International Journal of Engineering Science Invention Research & Development; Vol. 11, Issue 9, March 2025
www.ijesird.com, E-ISSN: 2349-6185

REVIEW ON CREDIT CARD FRAUD DETECTION SYSTEM USING MACHINE LEARNING TECHNIQUES

Dr. Vikas Srivastava[1], Dr. Parul Preet Singh[2]

Axis Institute of Technology and Management, Kanpur[1,2], Lovely Professional University, Phagwara[3]
Vikassr2009@gmail.com[1], surabhisr20014@gmail.com[3]

Abstract- Today, credit cards are small plastic cards issued by banks or financial institutions, allowing the holder to buy goods or services on credit. Debit cards enable holders to purchase items or services directly from their checking account. The use of both credit and debit cards is increasing steadily, with more people relying on them for online and in-person purchases. As these cards become the most common payment method, instances of fraud are also on the rise. Fraudulent transactions are often mixed with legitimate ones, making them difficult to detect with simple pattern matching techniques. To address this, we propose a window sliding structure to analyze transactions over time. This paper introduces a credit card fraud detection system that leverages operational and transaction features using a machine learning algorithm. In the first phase of the system, users' operational features are extracted and classified using machine learning. In the second phase, further operational features are analyzed to enhance detection accuracy.

Keywords: Credit Card fraud detection, Machine learning, feature, classifier

1. INTRODUCTION

In the current global situation, financial institutions are increasing the availability of financial services through new services such as CCs (CCs), ATMs, the Internet, and mobile banking services are all examples of automated teller machines (ATMs). There are many benefits to using CCs such as easy purchase, maintain a customer credit history and purchase protection**:** CCs can also provide customers with additional protection when purchases are sold, lost, or stolen. Both the consumer's and company's statements can confirm the purchase of the customer.

1.1 How CC Processing Works

There are four main players involved in CC processing. (1) Issuing bank (2) Processor (3) Issuer's fraud security team and (4) Acquiring bank. CC processing goes through six stages. The first one is when a customer purchases goods or services and pays with a CC. The second is when the vendor runs the CC. The customer's information is transmitted via the vendor's terminal to the acquirer's network. The acquirer forwards this information to the processor. The processor's network then communicates with the issuer's fraud detection company and waits for the transaction to pass the fraud test. Once the transaction is deemed non-fraudulent, it is forwarded to the issuer for final approval. When this approval is sent, the customer leaves with the goods or receives the services provided by the vendor. The issuer then sends a bill to the customer.

CCs were explicitly intended to provide retail payments from a customer to a vendor. In the typical CC processing cycle, 6 stakeholders are involved: client, an issuer of cards, seller, vendor, purchaser, and a CC processor. Customers are issued by the card-issuing bank and their accounts are maintained. The seller establishes a bank account for payments. The seller wants to register with an acquisitor, a bank, or a financial institution, in order to obtain CCs. The processor is an enormous data center supported by the CC network and serves as an intermediary for all CC companies.

For each CC procurement, there are two steps of transaction: payment approval and collection. Authorization indicates that the account number to collect remains valid, has enough credit, and is not misplaced or malicious. Capture refers to transaction authorization and publishing. When a client buys the terminal, the seller uses it to route the purchaser's payment data. The buyer shall assign an approval with the card processor, which shall consolidate credit availability with the bank of the client and if everything goes smoothly, shall provide the buyer with an authorisation number. The purchaser returns the permission to the seller. All transactions take place in a matter of seconds and no money is transacted to date.

The purchaser receives multiple payment authorizations to collect the monies and sends them on an hourly or daily basis to the processor. The purchaser pays the remainder to the seller's bank when the fund has been received. Therefore, the suppliers are responsible for all the costs of CC processing. There is also a refund, in addition to the authorization and capture, following a series of transactions. Interactions between several entities inside CC transactions are displayed in Figure 1. The solid lines imply a true transmission of data and the points express the relationship between two parties.

