International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/IJSRCSEIT

Credit Card Fraud Detection Using Machine Learning Techniques

Aruna Kumar Joshi[1], Vikram Shirol[2], Shreekanth Jogar[3], Pavankumar Naik[4], Annapoorna Yaligar[5]

[1,2,3,4,5] Department of Computer Science and Engineering, SKSVMACET Laxmeshwar, Karnataka, India

ABSTRACT

Credit Card Fraud is one of the major moral issues in the public and private bans sector. The effect of this problems leads to the several ethical trouble. The important themes are to notice the distinctive kinds of credit card fraud and to locate different methods that have been used in fraud detection. The sub-point is to suppose about existing and ruin down as of late dispensed discoveries in fraud detection. Probable upon the variety of extortion appeared with the banks or different financial organizations, exceptional measures can be embraced and executed. The work carried out in this paper are usually going to have really beneficial residences as a approaches as expenditure reserve fund and time capability. The cost utilization of the strategies investigated proper right here is in the minimization of credit card fraud. Anyway, there are up to now moral troubles when appropriate credit card customers are unsorted as fraudulent. Credit Card Fraud Detection is an method which will help people for their transaction process in shopping mall and any other transaction process nowadays fraud detection is nothing but an process where the criminals are found and there are many illegal activities are taking place which causes difficulty for people. Here in this paper we are using SMOTE technique to find fraud and this technique will help to sort both the normal transaction and fraud transaction this process can make easy to find fraudulent. And Neural Network KNN are also taken place to find Credit Card Fraud.

Keywords : Card Fraud, Recognition Systems, Credit Bureau, Information Mining Methods.

I. INTRODUCTION

The credit / Debit / any financial service card is a tiny plastic card given to members of that specific financial organization with the proper identity and verification. This tiny plastic card helps for money transaction as instalment bases or one-time settlement. Credit card safety relies upon on the bodily protection of the plastic card simply as the safety of the debit/credit card identity number. People are utilizing public internet for the on-line payment services. Which is completely based on the agreement between card holder and financial institution. After introducing this method, the tremendous improvement in the purchasing through e-payment worldwide. Credit /debit/financial card fraud is a worldwide running problem. The hackers are also updating and finding alternative ways to carry out the financial fraud especially with the credit card. Fraud identification are persistently developed to shield lawbreakers in adjusting to their fake procedures.

Extortion in credit card exchange is unapproved and undesirable use of a record by somebody apart from the different kinds of asset or properties of that account holder. The vital expectation measures can be taken to prevent this maltreatment and then conduct fake practices which can be concentrated to limit it and characterized as a situation where a stranger uses another person's credit card for the way that the card is being used.

This is an exceptionally significant issue that requests the consideration of networks, for example AI and information science where the answer for this issue can be automated. These are now not solely challenging in the implementation of a real-world fraud detection system, however. In actual world examples, the big movement of payment requests is rapidly scanned via computerized gadgets that decide which transaction to authorize.

The new methods of Machine Learning specific algorithms are applied to break down all the approved exchanges and report the suspicious ones. These reports are examined by experts who contact the cardholders to confirm if the exchange was certifiable tricky. The specialists give an input to the mechanized framework which is utilized to prepare and refresh the calculation to run the fraud recognition execution.

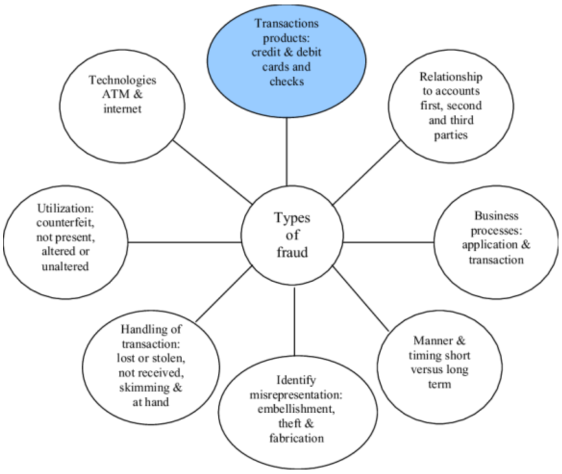

Transactions products: credit & debit cards and checks
Technologies ATM & internet
Relationship to accounts first, second and third parties
Utilization: counterfeit, not present, altered or unaltered
Types of fraud
Business processes: application & transaction
Handling of transaction: lost or stolen, not received, skimming & at hand
Identify misrepresentation: embellishment, theft & fabrication
Manner & timing short versus long term

Fig1: Types of Fraud

Fraud recognition techniques are consistently evolved to safeguard them in adjusting to their fraudulent methodologies. These frauds are named.

