IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111221

# A Survey for Credit Card Fraud Detection Using Machine Learning

**Poonam Sushen Halder[1], Vijay M. Rakhade[2], Lowlesh N. Yadav[3]**

Student Computer Science & Engineering SSCET, Bhadrawati India[1]

Professor Computer Science & Engineering SSCET, Bhadrawati India[2]

Head of Department Computer Science & Engineering SSCET, Bhadrawati India[3]

**Abstract:** Fraud is increasing with the expansion of modern technology and the globe of communication, results in the loss of billions of dollars every year. Though preventions are the best way to reduce fraud, fraudsters are adaptive, they will usually find there ways to avoid such measures. Methods for the detection of fraud are vital. If we are to catch the fraudsters once fraud prevention has failed. Effective technologies for fraud detection has been provided by statistics and machine learning and they have been applied successfully to detect activities such as money laundering, e-commerce credit card fraud, computer intrusion and telecommunications frauds. The areas in which fraud detection technologies are most used are describes the tools available for statistical fraud detection

**Keywords:** Fraud detection, credit card fraud, money laundering, computer intrusion, telecommunication fraud.

## I. INTRODUCTION

The fraud detection is defines as "criminal deception; the use of false representations to gain an unjust advantages." Fraud is really old as humanity itself and can take thousands of variety of various forms. However, in last few years, the development of new technologies has also provided. Money laundering the traditional forms of fraudulent behavior have become easier to perpetrate and have been joined by latest kind of fraud like computer intrusion and mobile telecommunications. Difference between fraud avoidance and fraud detection, fraud avoidance describes measures to stop fraud from occurring in the first place. These include watermark, elaborate designs, fluorescent fibers, laminated metal strips, drawings and holographs on banknotes, Subscriber Identity Module (SIM) cards for mobile phones, and passwords on computer system. Fraud detection comes into play once fraud detection must be used unsealing, as one will typically be uninformed that fraud prevention has been failed. We can try to prevent credit card fraud by guarding our credit cards, but if the cards details are stolen, then we are able to detect, as soon as possible, the fraud is being committed. Statistical fraud detection methods are supervised or unsupervised. In supervised methods, samples of both non fraudulent records and fraudulent records are used which allow one to assign one of the two classes. In contrast, unsupervised methods simply seek those accounts, customers and so forth which are most different from the norm. Tools used for inspection data ability can be used, but the detection of errors is rather different problem from the detection of false data which describe a fraudulent pattern. We cannot cover all the areas of statistical methods can be applied. Here we have selected a few areas in which statistical methods can be applied. In those areas such methods are used and there is a body of expertise describing the literature. Second section will provides a brief overview of some tools for fraud detection.

## II. FRAUD DETECTION TOOLS

As we mentioned the above that fraud detection can be supervised or unsupervised. Supervised methods use fraudulent cases from which to construct a model which yields a fraud score for new cases. Such as linear analysis tools for many application, have been proved to be effective tools for many applications, but there are more powerful tools, especially neural networks, have also been applied. Rule based methods are supervised learning algorithms that generates classifiers using rules of form.

Major considerations are when building a supervised tool for fraud detection include those of uneven class sizes and different costs of various types of misclassification. We must also take into consideration the cost of investing and the profits if identifying fraud. Moreover, class membership is uncertain. For example, credit transactions may be labelled incorrectly: a fraud transaction may remain unseen and thus be labeled or legitimate transaction. Link analysis relates known fraud to other individuals using social network and record linkage. For, example, in telecommunications networks, security investigators have found that fraudsters in work isolation from each other. Also, after an account has been disconnected for fraud, the fraudster will often call the same amount from another account. Telephone calls can cause to fraudulent accounts to indicate instruction. (Goldberg and Senator, 1995, 1998; Senator et al., 1995).Unsupervised

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022
DOI: 10.17148/IJARCCE.2022.111221

methods are used when there are no prior sets of fraudulent observations and legitimate. Techniques employed are usually a combination of profiling and outlier methods. There are likenesses to author identification in text investigation. Credit Card Fraud

Use of a stolen cards is most straightforward type of credit card fraud. In this case, the fraudster spends as much as possible space of time as possible, before the theft is detected and card stopped and hence the detecting theft can prevent large losses. Application of fraud arises when individuals get new credit card from issuing companies using fake personal information. New credit scorecards are used to detect customers default, and the reasons for this may include fraud. With application fraud, however it might not be sent out or repayment dates begin to pass that fraud is suspected. Cardholder not present fraud occurs when the tractions is make remotely, so that only the card's details are needed. Such transactions include telephone sales and online transactions, and this type of fraud is necessary to obtain the details of the card without the cardholder's knowledge. Transactions are made by fraudsters using this counterfeit cards and making purchases can be detected through methods which changes in transaction patterns, as well as checking for particular patterns which are known to be indicative of counterfeiting.

## III. CREDIT CARD FRAUD

The extent of credit card fraud is hard to find because companies are often to release fraud figures in case they spending the figures change over time. Various estimates have been given. For example, Leonard suggested the cost of MasterCard fraud in Canada in 1989, 1990 and 1991 was $19, 29 and 46 million respectively.

Ghosh and Reilly (1994) suggest a figure of $850 million (U.S.) per year for all the types of credit card fraud in the United States, and Aleskerov, Freisleben and Rao (1997) cited estimates of $700 million in the United States each year for Visa and $10 billion worldwide in 1996. Total losses through credit card fraud in the United Kingdom have been growing very fast over the last 4 years [1997, $122 million; 1998, $135 million. Source: Association for Payment Clearing Services, London (APACS)] and recently APACS reported $373.7 million losses in the 12 months ending August 2001. Since these are generally regarded as charge-off losses, Ghose and Reilly (1994) cited one estimate for bankruptcy fraud in 1992.

