International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 4 Issue 3, March 2017

ISSN: 2394-4404

Computer Based Forecasting In Managing Risks Associated With Electronic Banking In Nigeria

Onu, Fergus U. (Ph.D)

Umeakuka, Chinelo V.

Department of Computer Science, Ebonyi State University, Abakaliki

Eneji, Samuel E

Department of Computer Science,
Federal College of Education, Obudu

Abstract: ***Electronic banking which is one of the fastest growing trends in the banking industry in the world is faced with a lot electronic risks and electronic fraud challenges. This constitutes a major problem in the acceptance and use of electronic banking by some banking customers. In Nigeria where insecurity and lack of awareness of digital convergent systems in electronic banking is prevalent, it has also given rise to new orientation of risks in business transactions. It becomes pertinent for a way forward for efficient and effective utilization of electronic banking services in Nigeria. This paper proposes an integration of intelligent systems that will forecast the incidence of the challenges to electronic banking using the past and present data and present reports to management for right and timely decision making. The paper also presents a system that uses regression analysis to forecast the risks associated with electronic banking in Nigeria. Object Oriented Methodology was used in analyzing the proposed system and the system was implemented using VB.net. The analysis of electronic banking fraud, application of computer based forecasting in managing electronic banking risks were presented. The results achieve showed an easier and better way of analyzing and managing electronic banking risks in Nigeria.***

Keywords: Forecasting, Electronic, Risks

I. INTRODUCTION

The banking sector is an essential aspect of the nation's economy. It is a medium through which the economy of a country is regulated, and also provides platforms for citizens to go about their financial transactions. It creates the opportunities for saving of money and valuable assets, as well as lends money to individuals and corporate bodies to go about their normal and legal business. The financial trunk of the country is the banking industry. As such a struck on the power house of the country is also a struck on the country's economy. It becomes therefore pertinent to safe guide the components that made up the banking industries physically, electronically, technologically and otherwise. This is the reason why the banking industries do not toy with security. Despite the security awareness and strategies to sustained satisfactory security situation by the banking industries, the bank is still security vulnerable.

The banking industries renders services to the entire population of the country on daily basis, as such become chunked with so much activities that need technology and any other measures to ensure efficiency and effectiveness. In the 19^{th} century and earlier, irrespective of the fact that countries population were not as much as today, and banking awareness of the citizens was not informed as today, the banking transactions was face-to-face with each customer in each transaction and recorded in spreadsheets and ledgers to maintain continuity (Ikpefan, 2006). This method though effective, it was characterized with much delay, inefficiency, tasking, burdensome etc. In the later part of the 19^{th} century till date, there had been significant improvements in the banking industries with adequate integration of modern technology which has been able to ease the burdens associated with the earlier operations of the bank. The new and improved banking operations had also introduced with it new problems especially in security (NDIC, 2015).

ISSN: 2394-4404

Electronic banking which is the integration of computer technology (Information Technology (IT)) in banking has provided the banking industries with better opportunities to render better and satisfactory services to the public. Though, there are challenges of customers' awareness, inability to operate and use ICT gadgets, problem of power, poor or no network access, and mostly, issue of electronic fund. Fraud has become one of the major problems of the banking industries worldwide and there is every need to curb these ills. Some banks in Nigeria were almost distressed due to activities of fraudsters (Hur-Yagba, 2003).

Electronic banking fraud is concern with the use of ICT facilities and techniques to frequently steel money from the bank directly or from customers' accounts using any of the electronic banking platforms. It is the believe of the researcher that to curb these challenges (frauds) in the banking industries, adequate records of fraudulent activities in the banking industries should be tracked and recorded. A projection using computer based forecasting to predict future risks associated with electronic banking should be projected and presented as reports to management to suggest and implement a quick intervention measures to curb the future occurrence of such crimes.

