EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Framework for Detection of Fraud at Point of Sale on Electronic Commerce sites using Logistic Regression

O.F. Alabi[1,*], A.A. David[2]

[1]Ph.D. Scholar Computer/IT, African University of Science and Technology/ Department of Computer Science, Abuja, Nigeria.

[2]Professor, University of Lorraine, Department of Computer Science, Nancy, France.

Abstract

Many businesses have been positively impacted by electronic commerce (ecommerce). It has enabled enterprises and consumers transact business digitally and experience diversity as long as the internet is accessible and there is a gadget to surf the internet. Several governments have gradually adopted electronic payment throughout the country. The Nigerian government has also done a lot of prodding toward the adoption of a cashless economy, which includes embracing ecommerce. As ecommerce expands, so does actual and attempted fraud through this channel. According to the Nigerian Central Bank, electronic fraud reached trillions of Naira by 2021. The purpose of this work was to employ logistic regression as a decision-making tool for detecting fraud in e-commerce platforms at either the virtual or physical point of sale. The main contribution of this research is a model developed using logistic regression for detecting fraud at the point of sale on electronic commerce platforms. The accuracy of the result is 97.8 percent. The result of this study will provide key decision makers in ecommerce firms with information on fraud patterns on their ecommerce platforms, this will enable them take quick actions to forestall these fraudulent attempts. Further research should be carried out using data from other developing countries.

Keywords: E-commerce, point of sale, decision making, fraud detection, logistic regression.

Received on 24 June 2022, accepted on 13 November 2022, published on 23 November 2022

doi: 10.4108/eetsis.v10i2.1596

1. Introduction

The financial system of the twenty-first century is dynamic and has seen significant changes as a result of technological improvements; these innovations have changed old payment systems and ushered in an era of electronic payment. Electronic payment is any type of transaction conducted through an electronic medium that does not include the use of a cheque or cash. Similarly, electronic payment has facilitated the birth of electronic commerce(ecommerce) which has improved consumer preferences, convenience of use, cost, security, relevancy, and acceptance all of which play a role in the success of ecommerce payment systems. The advent of ecommerce has enabled; several firms expand their operations outside geographical boundaries in order to reach a wider audience. Organizations may now do business all year round because of ecommerce. Ecommerce is the purchase and sale of products and services over the Internet. It occurs on computers, tablets, cell phones, and other smart devices [1]. There are many types of e-commerce, the varieties includes: Business-to-Business (B2B), Business-to-Consumer (B2C), Consumer-to-Consumer (C2C), Consumer-to-Business (C2B), Business-to-Administration (B2A) and Consumer-to-Administration (C2A).

Ecommerce promises clients ease; speed, variety, price comparison, and much more. It eliminates the need for customers to visit physical businesses every time they need to make a purchase. Customers have embraced online shopping compared to brick and mortar shopping, as seen by the success of companies such as Amazon, Alibaba, and others. The number of electronic transactions has grown

*Corresponding author. Email: oalabi@aust.edu.ng

dramatically over the years, the industry's expansion has also attracted fraudsters seeking to abuse every area of ecommerce, from payment methods to client records and merchandise. According to [2], Criminals pursue enterprises that transfer or develop from bricks to clicks.

Point of sale(POS) has made ecommerce transactions even easier. POS can be defined as any system that allows customers make purchase and pay necessary sales tax either at an internal store terminal or a virtual POS terminal [3].

POS systems are classified into numerous types:

(1) Mobile point-of-sale systems: these services are available for smartphones and tablets may handle payments as well as manage inventory and customer information.
(2) Tablet POS systems: iPad and Android point-of-sale solutions are becoming increasingly popular since it requires less upfront investment and can frequently be utilized with an existing tablet. Some tablet POS providers include credit card processing for "free."
(3) Terminal point-of-sale systems: These are the most frequent at the counter. While they are hardware and software-based, the majority of them require internet connectivity and may even employ cloud-based applications.
(4) POS kiosks are tailored solutions for a specific purpose. A self-service kiosk for purchasing cinema tickets is one example.

