ISSN No:-2456-2165

A Study of Electronic Banking Fraud, Fraud Detection and Control

Dr. Eneji, Samuel Eneeji; Angib, Maurice Udie; Ibe, Walter Eyong; Ekwegh, Kelechukwu Chimdike
Department of Computer Science, Federal College of Education,
Obudu, Cross River State, Nigeria

Abstract:- Electronic banking frauds have been issue of concern all over the world. It has left so many banks bankrupt, and caused many customers so much pain. Fraudsters are inventing newer techniques continually to elude detection and rub banks and customers of their possessions. This paper critically examines electronic banking frauds, detection of electronic banking frauds, control of electronic banking frauds, and challenges associated with the detection and control of electronic banking frauds.

***Keywords**:- Detection, Control, Analysis.*

I. INTRODUCTION

A bank is an industry that houses monies and other valuables for safe keeping pending when such monies or valuables would be needed by their owners. Bank exist in different forms depending on the scope and purpose for establishing the bank such as; Savings Banks, Commercial Banks, Industrial Development Banks, Land development Banks, Indigenous Banks, Mortgage Banks, Spare Bank, Federal or National Banks, Exchange Banks, Consumer's Bank, and Community Development Banks, [10]. Enhancement on the banking system led to the internet or electronic banking.

Internet banking is an online that uses communication gadgets such as the computer, phones, Automated Teller Machine (ATM), etc. It improves greatly on banking services to customers and makes transactions more convenient [14]. The internet banking enables one to buy and sell without physical cash, make deposits, transfer, pay bills, etc. with ease [1]. Electronic banking is driving the world toward cashless banking.

The electronic banking though beneficial to the banking system, has introduced great security threats to banks, and their customers. Electronic banking makes use of access codes, which is in the form of Personal Identification Number (PIN), before access is granted to the user of the bank services. This has not always safe the banks from the antics of fraudsters , fraudsters use various avenues to divulge or steel customers secret access codes which they personalize, and use the opportunity to impersonate and rob their victims of their valuables from the bank. Some robbers confiscate ATM cards from owners with their PINs, seize tokens and other electronic banking applications access codes; which they use in defrauding their victims [14]. Many banking customers resist electronic banking for fear of being defrauded. Some internet thieves use phishing and spooling to bait their victims. Bank customers who do not seek verification from their banks easily fall prey.

In order to fully utilize and enjoy the internet banking as conceived, there is the need for a sure security system more reliable than the pin, password, user name or token for the electronic banking [1].

The integration of Global Positioning System (GPS) with electronic transaction was provided as a means to identify and locate users, such that, a fraudster can easily be identified and traced [2]. User anonymity is believed to be one of the reasons fraudsters has the courage to involve in falsehood in electronic transactions [2]. Ref "[2]" observed that if users of electronic transaction systems can be known at each time of transaction with the electronic systems, then the fear of being identified can curtail most of their fraudulent intentions.

A security system should be able to defend itself from external attack; otherwise, fraudsters can choose to attack the system by rendering it inactive [5]. It therefore becomes pertinent that an electronic banking application should have some levels of security intelligence, and should be able to defend itself against external attacks.

This research work focuses on the detailed study of electronic banking frauds, fraud detection and control.

II. ELECTRONIC BANKING FRAUD

Ref "[14]" defined fraud as a conscious and deliberate action by a person, or group of persons, with the intention of altering the truth or fact for selfish personal gain. Ref "[6]" defined fraud as any premeditated act of criminal deceit, trickery or falsification by a person or group of persons with the intention of altering facts, in order to obtain undue personal monetary advantage. Frauds committed in the banks are called banking frauds, while the use of electronic to commit banking frauds is termed electronic banking fraud. Ref "[13]" defined electronic banking frauds as frauds associated with electronic banking perpetrated using ATM, POS, internet and mobile banking platforms. They further stated that, electronic banking frauds are achieved through the following;

i) Impersonation: exposing secrete identities to a third party who impersonate and defraud the owner.
ii) Phishing and spooling: giving response to futile text messages by revealing identities which are later used to defraud victims.
iii) Hacking: using random code generating software developed specifically for frauds purpose to hack into any matching account and defraud victims.
iv) Bankers: liaise with fraudsters by providing identities that are used to defraud banks and customers
v) Trojan horse: the interface with user login to divulge user's secret personal codes/identities which is in turn used to defraud victims.