- Different Credit Card Frauds: Online and Offline mode.
- Credit Card Theft.
- Account Eradication
- Credit Card Device Interruption.
- Application by Illegal Person.
- Fake Card.
- Media Transmission Theft.

II. LITERATURE SURVEY

In earlier investigations, man approaches have been proposed to bring arrangements to detect fraud from supervised approaches, unsupervised ways to deal with crossover ones which makes it an unquestionable requirement to become familiar with the advancements related in credit card fakes discovery and to have an away from the such kinds of credit card fraud. As time advanced fraud designs developed presenting new types of extortion making it a sharp territory of enthusiasm for examines. An examination area was introduced by different authors where they utilized anomaly mining, Anomaly discovery mining and separation entirety calculations to precisely foresee deceitful exchange in a copying test of credit card exchange informational collection of one certain business bank. Anomaly mining is a field of information mining which is essentially utilized in monetary and web fields. It manages recognizing objects that are confined from the first framework that is exchange that aren't regular.

S.P. Maniraj et.al.[1] has machine learning and data science on credit card fraud detection algorithm, different algorithm used Artificial neural network, Logistic algorithms, Bayesian networks, K-nearest neighbour. To identify fraudulent credit card transactions so that customers are not charged for items that they did not purchase but data size is smaller and takes less number of features.

Anuruddha thennakoon et.al [2] has Real-time credit card fraud detection using machine learning in this paper different algorithms are used but the use of predictive analytics done by the implemented machine learning models and an API module to decide if a particular transaction is genuine or fraudulent.

Lindadela maire et.al [3] Credit card fraud detection techniques explained types of frauds by using data mining techniques.The main usage is to identify the different types of credit card fraud, and secondly to review alternative techniques that have been used in fraud personals loans, home loans and retail but result of finding fraud in not up to marks

Aishwarya kaneri et.al [4] Fraud detection in online credit card payment, explained about online credit card fraud by outlier analysis but false alerts and improving existing models for detection of fraud is still faces the problem

Gurram sai kumar [5] Credit card fraud detection system based on machine learning techniques, in this paper authors explained how to reduce credit card application fraud and risk based on decision tree induction using genetic algorithms but due to sensitivity of customers' financial information, getting clean data is hard for mining applications

Shiv shankar singh et.al [6] Electronic credit card fraud detection system by collaboration of machine learning models, the author of this paper explained fraud detection with the collaboration of different techniques bur fraud activities that cannot be detected completely by examine the results of logistic regression, decision tree and support vector machine .

III. DESCRIPTION OF PROPOSED TECHNIQUES

Every single project should be contained objectives of a project here in this paper we have used four main objectives they are:

- ❖ Collection of datasets.
- ❖ Classification of dataset.
- ❖ Using specific algorithm.
- ❖ Fraud detection.

At first the dataset should be collect the data from bank to sort normal transaction and fraud transaction and the SMOTE technique should be applied into the program which will be running by bank holder and then the algorithm will find the difference between both the transaction which helps to find the credit card fraud.

DETECTION PROCESS:

Step 1: Separate every individual customer's transactions from the entire transaction database.

Step 2: From the transaction of all the customers' database separate the transaction of his/her legal and fraud transactions.

Step 3: Apply the specific standard algorithm to the set of legal transaction of different customers find the difference between both transactions.

The main architecture of a credit card fraud detection is shown below with the flow of a fraud detection process. When looked at in detail for a bigger scope alongside genuine components, the full design can be spoken to as follows:

