IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 15, May 2023

Credit Card Fraud Detection using Image Processing System

P. V. Pethe, C. P. Nashte, N. N. Ghadge, S. S. Kavathekar,S. S. Upase
Department of Computer Science and Engineering,
SVERI's College of Engineering, Pandharpur, India

Abstract: *In recent year credit card become one of the essential parts of the people sudden increase in E-commerce customer, started using credit card for online purchasing therefor for Risk of fraud also increases. Instead of carrying a huge amount in hand. It is easier to keep credit cards. But now a days that to become on safe now a days we are facing a big problem on credit card fraud, which in increasing in a good percentage. The main purpose is the survey on the various method applied to detect credit card frauds from the abnormality in the transaction. The fraudulent one is identified. We address these issues in order to implement some machine learning algorithm, like random forest Logistic regression in order to detect this kind of fraud in this paper. We increase the efficiency in finding the fraud how where we discussed and evaluated employee criteria currently the issues of credit card fraud detection have become a big problem from new researches. We implement and intelligent algorithm, which will detect all kind of fraud in a credit card transaction. We handle the problem by finding a pattern of each customer in between fraud and legal transaction isolation forest algorithm and local outlier factor are used to predict the pattern of transaction for each customer and a decision is made according to them in order to prevent data from miss matching all attributes are marked equally.*

I. INTRODUCTION

Today, as we can see, there is a significant increase in online payments, and the majority of these payments are made using credit cards. The unauthorised use of credit cards is a significant challenge for marketing firms. Fraudulent can be done in many ways such as tax return in any other account, taking loans with wrong information etc. Therefore, we need an efficient fraudulent detection model to minimize fraudulent activity and to minimize their losses. There are a huge number of new techniques which provide different algorithms which help in detecting number of credit card fraudulent activity. Basic understanding of these algorithms will propose computer learning methods that assist in locating questionable credit card transactions. The goal of machine learning's credit card fraud detection is to lessen this kind of fraudulent conduct. Credit Card Fraudulent detection comes under machine learning, and the objective is to reduce such type of fraudulent activity. This type of fraud is happening from past, and till now not much research has done here in this particular area.

II.LITERATURE SURVEY

he effectiveness of the model is assessed using a collection of credit card data that is openly accessible. Then an actual MasterCard data set from a financial institution is examined. To further evaluate the algorithms' robustness, noise is also injected into the information samples. In the empirical evaluation, a number of ordinary models, including NB, SVM, and DL, are used. The accuracy rates have all been above 99% when employing individual (standard) models and hybrid models that combine AdaBoost and majority voting methods on a publicly available Visa data set. AdaBoost-based hybrid techniques and majority voting techniques are used. Distinguish the fraudulent transactions from the cardholders' original transactions. Under sampling could result in the loss of important information, and oversampling could result in overfitting.

For many types of fraud cases, a solid grasp of normal and abnormal behaviours is required. For high dimensional data, SMOTE is not particularly useful. The convergence speed and reliability are improvised by the WOA. The ideal transaction weight is obtained via the whale optimisation code. The system becomes more effective because to the

DOI: 10.48175/IJARSCT-10940

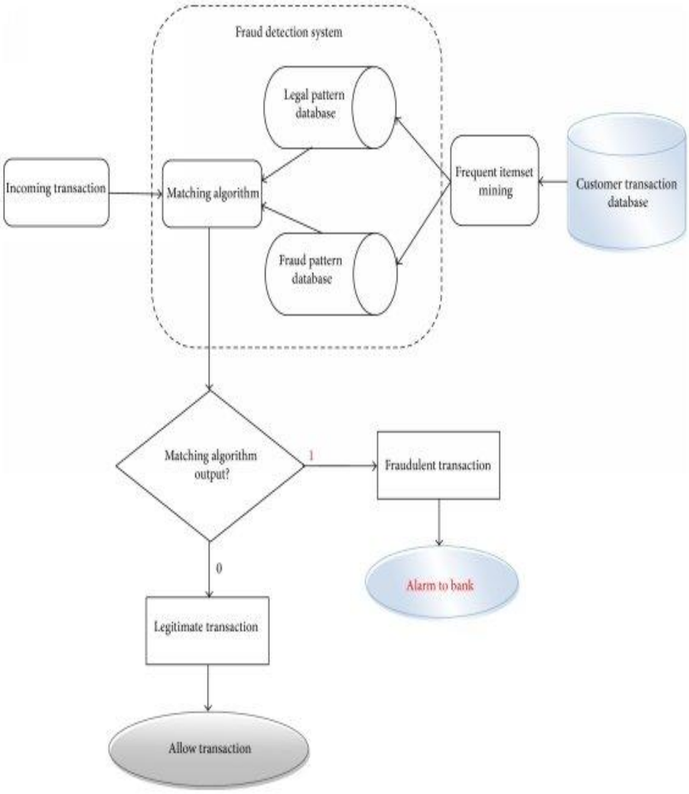
whale algorithm. The WOA formula adjusts the weight, detects inaccuracy, and optimises fraud transactions. The training and testing phases of the credit card fraud detection system's architectural design are separate processes.
There are two separate processes for the training component.