A. RESEARCH OBJECTIVE

The main aim of this work is to develop a sub-system that will use apropriate technique to forecast future risks associated with electronic banking in Nigeria. The objectives include:

- ✓ To create a database of electronic banking fraud in Nigeria per year
- ✓ To generate reports proponent of the risks associated with electronic banking in Nigeria
- ✓ To create a software module capable of forecasting future incidence of fraud associated with electronic banking in Nigeria

II. LITERATURE REVIEW

This research work discussed two major expertise areas namely Computer based forecasting and Electronic banking. It pays particular attension to electronic banking fraud and their ditection. These areas are discussed precisely in the subsections that follow.

A. COMPUTER BASED FORECASTING

Forecasting is primarily concerned with predictions. Any successful business must plan into the future. This implies that the idea of the future should be known as to be able to programme the future. One of the methods of predicting or looking into the future is forecasting (Rekhi, 2016).

Hence the future is unknown; management decisions are based on forecast. According to Gov (2014), forecasting can be defined as attempting to predict the future by using qualitative or quantitative methods. He went further to define forecasting as the process of estimating a future event by casting forward past data. The process of making prediction of the future using the past and present data and the analysis of trends is forecasting.

Forecasting employs various statistical tools such as regression analysis, moving average, weighted moving average, exponential moving average etc using present and past data with its interplay to predict the future. This prediction, help management to be able to formulate the most important tasks of the organization such as:

- ✓ Organization's mission
- ✓ Domain for activities
- ✓ Long term goals
- ✓ Strategy for achievement of the goals
- ✓ Type of production and
- ✓ Technology level of development (Kurzak, 2012)

To improve the accuracy of decision making, forecasting is needed in decision-making process. According to Banu (1985), forecasting in production enterprise allow for finding the most probable course of processes.

As a case study, forecasting will help the bank management to predict as follows:

- ✓ Demand/provide services that will be self sustaining
- ✓ Know demand in individual market segments
- ✓ Know general economic state of the society
- ✓ Predict technology changes needed to give efficient and satisfactory services to customers
- ✓ Know actions taken by competitors as to formulate sustenance policy
- ✓ Know level of frauds on the banking industry and measures to combat it
- ✓ Customers' satisfaction and confidence with the bank (Banu, 1985)

Computer based forecasting is concern with the use of computer in forecasting. Computer from its conception was tough of a machine that can do computation which is primarily mathematical. But the introduction of stored program by the French mathematician and physics, John Von Neuman, the computer of today has become versatile and finds its application in almost every sphere of human endeavour (Angib, Bassey, Eneji, Ibe & Omonu, 2005). The basis of automation is all about translating the manual processes into computer processes.

Computer based forecasting is therefore the automation of forecasting processes. Computer based forecasting receives the present and past records of the bank on area of interest, uses a more suitable technique to forecast the record as to present a prediction- for the future which will help the bank management to act early enough and avert impending doom. The detail description of the computer based forecasting is shown on Fig 1 below

