Neuro-Fuzzy Models for Electronic Banking Fraud Detection and Prevention: A Review of Recent Advances

***Mohammed Usman[1], Etemi Joshua Garba[2], Usman Idris Ismai'il[3]**

[1, 2]Department of Computer Science, Modibbo Adama University, Yola, Nigeria

[3]Department of Computer Science, Federal University of Kashere, Nigeria

***Corresponding Author**

DOI: https://doi.org/10.51584/IJRIAS.2024.907037

Received: 01 July 2024; Accepted: 11 July 2024; Published: 13 August 2024

ABSTRACT

Online payments have evolved over the years. Today, more people are choosing electronic payments platforms over method traditional banking. From POS, mobile banking, to virtual banking services, there are lots of trends to facilitate seamless payments for customers. However, electronic fraud is affecting Nigeria's financial system, costing the economy dearly and holding back the adoption of cashless technologies due to rise in fraudulent activities. This work focused on informing and helping the public to understand payment fraud issues occurring on various channels, as well as aid financial institutions with more effective fraud monitoring and preventive measures to combat the fraud. In this study, five feature of electronic banking transaction were selected and used to obtain universe of discourse, membership functions and their linguistic variables for the fuzzy system and are classified based on ANFIS to allow an E-banking fraud detection system to test and classify transactions as fraudulent or safe.

Keywords: Fraud, Neuro-Fuzzy, Transaction, CVV, Rationalization

INTRODUCTION

Electronic fraud is a significant issue in Nigeria, as it is in many other countries. Nigeria has gained a reputation for being associated with certain types of electronic fraud, including various email scams, phishing attacks, and advance-fee fraud schemes. It's important to note that while these types of fraud do occur in Nigeria, they are not exclusive to the country, and there are many legitimate and law-abiding individuals in Nigeria. It's important to approach electronic communication and online transactions with caution, regardless of the location of the individuals involved. Because electronic fraud is growing rapidly due to advancement in technology. Data shows that in 2016, electronic fraud accounts for more than 50% of total fraud in the Nigerian financial service industry. Due to this, customers who already have a bank account are reluctant to adopt digital platforms, which became an obstacle to drawing customers who don't have bank accounts into the financial system.

Irawan, Hidayat, and Wibowo (2017) explained that Internet banking, POS, ATM, and mobile payment systems have accelerated the growth of fraudulent activities, given more room for sophisticated electronic fraud. They found that 40.5% of fraudulent banking transactions were committed on the digital platforms. Additionally, fraudulent mobile banking transactions were responsible for loss of over ₦500m between 2015 and 2016.

Gosh and Roy (2021) stated that electronic banking has grown to such a large extent that most customers rely on it for their needs, becoming a great boon to the modern world as an easy way of life. As banking increasingly become digital, a growing number of financial transactions are conducted online. Fraudsters have been quick to adapt, and to devise clever ways to defraud online payment platforms. While this type of activity usually involves group of fraudsters, a well-educated fraudster can create a number of synthetic identities on his own, which he then uses to carry on different fraud, or devise a new fraudulent scheme. This puts many financial institutions and customers in trouble. Therefore, efficient way of fraud monitoring is very much necessary.

Yang, Li, Zhang, and Wang (2021) asserted that fraud inflicts substantial economic damage. More so, the perpetrators of fraud play a dynamic cat and mouse game with those trying to stop them. Preventing a particular kind of fraud does not mean the fraudsters give up, but merely that they change their tactics: they are constantly on the lookout for new avenues for fraud, and new weaknesses in the system to perpetrate their game plan.

Zhang, Lu, and Chen (2021) believed that "due to the fact that our social and financial systems are forever developing, there are always new opportunities to be exploited. Fraud can result in significant financial losses for individuals and businesses alike, and can also have a negative impact on the overall trust and confidence in electronic banking systems, it will tarnish brand image, cause attrition in customer base and diminish customer loyalty".

LITERATURE REVIEW

Fraud is an intentional deception or misrepresentation made by a person or entity with the purpose of gaining an unfair advantage or causing harm to another person or entity. This can involve financial theft, making false statements, concealing important information, or manipulating documents or data.

According to Bart, Vlasselaer, and Wouter (2015):Fraud is an uncommon, well-considered, imperceptibly concealed, time-evolving and often carefully organized crime which appears in many types of forms.