According to Cyber Source's 12th annual online fraud study, merchants' online fraud losses increased the most during the current decade, peaking at $4 billion in 2013 [4]. Credit card fraudsters in European nations are continuously focusing on "card less" activities like ecommerce purchase [5]. According to data from the UK Payments industry, the worth of cell phone, web, and mail order fraud (card less fraud) grew by 118% between 2004 and 2008. Between 2001 and 2008, card less fraud losses in the UK increased by 243 %, while the overall amount of online shopping transactions increased by 524 % [6]. According to [7], Cybercrime is currently predicted to cost the globe almost $600 billion, or 0.8 percent of global GDP (GDP). The Central Bank of Nigeria (CBN) forecasted that the value of electronic fraud losses in Nigeria will reach N6.1 trillion by 2021[8]. According to Nigeria Inter-Bank Settlement System(NIBSS) (2022), the amount of POS transactions recorded between January and August 2021 was 619.3 million, an increase of 61.8 percent over the 382.9 million recorded during the same time in 2020. It is worth mentioning that as of August 2021, a total of 686,577 POS terminals were deployed countrywide, indicating an 84.4 percent growth over 372,333 reported in the same time in 2020 [9].

The identification of ecommerce fraud is critical in the prevention and protection of ecommerce consumers and owners. Artificial intelligence has been used in online fraud detection strategies for online card transactions, Support vector machines (SVM), artificial neural networks (ANN), Bayesian networks, Hidden Markov Model, K-Nearest Neighbours (KNN) Fuzzy Logic system, and decision Trees are among the new techniques offered in addition to previous approaches. The k-nearest neighbour, decision tree, and SVM algorithms all yield a moderate level of accuracy. Fuzzy Logic has the lowest accuracy of any algorithm. Neural networks, naive Bayes, and KNN [10] provide a good performance.

According to LexisNexis' 2021 True Costs of Fraud report, in 2020, the typical U.S. store experienced 1,515 point of sale(POS) fraud attempts each month, with roughly half of those efforts succeeding. According to industry information published by Nilson Report, almost $28.58 billion was lost to payment fraud globally during the same year [11]. Regardless of the different research conducted, none have used logistic regression to detect fraud at the point of sale on electronic commerce platforms.

Logistic regression is a data evaluation method used to identify and describe the relationship between a dependent binary variable and other independent nominal, ordinal, interval, or ratio-level variables. Logistic regression is an incredibly robust and adaptable method for dichotomous categorization prediction; that is, it is used to anticipate a binary outcome or condition, such as yes/no, success/failure, or will occur/will not occur [12]. The result of this study will provide key decision makers in ecommerce firms with information on fraud patterns on their ecommerce platforms, this will enable them take quick actions to forestall these fraudulent attempts.

This papers main contribution is a model suited for detecting fraud at the point of sale on electronic commerce platforms using logistic regression. The remainder of this work is structured as follows. Section II discusses some relevant research. Section III provides a brief overview of the approach used in this work: logistic regression. The outcome is shown in Section IV. Section V includes conclusions and future study.

2. Related Work

The growth of online transactions has been consistent over the years, and while these transactions may not be as safe as in-person. There has been an increase in demand for credit or debit card fraud detection as a result of the rise in fraudulent transactions associated with it. The illegal use of any system or product is characterized as fraud [13]. Several initiatives have been made to reduce ecommerce fraud, yet incidents of consumers being cheated online continue to make headlines throughout the world. According to the World Bank [14], the worldwide market opportunity for extending electronic payments by merchants is considerable; in 2016, micro, small, and medium retailers (MSMRs) made and received $1.9 trillion in payments. As these statistics rise, so do the likelihood of fraud. The graph below depicts total Global Payments and total Electronic Payments by region, using estimated data from [14]:

2.1 Types of fraud

There are five basic methods by which fraudsters perpetrate fraud on ecommerce stores:

True (classic) fraud: the theft or purchase of a victim's credit card information over the Internet is the most fundamental type of fraud.