ISSN: 2394-4404

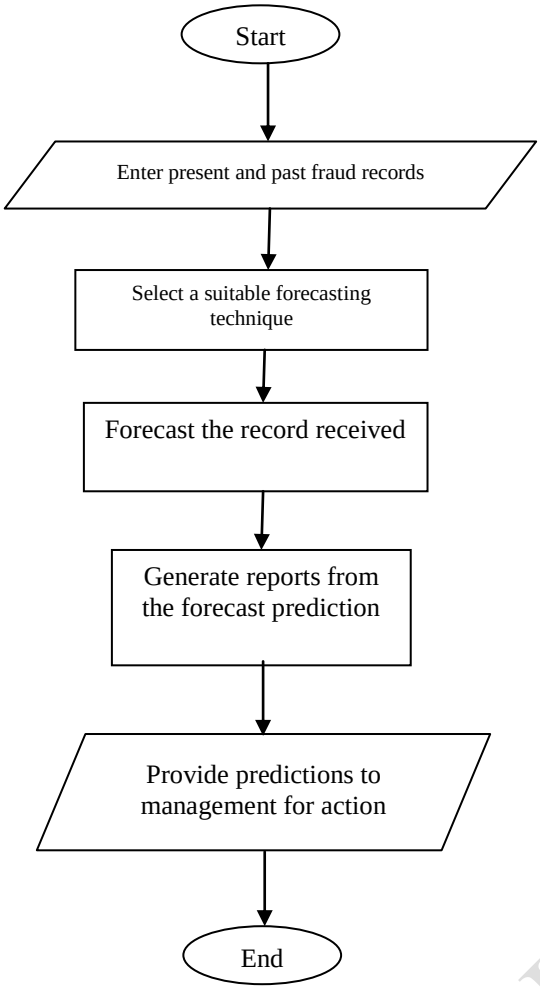

Figure 1: Computer Based Forecasting Flowchart

B. ELECTRONIC BANKING FRAUD

Banking industries of the 21st century integrates ICT in the banking industries thereby, making banking service delivery more of fund. The integration of ICT in the banking industries has as well brought with it new challenges in the banking system.

Electronic banking is simply the use of electronic in rendering banking service. It helps banks and customers to render and achieve twenty four hours banking services irrespective of distance, place or physical contacts. Electronic banking though a good development, fraudsters have seized the platform to commit frauds thereby affecting both the banks and customers. The activities of fraudsters have posed a lot of challenges to the use of electronic banking to banks and customers (Ikpetan, 2006).

Fraud according to Taiwo, Agwu, Babajide, Okafor and Isibor (2006), is 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; According to Boniface (1991), fraud is described 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; Olufidipe (1994) defined fraud as a deceit or trickery deliberately practiced in order to gain some advantages dishonestly; Idowu, (2009) defined fraud as a deliberate falsification, camouflage, or exclusion of the truth for the purpose of dishonesty/stage management to the financial damage of an individual or an organization. Fraud in the banking industry has become embarrassment to the nation and has become issue of national concern (Idolor, 2010).

Electronic banking fraud is simply frauds associated with electronic banking perpetrated using ATM, POS, internet and mobile banking platforms. Electronic banking fraud is achieved by fraudsters through:

- ✓ Impersonation: exposing your ATM or POS secrete identity to someone else who now interfaced as the owner and gain access to your account to defraud you.
- ✓ Phishing and fraudulent e-mails: responding to text messages or email requesting your bank secrete information which fraudsters run on fraud designed package to access and defraud victims electronically.
- ✓ Hacking: using random code generating system develops for purpose of fraud to hack into any matching account and defrauds victims.
- ✓ Bankers: giving out secrete information of bank/customers access to fraudsters who locked into such account using any of the electronic means that is achievable to defraud victims (Nwaze, 2006).

Irrespective of frauds associated with electronic banking, its advantage is enormous, as such; the need to improve on its security becomes a necessity while its usage is encouraged.

C. DETECTING AND MITIGATING ELECTRONIC BANKING FRAUD IN NIGERIA

Electronic Banking fraud is achieved primarily through phishing and spooling attacks. Detecting electronic banking fraud calls for strict monitoring of phishing and spooling activities. Electronic banking fraud is concern with the stealing and mis-use of banking customer's important credentials such as personal identification and credit card details (George and Paulose, 2015). Access to these identities gives fraudsters the opportunity to commit electronic banking fraud. It thereby becomes very difficult to identify who is a fraudster and who is the owner of the identity in the cause of accessing such an account. Detecting electronic banking fraud is better enhanced when the banking customers are able to keep their identity to themselves as secrete leaving the issues of phishing and spooling.

In the event that the customer divulge his or her secrete online banking identities to a third party by whatsoever reason, it becomes imperative to alert the banking industry immediately to place surveillance on such an account(s). According to George and Paulose (2015), fraud can be detected in online transactions in the following ways;

- ✓ Detecting unknown pattern for financial transactions
- ✓ Monitor transactions that are suspicious (i.e. operations the user is unsure exactly about what to do)
- ✓ Keeping track of new fraud scheme.
- ✓ Bunch, Ernst and Young (2014) stated that fraud can be detected as follows;
- ✓ Establishing procedures and avenues for reporting suspicious and fraudulent activities
- ✓ Financial statement analysis

- ✓ Targeted anti-fraud analytics
- ✓ Internal control monitoring
- ✓ Internal control testing
- ✓ Internal investigation
- ✓ Independent investigation

To mitigate electronic banking fraud and reduce risks in the banking industries, Simon, Adebayo and Emmanuel (2013) are of the view that anti fraud detection system could be set in place. The further recommended that the black listing approaches which are belt onto application web browsers for detecting phishing cites such as whitelisting and heuristics should be enforced.

