https://doi.org/10.46335/IJIES.2023.8.1.5 **e-ISSN: 2456-3463**
Vol. 8 , No. 1, 2023 , PP. 22-25

International Journal of Innovations in Engineering and Science, www.ijies.net

Review on Credit Card Fraud Detection System using Machine Learning

Dr. (Mrs.) Snehal S. Golait[1] , Ruthwick S. Masidkar[2] , Kunal S. Khobragade[3]
Prerna S. Bhanarkar[4] ,Purva Ganeshkar[5] , Prishita Ganeshkar[6]

[1]Priyadarshini College of Engineering, Nagpur

ruthwick000@gmail.com

***Received on**: 25 February,2023* ***Revised on**: 20 March,2023* ***Published on**: 22 March,2023*

***Abstract –** This review paper is discussing the use of machine learning in detecting cred-it card fraud. With the increasing number of online transactions, it is becoming more important to have accurate systems in place to identify fraudulent activity. The authors are proposing the use of machine learning algorithms to analyze and pre-process data sets in order to accurately detect fraudulent credit card transactions. The objective is to identify 100% of fraudulent transactions while minimizing false positive fraud classifications. The paper focuses on using machine learning techniques on transformed credit card transaction data to achieve this goal.*

Keywords- Credit Card, Fraud, Recognize, Detection, Transaction, Data Preprocessing, Model evaluation, Performance Analysis.

INTRODUCTION

Credit card fraud refers to the unauthorized use of someone else's credit card to make purchases or withdraw money. The person committing the fraud obtains the credit card information through illegal means, such as stealing the physical card, hacking into the cardholder's account, or by tricking the cardholder into revealing their information. The card issuing authority and the rightful owner of the card are not aware that the card is being used fraudulently until they receive a statement or notice of suspicious activity. The result of this illegal activity can cause financial harm to the cardholder and damage their credit score.

In technical terms, credit card fraud detection is a process that aims to identify and prevent unauthorized use of credit cards through the analysis of user behavior and transactions. With the growth of e-commerce, there has been a rise in credit card fraud, making it essential for credit card companies to implement effective fraud detection mechanisms. Machine learning algorithms are commonly used for this purpose, as they can analyze large datasets of authorized transactions to detect suspicious activity. The algorithms generate reports of potentially fraudulent transactions, which are then investigated by human experts to confirm their authenticity. Based on the feedback from the investigators, the machine learning algorithms are continuously trained and updated to improve their accuracy over time. The behavior of users is monitored and analyzed in order to pre-vent fraudulent activities such as unauthorized use of credit cards, intrusion, and defaulting, by fraud detection.

For identifying the different types of anomalies, we will use a machine learning base model. Figure. 1 shows the process flow diagram.

https://doi.org/10.46335/IJIES.2023.8.1.5 e-ISSN: 2456-3463
Vol. 8 , No. 1, 2023 , PP. 22-25

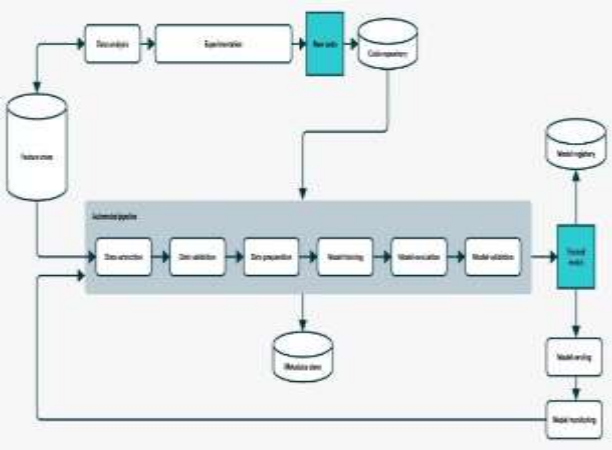

Fig. 1- Process flow.

MOTIVATION

Credit card fraud remains a pressing issue in today's digital age, with billions of dollars lost each year due to fraudulent activities (Garcia, E. A. & Nanni, M. 2020) [9]. In addition to financial losses, credit card fraud can also harm the reputation of financial institutions and erode customer trust (Othman, M., Choo, K. K. R., & Ling, L. H. 2020) [12]. To mitigate these risks, it is crucial to develop and implement effective credit card fraud detection systems.

Recent advancements in technology and the availability of large amounts of data have enabled the development of sophisticated credit card fraud detection systems, utilizing cutting-edge techniques such as machine learning (Yuan, X. & Lee, W. C. 2020) [13], deep learning (Komurcu, M. I. & Gokce, A. 2020) [10], and graph-based methods (Li, Y., Xu, Y., & Zhang, J. 2020) [11]. These systems monitor and analyze credit card transactions in real-time, and use advanced algorithms to identify and prevent fraudulent activities.

