DIFFERENT TECHNIQUES USED FOR CREDIT CARD FRAUD DETECTION – A LITERATURE SURVEY

Bushara Hamza[1], Santhi P[2], Dr. G Kiruthiga[3]

[1] *Student, Department of Computer Science & Engineering, IES College of Engineering, Thrissur, Kerala, India*

[2] *Assistant Professor, Department of Computer Science & Engineering, IES College of Engineering, Thrissur, Kerala, India*

[3] *Head of Department, Department of Computer Science & Engineering, IES College of Engineering, Thrissur, Kerala, India*

ABSTRACT

Credit cards are the most used type of electronic payment because of the rise in everyday electronic transactions, which increases their vulnerability to fraud. The cost of card fraud has been high for credit card companies. Currently, finding credit card fraud is the most common issue. The correct procedures & technology are being sought for by credit card firms to prevent & detect fraudulent credit card transactions. For clients to avoid being charged for products they didn't buy, credit card issuers must be able to recognise fraudulent credit card transactions. Data Science may be used to solve these issues, & coupled with machine learning; it is of utmost relevance. Modelling previous credit card transactions using information from those that turned out to be fraudulent is part of the Credit Card Fraud Detection Problem. The validity of a new transaction is then determined using this approach. A classic example of classification is the detection of credit card fraud. Fraudulent actions are often always meant to harm the second party financially. The number of fraudulent actions will rise even further as digital money becomes more widespread in different nations. Every year, these fraudulent activities cost banks & credit card firms billions of dollars in lost income & have a negative impact on many employees' careers. More information on the various credit card fraud schemes is covered in the planned study project. The technical & review publications on credit card fraud detection that have been published in recent years are categorised, compared, & summarised in this survey report.

Keywords: - *Machine Learning, Credit Card, Fraud Detection.*

1. INTRODUCTION

As a result of the explosive growth in non-cash electronic transactions in recent years, online payment methods have been widely used. One of the electronic payment options is a credit card. A consumer (cardholder) receives a thin, rectangular piece of plastic or metal called a credit card from a bank or financial services provider to make payments for products and services. It is based on the customer's assurance to the credit card company. The card issuer (often a bank) opens an account for the cardholder and provides them with a line of credit, through which the user may make a payment. Approximately 51% of transactions are made using credit or debit cards. In spite of the benefits of electronic payment, credit card firms are seeing a rise in card fraud as a result of the introduction of numerous new technologies. Scammers are cunning enough to exploit security flaws and constantly try to steal data using cuttingedge methods like phishing and skimming. There are instances where a website is made to look like a trustworthy site, tricking users into entering sensitive data like passwords, user names, and credit card numbers. In order to lure victims to their fake websites, the fraud artist sends out a large volume of emails (bait). The emails ask the victim to log their personal information in order to fix an issue, and they appear to be from companies like PayPal banks, AOL, and eBay. By stealing the victims' identities and later their money, the fraudster can profit. A significant financial loss resulted from credit card fraud. A 2017 US Payments Forum research claims that as chip card security has increased, thieves' attention has switched to CNP transaction-related crimes.

In 2018, $24.26 million was added to the anticipated global financial loss due to credit card theft. According to PR Newswire Association LLC, the global fraud losses reached US $ 27 billion by 2019. All activation processes have helped to lessen the impact of fraud. Programs are being used by retailers to assist stop credit card fraud. However, further safeguards must be taken to avoid fraud. Machine Learning techniques, which have a high processing or computing power and the capacity to handle big datasets, are effective at detecting fraudulent transactions. It offers hope for lowering credit card theft.

