International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S, August 2019

Machine Learning Methods for Analysis Fraud Credit Card Transaction

Megasari Gusandra Saragih, Jacky Chin, Rianti Setyawasih, Phong Thanh Nguyen, K. Shankar

Abstract: ***The use of online banking and credit card is increasing day by day. As the usage of credit/debit card or netbanking is increasing, the possibility of many fraud activities is also increasing. There are many incidents are happened in presently where because of lack of knowledge the credit card users are sharing their personal details, card details and one time password to a unknown fake call. And the result will be fraud happened with the account. Fraud is the problem that it is very difficult to trace the fraud person if he made call from a fake identity sim or call made by some internet services. So in this research some supervised methodologies and algorithms are used to detect fraud which gives approximate accurate results. The illegal or fraud activities put very negative impact on the business and customers loose trust on the company. It also affects the revenue and turnover of the company. In this research isolation forest algorithm is applied for classification to detect the fraud activities and the data sets are collected from the professional survey organizations.***

Keywords: Credit Debit Card Fraud Detection, Machine Learning Algorithms, Forest Algorithm, Classification Algorithm.

I. INTRODUCTION

Fraud is an activity in which a person directly or indirectly use the money of victim by fake transactions and without let him know about the transaction [1-3] . The fraud Levels can be categorized into two parts:

1. Management Fraud

If the fraud activity is committed by an big organization or an management team of the organization then it will be termed as Management Level Fraud.

2. Customer Fraud

If fraud is committed by an individual to individual then it will be categorized as Customer Level fraud.

Often such kind of frauds are committed on Credit/Debit Card [4-6]. This is happens because of using weak security system [7-9]. Many users use very common pin password such as birth date, vehicle number, mother or father's birth year etc. Such passwords are easy to crack using data mining algorithms. So it is necessary to built an anti-fraud automated system which will be able to detect the authorization of the user [10-12].

Manuscript published on 30 August 2019.
***** Correspondence Author (s)
Megasari Gusandra Saragih, Universitas Pembangunan Panca Budi, Medan, Indonesia.
Jacky Chin, Mercu Buana University, Indonesia.
Rianti Setyawasih, Universitas Islam 45, Bekasi, Indonesia.
Phong Thanh Nguyen, Department of Project Management, Ho Chi Minh City Open University, Vietnam.
K. Shankar, Department of Computer Applications Alagappa University, India.

Even if he is providing the accurate data. There are many machine learning algorithms are available which can be very useful in detecting such fraud activities. Even using these algorithms the tracing of the fraud becomes very easy. In order to make such anti fraud system a huge data sets are required for experiment purpose. The types of such frauds are shown in figure 1 below

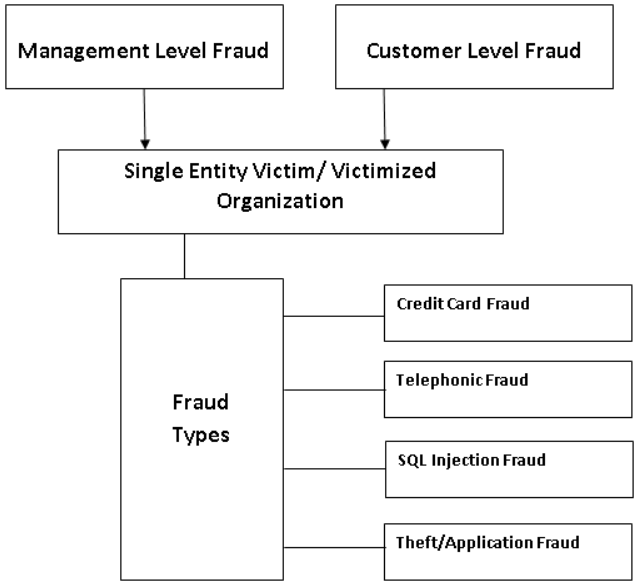

Figure 1. Fraud Detection Types

Regardless of whether he is giving the exact information. There are many AI calculations are accessible which can be helpful in distinguishing such misrepresentation exercises. Notwithstanding utilizing these calculations the following of the extortion turns out to be simple. So as to make such enemy of extortion framework a gigantic informational indexes are required for trial reason.

