Time Password generated to users phone. and another One Time Password given by the user to the server for authentication to secure Banking, this was related to the security issues associated with the existing three factor authentication protocols, which makes use of the RFID, Pin number and Biometrics. This proposed system makes use of RFID, Radio Frequency Identification which is a wireless non-contact radio system to transfer data from a tag attached to an object for the purpose of automatic tracking, it makes use of a five factor authentication which includes the OTP and keypad ID as additional authentication factor. It makes use of fingerprint recognition technologies to analyze global pattern schemata on the fingerprint along with small unique marks, (minutiae). The system works : the client insert card into a card reader, then input the pin and his/her fingerprint, if the inputted pin and fingerprint matches the transaction is allowed, if the pin doesn't match, the client cannot proceed, if only the pin matches and the fingerprint didn't not match up to 60% the fuzzy logic will be applied and the system will generate an OTP automatically and sent to the real user's mobile number using RSA algorithm, the generated OTP is then inputted by the user with the keypad I'd, if it matches perfectly transaction is allowed, else rejectedelse rejected

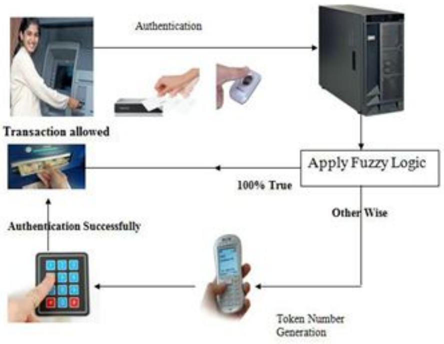


Fig 2.1 Login-Authentication Overview of the proposed system

The analysis shows that the work satisfies all security requirements on five factor authentication and has several other practice-friendly features.

In a recent observation byFadiAloul, Et al. (2012) in their paper entitled " two factor Authentication Using Mobile Phones" examined the problem associated with static password, as user tends to write them down on paper or store them, some users uses the same password for multiple accounts and some password are easy to guess, in addition to hackers techniques to steal password like, sniffing, snooping, dictionary attack, etc. They therefore proposed the use of two factor authentication which is a mechanism which uses a mobile based software token system that will supposedly replace the existing hardware and computer based software tokens, the proposed system according to them is secure and it's make up of 3 parts: software installed on client's phone, a server software and a GSM modem connected to the computer. The system works on two (2) mode of operation which is the “Connectionless Authentication System’ which generates a One Time Password without connecting to the client server. The mobile phone acts as a token and uses certain unique factor to generate the OTP locally. The client may use the password online or on ATM, the Second Mode which is the “SMS Based Authentication” works in case of failure in the first mode or the password is rejected, in this mode the mobile phone request for the OTP from the server by sending via SMS, a unique information to the client and the server verifies this message content, if correct it generate the OTP and sends it back to the originating phone number, with a time limit, all this messages are subjected to charges. In generating the OTP, the algorithm makes use of the IMEI number of the phone, the phone number, the Pin and the timestamp all concatenated and hashing the result with SHA-256 which returns a 256bits message. It's then XOR-ed with 256character, with a Base64 encoded that yields a 28 character password. They have design for the client, database and server for implementation and when tested with different method, they got 100% accuracy in the randomly generated number.

For Padmapriya and Prakasam(2013) in their paper entitled "Enhancing ATM security using fingerprint and GSM Technology", they highlighted that there wasthe need to improve security in ATM transactions due to the increase in criminal activities. They proposed a system which will add to the already existing method of using PIN as a fingerprint enrollment, and a GSM technology connected to the microcontroller which sends a 4 digit code to the user.