IIII.OBJECTIVE

To run a suitable business, vendors need to make a profit, which can be calculated by subtracting the cost of doing business from the total sell price. Therefore, fraudulent become a business's tolerance among online payment, among financing company, gross margin is calculated by (sell price - cost of goods sold). There will be low risk for fraudulent payment. In practice, whenever fraudulent occurs, the cardholder has to complain to the financing company and the debit from card is usually cancelled, which means there is a loss for either cardholder's bank or the finance company. Fraudulent turns as a financial risk to the financial company and the cardholder's bank. To overcome with fraudulent, fraudulent detection techniques should be used.
The main objective is to prevent the customer from fraud because if this kind of things keep happening then people will not show their interest in taking credit card and using their facility which is given by the banks and other financial company. Therefore, it's become an essential thing nowadays. People should also take care of their personal information by keeping it to the limited source. The fraudulent activity starts with the leaking of the someone personal information like credit number, one time password, registered mobile number and many more. The sharing of someone personal information should be reduced because fraudulent activity begins with the help of someone personal information like credit card number and many more.

IV.METHODOLOGY

The task which is performed for the prediction of transaction and labelled as fraud is detected on the basis of binaryclassification. We make two class for the prediction of fraud: class 0 and class 1.Class 0 if there is no fraud and class 1 to catch the fraud. This can be done with the help of binary classification.



DOI: 10.48175/IJARSCT-10940

V.ANALYSIS OF PROCESS

the credit card fraud detection process typically involves several steps and employs various techniques to identify and prevent fraudulent transactions. Here is a general outline of the credit card fraud detection process:

1. **Data Collection:** Credit card issuers and payment processors collect extensive transaction data, including cardholder information, transaction amounts, merchant details, timestamps, and other relevant data points.
2. **Data Pre-processing:** The collected data is pre-processed to remove noise, handle missing values, and transform it into a suitable format for analysis. This step may also involve data normalization and feature engineering to extract meaningful information.
3. **Rule-based Filtering:** Rule-based filters are applied to the data to identify suspicious patterns or activities. These rules are often based on predefined criteria such as transaction amount, location, merchant category codes, or user behavior. For example, if a transaction exceeds a certain threshold or occurs in a high-risk location, it may be flagged for further investigation.
4. **Machine Learning Models:** Advanced machine learning models are employed to analyze the transaction data and identify potential fraud patterns. These models are trained on historical data, including both fraudulent and non-fraudulent transactions, to learn patterns and make predictions. Commonly used techniques include logistic regression, decision trees, random forests, neural networks, or more sophisticated anomaly detection algorithms.
5. **Real-time Monitoring:** The transaction data is continuously monitored in real-time. As new transactions occur, they are compared against the learned patterns and statistical models. Any transaction that deviates significantly from normal behavior or exhibits suspicious characteristics is flagged for manual review or further analysis.
6. **Behavioral Analytics:** By analyzing the behavior of individual cardholders, including their spending patterns, geographic locations, and typical transaction types, behavioral analytics can identify deviations from the norm. This approach helps detect anomalies that may indicate fraudulent activity.
7. **Network Analysis:** Network analysis involves studying the relationships between different entities in the credit card ecosystem, such as merchants, cardholders, and payment processors. By examining the networks and connections, unusual patterns or links can be identified that may suggest fraudulent behavior.
8. **Collaboration and Data Sharing:** Credit card issuers and payment processors often collaborate and share data to enhance fraud detection. By pooling together information on fraudulent activities, they can identify patterns that may be missed by individual entities.
9. **Human Review:** Some flagged transactions are manually reviewed by fraud analysts. They investigate the suspicious activities, verify the legitimacy of the transaction, and take appropriate action, such as blocking the card, contacting the cardholder, or initiating a fraud investigation.

