A Review: On Types Of Credit Card Frauds

Abstract—Credit is a technique that is used to sell goods or services with the buyer having no cash in hand. An automatic way to proffer credit to a client is a credit card. An identifying number is carried by each credit card which speeds shopping transactions. The main problem in the credit card industry is Fraud. There are so many types of fraud. In order to prevent these frauds many fraud detection techniques are used. In this paper a general introduction to credit card fraud, types of fraud and fraud management developments is offered. In addition, an overview to the previous work done by many authors in this field is offered.

Index Terms— Credit card Fraud, Detection techniques, Neural Network

I. Introduction

Fraud alludes to achieve products/services and cash by unlawful manner. The events that include criminal motives that generally is complicated to identify, the Fraud deals with these events. Nowadays the credit card fraud is the major threat to business industry. Therefore, in order to combat the fraud efficiently, initially it is necessary to understand the methods of implementing a fraud [1]. In order to commit fraud, the credit card fraudsters use a huge number of modus operandi. Generally, Credit card Fraud is characterized as 'when a person utilizes credit card of other person for personal reasons whereas the card owner and the issuer of the card are don’t know about the way that the card is being utilized by someone else'. Additionally, the individual utilizing the card has no association with the cardholder or issuer, and has no goal of either reaching the owner of the card or making repayments for the buys made. Credit card frauds are submitted in the accompanying ways:

- A demonstration of criminal deception by utilization of unauthorized account and personal data.
- For personal benefit, Illegal or unauthorized utilization of account.
- In order to achieve goods and services, falsification of account data.

In opposition to mainstream idea, merchants are undeniably more in jeopardy from credit card fraud than the card owners. While clients may confront inconvenience trying to achieve a deceitful charge reversed, merchants lose the expense of the product, pay chargeback charges, and dread from the jeopardy of having their merchant account shut [2]. Progressively, the card not present situation, for example, shopping on the web represents a more prominent risk as the merchant (the site) is never again ensured with preferences of physical confirmation, for example, signature check, photograph recognizable proof.

II. Fraud Types

Several sorts of frauds are illustrated in this work that are Credit card frauds, computer intrusions, Theft fraud/counterfeit fraud, Behavioral fraud, telecommunication frauds, Bankruptcy fraud, Application fraud [4].

- 2.1 Credit Card Fraud: The credit card fraud is alienated into a couple of sorts that are

illustrated below as:

  - · Online Fraud: The online fraud is the type of fraud that can be commended through internet, shopping, phone, and web or in absence of card holder.
  - · Offline fraud: The offline fraud is the type of fraud that can be done through utilizing a stolen physical card at call centre or some other place.

- 2.2 Telecommunication Fraud: The other type of fraud is telecommunication fraud that is utilized to do other types of fraud. Business, Communication service provider and clients are the victims.
- 2.3 Computer Intrusion: The act of entering with no warrant or invitation is known as Intrusion which implies that “potential probability of unapproved endeavor to get to Information, Manipulate Information Purposefully. Intruders might be from any condition, A Hacker and an insider who knows the design of the system [3].
- 2.4 Bankruptcy Fraud: In this type of fraud a credit card is being utilized while being absent which is known as Bankruptcy fraud. The one of the most difficult sorts of fraud to expect is Bankruptcy fraud [3].
- 2.5 Theft Fraud/ Counterfeit Fraud: Theft Fraud is the fraud in which you are using another person’s card. Once the owner provides some detail by contacting to the bank, the bank will find the thief as soon as possible. Also, where just credit card details are required the counterfeit fraud can takes place as the credit card is utilized remotely [4].
- 2.6 Application Fraud: An application fraud is a fraud where a credit card is applied by someone with fake information. A couple of diverse situations have to be categorized in order to detect the application fraud. Duplicate Fraud means if same details are utilized by same client more than once. Identity Fraudsters means if the same details are used by the different users. Application fraud can be described [5] as “illustration of identity crime, happens when application forms contain conceivable, and synthetic, or genuine yet additionally stolen identity data.”
- 2.7 Lost/ Stolen cards: Lost/Stolen cards is the another type of fraud in which a card is achieved by a legitimate account holder and loses it or the card is stolen by someone for criminal purposes. This kind of fraud is generally the most effortless path for a fraudster to get hold of other user’s charge cards without interest in innovation. It is additionally maybe the hardest type of conventional credit card fraud to handle.
- 2.8 Account takeover: Account takeover is a fraud that happens at time a fraudster unlawfully achieves a valid user’s personal data. By giving the user’s account number or the card number, the fraudster can take over a legitimate account. Afterward the fraudster can contact the card issuer, attempted as a real card owner to request that mail be redirected to a novel address. A card lost can be reported by a fraudster through which, the fraudster can request for a replacement to make.