Triangulation fraud is characterized by the presence of a fraudster, a legitimate shopper, and an E-commerce business. A fraudster sets up an online store and provides great items at very minimal costs. He purchases things from a legitimate business and sends them to customers after getting credit card information from those who purchased.

Interception fraud happens when fraudsters place an order with matching billing and shipping addresses to the card's address. The fraudster will then attempt to hijack the package by asking the customer service representative to make alterations on the delivery address; requesting a change of address for the order to a location where the stolen item can be intercepted.

Card validity testing fraud happens when fraudster evaluate various card data to determine whether or not the credentials are legitimate and then uses them to conduct illicit transactions on another website.

Chargeback fraud happens when a client purchases goods online, then request a chargeback claiming their credit card was stolen. This is more likely to occur after the items have been delivered. This type of fraud is more common among consumers than among professional con artists, and it is more difficult to detect.

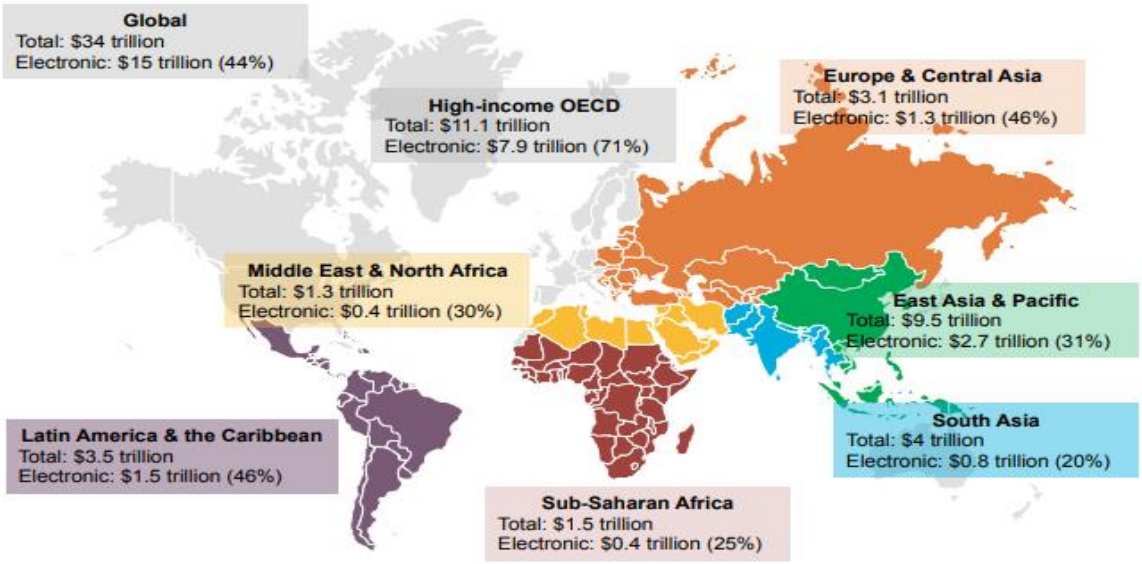

Figure 1. Global Payments Estimated Values Source: [14]

2.2 Previous research on credit card fraud detection

Several researches have been carried out to detect cards fraud:

[15] suggested a novel way to handle the issue of "low-frequency consumers with little transaction amounts," since current methodologies are incapable of appropriately depicting transaction activity for such clients. Furthermore, it considers "current trading group behaviour and current transaction status" while developing new behaviour for low-frequency users. They devise a method for recognizing the user's current transaction based on "user behaviour and Naive Bayes."

