International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V70I2P105

Volume 70 Issue 2, 29-34, February 2022
© 2022 Seventh Sense Research Group®

Original Article

Electronic Card Fraud Detection System in Nigeria Financial Institution Using Hybrid Model Approach

Amaefule I. A[1], Chilaka U. L[2], Elei F. O[3], Ibebuogu C. C[4]

[1&4]Doctor of Philosophy, Department of Computer Science Imo State University, Owerri. Imo State, Nigeria
[2] Doctor of Philosophy, Department of Computer Science, Federal Polytechnic Nekede, Owerri. Imo State, Nigeria
[3] Doctor of Philosophy, Department of Software Engineering, Federal University of Technology Imo State, Nigeria

Received Date: 15 January 2022
Revised Date: 14 February 2022
Accepted Date: 27 February 2022

Abstract - *Speed and accurate customer authentication and confirmation have become essential in the growing electronic transactions. High acceptability and expediency of e-transaction for payments has given individual comfort to customers and as well created a centre of attention for a huge number of fraudsters. From every indication, the existing preventive and detection policies were not sufficient to stop the electronic fraud issues; it is uncertain if the key authorities in the financial industry took enough measures in responding to this notification. Therefore, the need to ensure secured transactions for electronic purchases for goods and services in a virtual environment is inevitable. The purpose of this paper is to develop an electronic card transaction fraud detection system for Nigeria financial institutions using the Hidden Markov model and Neural Network that could combine proof from ongoing and past activities profile of customer usage to establish the anomaly level of each transaction. However, the incidence of e-fraud in Nigeria is also discussed.*

Keywords - *Electronic Payment, Internal Control, Fraud Detection System, E-fraud, Authentication.*

I. INTRODUCTION

The intricacy and dependence by modern institutions on technology, including the rising simplicity right of entry to the net by all sundry, have fashioned more possibilities for scam and various types of deception, particularly on the web and various electronic terminals. Thus, electronic fraud /cybercrime are increasing significantly. The financial industries have been coming up with novel advancements to battle impostors in creating a safe environment for monetary transactions.

From holograms and tamper-evident signature panels to card authentication codes and EMV chips, lots of this safety advancement has developed into institution standards. It has been more than six years since the CBN launched the Cashless guidelines. Its plan was to promote the utilization of electronic methods for every financial transaction. The guidelines have produced dividends: they make several transactions easier and secure for more individuals. However, payment systems and banks have been experiencing a steady rise in fraud.

These crimes are accomplished using the information and communications technology that has flourished in Nigeria since the early 2000s. Electronic fraud is rapidly becoming an effective threat to the financial institution in Nigeria. There is an increase in e-fraud in spite of several endeavours to prevent cybercrime in the nation. It has become essential to evaluate and reinforce existing laws and pass new rules to curtail the dilemma.

With the present worldwide economic slowdown elicited by the declining and fluctuating crude oil price, security issues, as well as continued convergence in technology (e.g. mobile, social media, cloud, etc.), organizations are expected to improve their optimization efforts by continually seeking to build efficiency and effectiveness into their businesses and reduce wastage and mislaying's, because of fraud. These efforts involve optimizing the following, among others: Workforce, Vendors/Suppliers, Technology, Other key expenditure lines [1].

However, these optimization efforts by organizations have been perceived by a considerable number of employees and vendors as a threat to their jobs/contracts. Inherently, these efforts increase exposure to the risk of fraud, bribery and misconduct by workers and vendors and consequently prompt them to seek fraudulent means to secure their jobs or fraudulently acquire companies' assets before the perceived imminent loss of their jobs. It is therefore expected that occupational fraud and misconduct will continue to increase.

Illegal method of acquiring funds, assets belonging to banks and other financial establishments or fraudulently gaining access rights of a bank and posing as a financial institution in other to defraud depositors' funds is called bank fraud [2]

"However, there is need to focus on effective ways to reduce the incidence of e fraud by reviewing, strengthening existing and enacting appropriate security laws that guarantee safe online transaction for users and stakeholders". [3]

A. Aim and Objectives of the study

The research focuses on the development and enhanced web-based fraud detection, monitoring and real-time notification system in electronic card transactions adopting Hidden Markov Model and Neural Network.

a) The research objectives include

1. Study the degree of electronic fraud in the Nigeria Banking System.
2. Identify the security problems inherent in the transmission channel by reviewing the information sources for bank card deals.
3. Develop a security system that will promote trust in transmission channels using a hybrid technology of Hidden Markov Model (HMM) and Neural Network (NN) that could combine proofs from current and legitimate regular activities of the credit-card owner to authenticate the bank card transaction in arrangement to ascertain the suspicious level of every transaction.
4. Develop an alerting system in the real-time transaction for detecting and preventing credit card fraud.