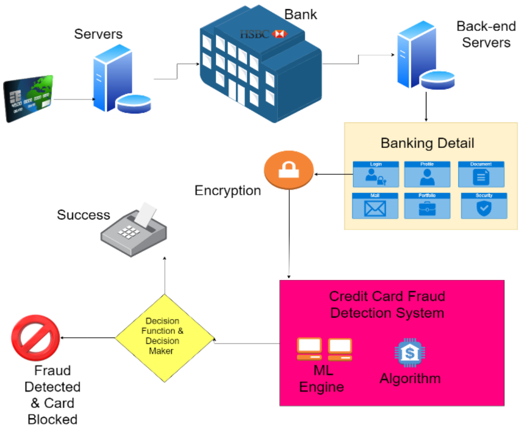


Fig 2(a) : Fraud Detection architecture

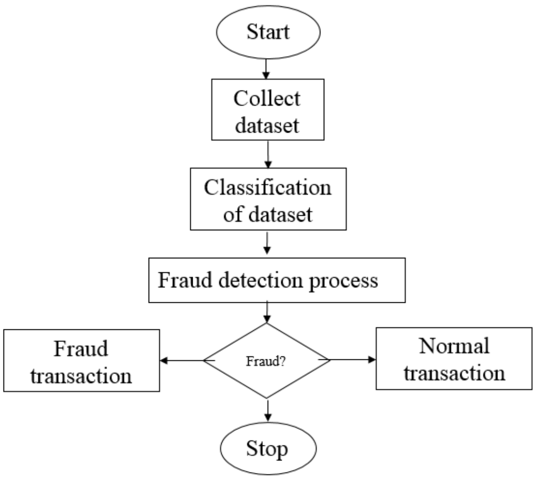


Fig 2(b): Farad detection flow

As a matter of first we acquired our dataset from Kaggle, an information examination site which gives sample datasets of bank which helps to identify the different intended transactions and also helps to separate these transactions Kaggle dataset contains 31 segments, out of these 31 segments 28 are named as v1-v28 to ensure delicate and identify the information. Different segments speak with respect to the time, amount and class. Time shows consumed duration between the main exchange and the fraud one. The amount is the money transacted from one unique account number to another unique account number. Class 0 stands for substantial exchange and 1 stands for fake. We plot various diagrams to check for irregularities in the dataset and to outwardly understand it:

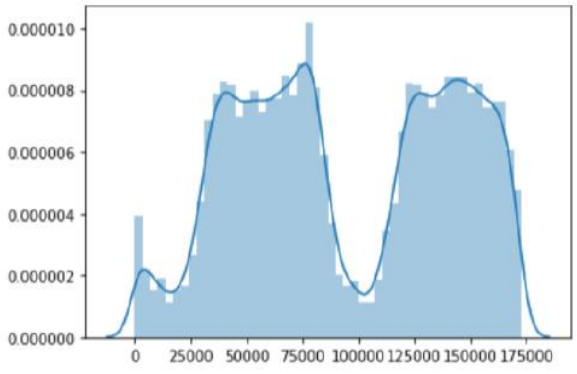


Fig3: Fraud Class Histogram

These are results when we got by executing the source code you can get dataset in Kaggle website this is fraud class histogram graphs which shows the graph of a normal transaction with 0 and fraud transaction with 1 as you can see in the graphs.

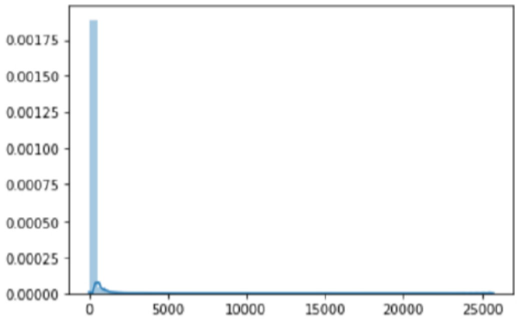
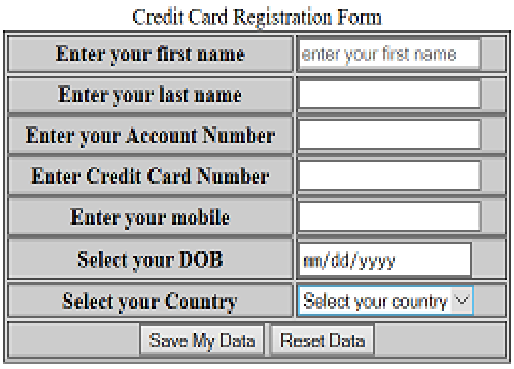


Fig4: Fraud class Histogram

Such histogram graphs are very familiar to understand the normal transaction and fraud transaction with the help of SMOTE technique which will clearly give the accurate results.

IV. WEB APPLICATION

Web application is nothing but an application which is handled by the bank which contains the details of an cardholder as shown below with registration form and detection form the details of an cardholder will help bankers to find the cardholder is genuine or not. The cardholder details are taken by bank to safeguard the account of an cardholder from fraud transaction and this web application will be directly connected to the source code to find the fraud instantly here is sample registration form.



