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. 6, Issue 8, August 2018

Logistic Regression based Unauthorized Transactions Detection of Credit Card

S. Vigneswaran[1], K. Vinothkumar[2]

Assistant Professor, Department of Computer Science and Engineering, Sri Vidya College of Engineering & Technology, Virudhunagar, India[1]

Assistant Professor, Department of Electronics and Communication Engineering, Sri Vidya College of Engineering & Technology, Virudhunagar, India[2]

ABSTRACT: Credit card fraud detection is by and by the most often happening issue in the current world. This is because of the ascent in both web-based transactions and online business stages. Credit card fraud for the most part happens when the credit card was taken for any unapproved purposes or in any event, when the fraudster involves the credit card data for his utilization. In the current world, we are confronting a ton of credit card issues. To identify fraudulent exercises the credit card fraud detection framework was presented. This undertaking means to zero in for the most part on machine learning algorithms. A hidden Markov model (HMM) is at first prepared with the ordinary way of behaving of a cardholder. In the event that an approaching credit card progress isn't acknowledged by the prepared HMM with adequately high likelihood, it is viewed as fraudulent. Simultaneously, we attempt to guarantee that veritable transactions are not dismissed.

KEYWORDS: Credit Card, Logistic Regression, Machine Learning and HMM.

I. INTRODUCTION

Fraud in credit card transactions is unapproved and undesirable utilization of a record by somebody other than the proprietor of that record. Fundamental avoidance measures can be taken to stop this maltreatment and the way of behaving of such fraudulent practices can be considered to limit it and safeguard against comparative events later on. At the end of the day, Credit Card Fraud can be characterized as a case where an individual purposes another person credit card for individual reasons while the proprietor and the card-giving specialists know nothing about the way that the card is being utilized. Fraud detection includes observing the exercises of populaces of clients to gauge, see or stay away from shocking way of behaving, which comprises of fraud, interruption, and defaulting. This is an exceptionally pertinent issue that requests the consideration of networks, for example, machine learning and information science where the answer for this issue can be computerized.

II. RELATED WORK

The authors start by making sense of the technique utilized for transactions through credit cards. They have proposed a framework in which they coordinate their algorithm with the installment door to recognize fraudulence progressively. The creators utilized seven strategies to foster the algorithm, which are Neural Networks, Rule

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. 6, Issue 8, August 2018

Induction, Case-based reasoning, Genetic Algorithms, Inductive Logic Programming, Expert Systems, Regression. Not entirely set in stone; the ANN technique would best serve this issue articulation.

- The output of the neural network will be as likelihood which tells the level of a transaction being fraudulent.
- Neural networks are prepared on data based on the different

Classifications about the cardholder like the calling of the cardholder, income, about a lot of bought are put. The framework will utilize a back-spread learning algorithm in this stage to prepare the organization. Contingent upon the numeric value of likelihood somewhere in the range of 0 and 1, a transaction will be ordered into one of the accompanying classifications: Non-Fraudulent, Doubtful, Suspicious, and Fraudulent.

III. RESEARCH METHODOLOGY

Supervised Machine Learning method is utilized for detection the fraud transactions, which accepts transaction information as input and decide if the transaction is being fraud or not. The Logistic Regression Model from classifier class is executed to report dubious transactions.

- Logistic regression is utilized to foresee the likelihood of an objective variable.
- Logistic regression predicts the output of an unmitigated ward variable that are fraud transactions. Thusly, the result should be an unmitigated or discrete value. It will be 1 for fraud transaction and 0 for typical transaction. Be that as it may, rather than giving the specific value as 0 and 1, it gives the probabilistic values which lie somewhere in the range of 0 and 1.

The fraud detection module will work in the accompanying advances:

1. The Incoming arrangement of transactions and sums are treated as credit card transactions.
2. Credit card transactions are given to Decision Function as an input.
3. The decision capability will contrast the transaction information and the output of the machine learning model.
4. On the off chance that the transaction will be experienced to be authentic, it will permit it. Any other way, it will caution the bank.
5. The framework will consequently produce a report for a fraudulent transaction.
6. These reports are explored by the experts and they give input to the framework.
7. These inputs are utilized to prepare and refresh the algorithm ultimately to further develop fraud detection execution.