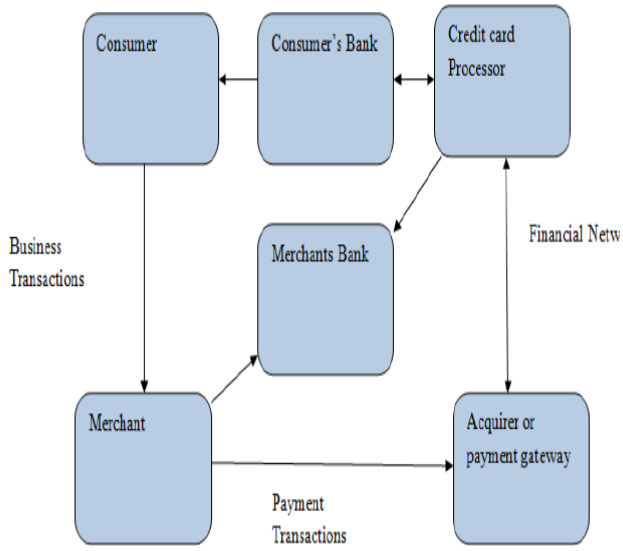

Figure 1 Interactions across various entities in CC transactions [12]

The CC processing technique was established by financial companies very long back and they are sternly preserved and organized by the financial companies. Accordingly, the fundamental method of authorization of payment and the collection of funds is carried out in the same way, whether it is from a store or over the Internet.
The big barrier for an online provider, however, is to have the customer's CC and personal information protected over the Internet. Once this information has been obtained, the seller has the choice of either completing the payment process through common means or systematizing the entire procurement and payment procedure.

1.2 Types of CC Transactions

CC transactions fall under two categories.
- The first one is a card present.
- The second type is known as a card not present. All e-commerce transactions fall under this category and they are the most susceptible to CC fraud.

A vendor can process CC payments in many ways like Touch-tone telephone systems, Point-of-sale (POS) terminals, POS-like-PC terminal, and Web-based solutions.

1.3 Fraud Detection

Fraud is an action in which someone directly or indirectly steals the amount of a victim by making forged transactions without allowing them to know about it [1]. The main category of frauds are management Fraud and customer fraud. These kinds of frauds are always performed on Credit or Debit cards [2], due to the poor security system.
Most of the users have well-known passwords or pin numbers which can be easily captured by third parties using some algorithms. Hence it is mandatory to build an anti-fraud system which will be able to detect the unauthorized access of user accounts [3].
There are plenty of ML algorithms that can be used to detect CC fraud activities and to trace the fraud users. There are four types of fraud. They are CC fraud, Telephonic fraud, SQL injection fraud, and Theft/Application Fraud.

1.4 CC Fraud

The introduction of communication techniques has resulted in an increase in e-commerce, as well as online payment, deals daily. Together with this tax fraud associated with these transactions they are also growing, resulting in trillions of dollars being forfeited globally every year. CC scam is the longest standing, most frequent, and most dangerous among the many fiscal scams because of its broad practice due to the convenience of the customer. Likewise, several types of benefits such as a rebate and deduction suggestions for procurements in particular stores would induce customers to use CC for their consumption as an alternative to cash [4].

CC scams are an encompassing term for frauds used as a stained source of cash for dealing with imbursement cards. CC scam identification method is used to detect these illicit sources of transactions. The amount of scams occurring all across the world has increased unbelievably. Scam transactions are wrong transactions by means of CCs without the genuine owner of the card. Deceptive transactions were performed in private products, everyday transactions, bills, etc [5].

A scam is an operation when a person uses the cash of a beast without reluctance or accidentally via fraudulent transactions and is deprived of informing him of the agreement [6]. It is a very complicated problem to perceive unlawful CC transactions since structures are seldom helpful when taken alone.Although data removal techniques may sense disguised data designs, they typically lack the capacity to develop methods that define the universal building formed by communications among the various structure [7]. Despite these benefits, fraud is a significant concern in e-banking services and poses a danger to credit card transactions. CC fraud is growing to a large extent with the emerging of modern technologies because of which there are huge losses across the world every year.