Credit Card Registration Form

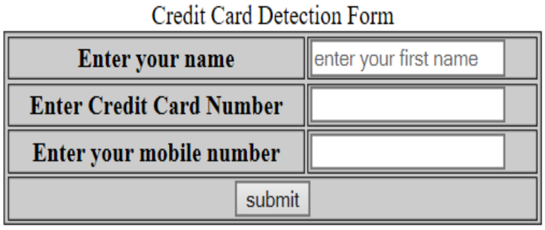
Enter your first name	enter your first name
Enter your last name	
Enter your Account Number	
Enter Credit Card Number	
Enter your mobile	
Select your DOB	mm/dd/yyyy
Select your Country	Select your country
	Save My Data Reset Data

Fig5: Registration Form

The detection form is a procedure taken by bank to know the card is belongs to the person holding card or not it is shown. As shows in fig it contains the name, credit card number, and mobile number. By taking these information the bank will get them to know the credit card fraud because the algorithm used by the bank will be different and that algorithm is instructed as to find the fraud by knowing algorithm used by hackers into the fraudulent transaction this process will be useful to find the fraud detection.

If the card has been lost from card holder can go to bank and block their card transaction and take another card with same account number the card which is rubbed will be blocked and the hacker/theft can't be done any transaction. This process will help card holder to protect their money.

Fig6: Detection Form



Credit Card Detection Form

Enter your name	enter your first name
Enter Credit Card Number	
Enter your mobile number	
submit	

Sorts of Frauds: Different kinds of frauds in this article embrace credit card frauds, telecommunication frauds, computer disturbance, Eradication fraud, Robberies fraud/fake fraud, Application fraud, Behavioural fraud.

Credit Card Fraud are classified into two types:

1) Offline fraud: It is a type of fraud when the card is lost or if any duplicate cards have been used for fraud transaction.
2) Online fraud: It is a type of fraud where hackers make use of internet and make fraud transaction by collecting card holder information.

SMOTE: Imbalanced order includes creating prescient models on characterization datasets that have an extreme class irregularity. Primary points is to recognize the fraud exchanges happening during the exchanges made by the card holder. The framework likewise means to improve the assembly speed and unravels the information imbalance. One approach is to address the imbalanced datasets to oversample the minority class. The simplest approach involves duplicating the examples in the minority class, although these examples do not add any new information to the model. Instead, new examples can be integrating from the present examples. This is a type of data augmentation for the minority class and is referred to as the Synthetic Minority Oversampling Technique, or SMOTE.

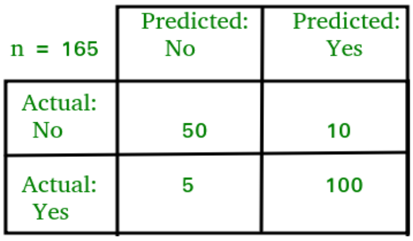
SMOTE first selects a minority class instance at random and finds its k-nearest minority class neighbour's. The synthetic instance is then created by choosing one of the k-nearest neighbour's b at random and connecting x and y to form a line segment in the feature space. The synthetic instances are generated as x convex combination of the two chosen instances x and y.

K-Nearest Neighbour: K-Nearest Neighbour Algorithm is one of the least difficult grouping and it is one of the most utilized learning calculations. It is a non-parametric, languid learning algorithm. Its motivation is to utilize a database where the information focuses are isolated into a few classes to anticipate the characterization of another example point. t the point when we state a system is non-parametric, it implies that it does not make any presumptions on the basic information circulation. The KNN keeps all the training data. To be more exact, all the training data is indeed during the testing phase. In this article KNN will be collecting financial characteristics vs. comparing customers with similar financial features to a database. By the very nature of a credit rating, people who have similar credit ratings. Therefore, they would like to be able to use this existing database to predict a new customer's credit rating, without having to perform all the calculations.

This is how both the techniques will work in credit card fraud detection process here detecting a fraud will be a major role to be done. This is how the flow will be move on.

V. RESULT

A confusion matrix is a table (shows in the below table 1) that is often used to describe the performance of a classification model (or "classifier") on a set of test data for which the true values are known.



n = 165	Predicted: No	Predicted: Yes
Actual: No	50	10
Actual: Yes	5	100

Table 1: confusion matrix format

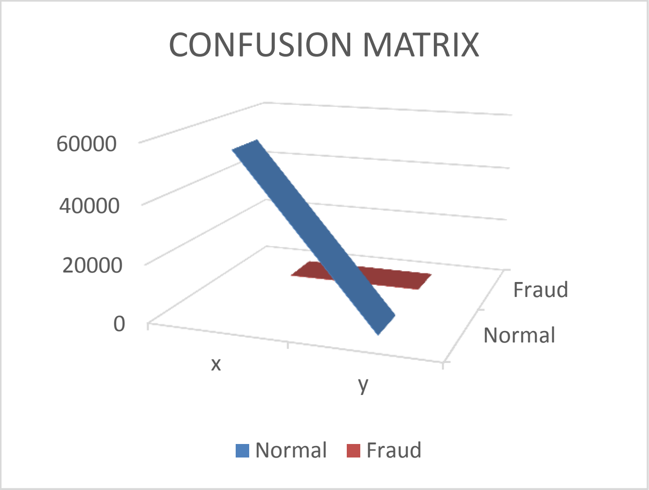


Fig 7: Confusion matrix

The above fig 7 shows the confusion matrix graph of normal and fraud transaction with X and Y axis. Where blue color indicates the normal transaction and yellow will indicate the fraud transaction. As shown in the below fig 8 confusion matrix will gives the fraud and normal transaction with the help of relationship shown in figure.