Chen and Liu (2020) noted that traditional fraud detection methods often rely on rule-based systems, which can be inflexible and may miss subtle changes in fraudulent behaviour. Additionally, these methods may be prone to false positives or false negatives, leading to inefficient use of resources. It is therefore important to regularly monitor account activity, and be wary of suspicious emails or requests for personal information.

This study focused on informing and helping the public understand payment fraud issues. The aggregated data will also inform consumers and businesses on how fraud occurs using various channels, as well as aid financial institutions with more effective fraud trend monitoring and preventive measures to combat the fraud.

In this study, five feature of electronic banking transaction were selected and used to obtain universe of discourse, membership functions and their linguistic variables classified based on ANFIS to allow an E-banking fraud detection system to be tested and classify transactions as fraudulent or safe. The dataset was collected from NIBBS, CBN and banks statistics and publications of two Commercial banks and two other financial institutions in Nigeria. It consists of fraud trends records between 2015 and 2020 from Fidelity bank, United Bank for Africa, Monie point and Opay. Interview, questionnaire and survey data was used as instruments to collect data while split half internal consistency reliability method was adopted to determine the reliability of the instruments.

The study attempts to gauge the trends and the challenges associated with E-banking fraud, and to provide more effective fraud trend monitoring. If we cannot stop fraud altogether, an awareness of the contents of this thesis will at least enable readers to reduce the extent of fraud, and make it harder for criminals to take advantage of the honest. The readers' organizations, be they public or private, will be better protected if they implement the strategies described in this thesis. In short, this thesis is a valuable contribution to the well-being of society and of the people within it.

Motives for Committing Fraud

There are wide set of techniques and approaches used by fraudsters as well as to the many different settings in which fraud occurs or economic activities that are susceptible to fraud.

Duman and Hamdi (2011) explains three factors that forms the reasons individuals commit financial fraud, which are; pressure, opportunity and rationalization.

Pressure is a contrasting force or impulse such as poverty, taxes, loan or problem of finance, social, or any other nature.

Ahmed, Maniraj, Saini, and Sarkar (2019) believed that a non-shareable problem, such as a gambling debt, medical expense, or money needed to finance an expensive lifestyle, is a common source of pressure. Pressure can also come from within the business, family members or from investors, in the form of performance pressure or the need to hide unfavourable outcomes in order to appear good.

Opportunity is the favourable circumstance for an individual to be able to commit fraud. Fraudulent activities can only be committed when the chance for advancement exists

Shah, Mahmood, and Tanwari (2018) explained that when an organization’s employees break trust, the opportunity is frequently far clearer than the pressure. Employees must have a certain degree of trust in order for any business to function, but this trust will be balanced by an efficient fraud detection system.

Rationalization is the psychological mechanism that explains why fraudsters do not refrain from committing fraud and think of their conduct as acceptable.

Chen, and Liu (2020) stated that rationalization is frequently used as an explanation for committing fraud. In many circumstances, fraudsters excuse their actions by claiming that they are merely borrowing money from the organization on a temporary basis. In other circumstances, con artists justify their actions by saying things such, “They won’t miss the money,” or “They deserve what they’re receiving.”

The fraud triangle as depicted in Figure 2.1 provides a more elaborate explanation for the underlying motives or drivers for committing fraud as explained above.

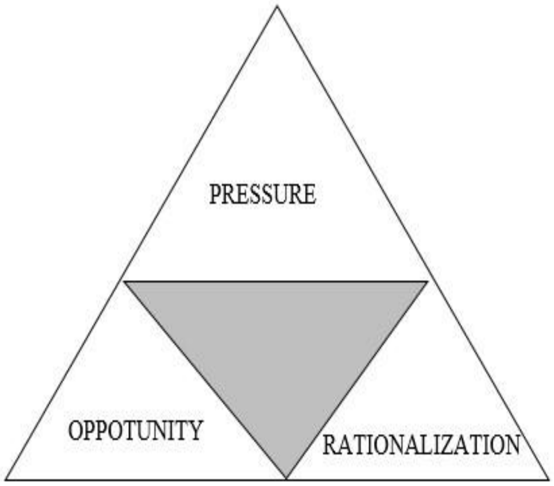


Figure: 2 Fraud Triangle (Duman & Hamdi, 2011).

The Fraud Diamond Theory

The Fraud Diamond Theory was first presented by Wolfe and Hermanson in December 2004. It is viewed as an expanded version of the fraud triangle. In this theory, an element named capability has been added to the three initial fraud components of the fraud triangle.

