ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

Credit Card Fraud Detection using Machine Learning Model

Aishwarya P. Shetty[1], Fouziya Afreen[2], Jeethesh M. Rai[3], Meghna N[4], Asha B Shetty[5]

[1,2,3,4]Bachelor of Engineering Student, Department of Information Science and Engineering, Sahyadri College of Engineering and Management, Mangalore, Karnataka, India

[5]Assistant Professor, Department of Information Science and Engineering, Sahyadri College of Engineering and Management, Mangalore, Karnataka, India

ABSTRACT*:* The project is on credit card fraud detection using machine learning models. As fraudster are increasing day by day and transaction are done by credit card and there is various types of fraud. So to solve this problem the study of the machine learning models is done and to determines the model which effectively detects credit card fraud and prompts the user or combination of the model. By this transaction is tested individually and whatever suits the best is further proceeded and foremost goal is to detect fraud by filtering the above models to get better result.

KEYWORDS*:* Credit Card; Fraud Detection

I. Introduction

Machine Learning is a field of concentrate that enables PCs to learn without being expressly modified. Rather than composing code, you feed information to the generic algorithm, and it fabricates rationale dependent on the information given. This venture forestalls Credit card extortion by identifying the strange conduct of exchanges. Here we store the ordinary action of the clients exchange, if there is an abnormal exchanges, it will identify. The advanced e-voting technique makes use of main two phases- the registration and login phase. During the registration phase the user need to provide required information and can get a secured password in order to login the application for voting. In the second phase using the user-id and password provided the user can login and can cast the vote from home or office or anywhere securely. The votes are properly encrypted so that any third person cannot able to find voting information of any others. The whole operation is managed by an administrator. The admin can monitor the process and finally announces the result soon after voting session is completed. Even the vote counts are stored in the encrypted form while getting stored in the database maintained and managed by administrator. Hence the overall voting process will be safe and secure.

Credit card misrepresentation recognition is a pertinent issue that draws the consideration of AI and computational insight networks, where countless arrangements. Indeed, this issue gives off an impression of being especially testing from a learning viewpoint, since it is described in the meantime by class imbalance, namely, genuine exchanges far dwarf cheats, and idea float, to be specific, exchanges may change their factual proper-ties over time. In a genuine world FDS, the enormous stream of instalment demands is immediately filtered via programmed devices that figure out which exchanges to approve. Classifiers are regularly used to dissect all the approved exchanges and alarm the most suspicious ones.

Credit card extortion identification likewise has two other profoundly impossible to miss qualities. At first clearly the restricted time range in which the acknowledgment or dismissal choice must be made and then colossal measure of charge card tasks that must be handled at a given time. The circumstance in India is genuinely simple: more than 1.2 million Credit card activities happen in a given day, 98 levels of them being taken care of on line. Obviously, simply not very many will be deceitful; however this fair implies the bundle where these needles are to be found is essentially

DOI: 10.15680/IJIRCCE.2019. 0705002

gigantic.

These exchanges stay unlabelled until clients find and report fakes, or until a sufficient measure of time has passed with the end goal that non questioned exchanges are considered genuine. Fraud avoidance is critical to card guarantors, yet not making unrealistic or essentially awkward the day by day card use by a huge number of clients. At the point when all the time required for the remote associations and the fundamental activity handling is considered, a misrepresentation location framework more often than not has close to a somewhat little portion of one moment to play out its assignment. This allotted time probably won't be sufficient for huge database inquiries. Obviously, this might be lightened if uniquely configured and devoted equipment is accessible; however it will absolutely result in higher start up and support costs.

II. COMPARISON WITH THE EXISTING SYSTEMS

The project is on credit card fraud detection using machine learning models. As fraudster are increasing day by day and transaction are done by credit card and there is various types of fraud. So to solve this problem the study of the machine learning models is done and to determines the model which effectively detects credit card fraud and prompts the user or combination of the model. By this transaction is tested individually and whatever suits the best is further proceeded and foremost goal is to detect fraud by filtering the above models to get better result.

III. PROPOSED SYSTEM

Machine Learning is a field of concentrate that enables PCs to learn without being expressly modified. Rather than composing code, you feed information to the generic algorithm, and it fabricates rationale dependent on the information given. This venture forestalls Credit card extortion by identifying the strange conduct of exchanges. Here we store the ordinary action of the clients exchange, if there is an abnormal exchanges, it will identify.

