FRAUD DETECTION OF CREDIT CARD TRANSACTION AT CLIENT SIDE USING MACHINE LEARNING

[1]G. Ganesh krishnareddy, [2]B.V. V. A Narashima rao, [3]P. Maheshbabu
[4]K. Lokesh, [5]Mrs. R.C. Dyana Priyatharsini

[1,2,3,4]Students, [5]Assistant Professor,
Department of Computer Science and Engineering,
Bharath Institute of Higher Education and Research

Abstract- **Now a days due to the rise and rapid growth of Ecommerce, use of credit card for the online purchase has dramatically increased nowadays people using online mode it causes an explosion in the credit card fraud. As credit card becomes the most popular mode of payments for both online as well as regular purchase cases of fraud associated with it are also rising. In real life, more transactions are going on many people are using credit cards, Implementation of efficient system has become imperative for all credit card issuing banks to minimize their loses. many modern techniques based on AI, data mining, fuzzy logic, ML, sequence alignment, Genetic programming etc.., has evolved in detecting various credit cards fraudulent transactions. A clear understanding to all these approaches will certainly lead to an efficient credit card fraud detection system, this will present the various techniques used in credit card fraud detection system.**

INTRODUCTION:

Now, a days due to the rise and rapid growth of E-commerce, use of credit card for the online purchase has dramatically increased now a days people using online mode it causes an explosion in the credit card fraud. The aim of this project is to predict transaction through Machine Learning which predicts the transaction is fraud by using some techniques that are K-Means clustering, Neural Networks , Data Mining . The main objective is to scan transaction if any fraud occurs and to make other transactions automatically without any Hustle. Logistic Regression is used to check previous transaction and compare present transaction details and make a model to predict the future fraud transaction

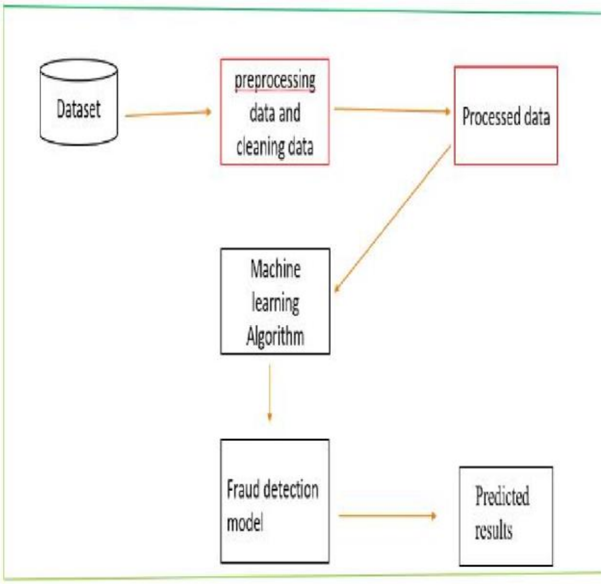
LITERATURE SURVEY:

The fraud detection is a complex task and there is no system that correctly predicts any transactions as fraudulent. The properties for a good fraud detection system are: Should identify the frauds accurately, should detect the frauds quickly, should not classify a genuine transaction as fraud. Outlier detection is a critical task as outliers indicate normal running conditions. Techniques used in fraud detection can be divided into two: 1) Supervised techniques where past known fraud cases are used to build a model which will produce the new transactions. 2) Unsupervised are those where there are no prior sets in which the state of the transactions is known to be fraud. Unsupervised outlier detection technique: An unsupervised outlier detection technique does not make any assumption about the availability of labelled data. This method simply seeks those accounts, customer etc, whose behaviour is “unusual”. Unsupervised methods are useful in applications where there is no prior knowledge about the particular class of observations in a data set. An advantage of using unsupervised methods over supervised methods is that previously occurred undiscovered types of fraud may be detected. There are some techniques which were used now a day they are as follows: Peer Group Analysis - Peer Group Analysis (PGA) is an unsupervised method for monitoring behaviour over time in data mining. The main task of PGA method is to identify peer groups for all the present target observations. The tool detects individual objects that begin to behave in a different manner from objects to which they had previously been similar. Each object is selected as a target object and is compared with all other objects in the database, using either external comparison criteria or internal criteria by summarizing earlier behaviour patterns of each object. A peer group of objects most similar to the target object is chosen on the basis of comparisons. The tool is a part of the data mining process that involves cycling between the detection of objects that behave in different ways and the detailed examination of those objects. PGA method is used in credit card fraud detection by changing the length of the time windows that is used initially to determine the peer group. Break Point Analysis - Break Point Analysis is another unsupervised outlier detection tool that is developed for behavioural fraud detection. A break point is an observation or time for detecting anomalous behaviour. Break point analysis is operated on the account level by comparing sequences of transactions so that a change in behaviour for a particular account is detected. In break point analysis, a fixed length moving window of transactions is present, as a transaction occurs it enters into the window and the oldest transaction from the window is removed. An advantage of using break point analysis is that the balanced, data is not required as the transactions between different accounts are not compared and the anomalous sequences of events that may indicate fraudulent behaviours can be identified.