Although services make electronic payments more comfortable, seamless, sufficient, & easy to use, we must not ignore the losses connected to electronic commerce. To employ them, businesses & banks offer sound security options. The deceptive tactics used by fraudsters change over time as a result of these problems. It is therefore essential to develop detection & prevention methods. In order to effectively combat fraud, it is essential to understand how it is carried out. The tool for detecting credit card fraud is dependent on the fraud technique itself. To do this, send the transaction information to the verification module, which will categorise it as fraud or not. It will be denied if it is determined to be fraudulent. If not, the transaction is approved. Artificial intelligence & statistical data analysis are 2 fraud detection methods that can be utilised to differentiate between the two. Data mining is a technique used in AI that can classify, group, & segment data so that it may be searched through millions of transactions to look for patterns & identify fraud. A method for automatically identifying fraud features is machine learning. Detection & prevention strategies are one way to combat fraud. To distinguish between genuine & fraudulent transactions & to stop fraudulent behaviour are the main objectives of fraud detection & prevention. The user's pattern & behaviour are examined using historical data to assess whether a transaction is fraudulent or not. Fraud detection steps are useful when the system is unable to identify & stop fraudulent activity. In supervised fraud detection systems, fresh transactions are categorised as fraudulent or real based on traits of deceptive & legal behaviours, but in unsupervised fraud detection systems, outliers' transactions are detected as potential fraudulent transactions. It is possible to find a conversation between supervised & unsupervised machine learning method. Numerous studies have been done on various strategies for resolving the card fraud detection problem. These methods include of DT, ANN, K-means Clustering, etc.

1.1 Kinds of Card Based Transaction Frauds

1) Physical Card Fraud

The cardholder must physically present the card to the merchant in order to complete the transaction in the majority of POS (point of sale) transactions. The customer may not even be aware that their credit card has been stolen & used fraudulently.

2) Virtual Card Fraud

In the majority of online buying transactions, a physical card is not required; instead, the card number, expiration date, & CVV number are used to complete the transaction. These details are susceptible to theft by scammers, who can then use them to conduct fraudulent online transactions.

2. LITERATURE SURVEY

This section of the paper discusses some of the studies on credit card fraud detection:
S P Maniraj, Aditya Saini, & Swarna Deep Sarkar developed a Credit Card Fraud Detection using Machine Learning & Data Science [1] Methodology. This paper [1] defines "fraud" in credit card transactions as the unauthorised & unwelcomed use of a credit card account by someone other than the account owner. The abuse can be stopped with the use of necessary preventative measures, & the behaviour of such fraudulent acts can be researched to lessen it & safeguard against recurrence. In other terms, credit card fraud is the use of another person's credit card for personal gain when neither the cardholder nor the organisation responsible for providing the card are aware that the card is being used. Monitoring user populations' behaviour is a key component of fraud detection since it helps identify,

detect, & prevent undesirable behaviours including fraud, intrusion, & defaulting. This is a really pertinent issue that has to be addressed by communities like machine learning & data science, where an automated solution is possible. Due to its varied characteristics, including class imbalance, this issue is particularly difficult to solve from the standpoint of learning. There are significantly more legitimate transactions than fraudulent ones. Additionally, the statistical characteristics of the transaction patterns frequently vary over time.

Unquestionably, using a credit card fraudulently is a criminal act of dishonesty. The most popular fraud schemes, as well as how to spot them, are listed in this article [1], which also reviews recent research in the area. Along with the method, pseudocode, explanation of its implementation, & experimentation findings, this work [1] has also provided a detailed explanation of how machine learning might be used to improve fraud detection. Even though the algorithm's accuracy exceeds 99.6%, when only a 10th of the data set is taken into account, its precision is still only 28%. However, the precision increases to 33% when the system is fed the whole dataset. Due to the vast disparity between the number of valid & authentic transactions, this high accuracy % is predicted.

Mohammed Azhan & Shazli Meraj published a journal named Credit Card Fraud Detection using Machine Learning & Deep Learning Techniques [2]. According to the journal [2], frauds relating to net banking have increased along with the industry's expansion. On a regular basis, fraudsters develop new, impenetrable methods to get through fraud detection systems. The term “financial fraud” refers to dishonest behaviour that results in financial gain for the fraudster. Credit card fraud is the most common type of financial fraud. Most credit card scams include either internal or external card fraud. Inner card thefts, which include identity theft, failure to pay fees, & tricking security systems, are the greatest ones to analyse for research purposes. In this journal [2], inner card scams are covered in great detail. When a credit card \ that has been stolen or lost ends up in the hands of fraudsters & is then used for fraudulent purchases, this is known as external card fraud. Analysis of the cardholder's spending habits, past transactions, & their descriptions is the sole time-consuming traditional method that can be utilised to find such frauds.

We can draw the following findings from the investigations that were done:

- In comparison to a shallow neural network, machine learning approaches have proven to be more adept at resolving the problem of class imbalance.
- Class weight distribution in neural networks contributes minimally to addressing the class imbalance.
- Additional methods can be utilised, including the use of cost-sensitive loss functions, over-sampling & under-sampling. It should be highlighted that a more evenly distributed sample would offer a much clearer understanding of the issue.

