International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-08, Issue-01, APR 2022

Credit-Cards Fraud Uncovering Technique Using Integrity Model Framework: An Analysis

[1]Deepali Bharadwaj, [2]Dr. LavKush Sharma, [3]Dr. Brajesh Kumar Singh

[1]Master of Technology, [2]Associate Professor, [3]Professor (R.B.S. Engineering Technical Campus, Bichpuri, Agra, India.

Abstract: Nowadays, the whole world does online shopping, online banking and almost all the work from home through the internet and it also takes time, as the trend of online shopping, e-learning, online banking is becoming more and more like credit cards. Fraud, online fraud, computer hacking is also increasing. Free online shopping, Credit card transactions are plays an important role in these days and mobile wallets are also plays an important role in Financial trading.

These growing number of low income jobs, the number of counterfeit jobs is also growing. Many peoples are already used in various methods such as Simulated Neural Network, Decision Tree, Independence Bayes, Random Forest algorithms, legal mining and many methods. But number of cases are related to Credit Card Fraud Detection, Computer Hacking, Spoofing are increased in day by day.

If any deviation is used funds in available patterns, it may be fraudulent activities. To detect fraudulent transactions, Banking and Credit Card Companies are used various data mining methods like a decentralization, legal mining, neural network, anonymous integration methods, the Markov Model and a combination of many methods.

This Paper present a Comparative study of Credit Card Fraud Detection Methods. This paper aims to provide a comprehensive review of the different Credit Card Fraud Detection Methods.

Keywords: Simulated Neural Network, Credit Card Fraud and Online Fraud Detection Methods.

I. INTRODUCTION

At a present time, Online payment methods are mostly used in electronic transactions. Credit Card Companies are representing the different types of electronic payment methods.

Nowadays, after online transactions, credit card frauds are also increasing through Fake Mails, Messages, Calling, Links and Fake Websites and through Fake OTP's the transactions are getting finished from the bank account of the people.

Internet Banking Fraud or Web Banking Fraud can be defined as " Unauthorized use of confidential Business Information to make purchases, or withdraw funds from user's account ".

Many Credit Card Companies are suffered from very heavy losses because of increased a different types of fraud Such as Credit Card Fraud, Computer Intrusion, Telecommunication Fraud, Counterfeit jobs, Application Fraud, Behavioral Fraud and so on. Fig 1. Shows the types of frauds.

According to a Statistical study [1] 42 % of Online Users are purchased in online products, in 2011, the number of digital customers are reached in 796.2 million. One Year ago, the numbers are increased to 903.6 million.

Banking Fraud can be increased by 48% in 2014 are compared to 2013 as customers continue to conduct their online trading activities. Therefore, With the growing number of such low cost jobs and E-Commerce, unscrupulous transactions are accumulating.

Online Fraud can be caused by the theft and negotiation of Credit Card information on Cyber Crime, email phishing, scams, malicious software, secure credentials, social networking sites and shoulder to shoulder filtering. Counterfeit transactions can be obtained through segmentation or external detection actions from normal actions. Fraudulent Fraud is the use of One's work to enrich Oneself through the will full misuse of the resources or assets of a hiring organization [11].

In this technology, Fraudulent activities are increased in many areas like a social sites, E-banking and so on. Fraud is leading to significant business losses.

 DOI : 10.35291/2454-9150.2022.0143

Figure 1: Taxonomy of frauds

II. LITERATURE SURVEY

M J Madhurya et al. [1] It has investigated the financial transactions problem in online banking and compared the various algorithms such as XG Boost, Decision Tree and KNN algorithms. It has shown the result is performance of machine learning algorithm based on different datasets and different patterns for credit card fraud detection.

Arun Kumar Rai et al. [2] It has proposed a scheme for detect some frauds in data are related to Credit Card uses Neural Network Technique based on Unsupervised Learning. It has shown the experimental results based on Neural Network Technique and Check the different accuracies of AE (Auto Encoder), IF (Isolation Factor), LOF (Location Outlier Factor) and K Means Clustering.

Ibstissan Benchaji et al. [3] It has been proposed a novel system are related to credit card fraud detection. This model is based on sequential modelling of data, attention mechanism and LSTM deep recurrent neural networks. This model is shown the strong results in terms of efficiency and effectiveness using a different classification such as GRU, LSTM, SVM, KNN and ANN methods.

Najia Majadi et al. [4] It has explained an overview of bidding patterns for detecting shill bidders in online auctions. It has analyzed the result of some bidding patterns represent the strong signs of shill bidding. And explain the challenges of shill bidding strategies such as selection of shill bidding strategies, paper selection to shill bidders after detection and the lack of ground truth.