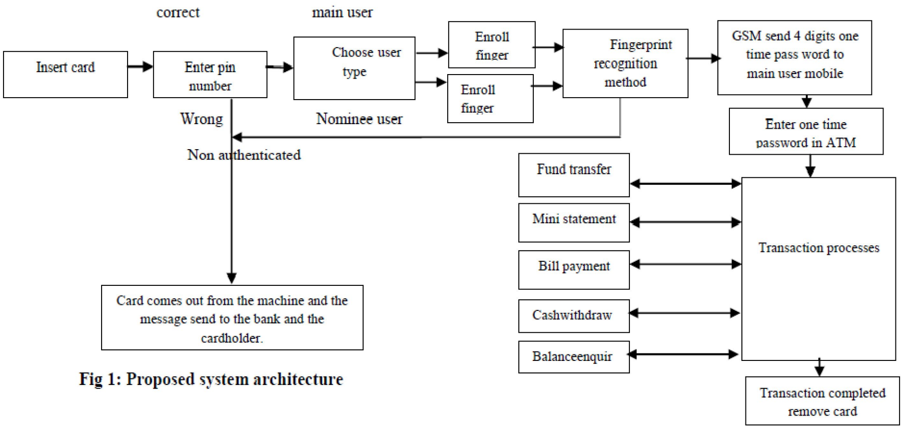

correct
main user
Insert card
Enter pin number
Choose user type
Enroll finger
Enroll finger
Fingerprint recognition method
GSM send 4 digits one time pass word to main user mobile
Wrong
Nominee user
Non authenticated
Enter one time password in ATM
Fund transfer
Mini statement
Bill payment
Cashwithdraw
Balanceenquir
Transaction processes
Card comes out from the machine and the message send to the bank and the cardholder.
Transaction completed remove card

Fig 1: Proposed system architecture

Fig 2.2 depicted an architectureof the proposed system

The system consisted of three validation functions, it first validates the pin number then the fingerprint, before the sending the 4 digit GSM modem to the phone number of the user. They did a survey collecting data on the effectiveness of the system with the result being recorded at twenty (20) people reported it has normal, fifty (50) people reported it good and seventy five (75) people reported it as the best. This survey was carried out amongthirty five (35) professors, twenty five (25) students, thirty five (35) bank employees and twenty five (25) government workers.

PROPOSAL DESIGN

With all the advantages of terminals, yet it comes with disadvantages in form of Plastic Fraud. Plastic fraud as defined earlier is the use of plastic payment cards such as Debit Card, Credit Card or ATM Card information to perform a transaction without the knowledge or the permission of the Owner, or the issuer. (Moon, et al,ibid).

In perspective of the above definition, plastic card fraud can be carried out only when the fraudster is able to acquire and/or use the card’s information and the PIN.

Plastic Fraud can be developed by many techniques, some of these techniques are:

i) Skimming: Skimming is a form of magnetic stripe counterfeiting where the fraudster is able to make a copy of the magnetic stripe track information (including Card Verification Value - CVV) from a valid card. Then this information can be embedded in a Counterfeit Plastic Card

ii) Use of Counterfeiting Plastic Card: This is when the fraudster reproduced a plastic card illegally by replicating and altering the magnetic stripes and changes the details on the face of the card thus using it to defraud.

iii) Spyware: is a type of malware that is installed on computers and collects little bits information at a time about users without their knowledge. This that collects the user's keystrokes as they are been typed and send remotely to the Criminal. Fraudster can use this to steal PIN of a card.

iv) Phishing: Refers to sending fake emails or instant messages to bank users asking them to provide sensitive information like PIN or Passwords. This is an online scam as the messages appears to have been from their banks or card issuer containing fake login pages, or fake links requiring them to provide sensitive information. Fraudsters also use this to steal information from cardholders.

v) Lebanese Loop: The fraudster inserts a device to the card slot of the ATM and when the cardholder inserts his/her card, the cardholder is tricked into inputting his/her pin with the fraudster watching, when the cardholder gets frustrated and eventually leaves, the fraudster removes the card and uses it with the pin to commit fraud.

vi) Shoulder Surfing: The fraudster stays very close to the cardholder and peeps through his/her shoulder and watches as the user input the pin, then later find use a technique to steal the card, either by pick-pocketing or hand-swap it.

3.2 Methodology

Our proposed feature for the security and enhancing the authentication of Plastic Payment Cardusage for the transactions in the financial institutions would be designed using the Java programming language with a front end interface backed with an SQL-server using the client/server architecture. The SQL server collects and saves information of customers and other information required for transaction to be completed.

An efficient algorithm will be developed to generate the one time password and a bulk Short Service Message (SMS) provider will be subscribed to, for the delivering of the One Time Password to the mobile number of the User.

There would be a link between the customer's identification and authentication information, customer's accounts and the records in the bank server. The system will be designed in a way to support a large number of users and it uses dedicated server to achieve this.

For the One Time Password (OTP) generator, a 6 digits random numbers will be used, which will be generated by an efficient algorithm and it will be sent over the network as an SMS to the bank user's phone who then input it to complete the authentication which would have been initiated earlier with the use of the previous authenticating mechanism for the existing system.

Client/Server model was chosen because for this application it provides sufficient security for the resources needed for an important application. Random number was chosen because it will be almost impossible for a fraudster to guess or crack the number as it has been generated randomly, it's only the customer that have access to his/her mobile phone which has been registered with the bank that will be able to view the number and input it to complete authentication.