Fraud detection is a process of quickly detecting doubtful actions among various normal transactions. Fraud detection techniques are growing fast in order to cope up with newly emerging frauds across the world. However, owing to the severe restrictions of the information exchange involved in the approaches, creating new fraud detection systems is not straightforward. Other analyses, detections of anomalies, exception mining, unusual mining classes, imbalanced mining data, and other approaches can be utilized for the identification of fraud. Because the quantity of harmful transactions is often low, properly detecting fraud transactions is extremely difficult. Hence it is necessary to develop effective techniques

to classify rare fraud actions from a huge set of normal transactions records. Some of the examples of CC frauds are as follows: Swipe Machine Fraud, eCommerce Website Fraud, CC Cloning, CC Theft, Leaking Card Information on Telephone.

1.5 Types of CC frauds

In specifically, there are three kinds of fraud: the card, the dealer, and the Internet. Some of them are listed below
(i) Card Related Frauds
● Application Frauds: This kind of extort is when the fraudster controls the program by collecting sensitive data from another person open a false account on his behalf.
● Stolen Card: This type of extort occurs when the imposter takes a customer's card effectively.
(ii) Dealer Related Frauds
● Vendor Collusion: this is the case when a dealer knowingly transmits critical data to their customer to fraudsters.
● Triangulation: In situations of fraud, as a retailer and customer indications with agreements and offers, the fraudster would surely be aware of them whenever the customer is interested and buys anything, the fraudster will then capture all payment information and then utilize them for unlawful operations.
(iii) Web Frauds
False sites: This is essentially a phishing attack in which a fraudster creates a fake website that looks identical to a number of well-known websites in a given country and then offers various discounts to entice customers to buy products when they buy specific products on the Internet, and the fraudster then uses all of the site's transaction information [8].
Defending your card against deceitful doings isn't problematic. It just means being conscious of the several gambits cheats that may utilize and making it a point to stay ahead of them with the correct data and the correct CC company you can guarantee that your money is in good hands.
● **Pick pocketing or physical theft**
The most clear method your CC could be compromised is by means of burglary.
● **Skimming card information**
A less apparent mode that your CC could be negotiated is via skimming which is the performance of pocketing the card data rather than the card itself.
● **Phishing and other scams**
Phishing is the action of asking for card data from you personally.
● **Carding or cyber-attacks**
The most solemn and destructive manner in which your card data could be conceded is carding in which hackers hack into payment servers and take data of thousands of accounts.
● **Card-not-present (CNP) fraud**
'Card not present' is a fraud, mostly online or by telephone, deprived of the use of a physical card. The transactions that do not occur via card are more common when clients refuse to use their cards and merely input their details to shop.
● **Malware and phishing attacks**
These are turning out to be progressively urbane, hence treat unwanted emails and messages from unknown people with doubt.
● Your credit limit is reached.
● Your account becomes empty.
● **False application fraud**
This fraud takes place where the account is identified using the identity or information of someone else.
Many CC suppliers take this fraud very seriously and perform a series of checks to ensure this doesn't occur. We should ensure to keep track of our bank accounts, keep delicate data concealed, and most prominently, take any sort of deceitful action extremely and report it at the earliest.

1.6 CC fraud detection techniques

There are two broad kinds of CC fraud detection techniques:
● Analysis of fraud (misuse detection): This approach is used to perform supervised classification tasks at the transaction level.
● User behavior analysis (anomaly detection): This technique may be used with unsupervised algorithms based on account activity.

1.7 Challenges

Fraud detection programs are prone through many difficulties and written challenges. An efficient fraud detection method should have the skills to fix this difficulty to achieve the best performance.
● Data that is unbalanced: The CC fraud detection data is unbalanced. That only a small fraction of all credit card transactions are fraudulent.
● Different misclassification errors have different degrees of impact when it comes to fraud detection. The risk of misclassifying a legitimate transaction as fraudulent is lower than the risk of misclassifying a fraudulent transaction as legitimate. Because the categorization error in the first case will be found through more study.
● Lack of adaptability: Normally, classification algorithms are incapable of detecting new forms of normal patterns. Machine learning to identify fraud is not good at distinguishing new behavioral patterns [9].
● · Costs for Fraud detection: both detection and prevention of fraud should be covered by the system. A fraudulent transaction with a lesser amount, for instance, may lead to no income [10].
● · There are no standard measurement settings under which fraud detection systems may be evaluated and comparable since they have no standard methods.