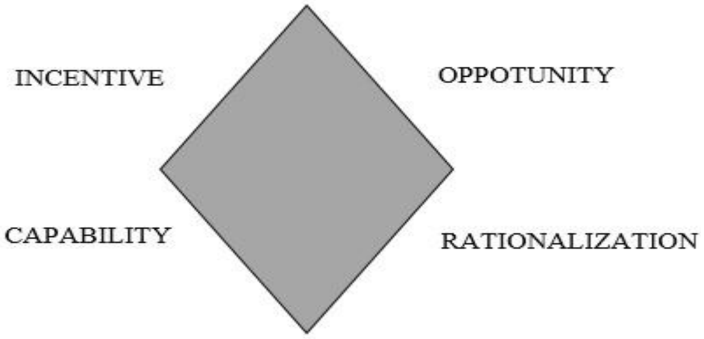


Figure 1: Fraud Diamond (Wolfe and Hermanson, 2004).

Fraud Pentagon (Crowe's fraud pentagon)

Fraud pentagon was introduced in 2011 by Crowe Howarth. Here, an element called arrogance was added to further elaborate the concept of fraud diamond. The elements of the fraud pentagon as proposed by Crowe are; Pressure, opportunity, rationalization, competence and arrogance.

Arrogance is the attitude shown by subjects who consider themselves the most superior, powerful, smart and great of the other party. The nature of arrogance is often attached to individuals who are in the top positions, brilliant careers or the rapid development of the business pioneered them to commit fraudulent act.

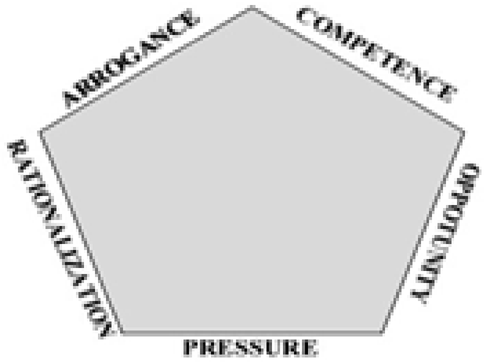


Figure: 3 Fraud Pentagon (Crowe, 2011)

Types of Electronic Banking Fraud

There are different forms of fraud, some common types are hereby highlighted below;

Card fraud

The leading source of fraud is automated teller machines (ATMs) where cards are compromised or swapped. Cards are swapped mostly at ATM galleries where illiterate account holders ask for help when trying to make withdrawals. The “helper” may have an expired ATM card and, in the process of offering assistance, swaps the victim’s card with a non-functional card. ATM fraud is also carried out by people very close to the victim including spouses, boyfriends and friends. Some common credit card fraud subtypes are counterfeiting credit cards, using lost or stolen cards, or fraudulently acquiring credit through mail or telephone conversation with the card holder.

Two subtypes have been identified, as described by Duman and Hamdi (2011) include;

(1) Application fraud, involving individuals obtaining new cards from issuing companies by using false personal information, and then spending as much as possible in a short space of time.

(2) Behavioural fraud, where details of legitimate cards are obtained fraudulently and sales are made on a "Cardholder Not Present" basis. This does not necessarily require stealing the physical card, only stealing the card credentials. Behavioural fraud concerns most of the card fraud.

Account Opening Fraud

Zhang, Lu, and Chen (2021) stated that this entails fraudsters opening new accounts by either impersonating legitimate customers or using stolen (or synthetic) identities to obtain credit. For instance, Paypal is a major victim of account opening and on boarding fraud. In 2021, the company identified over 1 million fake accounts, which directly resulted from their incentivized customer acquisition strategy. PayPal offered $5 or $10 to customers who signed up for PayPal, automatically attracting fraudsters who used large-scale bot networks to visit the registration site.

It's important to note that Paypal is an e-wallet provider. But with neobank accounts holding more value than e-wallets, Paypal's example highlights the extent of vulnerabilities all fintech might be exposed to.

Account Takeovers

Account takeover (ATO) fraud involves a criminal gaining unauthorized access to a user's account and using it for some type of personal gain. For instance, a fraudster may take over a social media account and invent a reason to request money from family and friends of the victim. Sometimes, bad actors dupe your company by leveraging phishing and hacking to access users' accounts. Once in the account, the scammer can spend the money within, change the credentials to lock the legitimate user out, or put the credentials up for sale on the dark web.