Greorge and Paulose (2015) are of the view that there are many approaches to reduce and control online fraud, but that it depends on the type of e-transaction. They further listed the following as preventive measures;

- ✓ Known pattern (set up rules to filter fraudulent transactions)
- ✓ Unknown pattern (anomaly detection)
- ✓ Complex pattern (advanced analytics)
- ✓ Associated linked pattern (social network analysis)
- ✓ Bunch, Ernst and Young (2014) also observed that to mitigate fraud, the following should be observed;
- ✓ Setting strong tone at the top
- ✓ Implementing policies and procedures in order to prevent fraud from occurring.
- ✓ Developing fraud training and awareness.
- ✓ Establishing strong internal control

III. SYSTEM ANALYSIS AND DESIGN METHODOLOGY

The study was analyzed using Objected Oriented Methodology (OOM). OOM has convenience features which suit competitiveness and corporation of components and as such, a better methodology for real time system. A part from the cardinal point mentioned above, OOP made room for easy restructuring of system, reusability of components, inheritance and data abstraction. These features allow for the design of portable but very powerful system with lesser memory consumption. OOM also suits for the design of both large and small system. (Onu, Eneji and Anigbogu, 2016)

A. SYSTEM ANALYSIS

System analysis is concern with the critical examination of an existing system with intend of improving on the system for better performance. Mbam (2002) defines system analysis as the process of analysing or evaluating the existing system to find out how it works and how it meets users' needs.

Electronic banking risk forecasting management system is a new concept conceived to be developed as part of electronic banking application that will present filtered report on fraud to management on intervals or on request to shape management decision in the fight against fraud and reduce risk of electronic banking transaction. The proposed system consists of the following modules;

- ✓ Record Banking Fraud: this module keep tracks of all banking frauds and the associated components such as amount involved, type of fraud, perpetuator of fraud, etc.
- ✓ Separate Fraud: this module filters fraud into electronic fraud, and other forms of fraud. It also separate frauds associated with bankers and other fraudsters.
- ✓ Compute Correlation: Uses regression analysis to compute the relationship between electronic fraud and other forms of fraud, and also the relationship between bankers and non- bankers' involvement in frauds.
- ✓ Forecast Fraud: use an appropriate forecasting technique to forecast probable future occurrence of fraud on demand. This will guide management on the rate of fraud per interval and what might be done to minimize fraud in the banking system.
- ✓ Generate Report: report from the analyses is generated for management consumption and application.

B. SYSTEM SPECIFICATION

The proposed system works as follows;

- ✓ Daily records of electronic and non-electronic banking fraud incidence are kept
- ✓ A correlation between electronic banking fraud and non-electronic banking fraud is computed using regression analysis.
- ✓ Exponential Moving Average forecasting technique is used to forecast the probable level of electronic banking fraud anticipated for the next n-1 years and its effect on electronic banking using the initial and present electronic banking fraud records stored in the system.
- ✓ Reports on the analysis and forecast is generated and submitted to management to corroborate appropriate steps needed to alleviate the bank from fraudsters, and boost customers' confidence in electronic banking.

MATHEMATICAL SPECIFICATIONS OF THE PROPOSED SYSTEM

The proposed system uses forecasting technique to;

- ✓ Determine the relationship between electronic bank frauds and other bank frauds to determine where more focus is needed in the fight against banking frauds
- ✓ Uses the past and present electronic banking frauds data to project the level of electronic banking fraud anticipated in the future. Both issues (i and ii above) made used of regression analysis and Exponential Moving Average (EMA) in its computation. The mathematical models are represented as follows
- ✓ $Fn_{i-1} = f(bo_{i-1}fi_{i-1} + b_{1\,i-1}f_{2\,i-1} + f_{3\,i-1})$

EQUATION 1

Where;
Fn = fraud expectation
bo,bi = intercepts
f_n = non-electronic bank fraud
f_2 = electronic bank fraud
f_3 = unidentified fraud elements
i = subscripts or number of iterations

$$f_n = \frac{n\sum f1f2 - \sum f1\sum f2}{\sqrt{n\sum f1^2 - (\sum f1)^2}\sqrt{n\sum f2 - (\sum f2)^2}}$$

EQUATION 2

The formula above determines the extent at which electronic bank fraud is related to non-electronic bank fraud.

