A Survey Paper On Credit Card Fraud Detection Techniques

Article *in* International Journal of Scientific & Technology Research · October 2021

Aisha Fayyomi
Al Istiqlal University (Palestinian Academy for Security Sciences)
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Derar Eleyan
Palestine Technical University- Kadoorie
47 PUBLICATIONS **335** CITATIONS
SEE PROFILE

A Survey Paper On Credit Card Fraud Detection Techniques

Aisha Mohammad Fayyomi, Derar Eleyan, Amina Eleyan

Abstract: A credit card is the most widely used electronic payment method because of the increasing volume of daily electronic transactions, making it more vulnerable to fraud. Credit card companies have suffered heavy losses from card fraud. The detection of credit card fraud is currently the most common issue. . Credit card companies are looking for the right technologies and systems to detect and reducing fraud of transactions on the credit card. There are several methods for identifying credit card fraud that has been surveyed and highlighted in this paper and has been compared in terms of disadvantages and advantages for each one.

Index Terms: Detection Techniques, Machine Learning, Credit Card, Fraud Detection.

1 INTRODUCTION

At recent years, online payment methods have been used widely as an outcome of the rapid increase in non-cash electronic transactions. Credit cards represent one of the electronic payment methods A credit card is a thin rectangular piece of plastic or metal issued by a bank or financial services company to a consumer (cardholder) to facilitate payment to a merchant of goods and services. It is based on the consumer's promise to the card issuer. The card issuer (usually a bank) opens an account, which is usually circling, and contributes a line of credit to the user. Which the user can use to make a payment. With a card-based payments accounting for approximately 51% of transactions. [1], [2], [3]. Despite the advantages of electronic payment, credit ca3rd companies are experiencing an increase in card fraud with the advent of many new technologies. Scammers are smart enough to take advantage of loopholes and always try to steal data using new technologies like Skimming and phishing. There are occurrences when a website is designed to match a legitimate site and victims enter personal information such as passwords, user names, and credit card information The hustler send out a major number of emails (bait) that direct victims to their bogus websites. The e-mails seem to be from organizations such as PayPal banks, AOL, and eBay, and they ask the victim to log their personal information in order to resolve “issue." The fraudster can earning by stealing the victim's identities and then theft their money [4]. Credit card fraud caused a heavy financial loss from card fraud. “According to a 2017 US Payments Forum report, criminals have shifted their focus to activities involving CNP transactions as chip card security has improved” [5]. “The estimated financial loss of credit card fraud worldwide in 2018 rose to $24.26 million” [6]. “By 2019, the global fraud losses have accounted for US $ 27.billion, according to PR Newswire Association LLC”.[7] “Moreover, it is estimated that it will surpass roughly $30 billion by 2020” [8]. Activation procedures have all contributed to a reduction in the impact of fraud. Merchants are putting programs in place to help prevent credit card fraud. although, more precautions must be taken to prevent fraud [4]. Fraudulent transactions are efficiently detected with the help of Machine Learning algorithms that have a high processing or computing power and the ability to handle large datasets. which is a promising way to reduce credit card frauds [9], [10]. This paper includes seven sections. Section II summarizes brief previous studies. Section III the approaches by which the elementary studies were systematically chosen are offered. In section IV. Several popular credit card fraud detection techniques have been briefed. Section V. presented a comparison of various fraud detection techniques. Section IV. Summarizes results and discussion. Finally section VII. Presented conclusion and future scope.

1.1 Credit Card Fraud

Fraud according to the Association of Certified is defined as any wilful or deliberate act of depriving another of ownership or money through wiliness, deception, or other unfair means [11]. “The unauthorized procedure of CC or information deprived of owner's data is called add the full name and then the abbreviation CCF. The dissimilar CCF trick applications & behaviors are related to two groups of frauds. Specify the first group and the second group. When app fraud occurs, fraudsters apply for a new card from the bank or provide it to companies that use false or other information. A user can file multiple applications with a single usual of describes (named duplicate fraud), or a different user with similar describes (named identity fraud). Instead, there are practically four main types of behavioural fraud: stolen/lost cards, mail theft, fake cards, & ‘current cardholder does not exist’ fraud. When a stolen / lost card fraud occurs, fraudsters steal a credit card or get lost card. Mail theft fraud when a fraudster receives personal information from a bank in the mail before a credit card or original card holder. Fake & Card Holders Fraud & credit card descriptions are not presented. In past, remote communications can be done using card details via mail, phone or internet. Second,(where is first) fake cards are created on card data" explain more here [12].