Credit Card Fraud

Types of Fraud

Theft Fraud/ Counterfeit Fraud

Telecommunication Fraud

Computer Intrusion

Bankruptcy Fraud

Account takeover

Lost/ Stolen cards

Application Fraud

Figure 1: Types of fraud [3]

III. Fraud Management Developments

In order to investigate the credit card frauds, the technology is advancing at quick speed- neural networks, biometrics, rule based systems, chip cards are various methods that are employed by Issuing and Acquiring Banks nowadays. Some of the techniques are illustrated as follows [6]:

3.1 Simple rule systems

The formation of ‘if…then’ principle in order to filter incoming authorizations/transactions. On the basis of a set of expert rules, the Rule-base methods are deliberated in order to identify certain sorts of high-risk transactions. By utilizing the information of what characterizes fraudulent transactions, the rules are formed. For example, a standard could be like – If transaction amount is > $100 and card acceptance area = Casino and Country = 'a high-risk nation'. Fraud rules empower to computerize the screening forms utilizing the information increased after some time with respect to the qualities of both false and genuine transactions. Generally, the adequacy of a rule-based framework will increment after some time, as more principles are added to the framework. It ought to be clear, be that as it may, that eventually the adequacy of the framework relies upon the information and mastery of the individual designing the rules. The demerit of this arrangement is that it can build the likelihood of throwing numerous legitimate transactions as special cases; nonetheless, there are routes by which this confinement can be conquered to some degree by organizing the rules and fixing limits on number of separated transactions.

3.2 Risk scoring technologies

Risk scoring tools are occurred on the basis of statistical models deliberated to identify fraudulent transactions on the basis of several indicators generated from the transaction features. Generally, a numeric score is generated by these tools signifying the likelihood of a transaction being fraudulent: the order will be more suspicious if the score is higher. One of the most efficient fraud prevention tools are offered by Risk scoring mechanisms. The major merit of risk scoring is the comprehensive computation of a transaction being captured by a single number.

3.3 Neural network technologies

The expansion of risk scoring methods is the Neural Network method. They are occurred on the basis of ‘statistical knowledge’ included in broad databases of historical transactions, as well as fraudulent ones in specific. These neural network models are essentially ‘trained’ by utilizing instances of both real and deceitful transactions and can connect and weigh different fraud indicators to the event of fraud. A neural network is an electronic framework that sorts

information consistently by performing the accompanying errands:

- Buying of card owners and fraudulent activity patterns are identified.
- Through trial and elimination the data is processed.
- In the patterns and current transaction data, the relationships are found.

The standards of neural networking are inspired by the functions of the brain – particularly pattern recognition and associative memory. The neural system identifies comparable examples, anticipating future qualities or occasions dependent on the acquainted memory of the examples it has learned. The preferences neural systems offer over different procedures are that these models can gain from the past and along these lines, improve results over the long haul. They can likewise extricate rules and anticipate future action dependent on the present circumstance. By utilizing neural systems viably, banks can identify false utilization of a card, quicker and all the more proficiently.