[16] worked on detecting credit card fraud. The projects goal with Machine Learning was to concentrate primarily on machine learning techniques. The Adaboost approach and the random forest algorithm were used. The results are calculated using the accuracy, precision, recall, and F1-score of the two approaches. The confusion matrix was used as a reference to create the ROC curve. The Random Forest and Adaboost algorithms were assessed, and the technique with the highest accuracy, precision, recall, and F1-score was determined to be the most effective at identifying fraud. The findings revealed that, despite the numerous machine learning techniques employed to identify fraud, the researchers found the outcomes to be unsatisfactory. They advocated using deep learning algorithms to properly identify credit card fraud.

[17] research created a fraud detection model without a supervised label that was based on anomaly detection and was successful in finding certified fraud contracts in the top tier. He overcame the difficulty of detecting fraud in the supervised label when the quantity of fraudulent transactions is really low.

In 2019, [18] Support vector machines (SVM), artificial neural networks (ANN), Bayesian networks, Hidden Markov Model, K-Nearest Neighbours (KNN) Fuzzy Logic system, and Decision Trees were all investigated for credit card fraud detection. In their research, they discovered that the k-nearest neighbour, decision trees, and SVM algorithms provide a medium degree of accuracy.

According to [19] which discussed their research on identifying online fraud utilizing decision trees, random forest, SVM, and Logistic Regression They had to work with a highly skewed dataset. Accuracy, sensitivity, specificity, and precision are used to evaluate performance. The findings show that Logistic Regression has a 97.7 percent accuracy, Decision Trees have a 95.5 percent accuracy, Random Forest has a 98.6 percent accuracy, and SVM classifier has a 97.5 percent accuracy. They concluded that the Random Forest algorithm outperforms the other algorithms in terms of accuracy and is the best algorithm for identifying fraud.

[20] used the Hidden Markov Model(HMM) to provide a generic technique to detecting fraud. During the registration step, the authors advocated employing a legal parameter to limit users' ability to establish numerous accounts. The generic Markov model is composed of the training and detection layer. To generate the previous probability set for analysing bidding behaviour for authentication purposes, the researchers used K-means clustering. After then, the detection layer is used to identify fraud, and users are divided into the high, medium, and low categories based on a cognitive technique that analyses transaction activities. Finally, HMM was used in order to detect consumer fraud by observing their behaviour. Only two parameters in this study give inadequate information to detect fraud. Furthermore, no type of transaction fraud was not found, and no testing to confirm the proposed approach have been performed.

[21] asserted that a Naive Bayesian classifier is an effective probabilistic algorithm that employs class sequence from the training class of potential examples. Similarly, they stated other approaches used to identify fraud include self-organizing maps (SOM), K-Nearest Neighbour, Outlier Techniques, and the Boat algorithm.

Between 1997 and 2008, [22] conducted a literature review on the use of data mining tools for the detection of financial fraud. 49 journal articles on the subject were assessed and grouped into four categories of financial fraud; financial institution fraud, insurance fraud, securities and commodities fraud and others. Six kinds of data mining techniques were also identified namely classification, regression, clustering, prediction, outlier detection and visualization. The findings of this study show that data mining techniques have been widely employed to detect insurance fraud, while corporate fraud and credit card fraud have also attracted significant attention in recent years. The core data mining techniques used for FFD include logistic models, neural networks, the Bayesian belief network, and decision trees, and they all provide fundamental answers to the issues inherent in the identification and classification of false data. However, measuring neural network performance in electronic fraud detection against other algorithms remained mostly unexplored until Patidar and Sharma discovered that artificial neural networks outperformed Random Forest [23].

[24] To identify online fraudulent transactions, artificial immune systems were used. The study evaluated the efficacy of Artificial Immune Systems (AIS) for credit card fraud detection using a large dataset acquired from an online store. Three AIS algorithms were created. Despite the fact that the canonical Negative Selection Algorithm achieved high overall accuracy, the system misclassified far too many fraudulent transactions to be operationalized. The seminal AIS studies for computer security were those that presented the immune system as an analogy for intrusion detection systems. Negative Selection (NS) [25], an abstract model of biological NS, is one of the traditional theories. According to this hypothesis, the detector model created during the censoring phase is meant to monitor the self-state and determine whether or not it has changed.