- *Aisha Mohammad Fayyomi is Currently a graduate student at Technical University-Kadoorie, Tulkarem, Palestine*
  E-mail: aishafayyomi@gmail.com
- *Department of Applied Computing, Technical University-Kadoorie, Tulkarem, Palestine*
  E-mail: d.eleyan@ptuk.edu.ps
- *Department of Computing and Mathematics, Manchester Metropolitan University, Manchester M15 6BH, United Kingdom,*
  E-mail: a.eleyan@mmu.ac.uk

1.2 Credit Card Fraud Detection

Services make electronic payments more restful, seamless, adequate, and simple to use; however, we must not overlook the losses associated with electronic commerce. Organizations and banks to use them propose good security solutions. To address these issues, but fraudsters' subtle techniques evolve over time. As a result, it is critical to improving detection and prevention techniques [7]. It is critical to understand the mechanisms for carrying a fraud in order to combat the fraud effectively. The gadget for identifying credit score card fraud relies upon on the fraud manner itself [13]. To accomplish this, provide the transaction details to the verification module, which will classify them as either fraud or non-fraud. If it classified as fraudulent, it will be rejected. Otherwise, the transaction is accepted [14]. Fraud detection techniques such as statistical data analysis and artificial intelligence can be used to distinguish between the two. AI technique includes data mining that used to detect fraud, which can classify, group, and segment data to search through millions of transactions to find patterns and detect fraud. Machine learning is a technique for automatically detecting fraud characteristics. One method of dealing with fraud is through both prevention and detection. Fraud detection and prevention's primary goal is to tell the difference between legitimate and fraudulent transactions and to prevent fraudulent activity. Using historical data, the user's pattern and behavior are analysed to determine if a transaction is fraudulent or not. When the system fails to detect and prevent fraudulent activities, fraud detection takes over. [15]. In supervised fraud detection systems, new transactions are classified as fraudulent or genuine based on characteristics of deceptive and legitimate activities, whereas outliers' transactions are identified as prospective fraudulent transactions in unsupervised fraud detection systems. A point-by-point dialogue between supervised and unsupervised machine learning techniques can be discovered. Diversity of studies have been conducted on several methods to solve the issue of card fraud detection. These approaches include, ANN, K-means Clustering, DT, etc.[16].

1.3 Fraud types in Card-based transactions

1) Physical Card Fraud in most POS (point of sale) transactions, as it is essential that the cardholder must have to be physically presenting the card to the merchant to carry out the transaction. There are chances that the customer's card can be stolen and misused by fraudsters without the customer’s knowledge. 2)Virtual Card Fraud: In most Online shopping transactions there is no need for a physical card and instead we use the Card Number, Expiry Date, and CVV number to perform the transaction. Fraudsters can steal this information and they can use it to perform fraudulent online transactions” [17].