F. Carcillo et al. [5] It has introduced a hybrid approach with a combination of Unconventional and Surveillance methods with increase the accuracy is related to fraud detection. External Schools are counted in a few granular categories and are found to exceed the existing schemes.

Ghosh and Reilly et al. [6] It used the neural network to transmit three layers' fraud detection in 1994. This technique was trained in fraudulent content contain the stolen cards, application fraud, fraudulent fraud, illegal fraud, Non Received Issue (NRI) fraud, Undetectable fraud and post order fraud.

Vaishnavi Nath Dornadula et al. [7] It has designed a novel fraud detection method for streaming transaction data and analyze the past transaction details are related to customers and extract the behavioral patterns. Find the better rating score with choose the best methods to predict the frauds and solve the problems of drift.

Asha RB et al. [8] It has predicted the occurrence of fraud and differentiate between the fraud and no fraud transactions based on supervised learning and unsupervised learning technique using the multiple algorithms such as Support vector machine (SVM), K Nearest Neighbor

(KNN) and Simulated Neural Network (SNN). It shows the results is performance metrics such as accuracy, precision and recall.

Javad Forough et al. [9] It has proposed an ensemble model using a novel voting mechanism. This mechanism is based on artificial neural networks. And Proposed on three phase training algorithm and comparison of the ensemble model with state of art solo and ensemble model. An applying the deep recurrent neural networks as a classifier in ensemble for the first time.

Victor Chang et al. [10] It identifies an efficient and stable model for fraud detection platforms. And compare the five different learning models such as decision tree, logistic regression, random forest and Auto encoder. It shows the result is better work under the logistic regression algorithm and random forest algorithm rather than other algorithms. And solve the problems of digital economy and industrial economy to detect some fraudulent activities.

Alex G.C. de Sa et al. [11] It is used a hyper-heuristic searching method to create a Fraud - BNC a customized classification algorithm. Fraud-BNC algorithm is an

 DOI : 10.35291/2454-9150.2022.0143

interpretable by decision makers. It is evaluated by classification and economical measures. It shows the result is improved the current company's economical efficiency in 72.64%.

Deshen Wang et al. [12] It proposed a new consumer incentivized secondary verification strategy. Incentivized Secondary Verification strategy are more accurate to inconvenient consumers. This strategy may lead to wins some consumers, merchant and bank It shows the effectiveness of this strategy is demonstrated using actual credit card transaction data.

Yvan Lucas et al. [13] It proposed a sequence of credit card transactions model using a machine learning and data mining techniques. And explain the three different perspectives such as (i) The sequence contains or does not contains a fraud (ii) The sequence is obtained by fixing the card holder or the payment terminal (iii) It is a sequence of spend amount or elapsed time between the current or previous data.

Toluwase Ayobami Olowookere et al. [14] It proposed the framework with combination of meta learning ensemble techniques and cost sensitive learning paradigm to credit card fraud detection. This framework is allowed the base classifiers. This framework is evaluated the accuracy of meta classifier using Area under the curve (AUC). It shows that the result is cost sensitive ensemble framework sensitive ensemble framework the sensitive ensemble framework is efficient for producing the cost sensitive ensemble classifiers.

III. METHODOLOGY

A. Simulated Neural Network

The Simulated neural network (SNN) is the top level for discovering hidden configuration features. The SNN works in the same way as a human brain. It consists of different layers. So, first layer is an input layer and the last layer is an output layer. It may contain some hidden layers.

B. Neural Network

Neural Network is a machine learning technique. It works similar a human brain. It is a computing system that is connected from one node to another node. For example: Facial Recognition. It is mostly used in sigmoid function. It is a customizable Neuro Network based on fraud detection system based on an unregulated learning program.

C. Hamming Network

For more sensory networks that use unchecked reading. It is used to calculate the distance and some comparisons. It is a type of network, in which all input vectors provided can be grouped into separate groups. It performs a template matching between stored templates and inputs.

D. Decision Tree

This is a controlled learning technology. It can be used for classification and regression issues, but basically it is easily solved in classification. This is a classification of a tree structure that represents the function of internal nodes. The branch is a rule to decide, and each leaf nodule represents the result.

Decision Tree has two types:

1. Decision Crystal Nodule = They are used to make decisions and have some branches.
2. Leaf Node = The result of these decisions and contains no additional branches.

A decision or test is made based on the capabilities of a given dataset.

E. Logistic Regression

It is one of the most used machine learning methods and refers to supervised learning methods. It is used to predict a categorical dependent variable using a given set of dependent variables.