1.8 Machine Learning (ML) algorithms

Machine learning (ML) techniques enable systems to learn from experience. ML refers to a system's ability to acquire and integrate knowledge through large-scale observations and to improve and extend itself by learning new knowledge rather than by being programmed with that knowledge[11].

1.9 ML Techniques in CC Fraud Detection

Some current ways to detect CC fraud are discussed as follows.

1.9.1 Artificial Neural Network (ANN)

ANN is a network of linked nodes that are meant to mimic operations of the human brain. Individual areas employ weights and a simple output calculation method to collect input from related nodes. NN works come in a variety of shapes and sizes [12]. The bulk of NN architectures are controlled by the user. Recordings of both false and misleading records used by their labels were utilized to construct models in the supervised approaches.

These approaches are frequently used in fraud analysis. The widely monitored type of NN is the Back Propagation Network (BPN). Reduces objective operation using a more powerful approach named multi-stage dynamic optimization and is inspired by enforcing delta law. The BPN method is often useful in a forwarding network without feedback. To obtain ideal performance, the method frequently demands time, and factors such as the number of hidden neurons and the amount of learning of the delta rules necessitate extensive tweaking and training. Monitored neural networks, such as back-distribution, are a useful technology with numerous applications in the field of fraud detection.

These approaches are frequently used to analyze user activity. For large enough databases, ANNs can give satisfactory results. They require a large training database. In order to prevent credit card fraud, (self-organizing map)SOM offers an integrated method that is excellent for developing and evaluating consumer profiles. Training and mapping are the two processes of SOM. Based on input samples, the map is constructed and the neurons are assessed sequentially in the previous phase, and the test data is then automatically divided into standard and deceptive phases by the mapping process. After SOM training, fresh non-existent transactions are compared to standard transactions, and fraudulent transactions are regarded normal if they match all standard records.

One advantage of using similarly controlled NNs is that these mechanisms may learn by transferring information. The more data is passed on to the SOM model, the more chances are made available for finding and improving results. This might result in banks and other financial institutions being used and updated online. The use of a falsified card can therefore be quickly and accurately recognized. NNs, on the other hand, have various issues and challenges that are strongly connected to choosing the correct model on the one hand and further training necessary to attain optimal performance on the other.

1.9.2 Artificial Immune System (AIS)

AIS is a new domain depend on the immune system's natural picture [13]. Engineers in various fields have aimed to find patterns, identify and eliminate disease immediately. Immunology concepts have been used to construct algorithms like the negative selection algorithm, immune network algorithm, and dendritic cell algorithm.

1.9.3 Genetic Algorithm (GA)

GA is looking for a great solution for a number of solutions based on chromosomes. The main concept is that strong nation members have a better chance of surviving and reproducing. The strength of the solution determines its efficacy in solving the given challenge [14].

Genetic Programming (GP) [15] is a more advanced form of GA in which each tree represents a single human rather than a narrow string of characters. Because of the vastness of the tree position, the GP may create a wide range of models, including mathematical functions, logical and mathematical expressions, computer programs, and so on.

1.9.4 Hidden Markov Model (HMM)

Markov's hidden model is an entrenched process used to model more complex stochastic processes in contrast to the conventional Markov model. For simple Markov models such as Markov chains, provinces have the potential for a clear switch with only unknown parameters. In contrast, HMM regions are hidden, but the results are dependent on the government. In the discovery of CC fraud, HMM is trained to model the standard behavior included in user records [16]. In this regard, newly added transactions will be separated from fraud if the model is not validated with high enough opportunities. Each user record provides information about the user's past ten transactions, such as the time, category, and value of each transaction. HMM produces a high amount of falsity.