IV. Related Work

Johannes Jurgovsky, Michael Granitzer et al., 2018, [7] In this paper the author had phrased the fraud detection issue as a sequence classification task and use LSTM networks in order to integrate transaction sequences. The author had additionally incorporated modern characteristic aggregation systems and reports the outcomes with the help of conventional retrieval metrics. A connection with a baseline random forest (RF) classifier exhibited that the LSTM improved recognition exactness on disconnected transactions where the card-holder was physically present at a vendor. Both the sequential and non-sequential learning methodologies advantage powerfully from manual feature aggregation techniques. A consequent investigation of genuine positives uncovered that the two methodologies be liable to distinguish diverse frauds, which recommends an arrangement of the two. The author had concluded the investigation with a discourse on both useful and logical difficulties that stay unsolved.

Alex G.C.de Sá Adriano, C.M. Pereira Gisele et al., 2018, [8] in this paper the author had represented a customized Bayesian Network Classifier (BNC) algorithm, a Fraud-BNC for a genuine credit card fraud detection issue. The operation of generating Fraud-BNC was automatically presented through a Hyper-Heuristic Evolutionary Algorithm that arranges the information regarding the BNC paradigms into taxonomy and investigates for the finest arrangement of these components for a given dataset. By utilizing a dataset from PagSeguro, the Fraud BNC was automatically created, the well known Brazilian online payment service, and tested together among a couple of techniques for dealing along with cost-sensitive categorization. The simulation results were evaluated with seven more paradigms and examined in view of the data categorization issue, as well as the economic effectiveness of the mechanism. In order to offer a better trade-off in both perspectives, enhancing the present economic effectiveness of the company in up to 72.64%, the Fraud- BNC represented itself as the finest paradigm.

Alejandro Correa Bahnsen, Djamila Aouada, 2016, [9] In this paper the author had illustrated that currently, in order to address the issue, many authors have projected the utilization of machine learning and data mining methods. Therefore, various studies utilized various type of mis-categorization measure to estimate the diverse resolutions, and did not consider the real financial costs connected to the fraud detection procedure. Also, while building a credit card

fraud detection model, it was critical how to remove the correct highlights from the transactional information. This was typically done by collecting the exchanges so as to monitor the spending personal conduct standards of the clients. In this paper the author had extended the transaction accumulation system, and proposed to make another arrangement of highlights dependent on examining the intermittent conduct of the time of a transaction utilizing the von Mises distribution. At that point, utilizing a genuine credit card fraud dataset given by a vast European card preparing organization, it was analyzed modern credit card fraud detection models, and estimated how the diverse arrangements of highlights affect the outcomes. By including the proposed periodic highlights into the techniques, the outcomes demonstrate a normal increment in reserve funds of 13%.

Akila S, Srinivasulu Reddy U, 2018, [10] In this work the author had illustrated the credit card fraud had presented a major threat for arrangements because of the possibility o0f large losses connected to it. The author had presented a cost sensitive Risk Induced Bayesian Inference Bagging model, for credit card fraud investigation. A Risk Induced Bayesian Inference mechanism as a base learner and a cost-sensitive weighted voting combiner was projected that was a new bagging architecture incorporating a constrained bag creation mechanism.

Fabrizio Carcillo, Andrea Dal Pozzolo, 2018, [11] in this paper the author had illustrated that the extension of the electronic commerce, among an enhancing confidence of customers in electronic payments, made the fraud detection a crucial factor. Distinguishing frauds in (about) ongoing setting requests the structure and the usage of adaptable learning procedures ready to ingest and dissect huge measures of streaming information. Late advances in examination and the accessibility of open source answers for Big Data stockpiling and handling open new points of view to the fraud detection field. In this paper the author had presented a Scalable Real-time Fraud Finder (SCARFF) which coordinates Big Data instruments (Kafka, Spark and Cassandra) with a machine learning approach which manages irregularity, non-stationary and input inertness. Test results on a huge dataset of genuine credit card transactions demonstrate that this system is adaptable, effective and exact over a major stream of transactions.