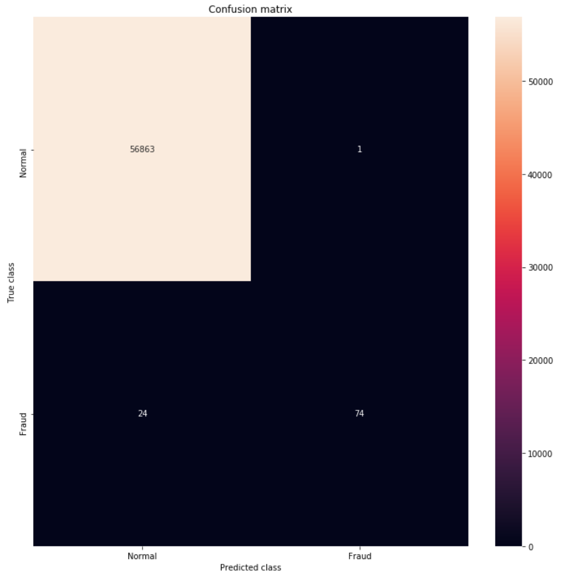


Fig 8: Confusion Matrix – True class and predicted class result

From the Table 1 actual and predicted fraud are need to be calculated where n number of fraudulent activities are done but in that there need to be and normal and fraud transaction history are need to be predicted with Yes as fraud transaction and No as normal transaction.

The confusion matric will give the true positive and false positive result by showing difference between both actual and predicted transaction.

By suing SMOTE method we get 98.7 percent of detection result which will give best result of detection of fraud transaction.

VI. CONCLUSION & FUTURE SCOPE

Hence there are numerous character check techniques accessible today nobody can recognize all cheats altogether while they are really occurring, they generally detect it till the fraud has been found. This happens on the grounds that an exceptionally little number of exchanges from the all-out exchanges are deceitful in nature. SMOTE technique will find the fraud detection by sorting both normal transaction and fraud transaction. Credit card fraud detection system using KNN algorithm and SMOTE (Synthetic minority optimization technique) points in distinguishing the extortion exchanges happening during the exchanges made by the card holder. The system also points to improve the assembly speed and understands the information imbalance. The receiver operating characteristics (ROC) shows that the relation between the normal transaction rate and fraud transaction rate.

VII. REFERENCES

[1]. S P maniraj ,aditya saini,swarna deep sarkar,shadab ahmad, Credit card fraud detection using machine learning and data science. International Journal of Engineering Research & Technology (IJERT), volume8, issue 09, september-2019.

[2]. Anuruddha thennakoon chee bhagyani, sasitha premadasa, shalitha mihiranga, nuwan kuruwitaarachchi. Real-time credit card fraud detection using machine learning in 2019.

[3]. lindadelamaire(uk), Hussein abdou(uk), john pointon (uk), Credit card fraud detection techniques. in volume4, issue 2, 2009.

[4]. Aishwarya kaneri et al. Fraud detection in online credit card payment. International Research Journal of Engineering and Technology (IRJET), In volume 05 issue 03 mar-2018.

[5]. Gaurram sai kumar, madala venkaiah naidu, dr.Madugula sujatha. Credit card fraud detection system based on machine learning techniques, IOSR Journal of Computer Engineering (IOSR-JCE) in volume 21, issue 3, ser. V (may - june 2019).

[6]. Shiv shankar singh et al. Electronic credit card fraud detection system by collaboration of machine learning models, International Journal of Innovative Technology and Exploring Engineering (IJITEE) in volume-8 issue-12s, october 201

Cite this article as :

Aruna Kumar Joshi, Vikram Shirol, Shreekanth Jogar, Pavankumar Naik, Annapoorna Yaligar, "Credit Card Fraud Detection Using Machine Learning Techniques", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 3, pp. 436-442, May-June 2020.
Journal URL : http://ijsrcseit.com/CSEIT2063114