B. Scope of the study

This study covers the detection and monitoring of fraudulent pursuits in electronic card transactions. It centres on a predictive model using Hybrid technology that scores every transaction with a high or low threat of fraud, and those with high threat generate notifications. The Hidden Markov Model performs interference on the current data to make predictions. The neural network checks those notifications and gives a response for each notification, i.e. true positive (genuine) or false positive (fraud). Also, confirmation code and personal security questions in addition; to geo-location, mobile phone number and electronic mail address will be captured. However, the delivery of a real-time notification system to allow financial bodies to discontinue or disengage financial transactions identified to be fraud will also be captured.

C. Significance of the Study

If fraud detection methods can be improved, then fraud can be reduced, which produces a few benefits – apart from reducing financial losses sustained from fraud, it will also have the effects of increasing the confidence of electronic card users and increasing acceptance and application of e-commerce systems. This research will provide an improved comprehension of fraud recognition methods that have been evaluated by experts in the discipline of auditing and will produce a continuous assurance system that can be utilized as a tool in future research.

With a hybrid technology fraud recognition system in place to check unusual transactions, the workload is distributed among the techniques; thus, a search is faster and blocks any transaction identified to be fraudulent. This allows auditors to better meet their responsibilities in identifying fraud and irregularities induced by fraud and its negative effects on business by presenting to them a tool that can manage fraud detection.

II. INCIDENCE OF ELECTRONIC FRAUD IN NIGERIA FINANCIAL INSTITUTIONS

The emergence of virtual banking made it feasible for individuals to perform monetary transactions online. However, like the preponderance of high-quality kinds of stuff, its exploitation is virtually expected. Nigeria's electronic fraud is the obvious misuse of e-payment and banking. The acceptance of virtual banking terminals and the fast development of the e-terminals ecosystem raised the circumstance of electronic financial fraud [4].

As e-payments attain huge new customer populations, cyber fraudsters are bringing out progressively inventive means to pilfer your funds. The Nigerian banking industry has disclosed a steady acceptance of electronic remittance terminals. The parties involved and the entire actors in the banking sector have been building intensive attempts the make sure the financial sector is following the current international trends in electronic remittance progression with the vision to ensure effectiveness in the system and also customer satisfaction. The acceptance of the e- remittance terminals as an ideal channel of transactions raises the emergence of electronic scams.

[5] Highlighted the gravity of this issue recently when it revealed an N2.19 billion loss by the nation's financial sector to virtual fraud in the 2016 fiscal year. There were 19,531 reported cases in 2016, compared with 10,743 in 2015. This is an 82 per cent rise in e-fraud cases between 2015 and 2016. The number may even be higher.

[6] The account revealed various sections of the financial sector where the frauds occurred and the value of losses documented. A breakdown has shown that over the counter dealings has the highest recorded fraud with N511.07 million values; this was preceded by (ATM) Automated Teller Machine operations with N464.5m; mobile transactions, N235.17m; and Online banking N320.66m. Other losses came from electronic commerce transactions, N132.25m; web transacts N83.77m; cheques, N4.55m; booths, N10.19m; and others, N190.97m.

The statement pointed, “Based on happenings and human view, it is presumed that fraud incidence increase heading to the yearend owing to revels…and the quest for individuals to acquire more funds.” Nevertheless, fraud can happen at any time, as affirmed by the report, and thus, called for "preventive and identifying policies".

From every indication, the existing preventive and identification policies were not enough to stop the electronic fraud issues. For example, between the years 2000 to 2014, the Nigerian financial industry lost a bulky N199bn, mostly caused by improper and irresponsible management of clients' data, according to a security evaluation performed by Easy Solution Limited, a global electronic fraud protection firm. Electronic fraudsters had attacked financial institutions in Nigeria, creating more than 185 forged mobile applications on sites of 15 financial institutions, which they are using to extract clients' private and financial details with the intention to defraud.

