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

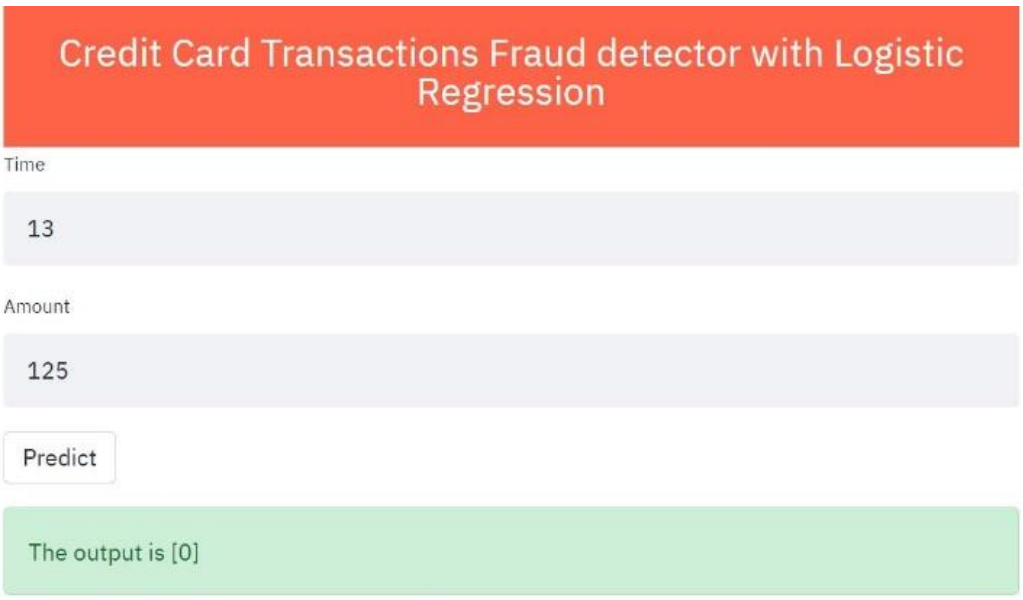

Figure 3. Model results of credit card fraud detection model showing a flagged transaction amount and time of attempted transaction

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.