✓ $Fn_{i-1} = fo_{i-1} + \propto(lo_{i-1} - fo_{i-1})$

EQUATION 3

$\propto$ - 2/(n + 1)

Where;
Fn = new forecast
Fo = old forecast
N = number of fraud incidence
Lo = latest observation
$\propto$ = smoothing constant
i = subscripts or number of iterations

$Fn_{i-1} = fo_{i-1} + 2/(n+1)\ [lo_{i-1} - fo_{i-1}]$

This will take care of an n forecast of future expected electronic fraud.

C. SYSTEM DESIGN

System design is concern with the process of defining the architecture, components, modules, interfaces and data for a system to satisfy specified requirements. Figures 2, 3, 4, and 5 below discussed the system design as specified in 3.1.

✓ High level model of the proposed Computer Based Electronic Banking Forecasting Risk Management System

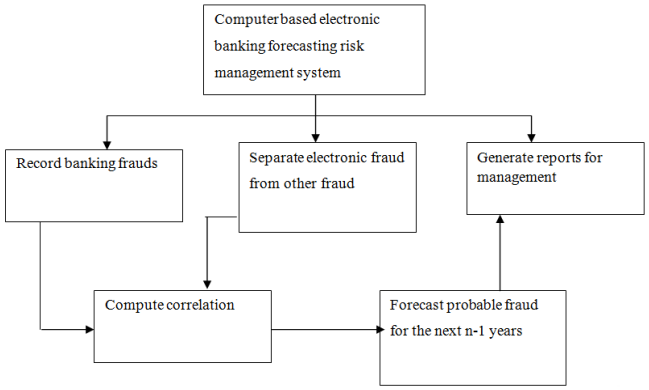

Figure 2: High level model of computer based electronic banking forecasting risk management system

✓ SYSTEM FLOW REPRESENTATION

The class diagram and flowchart below explain the flow of data in the system in detail. All the key procedures of the system, their inputs output are depicted in fig 2 and fig 3.