The OTP code will be generated based on the 'Challenge-based OTPs" because it is a special case and also oftenuse a hardware device. However, the user must possess a Plastic Payment Card which contains certain information (Card number, Customer Details etc.), the user must also provide a known value, which is a personal identification number (PIN), to prompt the OTP to begenerated.

All the communications shall take place over a secure channel, e.g.,Secure Socket Layer/Transport Layer Security (SSL/TLS). And the keys will securely be stored in the validation system with it been encrypted, and exposing them only when required

3.3 Algorithm and Architecture of the System

The software is designed solely to use a two factor authentication, to solve the problem caused by static pin used conventionally for ATM and POS transactions. To the already in place authentication mechanism that makes use of the card information on the magnetic stripe and the pin provided by the user, the software adds the One Time Password which is a temporary password as an additional authentication mechanism.

In Figure 3.1, the architecture of the software shows when a customer wants to perform a transaction, after inserting the card and inputting the PIN, the system generates the OTP and sends to the registered number of the customer, the customer then input the OTP before authentication can finally be completed and the user will carry out the normal transaction

The algorithm of the software is represented by a Pseudo-code and a Flowchart (In figure 3.3)

Pseudo-code is a method employed in expressing an algorithm in an English text format without using the syntax of any programming language and therefore, it is not executable on a real system. It is the easiest way of writing an algorithm and relatively less complex. A pseudo-code is self-explanatory. The pseudo-code of the proposed system is written below:

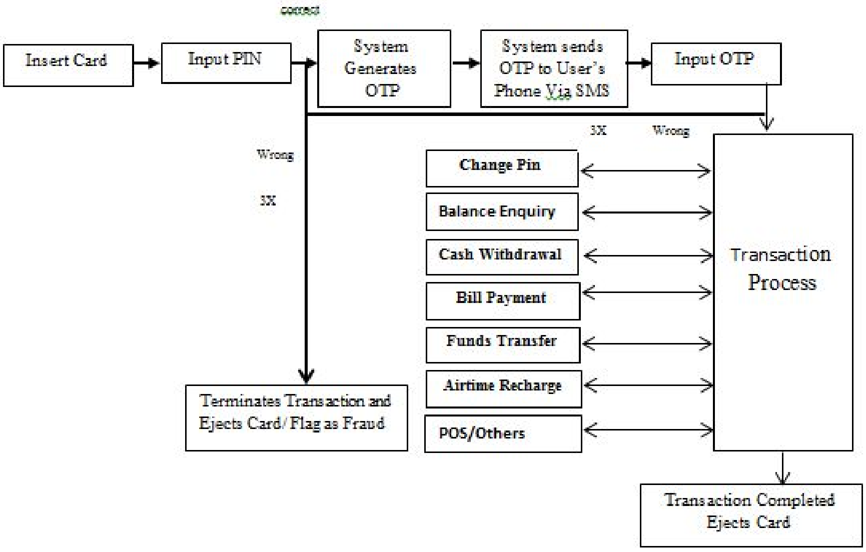


Fig 3.1 Architecture of the Proposed System

The Algorithm (Pseudo-code) for the proposed system:

```
Start
    Step 1: Insert the card/Swipe card
    Step 2: Terminal Prompt for Pin
    Step 3: Input card's pin. If Pin is correct,skip to step -5. If pin is false after 3 trials,
        Go to the next step
    Step 4: Terminate transaction and Ejects the card.
    Step 5: System Generates OTP, and sends it to the user.
    Step 6: Terminal Prompt for OTP
    Step 7: Input OTP, if Correct skip to step 9. If OTP is wrong after 3 trials, proceed to
        the next step
    Step 8: Flag as fraudulent, Terminate transaction and Eject the card
    Step 9: Select Account Type.
    Step 10: Select Transaction Type
    Step 11: If transaction ≤ Balance, Complete Transaction, Else Display "Insufficient
        Fund" and Repeat step
    Step 12: Prompt for another Transaction, if yes, go to step 9, Else Proceed to next step
    Step 13: Display transaction completed and Eject Card
End
```

3.3.2 Algorithm for Generating the One Time Password.

To make the system secure, the generated One Time Password must be very complex (hard) to guess, trace, or salvage by fraudsters. It is therefore, very important to come up with a secure algorithm for generating the One Time Password. Quite a lot of factors can be used by the One Time Password algorithm to generate a hard-to-guess password.The proposed system design uses the following factors for generating the 6 digits random number as the One Time Password:

i. **Plastic Payment Card number:** On every Plastic Payment Card there is a unique Identity in form of numbers which include the card number and Card Verification Value (CVV) number allowing each user to be identified by his/hercard.