Extortion is an action where an individual legitimately or in a roundabout way utilize the cash of unfortunate casualty by phony exchanges and without let him think about the exchange. Regularly such sort of cheats are submitted on Credit/Debit Card. This is happens as a result of utilizing feeble security framework. Numerous clients utilize basic stick secret key, for example, birth date, vehicle number, mother or father's introduction to the world year and so forth. Such passwords are anything but difficult to split utilizing information mining calculations. So it is important to manufactured an enemy of misrepresentation mechanized framework which will almost certainly recognize the approval of the client. Figure 2 shows real time credit card fraud detection system.

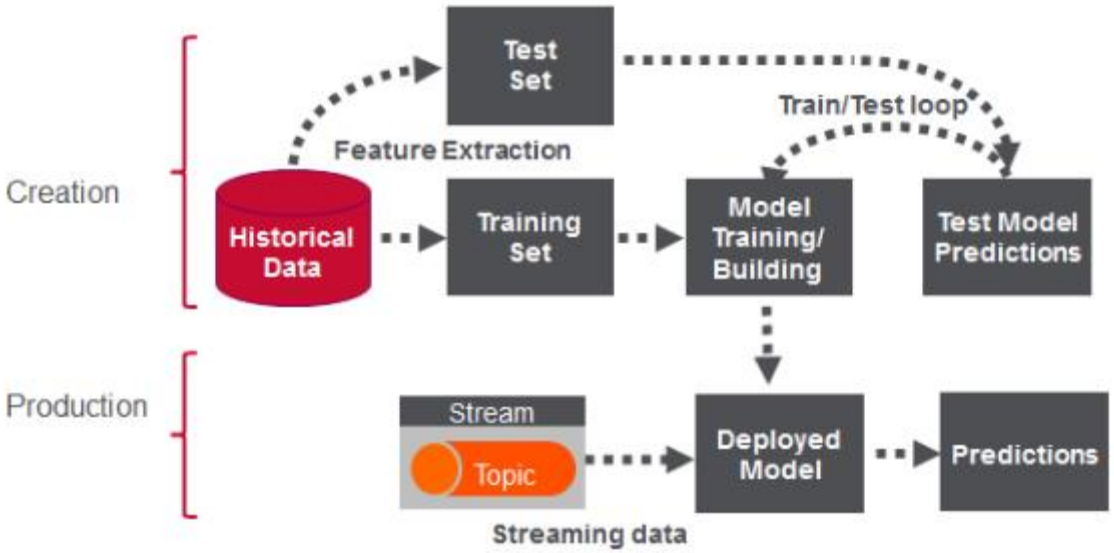

Figure 2. Real time Credit Card Fraud Detection System

The utilization of web based banking and Visa is expanding step by step. As the use of credit/platinum card or netbanking is expanding, the likelihood of numerous extortion exercises is likewise expanding. There are numerous episodes are occurred in directly where in light of absence of information the charge card clients are sharing their own subtleties, card subtleties and one time secret word to an obscure phony call. The charge card or plastic extortion exercises are expanding step by step in past years. There are numerous occurrences are occurred in by and by where in view of absence of learning the Visa clients are sharing their own subtleties, card subtleties and one time secret word to an obscure phony call. Coercion is an action where an individual genuinely or in a circuitous way utilize the cash of shocking misfortune by phony exchanges and without let him think about the exchange. Reliably such sort of cheats are submitted on Credit/Debit Card. This is happens due to utilizing powerless security structure. Different clients utilize central stick puzzle key, for example, birth date, vehicle number, mother or's first involvement with the world year, and so on. Such passwords are unquestionably not difficult to part utilizing information mining figurings.

Credit Card Fraud Examples

1. Swipe Machine Fraud
2. eCommerce Website Fraud
3. Credit Card Cloning
4. Credit Card Theft
5. Leaking Card Information on Telephone
6. Give card to other person to handle
7. Paying amount to unauthorized websites
8. Ignoring the security warnings and use the credit card payment
9. Buying from entrusted websites may cause credit card fraud
10. Linking the credit card for autodebit to unauthorized website.