Aisha Mohammad Fayyomi, Derar Eleyan & Amina Eleyan published an International Journal of Scientific & Technology Research introducing A Survey on Credit Card Fraud Detection Techniques [3]. Their poll indicates that credit card fraud has grown to be a major global threat. Globally, fraud causes enormous financial losses. This pushed credit card firms to spend money developing & creating methods to detect & lessen fraud. The main objective of this study [3] is to establish acceptable algorithms that credit card issuers can use to more quickly & cheaply identify fraudulent transactions. The survey [3] compares various machine learning methods, such as K-Nearest Neighbours, Decision Trees, Random Forest, Artificial Neural Networks, Logistic Regression, & K-means clustering. A scenario-based algorithm can be used to choose the scenario that is the greatest fit for a given scenario because no 2 scenarios are the same. In this survey article [3], all these fraud detection methods are covered.

Emmanuel Ileberi, Yanxia Sun & Zenghui Wang introduced A Machine Learning Based Credit Card Fraud Detection Using the GA Algorithm for Feature Selection [4]. Using this strategy [4], it was discovered that the Internet has grown exponentially over the past 10 years. As a result, services like e-commerce, tap-and-pay systems, online bill payment systems, etc. have proliferated & become more widely used. As a result, credit card thieves are now more active than ever in their attacks on transactions. Credit card data encryption & tokenization are just 2 of the safeguards in place to protect credit card transactions. Although most of the time these techniques work, they don’t completely safeguard credit card transactions from fraud.

A branch of artificial intelligence known as machine learning (ML) enables computers to learn from past experience (data) & enhance their predicting capabilities without being explicitly programmed to do so. Machine learning (ML) techniques are used in this work [4] to detect credit card fraud. A fraudulent transaction (payment) made with a credit or debit card by an unauthorised user is referred to as credit card fraud. The Federal Trade Commission (FTC) reports that there were about 1579 data breaches totalling 179 million data points, with credit card theft being the most common type of breach. Therefore, it is essential to build a reliable system for detecting credit card fraud that can shield people from losing money.

The RF, DT, ANN, NB, & LR were combined with a GA-based feature selection technique in this study [4]. The RF was used to implement the GA's fitness function. 5 ideal feature vectors were produced after the GA was further applied to the dataset of credit card transactions from European cardholders. The results of the experiments utilising the GA-selected characteristics showed that the GA-RF (using v5) had an overall accuracy of 99.98%, which was considered to be ideal. Additionally, using v1, other classifiers like the GA-DT attained a phenomenal accuracy of 99.92%. Results from this study were better than those from earlier studies using similar techniques. Additionally, the results from the European credit card fraud dataset were validated using the proposed framework on a synthetic dataset of credit card fraud. The results of the trial demonstrated that the GA-DT achieved an AUC of 1 & 100% accuracy backed up by the GA-ANN, which had a 100% accuracy rate & an AUC of 0.94. More datasets will be used in subsequent efforts to verify this framework.

John Richard D. Kho & Larry A. Vea developed a Credit Card Fraud Detection Based on Transaction Behavior [5]. According to this concept [5], credit card fraud occurs when someone uses another person's credit card for their own gain, often in complete secrecy or anonymity, & even the issuing banks are unaware that the card is being used. In addition, the offender has no connection to the cardholder or issuer & has no intention of telling the owner of the card about the missing card or making good on the transactions done.

The top 5 methods used by fraudsters in cases involving credit cards over the past 2 decades are as follows:

(i) Counterfeit credit cards
(ii) Lost or stolen
(iii) No-card fraud (e.g., giving card information to non-legitimate telemarketer)
(iv) Stolen cards during mailing fraud
(v) Identity-theft fraud.