ii. **PIN:** This is required to verify that no one other than the user is using the card to perform the transaction thus prompting the generation of the One Time Password.

iii. **Time-Stamp:** The system uses the Hour Minute Seconds and the date that the transaction takes place to generate the OTP. This timestamp is always unique and makes guessing the OTP code extremely difficult.\

The above factors are concatenated and the result is hashed using SHA-1 encryption algorithm which returns a 16 bit message. The message is then XOR-ed with generated random values replicated to 16 characters. The result is then Base8 encoded which yields a 6 character message which is used as OTP

Practical Example: giving that all the three (3) factors has been concatenated and the 16 bit output is: 1010011101110111, and the 16 bit equivalent of the generated random value is: 0011011011001011. Then it is XOR-ed:

$$xor\ \begin{array}{l}1010011101110111\\ \underline{0011011011oo1o11}\\ 0010011001000011\end{array}$$

3.3.4 Component of the System.

The One Time Password (OTP) Fraud prevention system consists of the following component:

i) **Insert/Swipe Card**: When the customer inserts or swipes it card as the case maybe, this component reads the information on the card, and also read the PIN of the customer which it further use to generate the One Time Password (OTP).

ii) **SQL-Server:** This stores the information of the customer, such as Name, Phone Number, Account Balance and other necessary data that is required to complete a transaction.

iii) **One Time Password (OTP) Generator:** This is the component of the system that generates the numbers before sending them to the registered phone number of the customer.

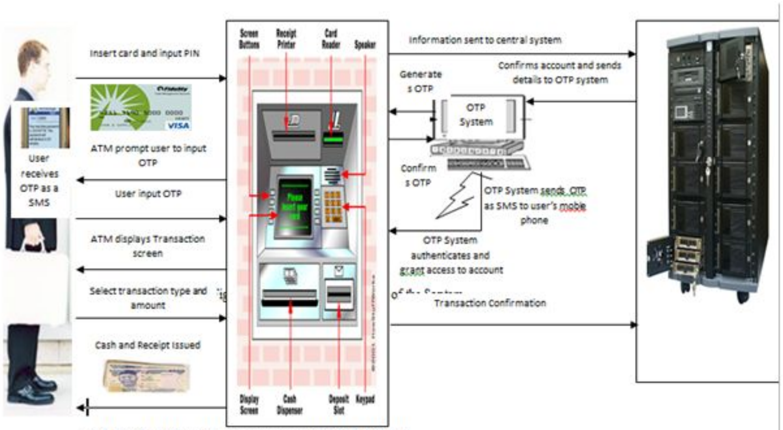
iv) **The Medium of Delivery**: The medium of Delivery of this the generated number after the system must have generated them will be by Short Messaging Service (SMS). This method sends the number in an out-band method to the Customer's mobile phone. A Bulk SMS service provider will be subscribed to.

v) **Latency:** After the delivering the One Time Password, there must be a timestamp for the expiration of the code, due to network latency it mustn't be too short and so also it mustn't be too long to ensure efficiency. So for this system the latency period will be 3 minutes.

vi) **Decision Module:** After the One Time Password must have been inputted, this component verifies if the OTP inputted matches the one sent, and if there is a match it authenticates the user, if it doesn't match, it denies authentication.

3.3.5 *How the system works*

Figure 3.2 displayed the graphical representation of the system, when a user wants to perform a transaction; he/her initiates it by inserting his/her plastic payment card into the ATM machine or the POS terminal, then the ATM prompt for his/her pin, if correct the information is sent to a central system, the system confirms the account and sends the factor required for the OTP system to generate the One Time Password, the OTP system then send this password the Users Phone number as a SMS, simultaneously the ATM prompt for the OTP, the user will input the received OTP, the system confirms the OTP if it matches with the one sent to the user, the OTP system grants access to the user. Then the user can perform any type of transaction giving that he has sufficient funds to complete it.


Insert card and input PIN
User receives OTP as a SMS
ATM prompt user to input OTP
User input OTP
ATM displays Transaction screen
Select transaction type and amount
Cash and Receipt Issued
Screen Buttons
Receipt Printer
Card Reader
Speaker
Display Screen
Cash Dispenser
Deposit Slot
Keypad
Information sent to central system
Confirms account and sends details to OTP system
Generates OTP
OTP System
Confirms OTP
OTP System sends OTP as SMS to user's mobile phone
OTP System authenticates and grant access to account
Transaction Confirmation

3.4 Unified Modeling Languages (UML) Model

Unified modeling language (UML) is a graphical language for specifying, constructing, visualizing and documenting the artifacts of system software (Chris Kobryn, 2000). System software that have been represented in a pictorial form is quite good because it helps the programmer or user understand the features of the system software and how it operates. UML is not used only for the purpose of representing software application; it can also be used for representing our day to day activities.

