DOI: dx.doi.org/10.22624/iSTEAMS/V26P7-IEEE-NG-TS
CrossREF Member Listing - https://www.crossref.org/06members/50go-

Development of One-Time Password (OTP) for ATM/POS : A Review of Related Works

S. Jurgene & O.B. Longe
Department of Information Technology
National Open University of Nigeria
Yola, Nigeria
sarahjuergenjrrs85@gmail.com

Abstract: This study is aimed at designing a One-Time Password (OTP) for ATM/POS. 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. But with this exciting innovation, it has also led to crime opportunities called "PLASTIC FRAUDS". Notwithstanding, this crime must be controlled and that is why the banks must adopt a preventive and proactive method to fight the crimes. This calls for a One-Time Password (OTP) for ATM/POS. In this paper, we reviuewed Related Literaure and set the agenda for the research.

Abstract- One-Time Password (OTP), ATM/POS, Security, Online Banking, Protection

I. INTRODUCTION

Plastic fraud is defined as 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. [1]. 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.

II. RELATED WORKS

[2] Carried out a study on Nigeria and their study revealed that (E-banking is still at the infant level in the country 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 crime and corruption which averages 75% and 71% respectively [3]

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) [4]. [8] [15]

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 thieves a loophole to operate freely. Finally, they provide insight into how cybercrime impacts on E-banking from a Nigerian perspective using social theories to explain causation with a view of guiding policy makers on behavioral issues that should be considered when formulating policies to address cyber-criminal activities in Nigeria [2] [6] [7] [14]

[5] defined computer crime as “any criminal activity 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. conducted an investigation and review criminal laws in Nigeria also they investigated on cybercrime and its socio-economic consequences and the damages on the image of Nigeria, they also analyze the activities of internet fraudsters also known as “Yahoo Yahoo boys” in Nigeria who uses false pretense to extort money from unsuspected victims.

Furthermore, the authors 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. However, they examine already existing laws that though they are not directly related to cybercrime, but can be used to limit it to some extent. Some of these laws are examined including the section 418 and 419 of the Nigeria constitution. The authors concluded that Cyber Crime is a threat to the economy and they also made recommendations which include:

The introduction of Cyber Police who will be trained to handle cybercrime related issues in the country. The introduction of a central computer crime response wing to serve as an agency to hint the government, organizations and other investigative agencies and guide in investigations.

Lastly the authors recommend the introduction of a resource center which will comprise of expert and professional on cyber-crime and related issues to establish rules and standards and also guide procedures.

Bhasin (2007) identified that business is subjected to (crime with the advent of computers especially the internet. He noted that cybercriminal uses information technology 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 cybercrimes 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 identifies 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.[8]

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.[8]

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 are 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. [9] 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.

[11] 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 Abuja.

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 the level 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”

[11] 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 rejected

The analysis shows that the work satisfies all security requirements on five factor authentication and has several other practice-friendly features. [12] in their paper entitled " two factor Authentication Using Mobile Phones" examine 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 propose 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 made up of 3 parts: software installed on client's phone, a server software and a GSM modem connected to the computer.

The system work 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 these 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.

[13] in their paper entitled "Enhancing ATM security using fingerprint and GSM Technology" highlighted that there is 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 a fingerprint enrollment, and a GSM technology connected to the microcontroller which sends a 4-digit code to the user.

The system consists 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 among thirty-five (35) professors, twenty-five (25) students, thirty-five (35) bank employees and twenty-five (25) government workers.

III CONCLUSION

With all this reviewed literature, it is a certainty that Plastic Payment Card has come to stay and its being generally accepted worldwide including Nigeria, with the Implementation of the Cashless economy policy, it is obvious that the usage plastic payment card will definitely increase which will lead to more crime rate and the need of these crimes to be curb, thus leading to the proposal of this software which serves as prevention for Plastic fraud.

All the methods reviewed (both proposed and already in use) are all very exciting, the reason to opt for using One Time Password to improve security is because of the following reasons:

i) Using the Biometric Technology (such as Fingerprint, Retina) will come with extra cost in purchasing devices for enrollment of the biometric trait, while OTP will make use of the already existing GSM technology in banks.

ii) ii) Also, the Biometric Technology will limit some Nigerians that are not used to going to ATM or other terminals to perform transaction but instead send people they trust (child) to perform the transaction. This may discourage them from using plastic payment card which will hinder the cashless economy policy. But with the OTP, it is still possible for them to send people they trust, all they need to do is to give them their mobile phone.

iii) Implementing the biometrics together will consume a lot of time which will not go down well with the Nigerians because of the long queues that are evident on the ATM terminals across the country

REFERENCES

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

[2] 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.

[3] National Fraud Authority (2012); Annual Fraud Indicator, United Kingdom, March 2012

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

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

[6] Longe, O.B & Danquah, P. (2012): Mitigating Socially Engineered Cyber Deception and Theft: An Ethnographic Approach. Information Technology in Developing Countries, IFIP Publication - Vol.22, No. 3. www.iimahd.ernet.in/egov/ifip/nov2012/longe.htm

[7] Longe, O.B. & Wada, F. (2012). Action Speaks Louder than Words - Understanding Cyber Criminal Behavior Using Criminological Theories. Journal of Internet Banking and Commerce.Vol. 17, No. 1.

[8] Longe, O.B, Lawal, B.O & A. Ibitola (2014): Strategic Sensor Placement for Intrusion Detection in Network-Based IDS. I.J. Intelligent Systems and Applications, 2014, 02, 61-68. Published Online January 2014 in MECS (http://www.mecs-press.org/). DOI: 10.5815/ijisa.2014.02.08 (Indexed in Scopus, IIJS)

[9] 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.

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

[11] 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.

[12] Aloul, F. S., Zahidi and W. El-Hajj (2012) “Two Factor Authentication Using Mobile Phones”.

[13] Padmapriya, V. and Prakasam, 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

[14] Nigeria Deposit Insurance corporation 2012; “Annual Reports”, Nigeria, December 2012

[15] Wikipedia, the free encyclopedia, on One-Time password.