International Journal of Innovative Research in Computerand Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

||Volume 8, Issue 7, July 2020||

Credit Card Fraud Detection Using Machine Learning

Kavyashree N[1], Gagana H D[2], Harshitha A N[3], Harshitha B G[4]

Assistant Professor, Dept. of CSE, BGS Institute of Technology, BG Nagar, Mandya, Karnataka, India [1]

B. E Scholar, Dept. of CSE, BGS Institute of Technology, BG Nagar, Mandya, Karnataka, India[2]

B. E Scholar, Dept. of CSE, BGS Institute of Technology, BG Nagar, Mandya, Karnataka, India[3]

B. E Scholar, Dept. of CSE, BGS Institute of Technology, B G Nagar, Mandya, Karnataka, India[4]

ABSTRACT: Credit card fraud is a very serious problem in the financial services. Credit card fraud is concerned with the illegal use of credit card information for all the areas. Data analytics is to describe hidden patterns and used it in the different situations. Credit card fraud is accelerating with the advanced modern technology and it became an easy and friendly target for fraud. In this paper, we are present a supervised machine learning algorithms using a real-world dataset to detect the credit card fraudulent transactions. These algorithms are using ensemble learning methods to implement a super classifier. We described a variable that initiate to get higher accuracy in credit card fraudulent transaction detection. The different supervised machine learning algorithms are used to compare and discuss the performance evaluation results in this paper.

KEYWORDS: Credit Card**,** Fraud detection, Supervised machine learning, Classification, Imbalanced dataset, Sampling.

I. INTRODUCTION

Now a day everyone using credit cards for online money transactions. The credit card is used to make purchases with a line of credit. Comparing with debit card credit card is more useful for users. Debit card is also a payment card but after purchase money directly reduce from the cardholders account. The advantage of using credit card is the user can purchase if the account does not have balance so the credit card can be used in all areas.

In these days the developers are more focused and developing the new opportunities of online transactions. the frauds are tried to steal and
abuse the credit card is also increasing. because without any risk the frauds can obtain amount which is sufficiently great in a short span of time, the fraud can easily abuse credit card so that credit card is friendlier object for fraud. when frauds are tried to steal credit card, they stole the important data of a card holder. the important data in case of a cardholder is card number, pin number and account details. then the frauds hack the cardholder's bank account to make transaction used by stolen information. as a result, cardholders face
financial losses and require a hard effort to recover their credits.

In this paper, we implement a new application which developing using decision tree algorithm based on machine learning technique. decision tree is under the category of supervised learning. credit card transaction is a common procedure in the recent years. in the case of an existing credit card fraud detection system it very difficult to detect whether a fraud is try to steal the card details or not. but using machine learning classifiers we can easily recognize the fraud transaction and legitimate transaction.

II. EXISTING SYSTEM

In the traditional fraud detection system, the frauds steal or abuse the credit card of a card holder. The cardholders came to know about this attack if they check their balance or try to make an online transaction it shows like "no balance for transaction". Then the card holder's complaint against this fraud attack after fraudulent transaction. An action will take based on card holder's complaint and then they may detect the fraud. Before finishing the investigation, the card holders have to face a lot of problems.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

||Volume 8, Issue 7, July 2020||

III. PROPOSED SYSTEM

The working of traditional fraud detection system is described above. From above observations, we understand that we have to propose a new application for improving the performance efficiency. So we proposed a new application based on a supervised learning and we are using decision tree classifier as algorithm to implement this new application. To overcome the disadvantages of traditional fraud detection system we are implemented a new application. The new implemented application provides more safety and security for the card holders. If any fraud is tried to steal or abuse the card holder details or tried to make a transaction is detected, the implemented application is automatically pass the message to the card holder through email or call immediately

IV. MATERIALS AND METHODS

A. Supervised learning and unsupervised learning

The most important type of learning is described in this project. Supervised learning is help to describe the label on the previous transactions, to check out the previous transactions the supervised learning is not powerful for recognize the fraud pattern or fraud transaction. Comparing supervised learning, unsupervised learning is more helps to recognize the fraud transaction classes.

B. Unbalanced data

To learn a balancing dataset and unbalancing dataset is quite challenging and difficult. A sampling method is used to learn balancing dataset and unbalancing dataset. At September 2013, the European cardholders attempt 284,807 transactions available in a dataset publicly.

From 284,807 transactions dataset 492 fraud transactions are detected. Finally they find that the detected fraud transactions are highly imbalanced. To overcome this big problem they used under-sampling technique. Under-sampling is the process of reducing the dataset imbalance in a transaction.

C. Fraud Detection Classifier

Ten different classifiers are used in this project. The important models such as accuracy, precision score, recall score, TPR, FPR, F1-score, G-mean and specificity used to compare the performance of above mentioned ten classifiers.

Logistic Regression

In this project LR is used to evaluate performance and compared result with other classifiers.

Decision Tree

DT classifier is used to implement this project. DT is used to evaluate performance and compared result.