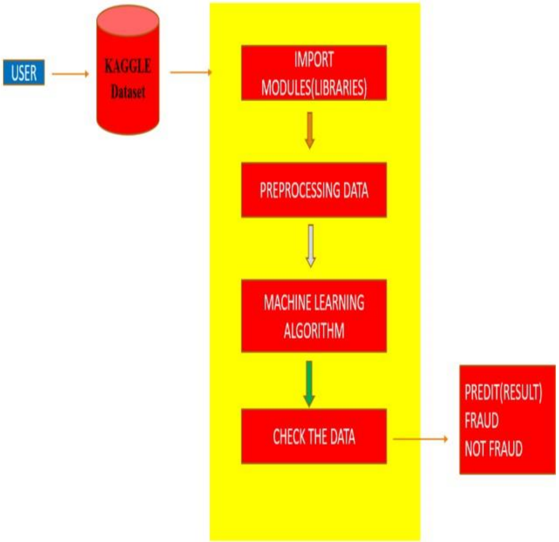
PROPOSED SYSTEM:

The two data mining approaches, are support vector machines and random forests, together with the well-known logistic regression, as part of an attempt to detect the credit card fraud. It is wellunderstood, easy to use, and it is most commonly used for data mining. Thus, it provides a useful baseline for comparing performance of newer methods. Supervised learning methods for fraud detection face two challenges. They are: 1. The unbalanced class sizes of legitimate and fraudulent transactions, with legitimate transactions far outnumbering fraudulent ones. 2. The second is to develop supervised models for fraud that can arise from potentially undetected fraud transactions, leading to mislabelled cases in the data to be used for building the model. For the purpose of the above problems, the fraudulent transactions are those specifically identified by the institutional auditors as those that caused an unlawful transfer of funds from the bank sponsoring the credit cards. These transactions were observed to be fraudulent expose. The study is based on real-life data of transactions from an international credit card operation.

SYSTEM ARCHITECTURE:


Dataset
preprocessing data and cleaning data
Processed data
Machine learning Algorithm
Fraud detection model
Predicted results

DATA FLOW DIAGRAM


USER
KAGGLE Dataset
IMPORT MODULES(LIBRARIES)
PREPROCESSING DATA
MACHINE LEARNING ALGORITHM
CHECK THE DATA
PREDIT(RESULT) FRAUD NOT FRAUD

MODULES:

- **DATA GATHERING**
- **DATA PREPROCESSING**
- **V SERIES CONVERTING INTO SENSTIVE INFORMATION**
- **FRAUD DETECTION USING LOGISTIC REGRESSION**

CONCLUSION:

Credit card fraud has become more and more rampant in recent years. Fraud detection methods are continuously developed to different criminals in adapting to their strategies a fraud detection, identifying fraud as quickly as possible once it has been done through fraud detection techniques, is now becoming easier and faster. The techniques which were studied here through which credit card fraud can be detected quickly and fast and the crime can be stopped

REFERENCES:

1. Iqra Malik; Hikmat Ullah khan; et.al, “Credit Card Fraud Detection Using Stateof-the-Art Machine Learning and Deep Learning Algorithms” 39700 - 39715:(2022).
2. Yanxia Sun; Zenghui Wang; et.al, “Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost” 165286 - 165294:(2021).
3. Ibomoiye Domor Mienye; Theo G. Swart; et.al, “A Neural Network Ensemble With Feature Engineering for Improved Credit Card Fraud Detection” 16400 - 16407:(2022).
4. Wendy Wang; YiLiu; et.al, “Integrating Machine Learning Algorithms with Quantum Annealing Solvers for Online Fraud Detection” 75908 - 75917:(2022).
5. Tian-Shyr Dal; yen-Wu Ti; et.al, “Feature Engineering and Resampling Strategies for Fund Transfer Fraud with Limited Transaction Data” 86101 - 86116(2022).
6. Theo Verhelst; Yann-Ael Le Borgne; el.at, “Transfer Learning Strategies for Credit Card Fraud Detection” 114754 - 114766:(2021)