Many study summaries in AIS reported revealed that HIS embodies robustness, dispersion, lightweight, self-organizing, and self-adapting characteristics. AISs are extremely abstract representations of their biological counterparts employed to address issues in numerous sectors [26]. The findings suggest that AIS algorithms have the potential to be employed in fraud detection systems across other financial institutions, but that further study is required to fully live up to their potential in this industry.

[27] Data from a Brazilian bank was studied to test the effectiveness of using an Artificial Immune System to detect fraud. They compared the outcomes of using an Artificial Immune System, Artificial Neural Network, Decision Tree, Naive Bayes, and Bayesian Nets with each of the strategies in their study. The study was more concerned with minimizing the cost of using each strategy and determining the best set of parameters than with the performance of each technique with classification. There is no data on the strategy they used or what variables were the most effective. To identify fraud in credit card transactions, [28] employed the STAGE method for Bayesian networks and the "back propagation" technique for neural networks. The findings show that while Bayesian networks seem to be more precise to train, they are slower to adapt to new conditions.

However, the detection of fraud at point of sale on electronic commerce sites using logistic regression remains largely unexplored. Our focus for this research is the Card validity testing fraud. Using logistic regression, this study presents a model for detecting fraud at the point of sale on e-commerce platforms. Currently, no recent study has taken into account the approach and data collection employed in this research. This study has made a

significant contribution by detecting suspected fraudulent transactions at the point of sale on ecommerce websites. The findings of this study will aid in a better understanding of potential fraudulent transactions on ecommerce sites. It can also help in the development of innovative strategies for preventing fraud on ecommerce websites. Following that, the outcome will aid ecommerce owners in analysing the fraud tendencies on their websites and responding proactively to the issue.

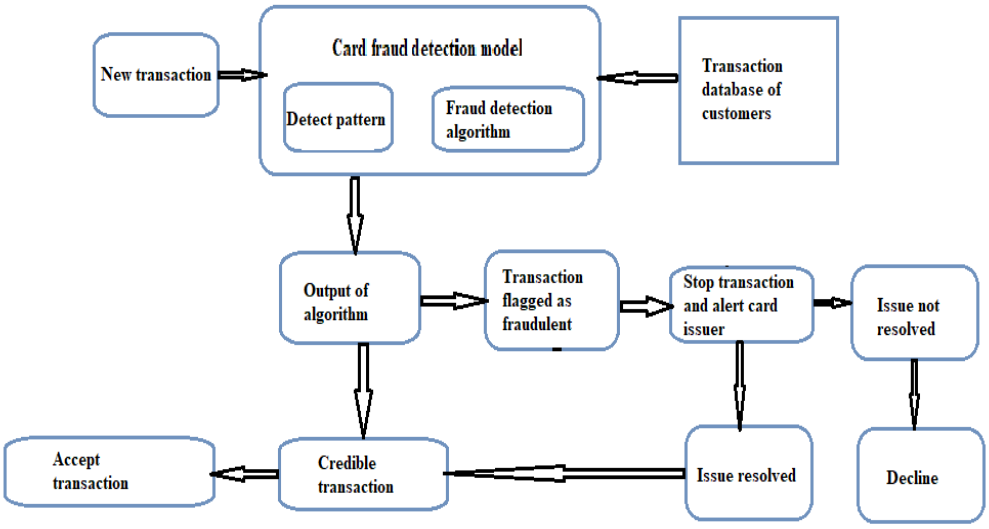

Figure 2. Proposed card fraud detection model

3. Proposed Method

3.1 Logistic Regression (LR)

Logistic Regression is a statistical method that creates a model that can predict the values of a categorical dependent variable based on a set of variables. The logarithm formula is depicted below:

$$\log_e\left(\frac{p}{1-p}\right), \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