Figure 2, shows the accuracy and comparison of false positive, F1 score, Specification and accuracy of unregulated learning models in the recognition of credit card fraud. Untreated Learning is a form of learning that is practiced without supervision by the supervisor. This method of independent study. During SNN training under unchecked reading, input vectors of the same type are combined to form clusters. If a new input pattern is used, then the neural network provides an output response indicating the phase input pattern that is part of it.

In this case, the site does not provide an answer to what the user wants the output to be, whether it is correct or incorrect. Thus, in this type of learning, the network itself must discover patterns, functions of the inputs, and relationships between inputs and outputs. The winner takes all nets. This type of network is based on the laws of competitive learning and uses a strategy to select the neuron with the most complete input as the winner. Connections between output neurons represent a competition between them, with one of them being "ON" to be the winner and the others being "OFF". Here are some networks based on this simple concept with invalidated reads.

Although these programs are effective against many forms of fraud, there are still serious problems.

1. First, you cannot support non-profile fraudulent activity.

2. Second, these systems must be upgraded to keep up with modern fraudulent techniques. Its development and maintenance costs are high and implies continued reliance on system vendors. 3. Third, a very precise description of the thresholds and parameters is required.

 DOI : 10.35291/2454-9150.2022.0143

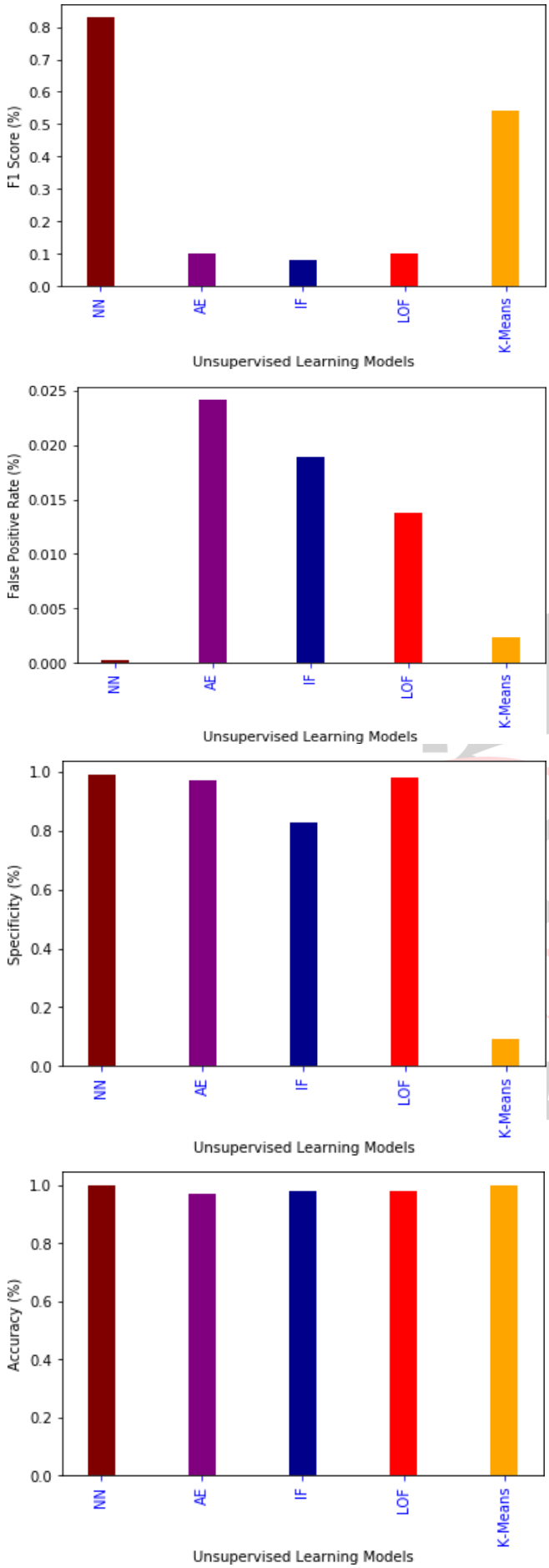

Figure 2: Accuracy, Specificity and Comparison

IV. CONCLUSION

This paper has reviewed three fraud scams, credit card fraud detection, computer access, and telecommunications. It identifies the characteristics of the types of fraud, the need for fraud detection programs, several current fraud detection strategies, and the possibility of future operations. Due to security issues, only a few credit card acquisitions are publicly available. Among them, the method of neural networks is the most popular tool. However, it is difficult to use due to the lack of available data set. In order to gain access, some techniques have been applied to the actual application. However, it is difficult to evaluate existing systems to gain access, mimic potential attack situations, and repeat known attacks. In addition, the access system has a disadvantage because the system and its set of rules must be clear in the monitor. Many communication fraud detection strategies check a set of toll ticket data and detect fraud in telephone patterns.