Ugo Fiore, Alfredo De Santis, 2017, [12] in this paper the author had illustrated that in previous years the quantity of frauds in credit card-based online installments had developed significantly, pushing banks and web based business associations to actualize automatic fraud recognition frameworks, performing information mining on tremendous exchange logs. Machine learning was by all accounts a standout amongst the most encouraging answers for spotting unlawful exchanges, by recognizing fraud and non-fraud occasions using managed parallel arrangement frameworks appropriately prepared from pre-screened test datasets. Nonetheless, in such a particular application area, datasets accessible for preparing were firmly imbalanced, with the class of intrigue extensively less spoke to than the other. This fundamentally lessens the viability of parallel classifiers, unfortunately biasing the outcomes toward the overall class, while the author was keen on the minority class. Oversampling the minority class had been embraced to reduce this issue, yet this strategy still had a few downsides. Generative Adversarial Networks were general, adaptable, and ground-breaking generative profound learning models that have made progress in delivering convincingly genuine looking pictures. The author had prepared a GAN to yield emulated minority class models, which were then converged with preparing information into an expanded preparing set so the adequacy of a classifier can be improved. Investigations demonstrate that a classifier prepared on the increased set beats a similar classifier prepared on the first information; particularly as far the affectability is concerned, bringing about a successful extortion discovery system.

Suraj Patil, VarshaNemade et al., 2018, [13] in this paper the author had illustrated that these days, by credit card and online net banking nearly all E-commerce application mechanism transactions are accomplished. Among novel assaults and mechanisms, these mechanisms are susceptible at alarming rate. Fraud detection in managing an account is one of the imperative viewpoints these days as fund is real division in life. As information is expanding as far as Peta Bytes (PB) and to improve the execution of expository server in model building, the author had have interface logical structure with Hadoop which can peruse information productively and provide for diagnostic server for extortion expectation. In this paper the author had examined a Big data scientific structure to process huge volume of information and executed different machine learning calculations for fraud recognition and monitored their execution on benchmark dataset to identify frauds on ongoing premise there by giving okay and high consumer satisfaction.

Nuno Carneiro, Gonçalo Figueira et al., 2017, [14] in this paper the author had illustrated that the credit-card fraud had directed to billions of dollars in losses for online merchants. With the advancement of machine learning calculations, researchers had been finding progressively refined approaches to recognize fraud, however commonsense usage are seldom detailed. We depict the improvement and organization of a fraud detection framework in an extensive e-tail merchant. The paper investigated the arrangement of manual and programmed grouping, given bits of knowledge into the total improvement procedure and measured various machine learning techniques. The paper would thus be able to support analysts and researchers to plan and execute information data mining based frameworks for fraud location or comparable issues. This undertaking had contributed with a programmed framework, yet in addition with bits of knowledge to the fraud investigators for improving their manual modification process, which brought about a general superior performance.

Table 1: Comparison of various Fraud Detection Techniques [15]

Parameters

Method

Fraud Detection TP%

Accuracy

Processing Speed

Cost

Research Issues Addressed

Research Challenges

Techniques

Artificial Neural Network

Artificial Intelligence, Machine Learning

70%

Moderate

High

Costly

Cellular phone fraud, Calling Card Fraud, Computer Networks Intrusion Applicable in E-commerce

In order to operate, training is required as well as for huge neural networks high processing time is needed.

Fuzzy Drawinian detection

Genetic Programming Fuzzy Logic

100%

Very High

Less

More Costly

Simply investigate stolen Credit card frauds. Examine Suspicious and Non-suspicious data.

Execution is complicated and it is not applicable in E-commerce.

Support Vector Machine

Clustering

70%

High

Moderate

Costly

The transaction must be suspicion only if a test case lies outside the hyper-sphere

Back Propagation has better performance in large data.