An engineering chart is a graphical portrayal that delineates a specific tale about a framework being described. The general design outline of Fraud Detection System utilizing Machine Learning Models is appeared in the figure. The graph incorporates stages like Pre-handling, preparing information, testing, assessing and checking whether the given informational collection is misrepresentation or not.

The outline portrays the general working of fraud detection system. At first the information is prepared or pre-handled subsequent to preparing we will get standardized information on which we can perform testing and assessing. In testing it will characterize the information and in assessment it will group and look at the information. Toward the end we will acquire perplexity network review store and to which class does the information have a place with accordingly.

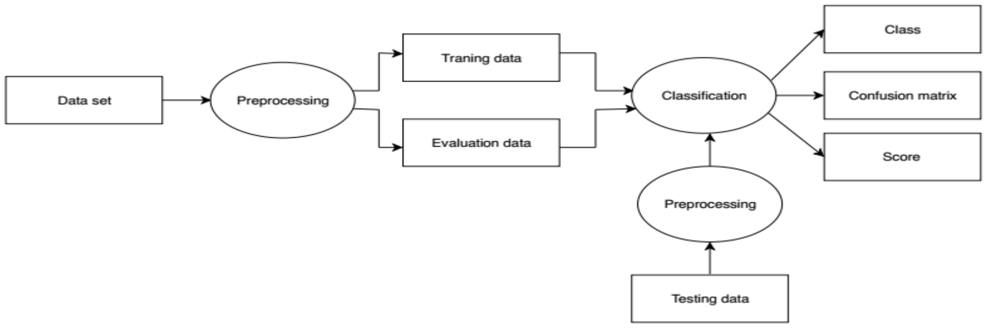

Figure 1: Architecture Diagram of Fraud Detection System

DOI: 10.15680/IJIRCCE.2019. 0705002

IV. RESULTS

The experimental results of credit card fraud detection using different learning models are shown in the confusion matrix

The experimental results of credit card fraud detection using different learning models are shown in the confusion matrix. A confusion matrix is a method for outlining the presentation of an order calculation.

Characterization exactness alone can be misdirecting in the event that you have an unequal number of perceptions in each class or on the off chance that you have multiple classes in your dataset.

Ascertaining a disarray network can give you a superior thought of what your order model is getting right and what sorts of blunders it is making.

Classification accuracy is the ratio of correct predictions to total predictions made.

Classification accuracy = correct predictions / total predictions

It is often presented as a percentage by multiplying the result by 100.

Classification accuracy = correct predictions / total predictions * 100

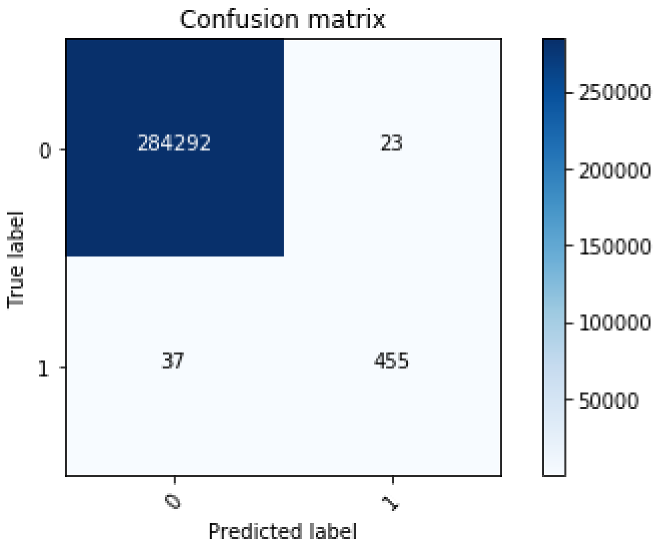

Figure 2: Confusion Matrix for Decision Tree

From the figure 2 the obtained accuracy is and the confusion matrix value for false negative is 284294, the value for false positive is 23, the value for true negative is 37, and the value for true positive is 455.