Random Forest

A collection of decision tree is used by random forest classifier, each decision tree is different from one another and this is used for the classification and regression.

Navies Bayes

Navies Bayes classifier is first introduced in 1995, it consists of a collection of classification algorithms. Navies Bayes classifier is using Bayes theorem concept for independence hypothesis.

KNN

KNN algorithm is used for both classification as well as regression, which is a calculation to store each and every single occurrence.

Gradient Boosted Tree Classifier (GBT)

GBT consist of a group of models and this model includes both classification as well as regression in which it is produce prediction model. Tree accuracy upgraded in the gradient boosted tree classifier.

XGB (XG boost Classifier)

XGB is a refined classifier means it is an implementation of gradient boosted decision trees, XGB classifier describes all different category of dataset. XGB classifier is mainly designed for high speed and better performance.

SVM

SVM presented in 1995. The support vector machines are useful in a mixture of group assignments.

V. AES ALGORITHM

Advanced Encryption standard (AES) calculation is one at the maximum famous and normally symmetric square figure calculation utilized in around the world. This calculation has a claim unique structure to scramble and decode

sensitive statistics and is connected in equipment and programming everywhere throughout the world. It's far highly tough to programmers to get the real facts even as encoding by way of AES calculation.

Until date isn't always any proof to crake this calculation. AES can manipulate three unique key sizes, as an example, AES128, 192and 256pieces and every considered one of these figures has 128 piece rectangular lengths. This paper will deliver a diagram of AES calculation and make clear some pressing highlights of this calculation in subtleties and exhibit a few beyond inquires about that have executed on it with contrasting with distinct calculations, for example,DES,3DES, Blowfish and so on.

Cryptography is a standout among the most noteworthy and well known systems to verify the statistics from aggressors by using utilising vital processes this is Encryption and Decryption. Encryption is the way towards encoding records to hold it from interlopers to peruse the first data successfully. This degree can trade over the primary information into combined up arrangement called Cipher content material. The following technique that as to be carryout by way of permitted man or woman is decryption procedure.

Interpreting is opposite of encryption. Its mile the method to change over discerns content material into plain content cloth without lacking any terms within the first content. To play out that method cryptography is predicated upon on numerical computations along advantageous substitutions and modifications with or without any key.

VI. CONCLUSION AND FUTURE WORK

This project presents a good fraudulent transaction detection system based on machine learning technique using decision tree algorithm. The admin is controlling all over the fraudulent transaction detection system. It is managing the Users card details, detecting fraud transaction, identify new unusual behaviour, providing authentication for user's card details to prevent fraud transaction. A proxy server is used to generate a private key to provide the authentication and authorization for the uses card details; it provides more security and reduces the fraudulent transaction. The main advantage of this proposed system is minimizing losses, providing high speed and security, saving time, increased performance, operational efficiency and accuracy, automatically find the pattern of frauds, and automatically create rules.

REFERENCES

[1] G. Rushin, C. Stancil, M. Sun, S. Adams, and P. Beling, "Horse race analysis in creditcardfraud - Deep learning, logistic regression, and Gradient Boosted Tree,"*2017 Syst.Inf. Eng. Des.Symp.SIEDS 2017*, pp. 117–121, 2017.

[2]M. Zeager, A. Sridhar, N. Fogal, S. Adams, D. Brown, P.Beling, "Adversarial Learning in Credit card Fraud Detection", IEEE, 2017, pp. 112-116.

[3] M.Zareapoor and P. Shamsolmoali, "Application of credit card fraud detection:Based on bagging ensemble classifier, "*ProcediaComput. Sci.*, vol. 48, no. C, pp. 679–686, 2015.

[4] A. Srivastava, A. Kundu, S. Sural, A. Majumdar, "Credit Card Fraud Detection using Hidden Markov Model", IEEE Transaction on Dependable and Secure Computing, 2008, pp. 37-48.

[5]NedaSoltaniHalvaiee , Mohammad KazemAkbari"A Novel Model for Credit Card Fraud Detection using Artificial Immune System", ELSEVIER – Journal 2014.

[6]M. Hegazy, A. Madian, and M. Ragaie, "Enhanced Fraud Miner: Credit Card FraudDetection using Clustering Data Mining Techniques," *Egypt. Comput.Sci.*, no. 03, pp.72–81, 2016.

[7] F. N. Ogwueleka, "Data Mining Application in Credit Card Fraud Detection System," vol. 6, no. 3, pp. 311–322, 2011.

[8] O. S. Yee, S. Sagadevan, N. Hashimah, and A. Hassain, "Credit Card Fraud DetectionUsing Machine Learning As Data Mining Technique," vol. 10, no. 1, pp. 23–27.

[9] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, "Credit Card FraudDetection Using AdaBoost and Majority Voting," *IEEE Access*, vol. 6, pp. 14277
14284, 2018.

[10] N. Mahmoudi and E. Duman, "Detecting credit card fraud by Modified Fisher Discriminant Analysis," *Expert Syst. Appl.*, vol. 42, no. 5, pp. 2510–2516, 2015.