1.9.5 Support Vector Machine (SVM)

The main idea behind SVM was to identify the best hyperplane that could discriminate between the criteria of two classes, respectively. Many of these planes were thought to be located in the middle of some of the lower levels called vector support. Introducing kernel functions, the concept is expanded with separate details.The kernel function is the point-product in the maximum space of two-point predictive data. It changes the data distribution by designating the input space for the new space, where conditions are typically sequentially categorized. To read composite input fields, characters such as radial base function (RBF) might be utilized. The SVM training process identifies a hyperplane in the classification functions, which are given to a set of training circumstances and labelled with a matching category label. This hyper-plane can offer fresh entries into one of the two categories [19].

1.9.6 Bayesian Network (BN)

BN is a recorded model that depicts the conditional dependency of random variables. Where there is ambiguity, BNs can help uncover prospective possibilities provided by recognized opportunities [18]. Bayesian networks can be useful and successful in modeling situations where certain fundamental elements are known but incoming data is unclear or scarce. In addition, BNs have been used to detect CC fraud or telecommunications networks.

1.9.7 Fuzzy Logic (FL) System

Fuzzy logic (FL) is a system that operates according to undefined rules. Due to complex sets and numbers in many languages, Fuzzy systems manage ambiguities with regard to input and output variables.
FNN: The purpose of using FNN is to learn from the many uncertain and inaccurate data sets of information, most common in real-world applications.

1.9.8 Expert Systems
Regulations can be developed with information from an expert who uses rules such as IF-THEN in order to preserve them in a system. The expert system's rules were utilized to perform operations on the data in order to produce the decision. Professional software provides powerful answers and conditions for a wide range of application issues. One of the most popular applications is fraud detection. A dubious activity can be generated by straying from "normal" expenditure habits utilizing professional software [19].

1.9.9 Inductive logic programming (ILP)
ILP explains the idea of adverbs using the initial concept of the adverb in a series of positive and negative examples. This mental system is used to isolate new situations. The complex relationships between elements or attributes can be easily demonstrated, in this way of differentiating. System functionality is enhanced by domain information that can be easily identified in an ILP system [20].

1.9.10 Case-based reasoning (CBR)
A straightforward notion of CBR is developing answers to current issues and utilizing them to tackle new challenges. Cases in CBR are provided as examples of prior professional human experience and are saved in a file for subsequent use when a handler meets a new case with identical characteristics. These situations can be used for segregation. When confronted with a new situation, the CBR system attempts to locate a comparable example. When the model is given with a new case or example during the test stage, all of the data are searched for a number of cases [21].

2. LITERATURE SURVEY ON CC FRAUD DETECTION USING MACHINE LEARNING TECHNIQUES

These approaches are always employed in the context of fraud detection. The most used NN is the BPN. It reduces the target function by using the process variety of powers that are easy to make delta law. The back-sharing process tends to benefit the transmission network without feedback. To obtain the best action, the BPN algorithm includes temporal complexity, and parameters [22] [23].
Researcher Gusandra Saragih et al [24] used some of the monitored methods and algorithms to detect fraud results. Illegal or fraudulent activities have a detrimental effect on a business and on customers who rely on the organization. In this algorithm, forest segregation has used a subdivision to detect fraudulent actions and data sets are collected from technology testing organizations.
In addition, Aleskerovet al. [25] created a network mining system based on the NN of CC fraud detection. The proposed method (CARD WATCH) has three layers of automatic configuration. Informative results yield the most effective estimates of fraud detection.
Krenkeret al. elevated the model of real-time fraud perception in terms of bidirectional NN [26-28]. They made use of a big amount of mobile transaction data supplied by a credit card firm. In order to avoid the worst-case situation, the system had to go through legal procedures.
In addition, in [29], a comparable granular NN (GNN) is proposed to speed up the data mining and data collection processes for detecting CC fraud. GNN is a kind of FNN that is knowledge-based (FNNKD). The fundamental data is taken from a SQL database containing an example Visa Card transaction and then processed utilizing fraudulent detection. In the presence of a large training database, they discovered modest training mistakes.