MAIN MENU DESIGN

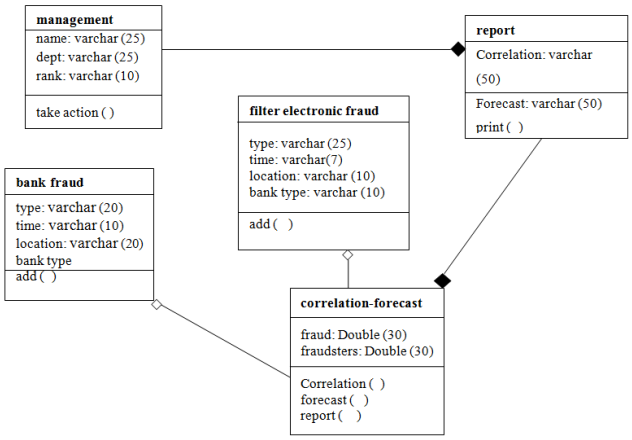

Figure 5: Interface Design of Electronic Banking Risk Forecasting System

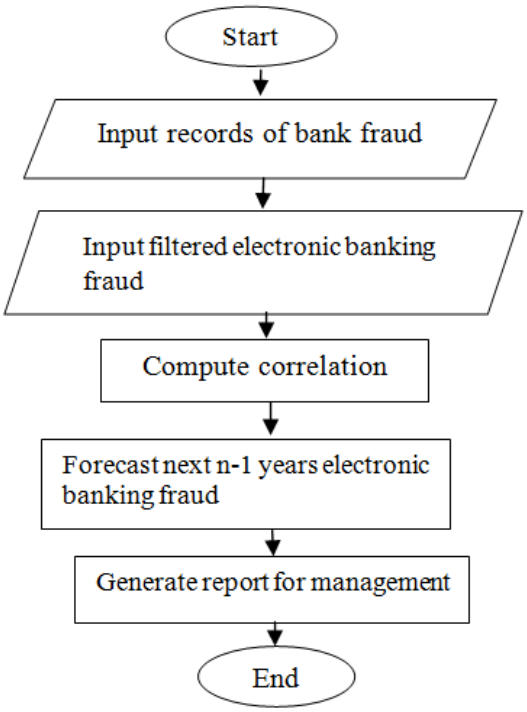

Figure 4: Flowchart for Computer based Electronic Banking Risk management System

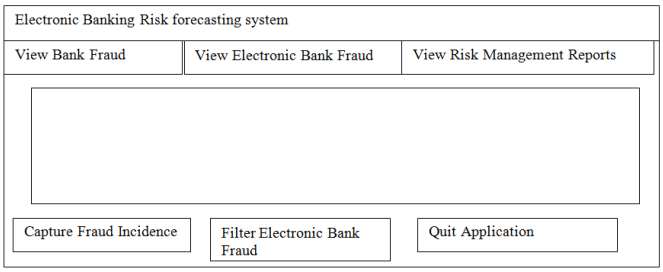

Figure 5: Interface Design of Electronic Banking Risk Forecasting System

D. SYSTEM IMPLEMENTATION

The user interface consists of the title of the application, view bank fraud, view electronic bank fraud, view risk

ISSN: 2394-4404

management reports, capture fraud incidence, filter electronic bank fraud and quit application. The view bank fraud will display the records of incidence of fraud generally in the bank presented in year-by-year summary. The view electronic bank fraud displays the records of electronic banking fraud over the years and presents the result per year. The essence of these (view bank fraud, and view electronic bank fraud) is to enable management and whoever may be designated to use the application to at a glance flip through the growth of both electronic and non-electronic frauds in the banking industries. The view risk management report contained records of analyzed reports and predictions to management as regards risks associated to electronic banking. The capture fraud incidence and filter electronic bank fraud provide avenue for either automatic or manual record of fraud incidence, and the possibility to separate electronic bank fraud from other frauds. The quit application is a button to exit the Electronic Banking Risk Forecasting System.

IV. RESULT PRESENTATION AND ANALYSIS OF FINDINGS

- ✓ The developed system is simple, scalable and flexible in operation. The system does not only keep records of electronic banking fraud and fraudsters, it also analyzes and determines the relationship between electronic fraud and non-electronic fraud associated with the bank, and also forecast future level of fraud. Fig 5 shows login interface of the designed system.

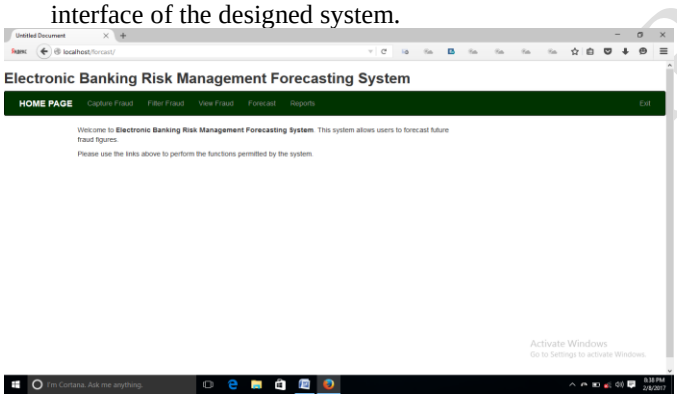

Figure 5a: Login Interface of Electronic Management Risk Forecasting System

- ✓ The proposed system can display records of the incidence of crime in the banking industry within a range as specified by the user. See fig 6.