2. LITERATURE REVIEW

Prajal Save et al. [18] have proposed a model based on a decision tree and a combination of Luhn's and Hunt's algorithms. Luhn's algorithm is used to determine whether an incoming transaction is fraudulent or not. It validates credit card numbers via the input, which is the credit card number. Address Mismatch and Degree of Outlierness are used to assess the deviation of each incoming transaction from the cardholder's normal profile. In the final step, the general belief is strengthened or weakened using Bayes Theorem, followed by recombination of the calculated probability with the initial belief of fraud using an advanced combination heuristic. Vimala Devi. J et al. [19] To detect counterfeit transactions, three machine-learning algorithms were presented and implemented. There are many measures used to evaluate the performance of classifiers or predictors, such as the Vector Machine, Random Forest, and Decision Tree. These metrics are either prevalence-dependent or prevalence-independent. Furthermore, these techniques are used in credit card fraud detection mechanisms, and the results of these algorithms have been compared. Popat and Chaudhary [20] supervised algorithms were presented Deep learning, Logistic Regression, Nave Bayesian, Support Vector Machine (SVM), Neural Network, Artificial Immune System, K Nearest Neighbour, Data Mining, Decision Tree, Fuzzy logic based System, and Genetic Algorithm are some of the techniques used. Credit card fraud detection algorithms identify transactions that have a high probability of being fraudulent. We compared machine-learning algorithms to prediction, clustering, and outlier detection. Shiyang Xuan et al. [21] For training the behavioral characteristics of credit card transactions, the Random Forest classifier was used. The following types are used to train the normal and fraudulent behavior features Random forest-based on random trees and random forest based on CART. To assess the model's effectiveness, performance measures are computed. Dornadula and Geetha S. [5] Using the Sliding-Window method, the transactions were aggregated into respective groups, i. , some features from the window were extracted to find cardholder's behavioral patterns. Features such as the maximum amount, the minimum amount of a transaction, the average amount in the window, and even the time elapsed are available. Sangeeta Mittal et al. [22] To evaluate the underlying problems, some popular machine learning-algorithms in the supervised and unsupervised categories were selected. A range of supervised learning algorithms, from classical to modern, have been considered. These include tree-based algorithms, classical and deep neural networks, hybrid algorithms and Bayesian approaches. The effectiveness of machine-learning algorithms in detecting credit card fraud has been assessed. On various metrics, a number of popular algorithms in the supervised, ensemble, and unsupervised categories were evaluated. It is concluded that unsupervised algorithms handle dataset skewness better and thus perform well across all metrics absolutely and in comparison to other techniques. Deepa and Akila [17] For fraud detection, different algorithms like Anomaly Detection Algorithm, K-Nearest Neighbor, Random Forest, K-Means and Decision Tree were used. Based on a given scenario, presented several techniques and predicted the best algorithm to detect deceitful transactions. To predict the fraud result, the system used various rules and algorithms to generate the Fraud score for that certain transaction. Xiaohan Yu et al. [23] have proposed a deep network algorithm for fraud detection A deep neural network algorithm for detecting credit card fraud was described in the paper. It has described the neural network algorithm approach as well as deep neural network applications. The preprocessing methods and focal loss; for resolving data skew issues in the dataset. Siddhant. Bagga et al. [24] presented several techniques for determining whether a transaction is real or fraudulent Evaluated and compared the accomplishment of 9 techniques on data of credit card fraud, including logistic regression, KNN, RF, quadrant discriminative analysis, naive Bayes, multilayer perceptron, ada boost, ensemble learning, and pipelining, using different parameters and metrics. ADASYN method is used to balance the dataset. Accuracy, recall, F1 score, Balanced Classification Rate are used to assess classifier performance and Matthews's correlation coefficient. This is to determine which technique is the best to use to solve the issue based on various metrics. Carrasco and Urban [25] Deep neural networks have been used to test and measure their ability to detect false positives by processing alerts generated by a fraud detection system. Ten neural network architectures classified a set of alerts triggered by an FDS as either valid alerts, representing real fraud cases, or incorrect alerts, representing false positives. When capturing 91.79 percent of fraud cases, optimal configuration achieved an alert reduction rate of 35.16 percent, and a reduction rate of 41.47 percent when capturing 87.75 percent of fraud cases. Kibria and Sevkli [26] Using the grid search technique, create a deep learning model. The built model's performance is compared to the performance of two other traditional machine-learning algorithms: logistic regression (LR) and support vector machine (SVM). The developed model is applied to the credit card data set and the results are compared to logistic regression and support vector machine models. Borse, Suhas and Dhotre. [27] Machine learning's Naive Bayes classification was used to predict common or fraudulent transactions. The accuracy, recall, precision, F1 score, and AUC score of the Naive Bayes classifier are all calculated. Asha R B et al. [14] have proposed a deep learning-based method for detecting fraud in credit card transactions. Using machine-learning algorithms such as support vector machine, k-nearest neighbor, and artificial neural network to predict the occurrence of fraud. used.

3. RESEARCH METHODOLOGY

Systematic literature reviews, for example, are a type of methodology, which conducts a literature review on a specifi topic, could be used to detect fraud. A systematic review's primary goal in this context is to identify, evaluate, and Interpret the available studies in the literature that address the authors' research questions. A secondary goal is to identify research gaps and opportunities in the area of interest. In this paper, we attempted to walk through the activities proposed by Kitchenham: analysis preparation, execution, and reporting in iterations. [28].

3.1 Selection of rudimentary Studies

To highlight primary research for selection, keywords were passed to the search engine, then they were chosen to enhance the development of research that wishes to aid in answering the study questions. The only Boolean factors that could be used were AND and OR. (”machine-learning” OR “machine learning”) AND “fraud detection” were the search terms. IEEE Explore Digital Library was one of the platforms looked into.

- Google Scholar
- Elsevier- Science Direct
- Web site

According on the search platforms, the title, keywords, and abstract were all searched for. On March 28, 2021, we conducted the searches, and we went over all of the previous studies. The outcome of these searches refined using the criteria described in Section 3.2, resulting in a collection of results that could be run.