Cheng and Wang (2021) explained that account takeovers (ATOs) pose a significant risk to your digital bank. According to survey conducted by Aberdeen Group, 84% of fintech companies experienced account takeovers in 2021, costing up to 8.3% of their annual revenue.

Fraudulent Fund Transfers

This occurs whenever fraudsters use an emulator or app cloners to make a bank transfer or top up an account. This digital bank fraudulent scheme is often put in motion in order to launder money. Additionally, there are cases where a scammer will open a legitimate-looking account to receive deposits for promised service or product they'll never deliver.

Identity Theft

The crime of obtaining the personal or financial information of another person for the purpose of assuming that person's name or identity in order to make transactions or purchases. Some identity thieves sift through trash bins looking for bank account and credit card statements; other more high-tech methods involve accessing corporate databases to steal lists of customer information.

Phishing

Phishing involve using fake mail, name, mobile phone number, address or website for fraudulent purposes, they are send to customers that look as if it is from their bank. This will eventually make clients to divulge their account security information. A person's personal details are obtained by fraudsters posing as bankers, who float a site or SMS similar to that of the person's bank. They are asked to provide all personal information about themselves and their account to the bank on the pretext of database upgrade. The number and password are then used to carry out transactions on their behalf without their knowledge.

Gosh and Roy (2021) believed that a phishing email will typically ask an online banking customer to follow a link in order to update personal bank account details. If the link is followed, the victim downloads a program which captures his or her banking login details and sends them to a third party.

Click Fraud

This is an illegal practice that occurs when individuals click on a website’s click-through advertisements (either banner ads or paid text links) to increase the payable number of clicks to the advertiser. The illegal clicks could either be performed by having a person manually click the advertising hyperlinks or by using automated software or online bots that are programmed to click these banner ads and pay-per-click text ad links.

SIM Swap fraud

This occurs when the phone number of a customer is hijacked through fraudulent SIM replacement at a bank premise or Telecommunication outlet/agent. The perpetrator then uses the mobile line to access the account of the victim and conduct all banking services including payments for goods and services and transfer of the fund to another account usually via mobile banking.

Triangulation schemes

This may take any of the form of; Skimming, site cloning, or vishing. In skimming, the actual data on a card is electronically copied to another. It is very difficult for cardholder to identify this type of fraud. In Site Cloning, the fraudster clones an entire site or just the payment page of the site where customer make a payment. Customer feels that they are viewing the real site. The customer handover a credit card detail to the fraudster and then fraudster sends the customer a transaction receipt via email as real site. Thus fraudsters have all detail of customer credit card so they can commit fraud without customer’s awareness. In vishing the e-fraud perpetrator sends text messages to defraud victims of e-fraud. Often, the text message will contain a phone number to call and once the victims call the number it would provide a ground for the e-fraud perpetrator to ask for confidential information of the unsuspecting victims. Also, it is vishing when the e-fraudsters use the hidden phone number to call the victims for sensitive information.

According to Ahmed, Maniraj, Saini, and Sarkar (2019) the various forms of fraud are committed in one of the following ways;

Outsider fraud committed by fraudsters external to the banking system that have internet dexterity and sometimes an understanding of the victims’ routine and identity.Insider fraud that is executed exclusively by staff members in the banking system. This is determined by the jobs they do and an understanding of the system. Here the banking institution is the victim. Collaborative fraud that involves bank staff and fraudsters outside the banking system. Here both the bank and individual account holders are victims.

Fraud Challenges for the Financial Sector

Strictly speaking, fraud detection focuses on identifying fraudsters’ attempts while fraud prevention is all about preventing them, but the two are practically interchangeable in reality, as these strategies go hand in hand. Financial institutions are mostly targeted by fraudsters, due to their immediate access to funds and their ability to transfer them.