As a result, using the function represented by the equation below, a regression model is used to determine the likelihood of an occurrence.

$$\pi(x) = e(\beta 0 + \beta 1X1 + \beta 2X2 + \cdots \beta iXi)1 + e(\beta 0 + \beta 1X1 + \beta 2X2 + \cdots \beta iXi), \ldots\ldots\ldots (2)$$

where $\pi(x)$ represents the success probability when the predictive variable has the value x. $\beta 0$ is an adjustment constant, and βi are the predictive variable coefficients. To understand LR, it is important to first define Generalized Linear Models (GLM). This is divided into three sections:

A random component representing the probability distribution of the dependent variable (Y).

A systematic component is comparable to a linear function between independent variables. • A link function explains the mathematical relationship between the systematic and random components.

The binary Logistic Regression model, which is a subset of the GLM model, includes the logit function. The coefficients are estimated using this function. The logistic regression model contrasts the likelihood of attempting again among individuals who have previously attempted and those who have not.

The odds ratio is the difference between those odds. A logistic regression examines a natural logarithmic transformation of the odds, known as the log odds, rather than the odds themselves. The analytical model is used to determine whether or not an incoming transaction is legitimate. To detect fraud, the logistic regression model is used. The proposed fraud detection system is as follows:

3.2 Dataset

European cardholders' credit card transactions from September 2013 are included in the dataset. In this data set, 492 frauds from 284,807 transactions happened in the previous two days. The transaction dataset is extremely skewed, with just 0.172% of transactions being positive (fraud). It only takes numerical input variables that have been transformed by PCA. Due to confidentiality concerns, this research is unable to provide the source data and

additional background information. The major items derived by PCA are V1, V2,....V28; the only characteristics that remain unchanged by PCA are 'Time' and 'Amount.' [29]. Ecommerce fraud issues are universal hence this research adopted the European dataset. To prepare a dataset for training and testing, we set aside some data for training and the other for testing.

3.3 Indicators of card validity fraud:

• Low cost transactions – a sequence of similar or recurring small transactions from the same IP address.
• Rapidity - a surge of transactions within a certain timeframe may suggest the usage of automated robots.
• High decline rate – a considerable rise in declines, and also decline reasons such as invalid card number, suspicious activities, stolen card, no card record, and so on.
• CVV Mistakes - Several stolen or counterfeit card numbers usually lack CVV information, erroneous CVV code errors are common. [31] seconded [30]'s proposition.

4. Result

Algorithm 1. The following steps were involved in the design of the Fraud detection model using Logistic Regression

Algorithm: Fraud detection model using Logistic Regression

Input: Credit Card transaction dataset (DS)

Output: Type of transaction (Legitimate or Fraud)

Import packages: pandas, numpy, pickle, LogisticRegression, train_test_split, accuracy_score

Read DS

Normalized DS
Handle class imbalance using (SMOTE)

Split DS into train and test sets

Train the LogisticRegression() model
Test the model
print the accuracy score

Save the model using pickle dump object

Develop fraud detection web app using Streamlit

load the save model using pickle load object

Predict the type of transaction

End

Figure 3. Model results of credit card fraud detection model showing a flagged transaction amount and time of attempted transaction

5. Discussion and conclusion

Credit card fraud on ecommerce sites is clearly an illegal act. This research examined current developments of fraud in the credit card industry with a focus on ecommerce firms. This study has outlined the many methods used to commit ecommerce fraud, including true (classic) fraud, triangulation fraud, interception fraud, card validity testing fraud, and chargeback fraud. This papers main contribution is developing a model that can detect fraud at the point of sale on electronic commerce sites using logistic regression. This provides key decision makers in ecommerce firms with information on fraud patterns on their ecommerce platforms, allowing them to make quick decisions on how to forestall these fraud attempts. The accuracy of the result is 97.8 percent. Previous studies reveal that if decision-makers in ecommerce firms do not quickly address threats on their ecommerce platforms, customers may choose alternative platforms where they feel safer if the fraudsters succeed in their attempt to defraud customers or even the company. This in turn will lead to lower income and ultimately lead to business shut down. Further research should focus on one of the African countries, most likely Nigeria or Ghana, before expanding the investigation to other countries.