A review paper on credit card fraud detection systems published after 2019 can provide valuable insights into the latest developments and innovations in this field. By summarizing the current state of the art and evaluating the strengths and weaknesses of different approaches, a review paper can assist researchers, practitioners, and policymakers in understanding the latest trends and advancements in credit card fraud detection (Garcia, E. A. & Nanni, M. 2020) [9].

LITERATURE REVIEW

Fraud is indeed a deliberate act of deception intended to result in financial or personal gain, committed in violation of the law, rule, or policy. Fraudsters engage in fraudulent activities with the aim of obtaining unauthorized financial benefits, such as using someone else's credit card information for unauthorized purchases or using false identities to obtain loans or benefits. Fraud can have serious consequences, both for the victims and for the economy as a whole, which is why it is considered a criminal offense and is punished by law. It is important to be aware of the different forms of fraud and to take steps to prevent it, such as being cautious when sharing personal information, checking financial statements regularly, and reporting suspicious activities immediately.

Lots of research work is available in literature. A survey conducted by Clifton Phua and his associates have revealed some of the techniques mentioned in stud-ies include data mining, automated fraud detection, adversarial detection, super-vised and unsupervised learning. However, despite these methods and algorithms having success in some areas, they have not provided a permanent and consistent solution to fraud detection.[1]

In another study, Fraudulent transactions in a credit card transaction data set from a commercial bank were detected by Wen-Fang YU and Na Wang using outlier mining and outlier detection mining [2], as well as distance sum algorithms. Objects that deviate from the main system, in this case transactions that are not genuine, are detected in the financial and internet industries by outlier mining, which is a field of data mining. The study used customer behavior attributes to calculate the distance between observed values and predetermined values, which was used to identify fraudulent transactions.

An unconventional technique, called hybrid data mining/complex network classification algorithm, has shown to be effective in detecting fraudulent transactions in a real credit card transaction data set. This technique is based on a network reconstruction algorithm that creates representations of deviations from a reference group. This method has proven to be efficient in medium-sized online trans-actions.

Efforts have also been made to approach the issue of fraud detection from a new perspective. One such effort is to improve the interaction between the system and the user in the event of a potential fraudulent transaction. When a potentially fraudulent transaction is detected, the system would alert the user and provide feedback to either confirm or deny the transaction.

https://doi.org/10.46335/IJIES.2023.8.1.5 **e-ISSN: 2456-3463**
Vol. 8 , No. 1, 2023 , PP. 22-25

International Journal of Innovations in Engineering and Science, www.ijies.net

In the event of a fraudulent transaction, the ongoing transaction would be denied and feedback would be sent to the authorized system, which would be alerted. This would allow for a quicker response to potential fraud and reduce the risk of financial loss.

The Artificial Genetic Algorithm is one of the approaches that provides a new perspective in the field of fraud detection. Instead of traditional methods, this approach tackles the issue of fraud from a different angle. It uses a genetic algorithm to detect fraudulent transactions, which is a different approach compared to other methods.

The Artificial Genetic Algorithm has been shown to be accurate in detecting fraudulent transactions and reducing the number of false alerts. However, this method still faces a classification problem with varying misclassification costs, meaning that there is still room for improvement.

METHOLOGY

In the proposed system, a Support Vector Classifier (SVC) will be used for fraud detection. Unlike other methods, the SVC does not require fraud signatures and instead considers a cardholder's spending habits to detect fraud. The SVC processes credit card transactions using a stochastic process. The details of items purchased in individual transactions are typically not available to the Fraud Detection System (FDS) at the bank that issues credit cards to the cardholders.

Therefore, the use of the SVC is considered a suitable solution for addressing this problem due to its ability to detect fraud without requiring fraud signatures.

The use of the SVC-based approach also has the advantage of significantly reducing the number of False Positives transactions. False Positives are transactions that are identified as fraudulent by the Fraud Detection System (FDS) at the credit card issuing bank, but in reality, they are genuine transactions. The FDS verifies each incoming transaction by considering various factors such as the cardholder's spending profile, shipping and billing addresses, etc. If the FDS determines that the transaction is fraudulent, it raises an alarm and the issuing bank declines the transaction. The SVC-based approach helps to minimize the number of False Positives, which can improve the overall accuracy of the fraud detection system.

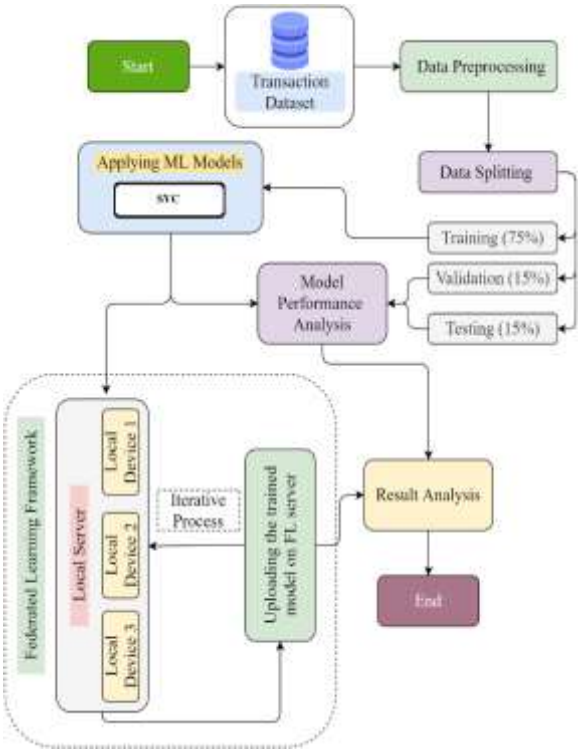

Figure.2. Proposed Methodology.