III. EMERGING TECHNIQUES IN ELECTRONIC BANKING FRAUD DETECTION AND CONTROL

The increasing level of banking frauds with the banking system has called for concern, and emerging techniques to mitigate the fraud. This research work reviewed two of such technologies.

The use of artificial neural network and geographic information system (GIS)

GIS is complemented with artificial neural network by providing intelligent predictions of the emergence of fraudulence activities in the banking system [1]. Ref "[1]" further opined that the emergence of artificial neural network and GIS has led to a system under development at Carnegie Mellon University and the Pitts burgh (PA). Bureau of police which is artificial neural network enables early warning system incorporated with GIS to track criminal activities in drug, hot-sports area. The system obtains inputs from cell-aggregated GIS-based data, processes the data with previously trained artificial neural network and gives out the result in the form of map. In the map, the regions where threats are predicated by the network are indicated. According to Ref "[2]" and "[3]", the Pittburgh DMAP is one of such artificial neural network that enables GIS systems that assist investigators in crime policing.

One of the important attributes of DMAP in fraud detection is that it gives early warning signals for administrators to analyze crime pattern trends according to geographical coordinates. According to [3], the concept is called "geocoding". Geocoding is a process of address coverage which is the matching of address against data [2], and [3].

Neural networks evolved from the research on biological neurons which metamorphosed into the study and design of mathematical neurons which have applications in computational tasks in electronic circuits [3]; [2]. Artificial neural networks are made up of a number of processing units. These processing units transmit signals to each other through some links that are weighted [2].

IV. CONTROLLING ELECTRONIC BANKING FRAUD

Electronic fraud is committed using communication platforms and can be control using the same medium. Information technology utilizes in full computer technology, which is the brain child of communication. Computer security which is concern with the protection of computer resources and infrastructure from misuse, theft, corruption and natural disaster as to make them remain accessible and functional to the user, is one of the media through which electronic banking fraud can be controlled. Ref "[2]" opined that computer security encompasses processes of protecting sensitive and valuable computer resources from misuse or destruction from unauthorized activities, users, and unplanned events. According to Ref "[90]", [[2]", the following ways can be measures to prevent fraudulent and sharp practices in the net;

- Blocking software: An example of blocking software is the surf watch that has the ability of filtering or disallowing any application that is suspicious or have the likelihood of causing security breaches.
- V-chip: v-chip is software developed and uses to control children access to websites. V-chip restricts children from viewing information that is considered dangerous to them. It can be installed on computers or televisions.
- Browsers with ratings: Browsers such as kidDeck, chiBrow, and seaMonkey are customized browsers for use by certain category of people such as children to guide them against falling prey to cyber criminals.
- Audit controls: Audit controls is a software installed and run in most networks to keep track, records and file of transactions by internet users. The records can be used to trace security breaches and their sources.
- Encryption: Encryption is used in data communication to convert data on transit or stored to an indecipherable forms such that, the data will be meaningless to fraudster in the cause of interception. The policy here is that, it is only the owner of the message that can decrypt the data and make it meaningful. Microsoft and Netscape email programs has synCrypt, and SIMIME encrypting program used in its data communication.
- People controls: Hence fraud is committed by people, people controls is rather a policy that regulates the right to use the net and other net applications. It is expected that organizations that use the net should prevent misuse, or abuse by screening who to employ or give right of usage, have job specifications for employees, limits to coverage and proper disposal of documents that may communicate the organization's secretes to the public.
- Fire walls: Firewalls is use in computer to block suspicious programs from running on the system, thereby, denying the suspicious programs control or access to the system.