Acknowledgements.

The authors would like to express their gratitude to African University of Science and Technology. The African Development Bank provided funding for this project.

References

[1] Shahid A.B., Keshav K. & Jenifur M. “A Review Paper on E-Commerce” TIMS 2016-International Conference. Available from: https://www.researchgate.net/publication/304703920_A_Review_Paper_on_Ecommerce#:~:text=E%2Dcommerce%20(Electronic%20commerce),both%20marketers%20and%20the%20customers.

[2] Global Cyber Executive Briefing E-Commerce & Online payments [Internet]. Deloitte; 2019. Available from: https://www2.deloitte.com/ng/en/pages/risk/articles/e-commerce.html.

[3] Max F. “Types of POS Systems” Available from: https://www.business.com/articles/types-of-pos-systems/

[4] Caldeira, E. B., Gabriel & Pereira A. “Fraud Analysis and Prevention in e-Commerce Transactions.” Proc 9th Latin American Web Congress [Internet]. Available from: https://www.researchgate.net/publication/287299598_Fraud_Analysis_and_Prevention_in_e-Commerce_Transactions.

[5] Herbst-Murphy S “Maintaining a safe environment for payment cards: Examining evolving threats posed by fraud.” 2009.

[6] APACS 2008 Fraud Loss Figures [Internet]. Available from: http://www.ukpayments.org.uk/media_centre/press_releases//page/685/

[7] McAfee. Economic Impact of Cybercrime - No Slowing Down [Internet]. 2018. Available from: https://www.mcafee.com/enterprise/en-us/forms/gated-form.html?docID=5fee1c652573999d75e4388122bf72f5&tag=ec&eid=18TL_ECGLQ1_CT_WW21/05/2020

[8] Central Bank of Nigeria. Electronic Fraud will hit N6.1 trillion by 2021 [Internet]. Central Bank of Nigeria; 2018. Available from: https://taskira.com.ng/2018/11/15/central-bank-electronic-fraud-will-hit-n6-1trillion-by-2021/

[9] Nigeria Inter-Bank Settlement System(NIBSS)(2022). Point of Sale Transaction Hits N6.4tn, Cheques Usage Up 3.9% in 2021. https://nibss-plc.com.ng/news/4te149br68n66xv24fake6ksm3

[10] Yashvi J, Namrata T, Shripriya D and Sarika J. “A Comparative Analysis of Various Credit Card Fraud Detection Techniques.” International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878. 2019 Jan;7(5S2).

[11] Lexis report 2021. LexisNexis® Risk Solutions 2021 True Cost of Fraud™ Study. https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study#financialservices

[12] Seufert EB, “Quantitative Methods for Product Management” [Internet]. 2014. Available from: http://dx.doi.org/10.1016/B978-0-12-416690-5.00003-807/08/2021

[13] Detecting credit card fraud by genetic algorithm and scatter search. EXPERT SYSTEMS WITH APPLICATIONS. 2018;38(10):13057–63.

[14] World Bank Group. Innovation in Electronic Payment Adoption: The case of small retailers [Internet]. 2017. Available from: http://www3.weforum.org/docs/Innovative_Solutions_Accelerate_Adoption_Electronic_Payments_Merchants_report_2016.pdf

[15] Zhang Y, Liu G, Luan W, Yan C and Jiang C. “Application of SIRUS in credit card fraud detection.” proc: International Conference on Computational Social Networks. 2020. p. 66–78.

[16] Ruttala S, Ramesh R, Gnaneswar V and Ramakoteswara G “Credit Card Fraud Detection Using Machine Learning”. In: International Conference on Intelligent Computing and Control Systems (ICICCS 2020) Number: CFP20K74-ART; ISBN: 978-1-7281-4876-2. IEEE Xplore Part; 2020.