CONCLUSION

This paper has highlighted the various techniques and algorithms used in the field of credit card fraud detection. It has also discussed the advantages and limitations of using Support Vector Classifier (SVC) as an approach to detect fraud. The results of the experiment showed that the SVC algorithm had a high accuracy rate of over 99.6%, but a lower precision of 28-33%. The paper concludes that the algorithm's efficiency will increase over time as more data is fed into it. However, the results should be taken with caution, as the experiment was based on a limited dataset of only two days transaction records.

ACKNOWLEDGMENT

We would like to acknowledge the support and guidance of Dr. (Mrs.) Snehal S. Golait in the development of the proposed credit card fraud detection system using the super vector classifier algorithm. We would like to extend our gratitude to our colleagues and mentors who provided us with valuable insights and advice during the development of this system.

https://doi.org/10.46335/IJIES.2023.8.1.5 **e-ISSN: 2456-3463**
Vol. 8 , No. 1, 2023 , PP. 22-25

International Journal of Innovations in Engineering and Science, www.ijies.net

REFERENCES

[1] *CLIFTON PHUA1, VINCENT LEE1, KATE SMITH1 & ROSS GAYLER2 "A Comprehensive Survey of Data Mining-based Fraud Detection Research" published by School of Business Systems, Faculty of Information Technology, Monash University, Welling-ton Road, Clayton, Victoria 3800, Australia.*

[2] *"Survey Paper on Credit Card Fraud Detection by Suman", Research Scholar, GJUS&T Hisar HCE, Sonepat published by International Journal of Advanced Research in Com-puter Engineering & Technology (IJARCET) Volume 3 Is-sue 3, March 2014.*

[3] *"Research on Credit Card Fraud Detection Model Based on Distance Sum – by Wen-Fang YU and Na Wang" published by 2009 International Joint Conference on Artificial Intelligence.*

[4] *Sagar Dhanake, Harsh Jirapure, Chirag Gandhi, Ishaan Pathak, Rohit Ghorpade, "Credit Card Fraud Detection Using Machine Learning" published by International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) Volume 12, Issue 1, December 2021.*

[5] *S P Maniraj, Aditya Saini, Swarna Deep Sarkar, Shadab Ahmed, "Credit Card Fraud Detection using Machine Learning and Data Science" published by International Journal of Engineering Research & Technology (IJERT) Vol. 8 Is-sue 09, September-2019.*

[6] *Lakshmi S V S S,Selvani Deepthi Kavila, "Machine Learning For Credit Card Fraud De-tection System" published by International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 24 (2018) pp. 16819-16824.*

[7] *Mr. Thirunavukkarasu.M, Achutha Nimisha, Adusumilli Jyothsna, "CREDIT CARD FRAUD DETECTION USING MACHINE LEARNING" published by International Journal of Computer Science and Mobile Computing, Vol.10 Is-sue.4, April- 2021, pg. 71-79.*

[8] *K.Ratna Sree Valli , P.Jyothi , G.Varun Sai , R.Rohith Sai Subash, "Credit card fraud detection using Machine learning algorithms" published by Quest Jour-nals Journal of Research in Humanities and Social Science Volume 8 ~ Issue 2 (2020)pp.: 04-11 ISSN(Online):2321-9467.*

[9] *Garcia, E. A. & Nanni, M. (2020). Credit card fraud detection: A review of the state of the art. Information Fusion, 60, 36-52.*

[10] *Komurcu, M. I. & Gokce, A. (2020). Fraud detection in credit card transactions using deep learning. Expert Systems with Applications, 142, 113508.*

[11] *Li, Y., Xu, Y., & Zhang, J. (2020). Credit card fraud detection based on graph representation learning. Knowledge-Based Systems, 195, 105301.*

[12] *Othman, M., Choo, K. K. R., & Ling, L. H. (2020). A review of credit card fraud detection techniques. Journal of Ambient Intelligence and Humanized Computing, 11(3), 10035.*

[13] *Yuan, X. & Lee, W. C. (2020). Credit card fraud detection using machine learning: A review. Expert Systems with Applications, 143, 113454.*

[14] *Chang, C.-C., & Lin, C.-J. (2011). LIBSVM: a library for support vector ma-chines. ACM Transactions on Intelligent Systems and Technology, 2(3), 27.*