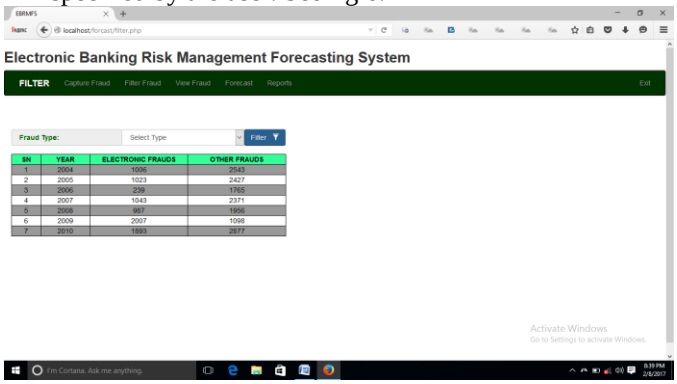

Figure 6: Display of Captured Fraud

- ✓ The proposed system is able to generate reports on the extent to which bankers contribute bank fraud and the relationship directly or indirectly to fraud incidence by non-bankers. This will guide management on the area of focus and control.
- ✓ The system can as well forecast future incidence of frauds as may be required which will help management to improve on risk management. See fig 7 & 8.

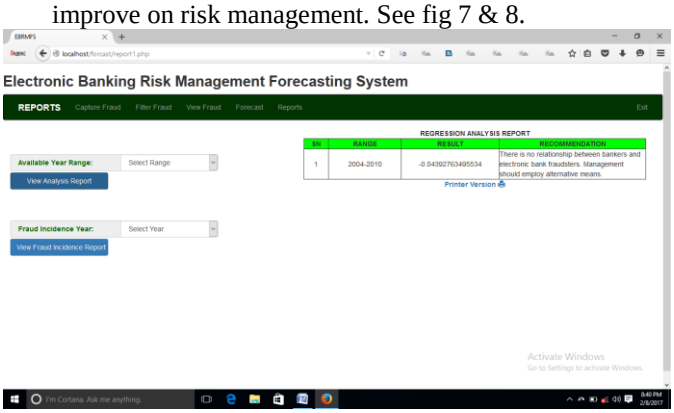

Figure 7a: Display of report on the relationship between banker fraudsters and others

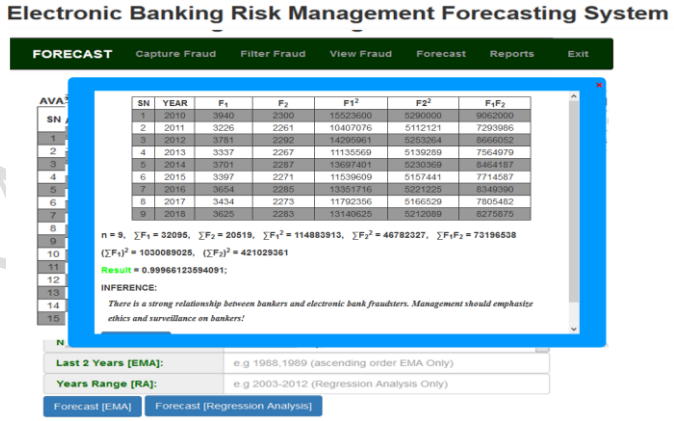

Figure 7b: Display of report on the relationship between banker fraudsters and others

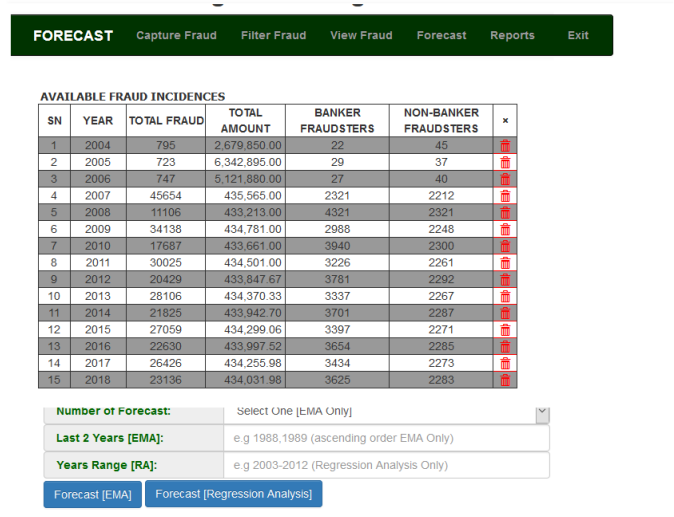

Figure 8: Display of report on 14 years fraud forecast

V. CONCLUSION

The proposed system was developed and it was able to achieve:

- ✓ Developed Electronic Banking Risk Forecasting system
- ✓ Creates banking fraud Database
- ✓ Generate reports of the incidences of banking fraud for management necessary action
- ✓ Forecast the involvement of bankers and non banker in banking fraud.

It is the expectation of the researchers that designed system if implemented will guide management on the area of focus and control in terms of using enhanced surveillance system, etc., for risks management.

REFERENCES

[1] Angib, M. U., Bassey, I. E., Eneji, S. E, Ibe, W. E., & Omonu, P. O., (2015), Computer Operations. Obudu, Adamade Printers (Nig)

[2] Banu, D. P., (1985), Science Education in Nigeria Secondary Schools, A reappraisal studies in science education, 9(0), 33-46

[3] Boniface, C., (1991), Fraud in the Banking Industry. The Nigerian Bankers, October – December 22 & 23, CIBN Press

[4] Bunch, D., Ernst, & Young (2014). Fraud Investigation and Dispute Services. Accessed from www.dean.bunch @ey.com on 01/03/2017

[5] George, T. K., & Paulose, J., (2015). Fraud Detection and Mitigation in Secure e-payment Transaction. International Journal of Scientific and Engineering Research, 6(2), 1217-1221

[6] Hur-Yagba, (2003), Frauds in the Nigerian Banking Industry. Abuja Management Review, Faculty of Management Sciences, University of Abuja

[7] Idolor, E. J., (2010), Bank Fraud in Nigeria: Underlying Causes, effects and Possible Remedies; African journal of accounting, economics, finance and banking research, 6(6), 62-67

[8] Idowu, I., (2009). An Assessment of fraud and its Management in Nigeria commercial Banks. European Journal of Social Sciences, 10(4), 628-640.

[9] Ikpefan, O. A., (2006), Growth of Bank Frauds and the Impact on the Nigerian Banking Industry

[10] Kurzak, K. L., (2012). Importance of Forecasting in Enterprise Management. Advanced Logistic System, 6(1), 173-182

[11] Mbam, B., C., E., (2002). Information Technology and Management System. Enugu. Our Saviour Press Ltd.

[12] NDIC, (2015), Nigeria Deposit Insurance Corporation-NDIC fraud report. Accessed from *http://ndic.gov.ng/ndic-release-1015-annual-report/* on the 16th of December, 2016.

[13] Nwaze, C., (2006). Bank Fraud Exposed with Cases and Preventive Measures, Lagos; Control and Surveillance Associates Ltd.

[14] Olufidipe, E. O., (1994), *Fraud in Nigeria and its Implication for bank and financial institutions.* Nigeria Institutes of Bankers; Lagos, 30(0), 7-10

[15] Onu, F. U., Eneji, S. E., & Anigbogu, G., (2016). The effect of Object Oriented Programming in the Implementation of Biometric Security System in Electronic Banking Transactions. *International Journal of Science and Research, 5(0), 935-941*

[16] Rekhi, S. (2016), Use of Computer in Economic Analysis and Forecasting. Information retrieved from *http://www.computer-forecasting.htm*, on 10th of December, 2016.

[17] Simon, E. Adebayo, K. J. &Emmanuel, A. (2013). Mitigating Cyber Identity Fraud Using Advanced Multi Anti-Phishing Techniques. International Journal of Advanced Computer Science and Application.

[18] Taiwo, J. N., Agwu, M. E., Babajide, A. A., Okafor, T. C., & Isibor, A. A., (2016). Growth of Bank Frauds and the Impact on Nigerian banking Industry. *Journal of Business Management and Economics, (1- 10)*