Use of a stolen card is perhaps the most of credit card fraud. In this case, the fraudster typically spends as much as possible in as short a space of time as possible, before the theft can prevent large losses. Application fraud arises when individuals obtain new credit cards from issuing false personal information. Traditional credit scorecards are used to detect who are likely to default, and the reasons for include fraud.

## IV. MONEY LAUNDERING

Money laundering is the process of obscuring the source, or use of funds, or usually cash, that are profits of illicit activity. The size of the problem is indicated in 1995 U.S. However, no prevention strategy is fool proof and recognition is essential. Wire transfers provided a natural domain for laundering according the OTA report, each day in 1995 about half million wire transfers, valued at more than $2 trillion (U.S.), were carried out using the Fed wire and CHIPS systems, along with a million transfers using SWIFT system. Wire transfers contain items such as date of transfer, identity of sender, routing number, identity of recipient, routing number of recipient. Sometimes those fields not needed for transfer are left blank, free text fields may be completed in various ways and worse still, but inevitable sometimes the data have errors. The detection of money laundering shows difficulties not encountered in areas such as, for example, the credit card industry. Whenever credit card fraud comes to light fairly early on, in money laundering it may be years before individual transfer and legally identified as part of a laundering process. As with further areas of fraud, money laundering recognition works in hand with prevention. For example, in the United States the Bank Secrecy Act need that banks report all currency transactions of over $10,000 to the authorities.

The number of currency transactions over $10,000 in value increased dramatically after the mid-1980s, to the extent that the number of reports filed is huge and this in itself can cause difficulties. In an attempt to the Financial Crimes Enforcement Network (FinCEN) of the U.S.

## V. COMPUTER INTRUSION

Computer intrusion fraud is big business and computer intrusion detection is a hugely area of research. Hackers can find passwords, read and change files, alter source code, and so on. However, as with all fraud when the prizes are high, the attacks are adaptive and intrusion has been familiar the hacker will try a various route. Because its importance is a great deal of effort has been put into developing methods, and there are several products available. Since the only record if a

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022
DOI: 10.17148/IJARCCE.2022.111221

hacker's activities is the sequence of commands that is computer intermission data use analysis techniques. As other fraud situations, both supervised and unsupervised methods are often called misuse detection.
Since intrusion symbolizes behavior and the aim to distinguish between usual conduct on sequences and intrusion behavior, Markov models have naturally been applied also used of events to define the profile. As the telecom data, both individual user patterns and overall network behavior change over time, but not adapt so fast that it can accepts intrusions changes.

## VI. TELECOMMUNICATIONS FRAUD

The telecommunications industry has expanded in the last few years to development of affordable number of mobile phone technology. With the increasingly number of global mobile phone fraud is also set to rise. Despite the variety in these figures, it's clear that they are very huge. Apart from this fact they are simply estimations, there are many unlike types of telecom fraud e.g., Shawe-Taylor et al., 2000) and these can occur at various levels. The two most prevalent types are subscription fraud and superimposed fraud is the use of a service without having the necessary authority and is usually detected by the appearance of calls on a bill.

## VII. CONCLUSIONS

The areas we have outline are those which statistical and other data analytic tools have made the fraud detection impact. There are huge quantities of evidence, and this information is numerical or can simply be converted into the numerical in the form of counts. However, in other areas above declared has also used statistical tools for fraud detection. Copy is also a type of fraud. We briefly referred to the use of statistical tools for verification and such methods can also be useful widely. For example, with the evolution of the students to copy articles and pass them off as their own in school or university coursework. As we mentioned in the introduction, fraud detection prevention has been failed. Statistical tools are applied in some fraud methods. For example, so-called biometric methods of fraud detection are becoming more widespread. In many of the essence. This is particularly the case in deal processing, especially with telecom and intrusion data. A key issue in all of this work is effective tool are in detecting fraud and a fundamental problem is that one typically does not know how cases slip through the net. A suitable overall strategy to use a graded system of search. While those with large but less dramatic scores it is a matter of choosing a suitable compromise. Fraud detection is an important area, one in many ways ideal for the application of data analytic tools, and one where can make a very substantial and important support.

## REFERENCES

[1] Callao & Ruisanchez, I. (2018). A synopsis of qualitative approaches for food fraud detection. Food Controller, 86, 283-293.
[2] Phua, C. and Lee , 2004. Underground report in scam detection: classification of twisted data. Explorations newsletter, 6(1).
[3] Bhowmik, R., 2008. Data mining techniques in fraud detection. Paper of Digital Forensics, Safety and Law, 3(2), p.3.
[4] Phua, C., Lee, V., Smith, K. and Gayler, R., 2010. A complete survey of data mining-based fraud detection study. arXiv preprint arXiv:1009.6119.
[5] Bolton, R.J. and Hand, D.J., 2001. Unsupervised profiling methods for fraud detection. Credit scoring and credit control, pp.235-255.
[6] Beigi, S. and Amin Naseri, M.R., 2020. Credit card scam detection using data mining and statistical methods. Paper of AI and Data Mining, pp.149-160.
[7] Bhowmik, Rekha. "Detection auto insurance fraud by data mining techniques." Journal of Emerging Trends in Computing and Information Sciences, no. 4 (2011).
[8] Baesens, Bart, Sebastiaan Höppner, and Tim Verdonck. "Data engineering for scam detection." Decision Support Systems (2021).