- Access point cloaking: this has to do with the configuration of access points, such that, request to connect from unknown sources are not responded to. The techniques used in Access point cloaking according to Ref "[7]" includes;

- Access authorization: Access authorization is a program that masquerade the access point requesting for authority, or permission to access an application or the net. The (a) Access authorization: Access authorization is a program that masquerade the access point requesting for authority, or permission to access an application or net. The user will be expected to enter the necessary requirements in the form of PIN (Personal Identity Number), user name, password or biometrics as the case may be before access is granted.
- Use of anti-virus software to debug viruses and malware
- Use of cryptography to transform data or information before transmitting, so that an unauthorized person who intercepts it cannot decipher it. Only the sender and the authorized recipient can decipher the message.

- Use of Biometric authentication: Biometric is the measure of physical feature or behavioural pattern of individuals. The physiological features scan is analyzed using mathematical algorithm. The analyzed physiological feature is stored in the database in the form of data (minutiae), which is used to verify and authenticate the person in subsequent transaction. Ref "[13]" opines that, biometric security is one of the most reliable security measures.
- Legislations and policies: The promulgation and implementation of legislations, and policies prohibiting electronic frauds with stipulated punishment for culprits, is a very important control measure for electronic fraud. Human are complex and trivial in behaviour. When given the opportunity to control themselves, they find it difficult to do the right. As such needs documented control measures that control their behaviours against excesses. Such document should specify in clear terms the punishment meted for any misconduct. As a matter of necessity and precedence, offenders should be made to face the consequences of their misconduct as stated in the constitutions. If this is enforced, human are expected to shape their behaviour to suit well in such a society, if this is equally implemented in electronic fraud, it should be a good control measure then. Ref "[2]" noted in his research work that, after the Pentagon Building attack in USA, in September 2001, that Federal Information Security Management Act (FISMA) was enacted in 2002, giving the Office of Management and Budget (OMB), the responsibility to coordinate information security standards and guidelines developed by federal agencies.

V. DETECTING AND CONTROLLING ELECTRONIC BANKING FRAUD

Fraud is committed by people who are conscious that their identities are not known to the public, as such, they would not be known hence, no consequence(s) to suffer. It will be ideal if the electronic banking application is integrated with technology that can identify users, and possibly keep a good record of their identities such that they can be trace in the case of unethical or fraudulent practices. Ref "[4] observed that, PIN is no longer secure enough to be used on the ATM, rather the use of facial recognition should be introduce as a means of identity.

Identity is concern with the verification of a person to be sure he is what he claims. Hence it is difficult to track down electronic banking fraudsters; it is expedient to identify who is the one on e-banking transaction at any point in time.

Ref "[2]" states the following as ways in which online users can be identify;

- Identify card and credentials
- Use of radio frequency identification (RFID)
- Use of Biometric technology and
- Surveillance system

VI. CHALLENGES IN DETECTION AND CONTROL OF ELECTRONIC BANKING FRAUD

Banking fraud is a crime with severe consequences, but to the fraudster it is a means of living. Worst is in the developing countries with the slogan of "survival of the fittest". The question is what happens to the unfit? It would have better been said "survival of the fittest and the elimination of the unfit". In this kind of a system, either side of the coin is consequential, as such; it becomes practically impossible to think that preaching of sanity would make meaning. It therefore becomes expedient for detection and control of banking fraud. The following discussed are the basic challenges associated with electronic banking fraud.

- i). Human Rights Implications: Human right struggle have place bounds or challenge most of the activities carried out for the purpose of identification. Human right has condemned the use of computer and networks in monitoring people, and maintain that the use of electronic in monitoring system and techniques on human bodies is tantamount to human right violation, abuse of privacy and abuse of power by authoritarian leaders who use their positions to humble their subjects and political opponents [8]; [2]). Ref "[11]" held the view that while emerging technologies are encouraged, there should be room for debate on the social implications and people's desired guiding principles on their usage should be established.

- ➢ Often time, some of these bottle necks pose challenges on the detection and control of electronic banking fraudsters.

- Complexity of technology: Technology is emerging continuously with different modus operandi. Some technologies relax certain restriction on users thereby making them anonymous. In such a situation, it becomes difficult to detect such criminal [12].