K-nearest Neighbor

Clustering

80%

Moderate

High

Costly

Classify through evaluating closest point if the closest neighbor is fraudulent, therefore the transaction is classified as fraudulent

On the basis of the measure of distance, accuracy is occurred.

Naïve Bayes

Probabilistic Classifier

66%

Moderate

Moderate

Costly

In order to evaluate the possibility of the exact class, the categorization is accomplished with the help of “Bayes” rule that demonstrates better performance.

If a fraudulent transaction is in progress the fraud cannot be detected by this technique.

The Table 1 shows the comparison of different parameters of various techniques that are Artificial Neural Network, Fuzzy Drawinian detection, Support Vector Machine, K-nearest Neighbor, Naïve Bayes.

V. Conclusion

Credit card fraud can be alienated into a couple of sorts that are inner card fraud and external card fraud. The main concern of Inner card fraud is to deceive the money. External card fraud is primarily encapsulated at utilizing the stolen, phony or fake credit card to expend, or utilizing cards to get money in hidden manners. In previous years, the credit card fraud has become growingly uncontrolled which is a criminal act. In this paper the author has offered an overview to the research that has been done in credit card field. Several sorts of frauds and fraud detection techniques are demonstrated in this work.

References

1. Chunzhi Wang, Yichao Wang, Zhiwei Ye, Lingyu Yan, Wencheng Cai, Shang Pan , “Credit card fraud detection based on whale algorithm optimized BP neural network”,

IEEE, pp 614-617, 2018.
2. Deshe, Wang, Bintong Chen, Jing Chen, “Credit card fraud detection strategies with consumer incentives”, ELSEVIER, 2018.
3. 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.
4. 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.
5. Vladimir Zaslavsky and Anna Strizhak,” credit card fraud detection using selforganizing maps”, information & security. An International Journal, Vol.18, 2006.
6. Suman and Nutan, “Review Paper on Credit Card Fraud Detection”, IJCTT, Volume 4, Issue 7, Pp 2206-2215, 2013.
7. Johannes Jurgovsky, Michael Granitzer, Konstantin Ziegler, “Sequence classification for credit-card fraud detection”, ELSEVIER, vol 100, pp 234-245, 2018.
8. Alex G.C.de Sá Adriano, C.M. Pereira Gisele, L.Pappa, “A customized classification algorithm for credit card fraud detection”, ELSEVIER, vol 72, pp 21-29, 2018.
9. Alejandro Correa Bahnsen, Djamila Aouada, “Feature engineering strategies for credit card fraud detection”, ELSEVIER, vol 51, pp 134-142, 2016.
10. Akila S, Srinivasulu Reddy U, “Cost-sensitive Risk Induced Bayesian Inference Bagging (RIBIB) for credit card fraud detection”, ELSEVIER, vol 27, pp 247-254, 2018.
11. Fabrizio Carcillo, Andrea Dal Pozzolo, “SCARFF: A scalable framework for streaming credit card fraud detection with spark”, ELSEVIER, vol 41, pp 182-194, 2018.
12. Ugo Fiore, Alfredo De Santis, “Using generative adversarial networks for improving classification effectiveness in credit card fraud detection”, ELSEVIER, 2017.
13. Suraj Patil, VarshaNemade, Piyush Kumar Soni, “Predictive Modelling For Credit Card Fraud Detection Using Data Analytics”, ELSEVIER, vol 132, pp 385-395, 2018.
14. Nuno Carneiro, Gonçalo Figueira, Miguel Costa, “A data mining based system for credit-card fraud detection in e-tail”, ELSEVIER, vol 95, pp 91-101, 2017.
15. Sunil Bhatia , Rashmi Bajaj , Santosh Hazari, “Analysis of Credit Card Fraud Detection Techniques”, IJSR, Volume 5, Issue 3, Pp 1302-1307, 2016.