2.1 Unsupervised learning techniques
Unsupervised tactics do not require prior acquaintance with fraud and general history. These methods increase the fear of those who are acting very differently from the norm. These approaches are frequently utilized in the study of user behavior. For a large enough transaction database, ANNs can produce good results. SOM provides a clustering process, suitable for creating and testing customer records, in detecting CC fraud, as proposed in [30]. SOM is divided into two phases: training and mapping. The map is built and the neurons are examined sequentially based on input samples in the first phase [31], and the test data is automatically classified into standard and deceptive phases by the mapping process in the second phase.
As stated in [32], after training SOM, the new activity's secret transaction is linked with common and fraudulent groups. If it is the same as normal records, it is considered normal. Fraudulent transactions are equally visible. One benefit that neural networks can be used in the same way as people is that they can learn via data transfer. The more information is inserted in the SOM model, the more the output is known and improved. SOM emphasizes its model in particular with the passage of time. This can result in banks and other financial institutions being used and updated online. Therefore, deceptive card use can be seen quickly and effectively. On the other hand, neural networks have some disadvantages and certain problems that are strongly associated with setting the proper structure on the one hand and the extra training needed to get good performance on the other [32].

2.2 Hybrid learning techniques
Kuldeep Randhawa et al [33] have used ML algorithms to detect CC fraud. After applying the standard models, Applied is hybrid AdaBoost techniques and majority voting systems. A publicly accessible CC data set is utilized to assess the model efficiency[34].

Branka Stojanovic et al [35] Examine current security problems in the digital realm of financial transactions and emphasis on anomalous (fraudulent) transactions when hostile activities for illegal financial gains are undertaken. Fraud is in several forms, which ultimately will have significant implications for the victims involved. Certain ML methods to identify fraud in financial transactions have previously been deployed successfully. Consequently, this paper has a double contribution. First, an examination of existing ML domain techniques and publicly available data sets is provided. Several techniques for the identification of fraudulent behavior are studied, which analyze and apply intelligent solutions. The second part is an assessment of anomaly detection ML techniques. Consequently, several algorithms including outlining techniques and ensemble methods have been built and ran to identify fraud in financial datasets with varying successes for this benchmarking experiment.

Yvan et al [36] have presented an automated feature engineering multiple-perspective HMM-based method to take into account a large sequential spectrum of information. In fact, they based on two distinct aspects the legitimate and fraudulent behaviours of sellers and cardholders: time and the quantity of the transactions. In addition, the HMM-based functionality is supervised and thus less expertise is required in creating a fraud detection system. Finally, their many views The HMM-based method enables automated function engineering in order to complement and supplement the usage of transaction aggregation strategies with a view to enhancing the efficiency of the classification task.

2.3 Others

Manoel Fernando Alonso Gadi et al [37] have presented a comparative study of five classification methods (Decision Tree, Neural Network, Bayesian Network, Naive Bayes, and Artificial Immune System). Aman Gulati et al [38] have This has been offered by means of a Behavioral and Locational analysis (Neural Logic), which takes into consideration cardholders' management of money and spending patterns, which enables the identification of fraudulent exchanges during processing. Massimiliano Zanin et al [39] have presented the First hybrid method for data mining/complex network classification, capable of detecting unlawful cases with a true card transaction data set.

3. CONCLUSION AND FUTURE SCOPE

This chapter presented a brief review of existing approaches to fraud detection. It includes ML based fraud detection techniques, optimization-based fraud detection techniques. The Machine learning on a banking website are gathered and evaluated using this approach. User deed covers all the actions that users reform on a banking site: where and where they are connected, how they roll a page, how they stagger, and where they don't leave the site at last, etc. The major characteristics of user behavior are: visited pages often, time spent on each page, clicking, and so on. The accessibility and the page usability from these details. The server log and navigation behavior of the web user are taken into consideration when determining page accessibility and the length of stay. The main challenge for today's CC fraud detection system is how to improve fraud detection accuracy with a growing number of transactions done by a user per second. Multiple Supervised and Semi-Supervised machine learning techniques are used for fraud detection. But CC dataset is highly imbalanced because there will be more legitimate transactions when compared with a fraudulent one. It is important to stress that feedbacks and delayed samples are different sets of supervised samples. While feedbacks provide recent, up-to-date information, delayed samples might be already obsolete for training a classifier.