EXPERIMENTAL OUTPUTS

This sectionexperiments the steps on how the designed software works. For want of space, we are constrained to give a report excluding the visualization figures acquired as exhibits of various interfaces obtained. But be assured that our details in various screensare as good as any modern ATM booth functionalities as designed in our algorithmic structure in section3 above.

4.2. Choice of Programming Language

Java programming Language was chosen for the design and implementation of the simulation software. It was implemented by packaging the java source code to a Java Application that runs on a program on the JDK (Java SE development kit) and backed by a My SQL database. The reasons for designing the Software with Java programming language are:

i) It is object oriented: It supports inheritance as codes can be reused

ii) Java is platform independent: Java can run on any Platform, it runs on the World Wide Web (WWW), on Automated Teller Machines (ATM), Pont of Sales (POS) terminals, Smaller Appliances (microwaves and so on) etc.

iii) Java is secure

iv) Javasupport distributed computing, with networking capability inherent integrated into it.

4.2.1 Requirements for the Software:

The simulating software requires the following to function:

a) A computer system: This serves as the input and output layer for the software, activities of the software are displayed on the monitor of the computer system and the keyboard of the computer system serves as the mode of input information in to the software.

b) Database: For the system to function, it requires a database, and the database for the software as indicated earlier is the MySQL database, the database stores information about each customer which include the name, address, account number, the PIN, the phone number that the Generated One Time Password will be sent to is also stored on the database.

c) The One Time Password (OTP) generating Software: This is a software component of the system that generates the One Time Password before it's sent to the user.

d) Internet. For the system to be able to send the generated OneTime Password, it must be connected to the internet. The internet enables communication between the SMS service provider subscribed to and the Mobile Phone of the user.

e) SMS Service provider: The SMS service provider provides the software with SMS in form of credit after been subscribed to. The system made use of this credit unit to send SMS to the Phone of the User using the Internet.

4.2.2 Security Feature of the Software.

The software security features include the SHA-1 encryption method used to encrypt the concatenated factor thatwill generate the pin, which makes it difficult for any fraudster to have access to the One-Time Password algorithm. This is in addition to the security provided by the software which makes it a necessity for the fraudster to possess the Card and also the phone of the customer to perform fraud.

4.2.3 Implementing the Software on Existing System.

Implementing this system on the existing system is very easy to implement, and it's also cost effective as there is no need to purchase any hardware. All thatneeds to be done is to integrate the system into the software of both the Automated Teller Machine(ATM) and the Point of Sales (POS) terminals, the commercial institutions in the country are already making use of the SMS technology, so this won't also come with extra cost.

4.3 ATM/Admin Interface

This interface(Fig 4.1) comes up after the welcome screen, it has two functionalities, it serves as a gateway to gain access to the admin account or to initiate the transaction. To have access to the admin account will be discussed now while to initiate the transactions will be discussed in later subsections. Clicking the Admin button (in red circle in Fig 4.1) will prompt for the admin login details.

4.3.1 The Admin Login Interface

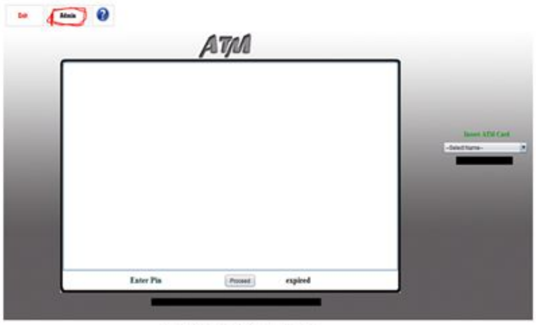


Fig 4.1 ATM/Admin Interface

This interfacescreen will prompt the user if the admin option is selected and it will require the login details of the administrator. Access is granted if the details are correct and denied if they are not.The Interface would present a screen if the admin login details are wrong as error

When the interface authenticates the outcomes, one is prompted to login in one's details by the administrator just as found in other POS provided this interface main function is to activate an account, deactivate an account, and delete an account. It also contains buttons to other admin functionalities like the customer details interface; view all customers and the new account form.

The Administrator provides the Customer details Interface and suggests further line of action. It rejects any errors found and suggests whether to continue or give up further processing. If negative, this process continues to run in a loop unless instructed to twiddle out.