Research Gap

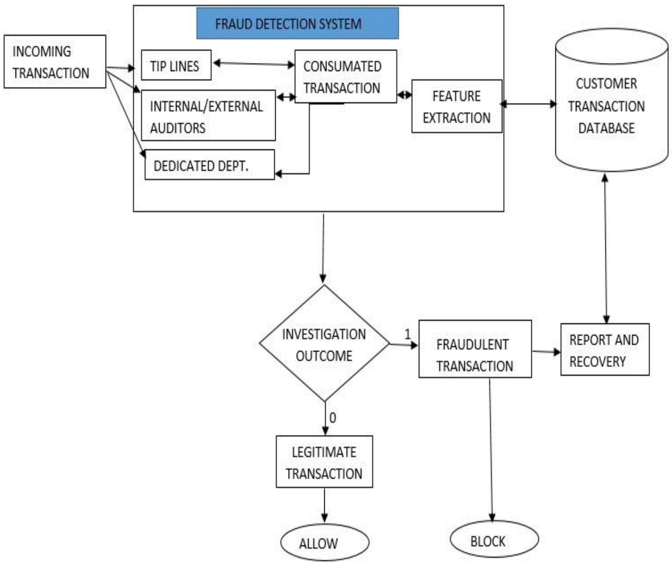
Most of the reviewed work laid emphasis on credit card transactions only, the size of datasets is mostly imbalanced. They do not include insurance and electronic commerce transactions. More so, most of the reviewed work does not focus on Nigeria’s financial sector. Additionally, the data outliers show that banks in

Nigeria have limited access to data points because they do not use machine learning algorithms for fraud data enrichment in real-time.

METHODOLOGY

The Existing Fraud Detection System in Nigerian Banks

Presently, the successful ways to identify fraud in banks include; using an anonymous tip line, also known as whistle blowing, using internal and external auditors during their periodic audit, using a dedicated department or detection by accident. The fraudulent transaction is usually detected by close monitoring in relation to the customer transaction history or spending pattern. Once a transaction is discovered fraudulent, the bank immediately blocked the transaction or the customer account or channel involved. In a situation where funds are taken away, a recovery management is enforced to recover the lost fund as quickly as possible.



i. **Changing fraud patterns over time**: Fraudsters are always in the lookout to find new and innovative ways to get around the systems to commit fraud. Thus it becomes all-important for the system to be updated with the evolving patterns to detect the fraudulent tendencies. The current system is inefficient to address this problem. Thus the machine learning or ensemble models need to be employed.

ii. **Class Imbalance**: Practically only a small percentage of customers have fraudulent intentions. Consequently, there’s an imbalance in the classification of the existing fraud detection system (that usually classify transactions as either fraudulent or non-fraudulent) which makes it harder for the banks. The fallout of this challenge is a poor user experience for genuine customers, since catching the fraudsters usually involves declining some legitimate transactions.

iii. **System Interpretations**: This limitation is associated with the concept of explain ability since the detection systems typically give a score indicating whether a transaction is likely to be fraudulent or not, the interpretations may sometimes be subjective from the experts and there may be the possibility of human error.

The Proposed Neuro-Fuzzy Model

The study was carried out to employ Neuro-fuzzy model for detection and prevention of electronic banking fraud using adaptive neuro-fuzzy inference system. In this model, six features of an electronic transaction were selected, each having three fuzzy logic membership functions and at least three linguistic variables as inputs to a Fuzzy Inference System (FIS). The fuzzy outputs are taken as neural inputs to determine the sub-blocks, with which the neural network is executed to make decisions about the likelihood of a transaction being fraudulent or safe.

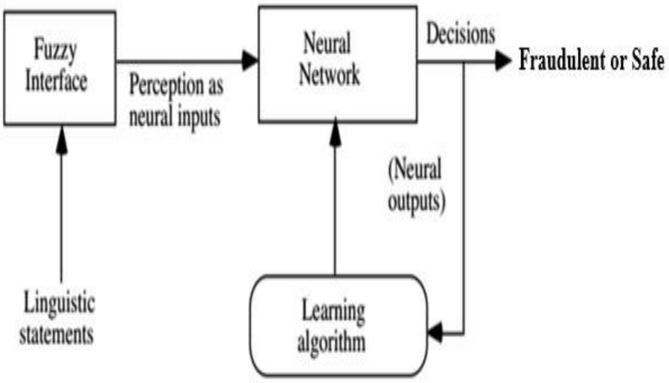


Figure 3.1: The Proposed Neuro fuzzy model for fraud detection.

Advantages of the proposed Neuro-fuzzy model for fraud detection include;

i. Improve the accuracy of fraud detection.
ii. Reduce false positives and negatives.
iii. Handle imbalanced data: The model can handle imbalanced data by using techniques that balance the data and prevent it from biasing the model's results.
iv. Adapt to changes in fraud patterns.

SUMMARY

This paper reviews recent advances in electronic banking fraud detection and prevention using Neuro-Fuzzy models.