[17] Nakai M, “Fraud Detection without Label”. School of Industrial Technology, Advanced Institute of Industrial Technology. 2020.

[18] Yashvi J, Namrata T, Shripriya D and Sarika. JA “Comparative Analysis of Various Credit Card Fraud Detection Techniques.” Volume-7 Issue-5S2, January 2019. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878. 2019;7(5S2)

[19] Navanshu K and Sait SY “Credit Card Fraud Detection Using Machine Learning Models and Collating Machine Learning Models” ISSN: 1314-3395. International Journal of Pure and Applied Mathematics. 2018;118(20):825–38.

[20] Gupta P. and Mudra A. “Online in-auction fraud detection using online hybrid model” In: Proc: IEEE International Conference on Computing, Communication & Automation (ICCCA). India: IEEE; p. 901–7.

[21] Gayathri R and Malathi A“Investigation of Data Mining Techniques in Fraud Detection: Credit Card” International Journal of Computer Applications. 2013;82(9):10–5.

[22] Ngai EW, Hu Y, Wong YH, Chen Y, and Sun Y, “The application of data mining techniques in financial fraud detection: A classification framework and an academic

review of literature," Decision Support Syst., vol. 50, no. 3, pp. 559–569, Feb. 2017. [Online]. Available: http://dx.doi.org/10.1016/j.dss.2010.08.006

[23] Patidar R and Sharma L,"Credit card fraud detection using neural network." International Journal of Soft Computing and Engineering (IJSCE). 2017;32–38.

[24] Anthony B, Jane C, Peter K and Daniel W "Identifying Online Credit Card Fraud using Artificial Immune Systems." In IEEE; 2011. Available from: https://ieeexplore.ieee.org/document/5586154/

[25] Forrest S, Allen L, Perelson AS, Cherukuri R. Self-nonself discrimination in a computer. Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy; May 1994; Oakland, Calif, USA. pp. 202–212.

[26] Andrews PS, Timmis J. Bioinformatics for Immunomics. Vol. 3. New York, NY, USA: Springer; 2010. Tunable detectors for artificial immune systems: from model to algorithm; pp. 103–127.

[27] Gadi M, "Credit Card Fraud Detection with Artificial Immune System," in artificial immune systems, ed, 2008, pp. 119-131.

[28] Maes S, Tuyls K, Vanschoenwinkel B, and Manderick B, "Credit card fraud detection using bayesian and neural networks," in: interactive image-guided neurosurgery. american association neurological surgeons, 2003, pp. 261–270

[29] Credit card fraud detection anonymized credit card transactions labeled as fraudulent or genuine. https://www.kaggle.com/mlg-ulb/creditcardfraud

[30] Jp morgan 2021 "Six Ways Merchants Can Help Prevent Card Testing Attacks." Online https://www.jpmorgan.com/merchant-services/insights/card-testing-prevention

[31] Leung J, "Card Testing Attacks in 2020: How to Identify and Prevent it." Online https://www.finextra.com/blogposting/19705/card-testing-attacks-in-2020-how-to-identify-and-prevent-it

[32] Yin, J., Tang, M., Cao, J. et al. Vulnerability exploitation time prediction: an integrated framework for dynamic imbalanced learning. World Wide Web 25, 401–423 (2022). https://doi.org/10.1007/s11280-021-00909-z

[33] Hua Wang, Yanchun Zhang, Jinli Cao and V. Varadharajan, "Achieving secure and flexible M-services through tickets," in IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 33, no. 6, pp. 697-708, Nov. 2003, doi: 10.1109/TSMCA.2003.819917

[34] H. Wang and Y. Zhang, "Untraceable off-line electronic cash flow in e-commerce," Proceedings 24th Australian Computer Science Conference. ACSC 2001, 2001, pp. 191-198, doi: 10.1109/ACSC.2001.906642.