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. 6, Issue 8, August 2018

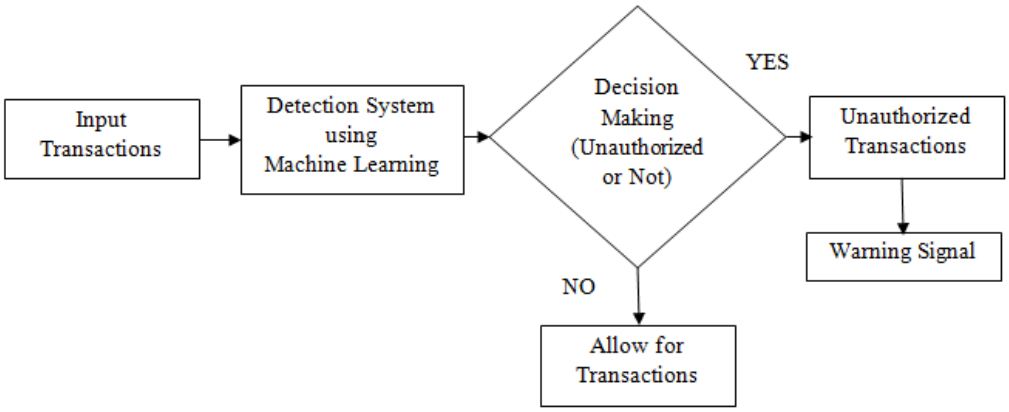

Figure.1 Detection of Unauthorized Transactions

IV. RESULTS AND DISCUSSIONS

The machine learning algorithm model that caught the fraud design has the most elevated precision rates as the created machine learning model presents a typical degree of exactness; we need to zero in on further developing the forecast level to gain a superior expectation.

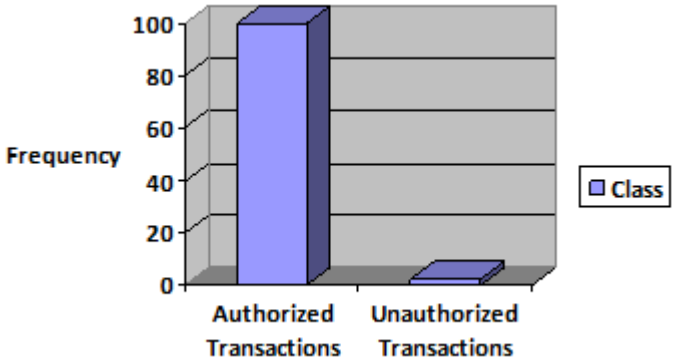

Figure.2 Graph for Transactions Class

This graph shows that the quantity of fraudulent transactions is a lot of lower than the real transactions. Here class typical addresses genuine transactions and class fraud addresses fraud transactions.

V. CONCLUSIONS

The code prints out the quantity of misleading up-sides it recognized and contrasts it and the genuine values. This is utilized to ascertain the exactness score and accuracy of the algorithms. The small portion of information we utilized for quicker testing is 75% of the whole dataset. These outcomes alongside the definite report of the

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. 6, Issue 8, August 2018

algorithm are given in the output, where class 0 methods the not entirely settled to be substantial and 1 method still up in the air as a fraud transaction. This outcome matched the class values to check for bogus up-sides.

REFERENCES

1. Mateos, Anderson M. (2008). _From Subprime Mortgages to Subprime Credit Cards‘. Communities and Banking, Federal Reserve Bank of Boston, pp. 21-23.
2. Anwer et al. (2009-2010). _Online Credit Card Fraud Prevention System for Developing Countries‘, International Journal of Reviews in Computing, ISSN: 2076-3328, Vol. 2, pp. 62-70.
3. Arias, J.C. & Miller R. (2009). _Market Analysis of Student about Credit Cards‘. Business Intelligence Journal, Vol. 3, No. 1, pp. 23-36.
4. Bhatla T.P. et al. (2003). _Understanding Credit Card Frauds‘. Cards Business Review, 01, pp. 01-15.
5. Bhusari V. & Patil S. (2011). _Study of Hidden Markov Model in Credit Card Fraudulent Detection‘. International Journal of Computer Applications, Vol. 20, No. 5, pp. 33-36.
6. Calem P. & Mester L. (1995). _Consumer Behavior and the Stickiness of Credit Card Interest Rates‘. The American Economic Review, Vol. 85, No. 5, pp. 1327-1333.
7. Chakravorti S. (2003). _Theory of Credit Card Networks: A Survey of the Literature‘, Review of Network Economics, Vol. 2, Issue 2, pp. 50-68.
8. Chan P.K. et al (1999). _Distributed Data Mining in Credit Card Fraud Detection‘, IEEE Intelligent Systems, pp. 67-74.
9. Chang C. & Chang S. (2010). _The Design of E-Traveler‘s Check with efficiency and Mutual Authentication‘. Journal of Networks, Vol. 5, No. 3, pp. 275-282.
10. Delamaire et al. (2009) ‘Credit Card Fraud Detection Techniques: A Review’, Banks and banks Systems, Vol. 4, Issue 2, pp. 57-68.
11. Dharwa J.N. & Patel A.R. (2011). _A Data mining with Hybrid Approach Based Transaction Risk Score Generation Model (TRSGM) for Fraud Detection of Online Financial Transaction‘. International Journal of Computer Applications, Vol. 6, No. 1, pp. 18-25.