It is uncertain if the key authorities in the financial industry took enough measures in responding to this notification. The details further disclosed that the financial sector would encounter what it described as “defacement assaults” on their sites. Other techniques of assaults, the details revealed, comprise electronic mails with the aim to pilfer financial records, electronic mails spamming, aiming both financial institutions’ and clients’

Moreover, in 2015, [7] cautioned that phishing and staff transactions continue to produce the main cyber risks to the financial institution in Nigeria, particularly as crude oil values depreciate continually in the international market. Also, the [8] on their Electronic Payment Fraud Landscape account formerly disclosed eighty-five (85%) per cent attainment in scam attempts, spotting Automated Teller Machine dealings as the most susceptible to electronic fraud. However, there is no refusal of the grave dangers these fraudulent activities have posed to the stability of Nigeria's financial industry. Consequently, it is imperative that regulatory bodies and the financial industry start to take cautions to contain electronic fraud critically and take required actions to prevent them.

Though the emergence of virtual banking has made it probable to perform online banking transactions with much ease, particularly in this period of cashless rule, it has been subjected to misuse, with the increasing occurrence of cybercrimes. More awareness is required on how to decrease cyber fraud and electronic banking crime, which, if not efficiently contained, might decrease public self-assurance in the banking industry.

According to the [9] annual report, Fraud issues in the financial industry in 2015 climbed by 15.71%, “a total of 12,279 fraud instances were reported, signifying a surge of 15.71% above the 10,612 scam issues revealed in 2014. However, the amount involved decreased significantly by ₦7.59 billion or 29.63% from ₦25.608 billion in 2014 to ₦18.021 billion in 2015.” Similarly, "the actual loss suffered by the insured banks decreased. By ₦3.02 billion or 48.79% from ₦6.19 billion in 2014 to ₦3.17 billion in 2015.” The report apprises that the real loss upholds in deference to online banking scam was ₦857 million, standing for 27% sum of real loss of the sector.

There was a regular occurrence of Card linked / Automated Teller Machine Fraud issues from 7,181 to 8,039 (in 2014 to 2015, respectively), an increment of 11.95%. However, the loss experienced by the sector owing to such scams reduced appreciably by 59.4% from the previous year's number of ₦1.242 billion to ₦0.504 billion, standing for 15.9% of the entire sector loss. To deceptions and forgeries."

Deposit Money Banks (DMBs) revealed that 425 instances of fraud were credited to employees in the 12,279 cases of fraud disclosed. The figures have reduced from 465 in 2014 to 425 in 2015 of scam cases committed by employees. Equally, from N3.165 billion in 2014 to ₦0.979 billion in 2015 of losses occurring has considerably reduced by 70%. The most proportion of deceptions and scam cases of 38.59% were committed by provisional personnel,

In a report released by [6], over ₦4 billion was lost to cases of virtual fraud in 2015. Similarly, data released by [10] disclosed that in 2015 a loss of $450 million and 3,500 electronic scams with 70% attainment rate.

As appalling it may appear, there is a strong view that the undisclosed cases exceed the disclosed cases of electronic fraud committed in the financial institution. More than ₦30 trillion in dealings is allegedly performed on different electronic payment terminals by merchants and customers in the nation, yet uncertainties over issues of electronic scams remain on the rise.

Altogether, it shows the supposed increase in electronic fraud invalidates every attempt to prevent it before it happens. There are sure plans made available intended to eradicate the plague of electronic fraud, but, numerous motives, they are not effectual as anticipated.

Reviews of trends all around the globe indicate that e-fraud is still largely driven by domestic transactions. This compelled the establishment of an industry agency (E-PPAN), Electronic Payment Providers Association of Nigeria, to deal with e-fraud in the country. However, the preference for a collaborative effort in combating e-fraud means a setback in execution; since every member of the organization has to play a causative part.

[11] The social media platform has developed into simple explorable, which imply that imposter will be able to effortlessly and incognito look for pals, locality, photos, status, video etc. of the innocent individual on social media, put up details of their possible preys and then assault.