The POS also contains the SMS cofiguration Interface whose function is to link the software to the SMS service provider, to link the software the provider, the email and password used for registering with the SMS service provider will be inputted.

4.2.1 Account Opening Form Interface

This is the enrolment stage, where customer data is collected and stored into the database. The new account form (Fig 4.2) enables the administrator to sign up new customers in to the application database. The customer names, address, phone number, passport photograph, marital status, email address are all provided while the account number and ATM PIN are generated and submitted.

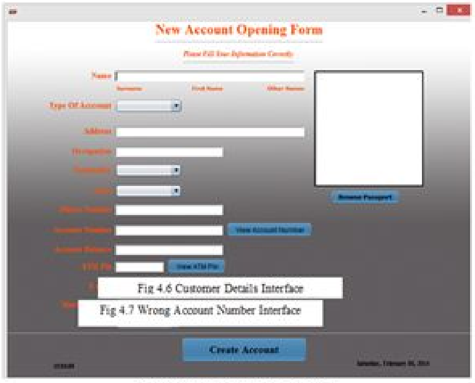


Fig 4.2 Account Opening Form Interface

The interfaceprocesses where the customer is being prompted to insert ATM card which is simulated by selecting customer's name from the selected user option drop tab(Dropdown table not shown), thus the process of selecting user simulates the acts of inserting ATM card in the machine and proceeds with the entire authentication processes of inputting PIN. If the user enters an invalid PIN, an error message, an interface is displayedwhich indicates an invalid PIN. After validating the customer's card and PIN number and if correct, the system generates the OTP and sends it to the phone number of the customer which will be used for the next phase of the authentication.

4.3 The OTP Interface Operation

After inputting the PIN, the system generates the OTP and sends it as an SMS to Mobile Number of the customer. The Customer then input the received code into the System through an interface (not shown due to space constraints). If it's correct, the authentication is process as validate and complete.Also displayed on this interface is the generated OTP pseudorandom number from the service providers.

Once the authorization is complete, the customer can start making transactions by selecting the type of account expedience. The user can perform any type of transaction given that it's within the account balance. The cash withdrawal interface (stimulates withdrawing of cash on the ATM booth.

4.2. Choice of Programming Language

Java programming was chosen for the design and implementation of the simulation software. It was implemented packaging the java source code to a Java Application that runs on a program on the JDK (Java SE development kit) and backed by a My SQL database. The reasons for designing the Software with Java programming language are:

I) It is object oriented:It supports inheritance as codes can be reused

II) Java is platform independent: Java can run on any Platform, it runs on the World Wide Web (WWW), on Automated Teller Machines (ATM), Pont of Sales (POS) terminals, Smaller Appliances (microwaves and so on) etc.

III) Java is secure

IV) Javasupport distributed computing, with networking capability inherent integrated into it.

4.3 Requirements for the Software:

The simulating software requires the following to function,

a) A computer system: This serves as the input and output layer for the software, activities of the software are displayed on the monitor of the computer system and the keyboard of the computer system serves as the mode of input information in to the software.

b) Database: For the system to function, it requires a database, and the database for the software as indicated earlier is the MySQL database, the database stores information about each customer which include the name, address, account number, the PIN, the phone number that the Generated One Time Password will be sent to is also stored on the database.

c) The One Time Password (OTP) generating Software: This is a software component of the system that generates the One Time Password before it's sent to the user.

d) Internet. For the system to be able to send the generated OneTime Password, it must be connected to the internet. The internet enables communication between the SMS service provider subscribed to and the Mobile Phone of the user.

e) SMS Service provider: The SMS service provider provides the software with SMS in form of credit after been subscribed to. The system made use of this credit unit to send SMS to the Phone of the User using the Internet.

4.4 Security Feature of the Software.

The software security features include the SHA-1 encryption method used to encrypt the concatenated factor used to generate the pin, which makes it difficult for any fraudster to have access to the One-Time Password algorithm, this is in addition to the security provided by the software which makes it a necessity for the fraudster to possess the Card and also the phone of the customer to perform fraud.

4.5 Implementing the Software on Existing System.

Implementing this system on the existing system is very easy to implement, and it's also cost effective as there is no need to purchase any hardware. All that need to be done is to integrate the system into the software of the both the Automated Teller Machine(ATM) and the Point of Sales (POS) terminals, the commercial institutions in the country are already making use of the SMS technology, so this won't also come with extra cost.