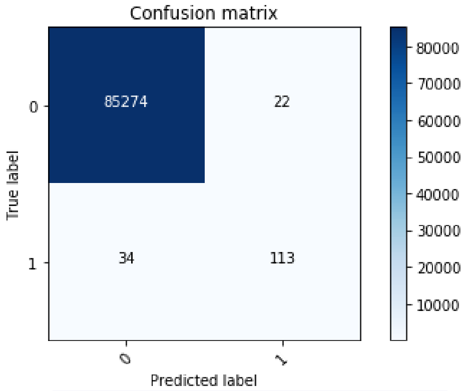

Figure 3: Confusion Matrix for Deep Learning

From the figure 3 the obtained accuracy is and the confusion matrix value for false negative is 85274, the value for false positive is 22, the value for true negative is 34, and the value for true positive is 113.

V. CONCLUSION

The proposed project predicts whether the transaction is fraudulent transaction or genuine transaction based on the different features. The analyses of choosing the useful attributes and normalizing those attributes that will increase the performance of the model. By using this project we can predict the fraudulent transaction. Depending on the diagonal value of confusion matrix of all three learning models, decision tree has got highest value when compared with other. The accuracy of the random forest is better than the deep learning and decision tree.

REFERENCES

[1] Andrea Dal Pozzolo, Giacomo Boracchi, Olivier Caelen, Cesare Alippi and Gianluca Bontempi, “Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy, ” IEEE Trans. vol. 29, no. 8, August 2018.

[2] C. Alippi, G. Boracchi, and M. Roveri, “Hierarchical change-detection tests,” IEEE Trans. Neural Netw. Learn. Syst., vol. 28, no. 2, pp. 246–258, Feb. 2016

[3] Krishna Modi, Reshma Dayma, “Review on fraud detection methods in credit card transactions”, Year: 2017, pp. 1 – 5

[4] S. Wang, L. L. Minku, and X. Yao, “Resampling-based ensemble methods for online class imbalance learning,” Trans. Knowl. Data Eng., vol. 27, no. 5, pp. 1356–1368, May 2015

[5] Ayushi Agrawal, Shiv Kumar, Amit Kumar Mishra, “Credit Card Fraud Detection: A case study”, Year: 2015, pp. 5 – 7

[6] Masoumeh Zareapoor ,Pourya Shamsolmoali, “Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier”, Procedia Conputer Science, 2015, pp. 679-685

[7] C. Alippi, G. Boracchi, and M. Roveri, “Just-in-time classifiers for recurrent concepts,” IEEE Trans. Neural Netw. Learn. Syst., vol. 24, no. 4, pp. 620–634, Apr. 2013

[8] G. Ditzler and R. Polikar, “Incremental learning of concept drift from streaming imbalanced data,” IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2283–2301, Oct. 2013

[9] Mohammed Ibrahim Alowais, Lay-Ki Soon, “Credit Card Fraud Detection: Personalized or Aggregated Model”, Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing, Year: 2012, pp. 114 – 119

[10] R. Elwell and R. Polikar, “Incremental learning of concept drift in nonstationary environments,” Trans. Neural Netw., vol. 22, no. 10, pp. 1517–1531, 2011

[11] Abhinav Srivastava, Amlan Kundu, Shamik Sural, Senior Member, IEEE, and Arun K. Majumdar, Senior Member, IEEE , “Credit Card Fraud Detection Using Hidden Markov Model” , IEEE transactions on dependable and secure computing, vol. 5, no. 1, january-march 2008.

[12] Janez Demsar, “Statistical Comparisons of Classifiers over Multiple Data Sets”, Journal of Machine Learning Research 7, Year: 2006, pp. 1–30

[13] D. K. Tasoulis, N. M. Adams, and D. J. Hand, “Unsupervised clustering in streaming data,” in Proc. Int. Conf. Data Mining Workshops, 2006, pp. 638–642

[14] E. Aleskerov, B. Freisleben, and B. Rao, “CARDWATCH: A neural network based database mining system for credit card fraud detection,” in Proc. IEEE/IAFE Computat. Intell. Financial Eng., Mar. 1997, pp. 220–226

[15] J. R. Dorronsoro, F. Ginel, C. Sgnchez, and C. S. Cruz, “Neural fraud detection in credit card operations,” IEEE Trans. Neural Netw., vol. 8, no. 4, pp. 827–834, Jul. 1997