The study highlights the growing concern of electronic fraud in Nigeria's financial sector, with a significant increase in fraudulent activities resulting in substantial financial losses. The traditional fraud detection methods are often inflexible and may miss subtle changes in fraudulent behaviour, leading to inefficient use of resources. The proposed Neuro-Fuzzy model employs adaptive neuro-fuzzy inference systems to detect and prevent electronic banking fraud. The model utilizes six features of electronic transactions as inputs to a Fuzzy Inference System, which are then taken as neural inputs to determine the likelihood of a transaction being fraudulent or safe.

CONCLUSION

The proposed Neuro-Fuzzy model offers several advantages, including improved accuracy in fraud detection, reduced false positives and negatives, handling imbalanced data, and adapting to changes in fraud patterns. The study contributes to the development of more effective fraud monitoring and preventive measures, aiding financial institutions in combating electronic banking fraud. The findings of this study are essential for the financial sector, as they provide insights into the detection and prevention of electronic banking fraud, ultimately reducing financial losses and enhancing the trust and confidence in electronic banking systems.

REFERENCES

1. Ahmad, B. H., Mohammad, A. A., and Ghada, A. (2018). Combating Web-Based Fraud using KNN. International Journal of Computer Science and Information Security 12 (8)
2. Andoni, A., and Indyk, P. (2018). Optimal Hashing Algorithms for Approximate Nearest Neighbor in Fraud Detection. IEEE Communications 51 (13) 117-122

3. Babatunde, O. and Sunday, O. (2017). E- Banking in Nigeria: Issues and Challenges. Research Journal of Finance and Accounting 8 (6), 222-284
4. Bart, B. Van Vlasselaer, Wouter, V. (2015). A Guide to Data Science for Fraud Detection. John Wiley & Sons, New Jersey, USA.
5. Benson, S., Edwin R., and Portia, A. (2011). Analysis on Credit Card Fraud Detection Methods. International Conference on Computer, Communication and Electrical Technology. Vol 5. (pp 152-156) McLaren Press Inc.
6. Central Bank of Nigeria (2019). Fraud and Investigation in the Nigerian Financial Sector.
7. Divya, I., Arti, M., Sneha, J., Rathod, D., and Amruta, S. (2011). Credit Card Fraud Detection Using Hidden Markov Model. IEEE Transactions on Information Theory, 9 (7) 78-85
8. Duman, M., and Hamdi, O. (2011). Detecting credit card fraud by genetic algorithm and scatter search. Elsevier, Expert Systems with Applications 38 (2) 13057–13063.
9. Dzomira, S. (2015). Online and Electronic Fraud Prevention & Safety Tips Cognizance.
10. Gou, J., Du, L. Zhang, Y. and Xiong, T. (2012). Distance-weighted k-nearest Neighbor Classifier. Journal of Information & Computational Science 9(6) 1429-1436
11. Graaff, A. J. and Engelbrecht, A.P. (2014). The Artificial Immune System for Fraud Detection in the Telecommunications Environment. IEEE Transactions on Dependable and Secure Computing 4 (6) 73-81
12. Imiefoh, P. (2012). Towards Effective Implementation of Electronic E-Banking in Nigeria. An International Multi-Disciplinary Journal 6. (2), 290-300.
13. Kalyani, K. R., and Devi, U. D. (2012). Fraud Detection of Credit Card Payment System by Genetic Algorithm. International Journal of Scientific and Engineering Research 3 (7) 2229-5518
14. Kataria, A. and Singh, M. D. (2013). A Review of Data Classification Using K-Nearest Neighbour Algorithm. International Journal of Emerging Technology and Advanced Engineering 3 (6) 354-360
15. Onodugo, I. C. (2018). Overview of electronic banking in Nigeria. International Journal of Multidisciplinary Research and Development 2 (7) 336-342
16. Palema, S. M (2013). Using Analytics to Detect Possible Fraud. John Wiley & Sons. Inc, New York
17. Renu, S. (2014). Analysis on Credit Card Fraud Detection Methods. International Journal of Computer Trends and Technology (IJCTT) 8 (1)
18. Sadegh, B. I., and Mohammad, B. (2013) Application of K-Nearest Neighbor (KNN) Approach for Predicting Fraudulent Transactions. Journal of Engineering Research and Applications 3 (5) 605-610
19. Sahin, Y., and Duman, E. (2011). Detecting Credit Card Fraud by Decision Trees and Support Vector Machines. International Multiconference of Engineers and computer scientists Vol 1. MKJ Press.
20. Srivastava, A. and Arkov, M. (2018). Fraud detection Model using Genetic algorithm. IEEE Transactions on Dependable and Secure Computing 5 (37)