SUMMARY

Plastic Payment Card are generally acceptable in ATM machine across the country and also in Point of Sales Terminal, with this cards, customers can perform transaction at their convenience, but this comes with liabilities in the form of Plastic Fraud where a fraudster can perform illegal transaction using a card without the consent of the owner or the issuer of the card. These crimes lead to the need for preventing them to protect customers from being extorted and also the image of the banks. In order to prevent these crimes in the institution, we propose the use of One Time Password as an additional means of authentication. This Password is generated using random numbers generated from the concatenation of the Card details, the PIN, the Timestamp of the transaction with the result hashed with the SHA-1 algorithm, then XOR-ed to give 6 digits password. Conventionally, to use a plastic payment card for a financial transaction, the user inserts or swipes it card on the terminal, then input his PIN for authentication, before transaction can be completed. But with the implementation of this software, after the user must have input the PIN, this system generates the One Time Password and sends it to the registered mobile number of the customer who then input this password before authentication can be completed. What makes this method to be unique to other methods of preventing plastic fraud is because this method generates a password that can be used once exclusively to the number of the customer, so for a customer to be defrauded, the fraudster must possess the card, must know the PIN, and also have the mobile phone of the customer. Also, this also supports the Nigeria factor of sending someone the customer trusted to make transaction on his behalf. The customer is always advice to suspend the account linked to their card in case of robbery or any other incident that results to the loss of their card and phones.

CONCLUSION

Plastic Payment Card usage will increase over the year due to the implementation of the cashless economy by the Central Bank of Nigeria; this will definitely lead to more crime being targeted at this mode of transaction prompting the need for it to be secure. Implementation of the Plastic Fraud Prevention system that we proposed will be easier and cheaper to achieve due to the fact that almost all the banks are already using the GSM technology of sending Text Messages to customers, either as to notify them of transactions or to advertise new products to them, thereby enabling them to avoid additional cost that other proposed prevention (e.g. Biometrics) system might bring. This system will definitely reduce plastic fraud by making sure the bank client is the one performing the transaction, or the person performing the transaction is authorized by the client, and also will boast the confidence of Nigerians in embracing the Cashless Economy Policy.

RECOMMENDATIONS

Any criminal activities cannot be totally stopped, but it can be reduced to the minimum. Therefore it is a necessity to make recommendations to enable these crimes reduced to the minimal, we will make recommendation for banks, recommendations for Clients and recommendation for further research.

5.3.1 Recommendation to Banks

In other to reduce plastic frauds, the following recommendations are for the financial institutions;

i) Enlighten their customers more on how to be safe while with their card information

ii) Report any type of Plastic Fraud that occurs to the appropriate anti-fraud authorities

iii) Reminding their customers not to disclose their card information to anybody for whatsoever reason

iv) Ensuring the ATM vicinity is secure to prevent fraud like Card Jamming etc.

5.3.2 Recommendations to Customers

Providing recommendations to bank customers is also important n other to prevent Plastic Fraud. The following recommendations are for bank customers:

i) Customers shouldn't disclose their PIN and other personal information to anybody whatsoever.

ii) Customer should report any form of fraud against them to bank and also to appropriate authority.

iii) Customer should report the loss of their Plastic Payment Card to the bank promptly.

5.4.3 Recommendations for Further Research

One Time Password is a lifelike method of preventing Plastic Fraud, it's easy to implement as it can be integrated easily into the already existing system as banks are already using GSM technology to deliver SMS to customer, it's also user friendly. Further research can be carried out on this research work, by using other method of generating random numbers. Research can also be carried out on hybrid technology that would enhance the One Time Password (OTP). Such can be accomplished using Baby-step/Giant step or by Block-stream enciphering using AES.

REFERENCES

[1]. Wada, F. and Odulaja, G.O. (2012); *Assessing Cybercrime and its Impact on E-Banking in Nigeria using Social Theories*. African Journal of Comp & ICTs.Vol 5.No. 1.pp 69-82.

[2]. Ehimen, O. R. andBola, A. (2009): *Cybercrime in Nigeria*. Business Intelligence Journal- January 2010 Vol3 No.1 pp 93-98.

[3]. Dr. MadanBhasin (2007): *Mitigating Cyber Threat to Banking Industry:*The Chartered Accountant. April 2007. pp 1619-1624.

[4]. Ayofe, A. N. and Oluwaseyifunmitan, O. (2009): *Towards Ameliorating Cybercrime and Cybersecurity*: International Journal of Computer Science and Information Security. Vol.3, No.1, 2009.

[5]. Adeoti,J. O. (2011): *Automated Teller Machine (ATM) Frauds in Nigeria: the Way out*: Journal of Social Science, 27(1): pp 53-58.