REFERENCE

[1] Linda Delamaire UK), Hussein Abdou UK), John Pointon UK), "CC fraud and detection techniques: a review", Banks and Bank Systems, Volume 4, Issue 2, 2009.
[2] L. Mukhanov, "Using bayesian belief networks for CC fraud detection," in Proc. of the IASTED International conference on Artificial Intelligence and Applications, Insbruck, Austria, Feb. 2008, pp. 221– 225.
[3] 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.
[4] Seeja, K. R., &Zareapoor, M. (2014). FraudMiner: A novel CC fraud detection model based on frequent itemset mining. The Scientific World Journal, 2014.
[5] Sailusha, R., Gnaneswar, V., Ramesh, R., & Rao, G. R. (2020, May). CC Fraud Detection Using Machine Learning. In 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1264-1270). IEEE.
[6] Saragih, M. G., Chin, J., Setyawasih, R., Nguyen, P. T., & Shankar, K. Machine Learning Methods for Analysis Fraud CC Transaction.
[7] Zanin, M., Romance, M., Moral, S., &Criado, R. (2018). CC fraud detection through parenclitic network analysis. Complexity, 2018.
[8] Gulati, A., Dubey, P., MdFuzail, C., Norman, J., &Mangayarkarasi, R. (2017, November). CC fraud detection using neural network and geolocation. In IOP Conference Series: Materials Science and Engineering (Vol. 263, No. 4, p. 042039).
[9] Salvatore J. Stolfo, David W. Fan, Wenke Lee and Andreas L. Prodromidis; "CC Fraud Detection Using Meta-Learning: Issues and Initial Results"; Department of Computer ScienceColumbia University; 1997.
[10] Maes S. Tuyls K. Vanschoenwinkel B. and Manderick B.; "CC Fraud Detection Using Bayesian and Neural Networks"; Vrije University Brussel – Belgium; 2002.
[11] Yvan Lucas. CC fraud detection using machine learning with integration of contextual knowledge. Artificial Intelligence [cs.AI]. Université de Lyon; Universität Passau (Deutsche land), 2019.
[12] S. Ghosh and D. L. Reilly, "CC fraud detection with a neural-network", Proceedings of the 27th Annual Conference on System Science, Volume 3: Information Systems: DSS/ Knowledge Based Systems, pages 621-630, 1994. IEEE Computer Society Press.
[13] L. N. de Castro, J. Timmis," Artificial immune systems as a novel soft computing paradigm", Journal of Soft Computing, PP 526–544, 2003.
[14] Holland, J. H. "Adaptation in natural and artificial systems." Ann Arbor: The University of Michigan Press. (1975).
[15] James V. Hansena, Paul Benjamin Lowrya, Rayman D. Meservya, Daniel M. c Donald," Genetic programming for prevention of cyber terrorism through dynamic and evolving intrusion detection "Journal Decision Support Systems, Volume 43, Issue 4, August 2007, Pages 1362–1374.
[16] AbhinavSrivastava, AmlanKundu, ShamikSural, Arun K. Majumdar. "CC Fraud Detection using Hidden Markov Model", IEEE Transactions on dependable and secure computing, Volume 5; (2008) (37-48).
[17] Cortes, C. & Vapnik, V "Support vector networks, Machine Learning", (1995). Vol. 20; (273–297).
[18] Inigo Monedero, Felix Biscarri, Carlos Leon, Juan I. Guerrero, Jesus Biscarri, Rocio Millan, "Detection of frauds and other non-technical losses in a power utility using Pearson coefficient, Bayesian networks, and decision trees", Journal of Electrical Power and Energy Systems 34 (2012) pp 90–98.