Erroneously, some organizations perceive cyber-crime / virtual fraud as a technology issue only and therefore look only at technology to reduce the menace of cyber criminals instead of looking at conventional swindlers involving People, Process and Technology issues. CBN has put into operation numerous programs in dealing with the difficulty of electronic fraud and cybercrime exclusively and scams in general. The programs comprise:

1. Execution of two-factor authentication for internal financial procedures, which commenced in January 2014.
2. Evaluation of procedures of the NIBSS' Instant Payment (NIP) System and additional e-Payment alternatives with similar characteristics
3. Establishment of industry fraud desk
4. Bank Verification (BVN) introduction
5. Deployment of the Central Anti-Fraud Solution

It is very important to state that impostors and cyber swindler are changing their patterns and techniques in the Internet of Things (IoT) and cloud. This is in reaction to the pace at which businesses and consumers are moving to the cloud because of its cost efficacy and "almost stress-free" lives enjoyed by consumers as a product of IoT, gaining mileage. To firmly avert the incidence of fraud on cloud communications and hacks into customer devices, organizations call for sufficient security from the cloud infrastructure and service providers as well as demand that manufacturers of IoT devices improve security on central servers in place of individual devices.

III. LITERATURE REVIEW

[12]; Stated that, at present, it is simple to conduct monetary transactions virtually, either on a computer or through cell phone; however, the financial institution – service rises and put into operations in multi-channels it creates an easy avenue for fraudsters to perform financial scams. In their research, they discovered the need to concentrate on investigating log-files from a Mobile Money system, and that makes it feasible to do banking transactions with a mobile phone. They developed a system whose main purpose is to assess whether it is probable to combine two statistical methods, Benford's law together with statistical quantities, to find a statistical way to find fraudsters within a Mobile Money system. To accomplish this, rules were laid hold of from the research with a focus on a Mobile Money system, and limits were computed with quantiles. A fraud detector is applied that employ these rules jointly with limits and Benford's law in order to identify fraud. The fraud detector utilized the techniques both separately and jointly. In conclusion, the outcomes achieved disclosed that it is probable to employ Benford's Law and statistical quantiles within the considered Mobile Money system. It' as well demonstrates an extremely little disparity when the two techniques are joint together or not, whether in discovery rate and accuracy (Precision!). Meanwhile, [12]; concluded that by putting together the selected techniques, it is probable to obtain an average-high true positive rate and extremely low false-positive rates. The major effectual technique to discover swindlers is by only using quantiles. However, [13] concluded that by combining the chosen method, it is possible to get medium-high true positive rates and very low false-positive rates. However, its limitations are one variable at a time, unable to match symptoms with a specific type of fraud and do not apply to all numeric populations.

[14]; Achieve a better fraud discovery using data mining tools such as neural networks and clementine. [15], Recommended a financial establishment having knowledge of fraud behaviour in a distributed environment using data mining techniques combination. [16] proposed a combination of two methods employing the hidden Markov model on the spending pattern and mobile implicit authentication system, which achieved fewer chances of authentic cardholders being treated as fraud (false positive). [17] Presented a multi-agent model which analyzes input from the user by monitoring, collating, diagnosing and reporting whether the transaction is genuine or fraudulent. Any significant deviation from the normal behaviour indicates potential fraud [18].

[19]; Proposed a credit card fraud discovery model using Hidden Markov Model. (HMMs) Hidden Markov Models is a statistical tool and a very potent technique employed for creative modelling sequences typified by a set of visible sequences. Hidden Markov Model is possibly the straightforward and uncomplicated model which can be employed to model chronological data, specifically, data samples that are reliant on themselves. An HMM is a dual fixed arbitrary procedure with two separate levels, the first is concealed, and the second is open to everyone. The Hidden Markov Model is a finite set of states, each of which is linked with a likelihood distribution. Transition probabilities are the Changes (Transitions) between the conditions that are ruled by a set of likelihoods. In one state, a result of observation can be generated according to the related likelihood distribution. It is just the result, not the state noticeable to an external spectator; thus, states are 'hidden" to the external; Its major setbacks are not scalable to large size data sets, and the speed of the software can be enhanced by the implementation of algorithms of less complexity.

[20]; Employed records from a cardholder financial institution, a fraud identification system based on the neural network was trained on a huge data of tagged credit card record transactions and examined on a present data set that contained every account transaction over a succeeding two months period. Instances of fraud owing to cards lost, email-order fraud, counterfeit fraud, stolen cards, non-received issue (NRI) fraud and application fraud was what the neural network was trained with. A three-layered feed-forward network with only two training passes of neural network system was utilized to accomplish a fall of twenty to forty per cent (20 - 40%) of entire fraud losses in credit cards. This technique as well drastically abridged the enormous analysis work by the fraud analysts, but the main flaws of the system are it is hard to train: training outcome can be nondeterministic and depend crucially on the choice of initial parameters; it has overfitting problems, the high processing time for large neural networks, excessive training