VII. CONCLUSION

Electronic banking has helped greatly in providing banking services with ease and efficiency globally. It has reduced time waist and high charges associated with the traditional banking system. It has led to banking-as-you-go, and encourages cashless banking. Fraudsters have as well taken advantage of the platform to perpetrate serious crimes that affect both the bank as an institution, and the bank customers. The damage caused by bank fraudsters has gone a long way affecting negatively the economy of many countries.

There is every need to curb this ugly trend with the banking sector. A number of proposals have been presented by researchers on measures to mitigate frauds associated with the banking system. This includes full integration biometrics in electronic banking, user identity at each transaction, use of personal identity, etc. Not all the findings have been integrated in electronic banking to mitigate frauds due to heavy weight of biometrics and its implementation in real time transactions as well as human rights violations.

The researchers are of the view that, the integration a biometric security and a system that unveils users anonymity with electronic banking system will help to mitigate and combat electronic banking frauds.

REFERENCES

[1]. Adewale, A., A., Ibunni, A., S., Badejo, J., and Odu, T., (2014). Biometric Enable E-Banking in Nigeria Management and Customers' Perspectives. Journal of Information and Knowledge Management; 4(11), 23-28.

[2]. Agana, M., A., (2016). A Model of Cyber Crime Detection and Control System. A PhD Thesis presented to Department of Computer, Faculty of Physical Sciences, Ebonyi State University, Abakaliki.

[3]. Andreas, M. O., (2011)Artificial Neural Networks and Crime Mapping accessed from http://www.popcenter.org/library/crimeprevention/volume08/11-olligschlaeger.pdf on 21st August, 2016.

[4]. Aru, O., E., and Ihekweaba, C., (2013). Facial Verification Technology for Use in ATM Transactions. American Journal of Engineering Research (AJER), 2(5), 188-193.

[5]. Bassey, I. E. (2015). Development of a Model of Intrusion Detection Systems for Local Area Networks. A Ph.D Thesis presented to department of computer science, faculty of Science, Ebonyi State University, Abakaliki.

[6]. Boniface, C., (1991). Fraud in the Banking Industry. Abuja, The Nigerian Bankers, CIBN press.

[7]. Echewodo, l. (2010). Management of Information Technology. Paper presented at the Executive Modularization Programme of the Computer Professionals (Registration Council) of Nigeria (CPN) held in Oweri, November 23-25.

[8]. Fox, R. G., (1987). Dr. Schwitzgebel's Machine Revisited. Electronic Monitoring of Offenders. Australian and New Zealand Journal of Criminology, 20(3),131-147.

[9]. Hurchinson, S. E., and Sawyer, S.C., (2000). Computer, Communication and Information: A User's Introduction. New York: DP Publications. http://typeslist.com/different-types-of-banks accessed on 24/3/2019

[10]. Kirby, M., (1998). Privacy in Cyberspace. University of New South Wale Journal, 21(2), 323-333.

[11]. Longe, O., Osofisan, A., Kvasny, L., Jones, C., and Nchise, A., (2010). "Towards a Real Time Response (RTR) Model for Policing the Cyberspace", Information Technology in Developing Countries; 2(3), accessed from http://www.iimahd.ernet.in/egov/ifip/oct2010/olumide-longe.html on the 30th of May, 2016.

[12]. Onu, F., U., Eneji, S., E., and Anigbogu, G., (2016). The Effect of Object Oriented Programming on the Implementation of Biometric Security System for Electronic Banking Transactions. International Journal of Science and Research (IJSR), 5(2), 935-941.

[13]. Onu, F.u, Umeakuka, C., V., Eneji, S., E., (2017). Computer Based Forecasting in Managing Risks Associated with Electronic Banking in Nigeria. Journal of Innovative Research and Advanced Studies (IJIRAS); 4(3), 390-396.

[14]. Taiwo, J., N., Agwu, M., E., Babajide, A., A., Okafor, T., C., and Isibor, A., A., (2006). Growth of Bank Frauds and the Impact on the Nigerian Banking Industry; Journal of Business Management and Economies (JBME), 4(12), 1-10.