[19] Kevin J. Leonard; "The development of a rule-based expert system model for fraud alert consumer credit"; European journal of operational research, vol. 80, p.p. 350-356; 1995.
[20] Adnan M. Al-Khatib, "Electronic Payment Fraud Detection Techniques", World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 4, 137-141, 2012.
[21] R. Wheeler, S. Aitken; "Multiple algorithms for fraud detection"; Knowledge-Based Systems 13; 2000; pp. 93-99.
[22] MasoumehZareapoor, Seeja. K.R, M.Afshar.Alam, "Analysis of CC Fraud Detection Techniques: based on Certain Design Criteria", International Journal of Computer Applications (0975 – 8887) Volume 52– No.3, 2012.
[23] Clear Commerce fraud prevention guide, Clear Commerce Corporation, 2002, http://www.clearcommerce.com.
[24] Megasari Gusandra Saragih, Jacky Chin, Rianti Setyawasih, Phong Thanh Nguyen, K. Shankar, "Machine Learning Methods for Analysis Fraud CC Transaction", International Journal of Engineering and Advanced Technology (IJEAT), Vol-8,No-5S,2019.
[25] E. Aleskerov, B. Freisleben, B. Rao, „CARDWATCH: A Neural Network-Based Database Mining System for CC Fraud Detection", the International Conference on Computational Intelligence for Financial Engineering, pp. 220-226, 1997.
[26] Moody and C. Darken, "Learning with localized receptive fields." In Proc. of the 1988 Connectionist Models Summer School, D.S. Touretzky, G.E. Hinton and T.J. Sejnowski, eds., Morgan Kaufmann Publishers, San Mateo, CA, 1989, pp. 133-143.
[27] S.J. Nowlan, "Max likelihood competition in RBP networks," Technical Report CRG-TR-90- 2, Dept. of Computer Science, University of Toronto, Canada, 1990.
[28] A. Krenker, M. Volk, U. Sedlar, J. Bester, A. Kosh, "Bidirectional Artificial Neural Networks for Mobile-Phone Fraud Detection," Journal of Artificial Neural Networks, Vol. 31, No. 1, pp. 92-98, 2009.
[29] Mubeena Syeda, Yan-Qing Zbang, and Yi Pan," Parallel granular neural networks for fast CC fraud detection", international conference on ecommerce application, 2002.
[30] Vladimir Zaslavsky and Anna Strizhak "CC fraud detection using self organizing maps". Information & Security. An International Journal, (2006). Vol.18; (48-63).
[31] Vesanto, J., &Alhoniemi, E. 2000). "Clustering of the self-organizing map".IEEE Transactions on Neural Networks, 2009). 11; 586–600).
[32] Serrano-Cinca, C "Self-organizing neural networks for financial diagnosis". Decision Support Systems, 1996). 17; 227–238).
[33] Masoumeh Zareapoor and Pourya Shamsolmoali, "Application of CC fraud detection: Based on Bagging Ensemble Classifier", Elsevier, Procedia Computer Science 48 (2015) 679 – 685, 2015.
[34] KULDEEP RANDHAWA,CHU KIONG LOO,MANJEEVAN SEERA,CHEE PENG LIM, and ASOKE K. NANDI, "CC Fraud Detection Using AdaBoost and Majority Voting", IEEE Access, 2018.
[35] Branka Stojanovic, Josip Bozic, Katharina Hofer-Schmitz, Kai Nahrgang, Andreas Weber, Atta Badii, Maheshkumar Sundaram, Elliot Jordan, and Joel Runevic, "Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications", Sensors, Vol-21, 2021.
[36] Yvan, François, Marcel LUCAS, "CC Fraud Detection using Machine Learning with Integration of Contextual Knowledge", Thesis, INSA, Universite De Lyon, 2019.
[37] Manoel Fernando Alonso Gadi, Xidi Wang and Alair Pereira do Lago, "CC Fraud Detection with Artificial Immune System", Springer,2008.
[38] Aman Gulati, Prakash Dubey, MdFuzailC, Jasmine Norman and Mangayarkarasi R, "CC fraud detection using neural network and geolocation", IOP Conf. Series: Materials Science and Engineering, 2017.
[39] Massimiliano Zanin, Miguel Romance, Santiago Moral and Regino Criado, "CC Fraud Detection through Parenclitic Network Analysis", Hindawi Complexity, Volume 2018.