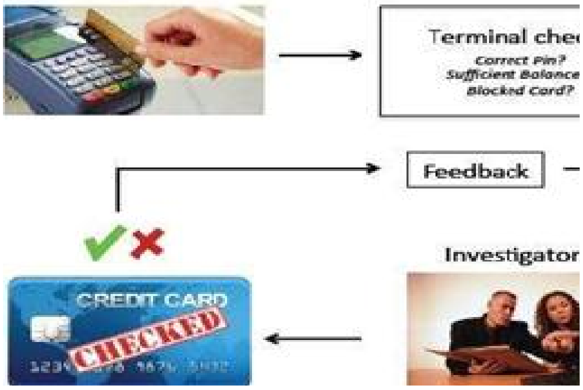


Figure 2: Use Case Diagram

VI.CONCLUSION

In this model, we discussed about credit card fraud detection using machine learning. The proposed model has been extensively tested on different types of transactions. The results were promising, almost all the fraudulent transactions could be detected successfully, and the proposed methodology has been compared with existing method and the results shows that proposed method performs superior than existing methods.

In this model, we detected the fraudulent transactions and recognized which illustrates the robustness of the proposed system. This proposed model took the trained dataset and performed classification on basis of them, if the transaction was legal then it moved to class 0 and if the transaction was fraud, then it moved to class 1, and significantly improve the detection accuracy.

The proposed method works efficiently in various platform, vivid environment and is a full- fledged cross platform application. The system has depicted robust, scalable and accurate performance to the degree that efficiency taken into consideration in the Credit Card Fraud Detection System. The system takes into consideration various factors and has been fulfilling or meeting all the project specifications documented.

VII.FUTURESCOPE

There is a very strong possibility of the system being adopted as a norm for the major banking and financial services applications as fraud detection and prevention is the major checkpoint in financial and banking sector.The above system is also likely to be embedded in other applications based, modified as per platform-specific/application specific environment. The banks, financial and retail institutes have faced huge losses owing to cause of a robust and accurate system to predict and prevent the fraudulent transactions going on in an institution. This in-turn affects the business capabilities and consumer trust of the company.Thus, the organizations have moved their focus onto implementing a system which can depict inconsistent transactions, providing banks a privilege to act upon it take necessary measures.

VIII.ACKNOWLEDGMENTS

We would like to express our deep sense of gratitude to our guide Prof. K.I. Chouhan madam for his invaluable help and guidance for the duration of project. We are highly indebted him for constantly encouraging us by giving critics on our work. We would like to thank our HOD Prof S. P. Pawar for his encouragement throughout the semester which gave us confidence that we can complete our project successfully. We express gratitude towards, Project Coordinator Prof P. D. Mane for providing the support and giving his valuable time, indispensable support and his priceless suggestions. We also express gratitude towards our all-teaching non-teaching staff, family members and our Friends for encouraging us with their valuable suggestions and motivating us from time to time.

REFERENCES

[1] V. Bhusari S. Patil, "Study of Hidden Markov Model in Credit Card Fraudulent Detection", International Journal of Computer Applications (0975-8887) Volume 20- No.5. April 2011

[2] Priya Ravindra Shimpi, Prof. VijayalaxmiKadroliAngrish. "Survey on Credit Card Fraud Detection Techniques". International Journal of Engineering and Computer Science ISSN: 2319-7242 [3] Salvatore J. Stolfo, Wei Fan, WenkeLee, "Cost-based Modeling for Fraud and Intrusion Detection Results from the JAM Project", In Proceedings of the ACM SIGMOD Conference on Management of Data, pages 207 216, 2014.

[3] Delamaire. L. Abdou, HAH and Pointon. J."Credit card fraud and detection techniques", Banks and Bank Systems, Volume 4, Issue 2, 2009.

[4] Suman, Nutan, "Review Paper on Credit Card Fraud Detection", International Journal of Computer Trends and Technology (ICTT)-volume 4 Issue 7-July 2013.

[5] Renu, Suman, "Analysis on Credit Card Fraud Detection Methods". International Journal of Computer Trends and Technology (IJCTT)-volume 8 number 1 - Feb 2014.

[6] Deepak Pawar, Swapnil Rabsc, Sameer Paradkar, NainaKaushi, "Detection of Fraud in Online Credit Card Transactions". International Journal of Technical Research and Applications e-ISSN: 2320-8163.

[7] Sushmito Ghosh and Douglas L. Reilly, "Credit Card Fraud Detection with a Neural- Network" Proc. IEEE First Int. Conf. on Neural Networks, 2014.

DOI: 10.48175/IJARSCT-10940