So it is basic to made a foe of double dealing mechanized structure which will no doubt see the underwriting of the client. What's more, the outcome will be misrepresentation occurred with the record. Extortion is the issue that it is hard to follow the misrepresentation individual in the event that he made call from a phony personality sim or call made by some internet providers. So as to limit the shipper hazard factor the AI is one of the most effective way. The reason for this exploration is to screen the essential procedure by the bank or online framework. The charge card extortion action might be occurs from multiple points of view and if any of the calculation talked about in this examination is connected by the site or business misrepresentation location, the likelihood of misrepresentation might be limited. There are numerous enemy of extortion techniques or applications are accessible to forestall the business misfortune. This exploration gives commitment towards the identifying such criminal operations utilizing AI and neural system calculations. The disconnection woods calculation is utilized for exception and the acquired exactness is 99.87 for complete arranged datasets.Figure 3 shows payment fraud in ecommerce and payment gateway by credit card

Figure 3. Payment fraud in ecommerce and payment gateway by credit card

What's more, the outcome will be misrepresentation occurred with the record. Misrepresentation is the issue that it is exceptionally hard to follow the extortion individual on the off chance that he made call from a phony character sim or call made by some internet providers. So in this examination some managed approaches and calculations are utilized to identify extortion which gives surmised precise outcomes.

II. RELATED WORK

There are a number of techniques and algorithms already have been introduced which are in use in detecting such frauds. Machine learning is also helping in this research. In Neural Network the datasets are obtained from many international survey agencies and trained ANN algorithms are used to research on data. The decision trees and SVM algorithms are used to solve the problem in case of fraud.

III. METHODOLOGY

When ever a transaction is occurred and if some one tried to do any fraud activity then the binary classification technique will be preferred for evaluation and by using classification techniques and the performance of system will be compared. Table 1 shows classification techniques for credit card fraud detection.

Table 1. Classification techniques for credit card fraud detection

Naive Bayes Algorithm	In this approach all the features are categorized into parts. Such extracted features are classified in a way such no other cluster know about the other features. Further the features are categorized as true or false fraud activity for the person.
Decision Tree Algorithm	Similar to binary system the DSS is categorized as regression and classification trees. The branch of decision true follows a structure where there will be one root node and other will be leaf or child. The decision are taken on the basis of traversing of the flow.
K-Nearest Neighbors Algorithm	The KNN technique is a straightforward occasion based calculation that plots all preparation examples and order unla-belled cases dependent on their nearest neighbors. In example based students occurrences themselves are utilized to speak to the model not at all like the choice tree calculations that utilization cases to build up a tree and that tree speaks to the model. Be that as it may, it is contended that all learning calculations are occurrence based since they all utilization occasions of the preparation set to build models.
Support Vector Machine (SVM)	SVM is presented by Vapnik, in 1992 [12] to take care of double classification issues and after that they are stretched out to nonlinear regression issues. SVMs depend on basic hazard minimization un-like ANNs which depends on observational hazard minimization. SVM map the information to a foreordained high-dimensional space through a piece capacity and finds the hyperplane that amplifies the edge between the two classes. The arrangement depends just on those information focuses, which are at the edge. These focuses are called support vectors.
Logistic Regression	This technique does not required a particular value or point to detect the fraud. It follows a simple strategy where it is measured that the flow is going in a normal way or not.
Artificial Neural Network	This technique works on the basis of trained data or data sets collected from many organizations. Such data performas operations and helps to detect the fraud Activity.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The unlawful or extortion exercises put negative effect on the business and clients free trust on the organization. It likewise influences the income and turnover of the organization. In this exploration confinement timberland calculation is connected for order to recognize the extortion exercises and the informational indexes are gathered from the expert overview associations.

IV. RESULT ANALYSIS

Comparison of Existing work and Proposed system is given below:

Isolation Forest: 449
0.9976861523768727

	Precision	recall	f1-score	support
0	1.00	1.00	1.00	283315
1	0.34	0.34	0.34	492
avg / total	**1.00**	**1.00**	**1.00**	**283807**

Local Outlier Factor: 735
0.9967170750718908

	Precision	**recall**	**f1-score**	**support**
0	1.00	1.00	1.00	283315
1	0.06	0.06	0.06	493
avg / total	**1.00**	**1.00**	**1.00**	**283807**

V. CONCLUSION

The credit card or debit card fraud activities are increasing day by day in past years. There are many incidents are happened in presently where because of lack of knowledge the credit card users are sharing their personal details, card details and one time password to a unknown fake call. Blackmail is an activity where an individual honestly or in an indirect manner use the money of appalling loss by fake trades and without let him consider the trade. Consistently such kind of cheats are submitted on Credit/Debit Card. This is occurs because of using weak security structure. Various customers use fundamental stick mystery key, for instance, birth date, vehicle number, mother or's first experience with the world year, etc.