These fraud cases account for 81% of all recognised fraud categories in the credit card sector. Banks & businesses are still a target of these attacks even if they may seem extremely common to them. The current state of the credit card industry with regard to fraud issues has been described in this report. Although there are new technologies that can be used to decrease or even eliminate the effects of credit card fraud, banks & merchants throughout the world are starting to question its conception & application. This study [5] advises creating a model based on cardholder spending patterns & utilising it to spot unusual transactions. Due to a non-disclosure agreement (NDA) between the participating bank & the proponent, this study [5] didn’t go into depth about the built model. But this study [5] was able to demonstrate the methods & procedures used to create the model. The author of this paper [5] expects that some banks or people may use it as a guide when implementing fraud detection systems in the financial industry in the near future. Benefits of putting in place such a detection system include lowering the expenses borne by banks for phone & SMS service; instead of sending SMS transaction notifications to all clients, message will be sent to those with detected anomalous transaction. The Random Tree outperformed J48 in the evaluation of classifiers conducted during the model's [5] development. J48 produced a tight constraint with respect to its variance in accuracy values, according to further examination of the 2 classifiers that involved introducing randomness into the dataset.

Clifton Phua, Vincent Lee, Kate Smith & Ross Gayler conducted A Comprehensive Survey of Data Mining-based Fraud Detection Research [6]. The major goal of this research [6] was to identify the problems that currently exist in this area for various kinds of huge data collections & streams. It [6] organises, contrasts, & summarises pertinent data mining-based fraud detection strategies from academic & commercial research that has been published.

Another goal was to draw attention to promising new directions in related hostile data mining domains & applications, such as the identification of epidemics & outbreaks, insider trading, intrusions, money laundering, spam, & terrorists. It will assist avoid “reinventing the wheel” & repetitions of common errors if knowledge & experience from various antagonistic disciplines are convertible.

Nearly all studies on fraud detection that have been published have been surveyed in this paper [6]. The adversary, fraud subtypes & types, technical aspects of data, performance indicators, & methods & tactics are all defined. This study [6] demonstrates how fraud detection can profit from other related topics after identifying the limitations in approaches & procedures. Future research on fraud detection can specifically benefit from unsupervised approaches from counterterrorism work, real monitoring systems & text mining from law enforcement, & semi-supervised & game-theoretic approaches from intrusion & spam detection fields. Fawcett & Provost (1999), who successfully applied their fraud detection system to news story monitoring but unsuccessfully to intrusion detection, demonstrate that there are no certainties. Future work will consist of detecting credit application fraud.

3. CONCLUSIONS

The most common techniques, datasets, & features used to identify credit card fraud around the world are listed in this paper. Each method used in this study is also evaluated for efficacy & accuracy. Additionally, other studies focus on reducing dataset misclassification or correlation. Accuracy & computation speed still have a wide gap that needs to be bridged. There are several prospects for research with the credit card transaction dataset.

4. ACKNOWLEDGEMENT

The authors would like to thank all of the instructors at the Department of Computer Science & Engineering at IES Engineering College in Thrissur, Kerala, India, for supporting this research work as part of the Master Research Project Phase I for the MTech Program.

5. REFERENCES

[1]. "Credit Card Fraud Detection using Machine Learning and Data Science – by S P Maniraj, Aditya Saini, Swarna Deep Sarkar, Shadab Ahmed" Published by International Journal of Engineering Research & Technology (IJERT) http://www.ijert.org ISSN: 2278-0181 IJERTV8IS090031 Vol. 8 Issue 09, September-2019

[2]. "Credit Card Fraud Detection using Machine Learning and Deep Learning Techniques – by Mohammed Azhan, Shazli Meraj" Published by Proceedings of the Third International Conference on Intelligent Sustainable Systems [ICISS 2020] IEEE Xplore Part Number: CFP20M19-ART; ISBN: 978-1-7281-7089-3

[3]. "A Survey Paper on Credit Card Fraud Detection Techniques – by Aisha Mohammad Fayyomi, Derar Eleyan, Amina Eleyan" Published by International Journal of Scientific & Technology Research Volume 10, Issue 09, September 2021 ISSN 2277-8616

[4]. "A Machine Learning Based Credit Card Fraud Detection Using the GA Algorithm for Feature Selection – by Emmanuel Ileberi, Yanxia Sun, Zenghui Wang" Published by Ileberi et al. Journal of Big Data (2022) https://doi.org/10.1186/s40537-022-00573-8

[5]. "Credit Card Fraud Detection Based on Transaction Behavior – by John Richard D. Kho, Larry A. Vea" Published by Proc. of the IEEE Region 10 Conference (TENCON), Malaysia.

[6]. "A Comprehensive Survey of Data Mining-based Fraud Detection Research – by Clifton Phua, Vincent Lee, Kate Smith, Ross Gayler"