[21]; Evaluated the effects of the performance of group distribution on a training set using several classifiers on the card fraud sphere. It was established that a rising number of minority cases in the training procedure bring in a smaller number of losses as a result of fraudulent dealings. Furthermore, ten to ninety per cent (10% - 90%) for training differed during fraud distribution, and it was established that during which the fraud percentage employed in training was 50% highest reductions were accomplished. The flaws of the system are; it suffers from the issue of incomplete or noisy data, and excessive training is required

IV. DATA COLLECTION TECHNIQUES

In this research, data were collected from various secondary sources such as (CBN) Central Bank of Nigeria, documents/archives which includes Annual Reports and Statements of Account, also from (NDIC) Nigeria Deposit Insurance Corporation, professional Pronouncement of Chartered Institute of Bankers of Nigeria, (NEFF) Nigeria Electronic Fraud Forum Stakeholders, (NIBSS) Nigeria Interbank Settlement System, (KPMG) Klynveld Peat Main Goerdeler Nigeria, research journals, newspapers, magazines and the Internet. However, the secondary information collected was very useful for easy trend analyses and relevant to predicting future occurrences of fraud.

V. METHODOLOGY ADOPTED

The Neural Network, Hidden Markov model and Object-Oriented Analysis and Design Methodology (OOADM) was adopted:

A. Neural Network will provide an effective method for systematic checking of electronic card fraud transactions in financial establishments to identify and alert the administrator of any unusual monetary operations that might indicate a high-risk fraud and various financial abnormalities. Such authentication tasks involve fraud discovery and electronic card monitoring. However, the neural network is appropriate in managing the difficulty of monitoring huge volumes of active records in a distributed style; thus, they are to discover concealed monetary problems, which consist of financial fraud, manage risks, and other abnormalities, by employing a group of data engines, each performing a detailed function separately, electronic card authentication and monitoring methods will be capable of analyzing electronic card excellently through the exchange of information concerning the individuals involved.

B. The hidden Markov model through the data engines (customer, bank and fraud databases) will help to generate confirmation code for the customer as well as help the financial institution to ascertain the fraudster that committed electronic card fraud. However, it assists to envisage when the card can no longer pay, and it utilizes the electronic card to ascertain and evaluate the activities and consistency of the customers. With the data engines, the Hidden Markov model can assist the financial institution do systematic profiling and placing of their local offices regarding electronic card fraud threats. To achieve this process, germane information can be congregated from the card risk record databases. These records hold all the necessary information related to electronic card fraud, which includes different distinctiveness such as cardholder’s identity, location of the local office of the financial institution that issued the card and where the modification of the electronic cards are executed.

C. Object-oriented analysis and design methodology (OOADM) was adopted in this paper is a popular methodological method for analyzing and designing an application, system, or business by applying object-oriented programming, in addition to using visual modelling all through the development life cycles to promote improved stakeholder communication and product quality; It utilizes a formal, methodical method to the analysis and design of information system. Object-oriented design (OOD) expands the analysis patterns to generate implementation requirements. The major disparity among object-oriented analysis and other kinds of methodology is that the object-oriented approach organizes requirements around objects that incorporate both behaviours (processes) and states (data) modelled after real-world objects that the system interrelates with.

VI. CONCLUSION

Neural Network and Hidden Markov Model can play an essential role in the virtual card fraud recognition domain. A conceptual structure for a hybrid method based on Electronic Card Fraud Detection (ECFD) process is developed, which a hybrid technique are proposed to provide a group of functionalities for ECFD in an electronic transaction environment for financial institutions. The research presented the following contributions to knowledge; design of data and expert-driven electronic card fraud discovery technique using hidden Markov model and neural network; design of virtual card fraud recognition hybrid architecture and design of fraud discovery alert. A hybrid approach is employed to develop the electronic card fraud discovery system that utilizes both hidden Markov model and neural network approaches to achieve a synergy that better handles the Nigeria electronic card fraud situation using a hybrid approach instead of the two-stage model normally employed in fraud discovery algorithm. This ensured accurate, reliable results and reinforced the validity and efficiency of the hidden Markov model and neural network as a research tool and laid a solid groundwork for intelligent detection methodologies designated in an operational electronic fraud discovery system.