ACKNOWLEDGEMENT

I would like to acknowledge the Computer Science and Engineering department of Raja Balwant Singh Engineering Technical Campus, Agra for their support.

REFERENCES

[1] A. A.Taha, S. J. Malebary, “Intelligent Approach to Credit Card Fraud Detection Using an O Light GBM”, IEEE Access (2020), pp. 25579- 25587.

[2] S. N. Kalid, K. H NG, G. K Tong, K. C Khore., “A Multiple Classifiers System for Anomaly Detection in Credit Card Data with Unbalanced and Overlapped Classes”, IEEE Access (2020), Vol. 8, pp. 28210- 28221.

[3] S. Makki, Z. A Assaghir, Y. Taher, R. Haque, M. S Hacid, H. Zeineddine, “An Experimental Study with Imbalanced Classification Approaches for Credit Card Fraud Detection”, Special Section On Advanced Software and Data Engineering for Secure Societies, IEEE Access (2019), Vol7, pp.93010-93022.

[4] K. Randhawa, C. K Loo, M. Seera, C. P Lim, A. K. Nandi, “Credit Card Fraud Detection Using Adaboost And Majority Voting”, Ieee Access, (2018) Vol 6, pp 14277-14284.

[5] Andrea Dal Pozzolo, Giacomo Boracchi, Olivier Caelen, Cesare Alippi, Gianluca Bontempi, “Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy”, Ieee TransactionsOn Neural Networks And Learning Systems, (2018) Vol. 29, No. 8, pp. 3784-3794.

[6] L. Meneghetti, M.Terzi, S. Del Favero, G. A Susto, C. Cobelli, “Data-Driven Anomaly Recognition for Unsupervised Model-Free Fault Detection in Artificial Pancreas”, Ieee Transactions On Control Systems Technology, (2018) pp. 1-15.

 DOI : 10.35291/2454-9150.2022.0143

[7] L. Zheng, G. Liu, C. Yan, C Jiang, "Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity", Ieee Transactions On Computational Social Systems (2018), pp. 1- 11.

[8] S. Bakshi, "Credit Card Fraud Detection A classification analysis", Second International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) IEEE (2018), ISBN 978-1-5386-1442-6, pp. 152- 156.

[9] R. K Dwivedi, A. K Rai, R. Kumar, "Outlier Detection in Wireless Sensor Network using Machine Learning Techniques", International Conference on Electrical and Electronics Engineering (ICE3), IEEE (2020), pp. 1-6.

[10] R. K Dwivedi, A. K Rai, R. Kumar, "A Study on Machine Learning Based Anomaly Detection approaches in Wireless Sensor Network", 10th International Conference on Cloud Computing, Data Science & Engineering, (Confluence). IEEE (2019), pp. 200-205.

[11] F. Carcillo, Y.-A. Le Borgne and O. Caelen et al., "Combining unsupervised and supervised learning in credit card fraud detection", Information Sciences, Elsevier (2019), pp. 1-15.

[12] Kang Fu, Dawei Cheng, Yi Tu, and Liqing Zhang, "Credit Card Fraud Detection Using Convolutional Neural Networks", Springer International Publishing AG 2016.

[13] St. S. Rajani, Prof. M. Padmavathamma, "A Model for Rule-Based Fraud Detection in telecommunications", International Journal of Engineering Research & Technology (IJERT), Vol.1 Issue 5, July – 2012.

[14] Y. Sahin and E. Duman, "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines", IMECS vol 1, 2011.

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

[16] Sam Maes, Karl Tuyls, Bram Vanschoenwinkel, Bernard Manderick, "Credit card fraud detection using bayesian and neural networks", International Naiso Congress on Neuro-Fuzzy Technology, 2002.

[17] Minewiskan, Microsoft Neural Network Algorithm Technical Reference (2017, March 14) available at https://docs.microsoft.com/en-us/sql/analysis-services/data-mining/microsoft-neural-network-algorithm-technical-reference Krishna Modi, Bhavesh Oza, "Outlier Analysis Approaches in Data Mining", IJIRT vol 3 issue 7.

[18] Raghavendra Patidar, Lokesh Sharma, "Credit card fraud detection using Neural Network", IJSCE Volume-1, Issue-NCAI2011, June 2011.

[19] Alejandro Correa Bahnsen, Djamila Aguada, Aleksandar Stojanovic, Björn Ottersten, "Feature engineering strategies for credit card fraud detection", 0957-4174/ 2016 Elsevier.

[20] A. A. Taha, S. J. Malebary, "Intelligent Approach to Credit Card Fraud Detection Using an O Light GBM", IEEE Access (2020), pp. 25579-25587.

 DOI : 10.35291/2454-9150.2022.0143