Such passwords are definitely not hard to part using data mining figurings.So it is essential to made an adversary of deception automated structure which will in all likelihood perceive the endorsement of the customer. And the result will be fraud happened with the account. Fraud is the problem that it is very difficult to trace the fraud person if he made call from a fake identity sim or call made by some internet services. In order to minimize the merchant risk factor the machine learning is one of the most efficient way. The purpose of this research is to monitor the basic process by the bank or online system. The credit card fraud activity may be happens in many ways and if any of the algorithm discussed in this study is applied by the website or business fraud detection, the probability of fraud may be minimized. There are many anti-fraud methods or applications are available to prevent the business loss. This research gives contribution towards the detecting such illegal activities using machine learning and neural network algorithms. The isolation forest algorithm is used for outlier and the obtained accuracy is 99.87 for total classified datasets.

VI. FUTURE WORK

The work can be enhanced by using hybrid algorithms and artificial intelligence system. The security can be enhanced on the level on which the credit card fraud activity cannot happen even if the fraud person knows the card number and secret pin.

REFERENCES

1. Linda Delamaire (UK), Hussein Abdou (UK), John Pointon (UK), “Credit card fraud and detection techniques: a review”, Banks and Bank Systems, Volume 4, Issue 2, 2009.
2. Khyati Chaudhary, Jyoti Yadav, Bhawna Mallick, “A review of Fraud Detection Techniques: Credit Card”, International Journal of Computer Applications (0975 – 8887) Volume 45– No.1, May 2012 .
3. Vladimir Zaslavsky and Anna Strizhak,” credit card fraud detection using selforganizing maps”, information & security. An International Journal, Vol.18,2006.
4. L. Mukhanov, “Using bayesian belief networks for credit card fraud detection,” in Proc. of the IASTED International conference on Artificial Intelligence and Applications, Insbruck, Austria, Feb. 2008, pp. 221– 225.
5. John T.S Quah,M Sriganesh “Real time Credit Card Fraud Detection using Computational Intelligence” ELSEVIER Science Direct,35 (2008) 1721-1732.
6. Joseph King –Fung Pun, “Improving Credit Card Fraud Detection using a Meta Heuristic Learning Strategy” Chemical Engineering and Applied Chemistry University of Tornto 2011.
7. Kenneth Revett,Magalhaes and Hanrique Santos “Data Mining a Keystroke dynamic Based Biometric Dtatabase Using Rough Set” IEEE

8. Linda Delamaire ,Hussein Abdou and John Pointon, "Credit Card Fraud and Detection technique", Bank and Bank System,Volume 4, 2009.
9. Fajarianto, M. I. Setiawan, A. Mursidi, D. Sundiman, and D. A. P. Sari, "The Development of Learning Materials for Introduction of Animals in Early Childhood Using Augmented Reality," 2018, pp. 722–727.
10. Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., & Arunkumar, N. (2018). Hybrid optimization with cryptography encryption for medical image security in Internet of Things. *Neural computing and applications*, 1-15.
11. Maheswari, P. U., Manickam, P., Kumar, K. S., Maseleno, A., & Shankar, K. Bat optimization algorithm with fuzzy based PIT sharing (BF-PIT) algorithm for Named Data Networking (NDN). *Journal of Intelligent & Fuzzy Systems*, (Preprint), 1-8.
12. Lydia, E. L., Kumar, P. K., Shankar, K., Lakshmanaprabu, S. K., Vidhyavathi, R. M., & Maseleno, A. (2018). Charismatic Document Clustering Through Novel K-Means Non-negative Matrix Factorization (KNMF) Algorithm Using Key Phrase Extraction. *International Journal of Parallel Programming*, 1-19.