REFERENCES

[1] KPMG (Klynveld Peat Main Goerdeler Nigeria): Top Five (5) Fraud Trends in Nigeria’s Commercial Banks in 2016 – Part I &II. KPMG. http://www.blog.kpmgafrica.com/category/kpmg-nigeria

[2] Siklos, & Pierre., Money, Banking, and Financial Institutions. Canada in the Global Environment. Toronto: McGraw-Hill Ryerson, 40 (2001)

[3] Amaefule I.A, Onu F.U: Prevalence of Electronic Fraud in Nigeria Banking System. International Journal of Computer Trends and Technology (IJCTT) 67(3) (2019). ISSN: 2231 – 2803. https://www.ijcttjournal.org

[4] Ifeanyi Ndiomewese.: How e-fraud can be tackled to reduce losses in Nigeria. Techpoint. Ng. (2016). http://www.techpoint.ng/authors/ifeco3show

[5] Central Bank of Nigeria (CBN):. Annual Report and Statement of Accounts. Central Bank of Nigeria. (2016) https://www.cbn.gov.ng/Documents/cbnannualreports.asp

[6] NEFF: Nigeria Electronic Fraud Forum: A Changing Payments Ecosystem: The Security Challenge. NEFF. (2016) http://www.cbn.gov.ng/Out/2017/CCD/A%20CHANGING%20PAYMENTS%20ECOSYSTEM%20NeFF%202016%20Annual%20Report.pdf

[7] Deloitte Cybersecurity Concern for Nigeria, (2015). https://techcabal.com/2015/03/19/deloittes-expose-on-cyber-security-concerns

[8] NIBSS (Nigerian Interbank Settlements System): E-payment Fraud Landscape Report. (2014), https://www.nibss-plc.com.ng/reports/2014-fruad/report

[9] NDIC: Nigeria Deposit Insurance Corporation: Annual Report and statement of Account. NDIC. (2015) https://ndic.gov.ng/ndic-releases-2015-annual-report/

[10] NITDA - Nigeria Information Technology Development Agency 2015.https://nitda.gov.ng

[11] Nigerian Cyber Threat Barometer Report (2014). https://www.wolfpackrisk.com/.../nigeriancyberthreatbarometer_2014 (med_res).

[12] Kappelin, F. & Rudvall, J: Fraud Detection within Mobile Money: A Mathematical Statistics Approach. MSc Thesis Submitted to the Dept. Computer Science & Engineering Blekinge Institute of Technology, (2015). SE-37179 Karlskrona Sweden. http://www.diva-portal.org/smash/get/diva2:865559/FULLTEXT02

[13] Kovach, S., & Ruggiero, W. V. (2011): Online BankingFraud Detection Based on Local and Global Behavior ICDS The Fifth International Conference on Digital Society, (2011).

[14] R. Brause, T. Langsdorf, and M. Hepp, ―Neural Data Mining for Credit Card Fraud Detection, | Proc. IEEE Int’l Conf. Tools with Artificial Intelligence, (1999) 103-106.

[15] C. Chiu and C. Tsai, ―A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection, ‖ Proc. IEEE Int'l Conf. e-Technology, e-Commerce and e-Service, (2004) 177-181.

[16] Sandeep Pratap Singh, Shiv Shanker P. Shukla, Nitin Rakesh and Vipin Tyagi Problem Reduction in online Payment System Using Hybrid Model, International Journal of Managing Information Technology , (2011). Doi.10.5121/ijmit_2011.3306.sourceDBLP

[17] Amanze B.C and Chinwe Onukwugha 2018 . An Enhanced Model for Bank Fraud Detection in Nigeria; International Educational Journal of Science and Engineering (IEJSE), EISSN No: 2581-6195, 1(5) (2018).

[18] Murad, U., & Pinkas, G. (2009). Unsupervised profiling for identifying superimposed fraud in proceedings of the 3rd European Conference on Principles of Data Mining and knowledge discovery, (2009) 251-266.

[19] Khan, A .P., Mahajan, V. S., Shaikh, S. H & Koli, A. B: Credit Card Fraud Detection System through Observation Probability Using Hidden Markov Model, International Journal of Thesis Projects and Dissertations (IJTPD), 1(1) (2013) 7–16.

[20] Ghosh, S., & Reilly, D. L: Credit Card Fraud Detection with a Neural- Network. Proceedings of the International Conference on System Science, (2004). 62–71. https://www.sciencedirect.com/science/article/pii/S1877050920306840

[21] Stolfo S.J., Fan D.W., Lee W., Prodromidis A.L., & Chan P.K: Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results. Proc. AAAI Workshop AI Methods in Fraud and Risk Management, (1997) 83–90.