[6]. Jenifer Raja Shermila,:*A Five Way Fuzzy Authentication For Secured Banking:*International Journal of Engineering Research and Application, Vol.2 Issue 4. July 2012, IJERA, pp 375-379.

[7]. Aloul, F. S., Zahidi and W. El-Hajj (2012) "*Two Factor Authentication Using Mobile Phones*" www.alou.net/Papers/faloul_aicca09.pdf

[8]. Padmapriya,V. andPrakasam, S. Ph.D. (2013):*Enhancing ATM security using Fingerprint and GSM Technology:*International journal of Computer Applications (0975-8887), Vol. 80 No.16.pp 234-238

[9]. Daily Independent News August 2012.:*Experts Worry Over Rising Cases, Sophistication, Unreported Bank Frauds.. August 2012*

[10]. Moon,D., Flatley, J., Green, B.& Murphy, R. (2010): *Acquisitive Crime and Plastic Card Fraud:* British Crime Survey, Home Office Statistical Bulletin.

[11]. Olasunkanmi, O. O (2010): "*Computer Crimes and Countermeasures in the Nigeria Banking Sector"* journal of internet banking and commerce. 15(1) pp 1-10

[12]. Hanna Mohamad (2011): *Plastic Card Fraud*. NSW Government, Attorney General & Justice, Australia. May 2011.

[13]. Nigeria Guardian News (2013): Nigeria's *POS terminals deployment hits 20000,* December 2013

[14]. National Fraud Authority (2012); *Annual Fraud Indicator,* United Kingdom, March 2012

[15]. Nigeria Deposit Insurance corporation 2012; "*Annual Reports"*, Nigeria, December 2012

[16]. Wikipedia, the free encyclopedia, 2013, *on One-Time_password.*

BIBLIOGRAPHY

	Dr. Victor OnomzaWaziri is an Associate Professor in the Department of Cyber Security Science, Federal University of Technology, Minna-Nigeria. He was the Pioneer Head of Cyber Security Science from 2009-2014; until in July 2014. He acquired his PhD in Applied Mathematics in the area of Computational Optimization in Wave diffusion Equations; 2004, from the Federal University of Technology, Minna-Nigeria. He has a Postdoctoral Certificate in Computer Science from the University of Zululand in South Africa; 2007. Other areas of his researches include Modern Cryptography, Data Mining and Machine Learning that involves Intelligent Soft Computing, Network Security; Malware Detection with concern in zero-day Malware, General Cyber Security Science and Big Data Analytics with indepth focus on Fully Homomorphic Encryption Schemes. In most cases, Matlab, Maple and Mathematica are the bases for his accessory in modeling and Simulations in Modern Cryptographic analyses. He has published many papers in reputable Journals at both International and Local Scenes. He Lectures various courses in the Department of Cyber Security Science that include Cryptography, Network Security, Clouds Security, Data Mining, Computational Theory, Automata and Programming Languages
	Dr. J. K. Alhassan was born at Ganmu-Alhaeri, in Kwara State, Nigeria on 9th January, 1974 and obtained Bachelor of Technology in Mathematics/Computer Science, at Federal University of Technology, Minna, Niger State, Nigeria in 2000. Then Master of Science in Computer Science, at University of Ibadan, Nigeria in 2006, and Doctor of Philosophy in Computer Science, at Federal University of Technology, Minna, Niger State, Nigeria in 2014. The major field of study is computer science. He carried out part of his PhD research at United Institute of Informatics Problems, National Academy of Sciences of Belarus (UIIP NASB) Minsk, Republic of Belarus. He is currently the Ag. Head, at the Department of Cyber Security Science, Federal University of Technology, Minna, Niger State, Nigeria. He has published twelve journal articles and four conference proceedings. His research interest includes Artificial Intelligence, Data Mining, Internet Technology, Database Management System, Software Architecture, Machine Learning, Human Computer Interaction and Computer Security. Dr. Alhassan is a member of Computer Professionals Registration Council of Nigeria (CPN).
	Dr. IsmailaIdris is with the Deparment of Cyber Security Science. He obtain his Bachelor degree with Federal University of Technology, Minna. M.Sc. with university of Ilorin and PhD degree with University of Teknologi Malaysia. His research interest are Information Security, Data Mining, Machine Learning, Evolutionary Algorithm.
	AlabeleweAbdulrahmanTunde Email: alabelewerahman@gmail.com Phone: 07037363957 Qualification: B.tech Computer Science (Cyber Securit) Futminna Area of Interest: Plastic Payment Card Security, network security, Fraud Detection.