3.2 Inclusion and Exclusion Criteria

Modern technological fraud detection, Case studies, and comments on how to improve existing mechanisms by building a hybrid approach could all be considered for inclusion in this SLR. Papers must be read and write in the English language. Any Google Scholar findings are tested for submission, as if Google Scholar has the ability to re-turn lower-grade papers. This SLR will only accept the most recent version of a sample. Table 1 lists the most important inclusion and exclusion requirement.

Table 1
INDICATES IMPLICATION AND EXCLUSION CRITERIA FOR THE PRELIMINARY STUDY

Inclusion	Exclusion
Must contain information related to fraud detection and learning machine technologies.	Cantering on the social or lawful ramifications of fraud.
The paper must include empirical data on credit card fraud as well as the use of machine learning techniques for detection.	paper on detecting fraud on individuals and public sites
The paper must have been published in a journal or a conference.	written in a language other than English.

.

3.3 Selection Results

The primary keyword searches against the pick platforms yielded 68 studies. After duplicate studies were removed, this was reduced to 52. After the procedure of the survey through the implication/exception criteria, there were 45 papers left to read. The 45 papers have been read in their entirety, after applying the inclusion/exclusion criteria a second time, 37 papers remained. As a result, SLR will comprise 37 papers in total, as illustrated in the diagram below:

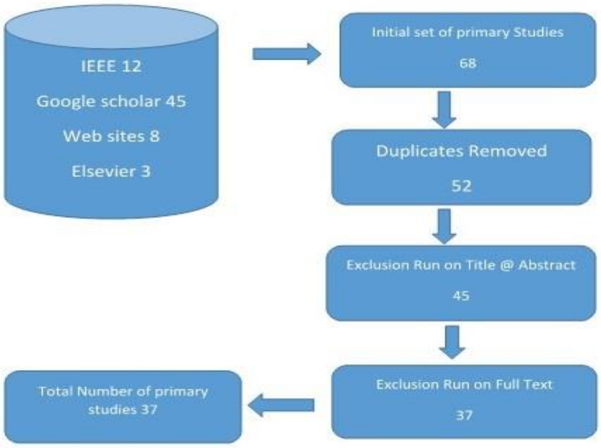
IEEE 12
Google scholar 45
Web sites 8
Elsevier 3
Initial set of primary Studies
68
Duplicates Removed
52
Exclusion Run on Title @ Abstract
45
Exclusion Run on Full Text
37
Total Number of primary studies 37

Fig. 1. Paper Attrition during Processing

4. CREDIT CARD FRAUD DETECTION TECHNIQUES

4.1 Decision trees

A supervised learning methodology, graphical representation of possible solutions to a choice based on certain situations [29] As in Figure 2 and it is a tree-structured classifier. It starts with a root node where inside nodes represent the features of a dataset, branches symbolize the decision rules and each leaf node represents the result. In a decision tree and they have the purposes of deciding and communicating respectively. A decision tree plainly asks a question and then divides it into sub trees based on the answer. Although DT can solve classification and regression problems, it is most commonly used to solve classification problems. To find the dataset class, the algorithm searches at the top of the tree. It compares the root Trait with the record attribute and follows the offshoot on way to the next node, which it calculates depending on the relation [30].

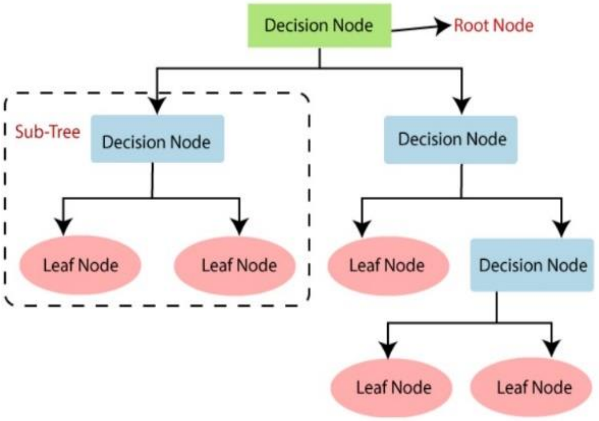

Fig. 2. General structure working of DT

Steps Working Of Decision Tree

In the first phase, start with S, which is the root node and includes the entire dataset. Second, discover the best Trait in the dataset using the Attribute Selection Measure. When the nodes cannot be categorized, in that time the final node is called a foliate node. Based on the labels, the root node is extra subdivided into the decision node and one leaf node. In the end, the node is divided into two leaves (accepted and declined offers).

4.2 Random Forest

Random Forest classifier finds decision trees in a subset of the data and then aggregates their information to that to get the full dataset's predictive power. Rather than relying on a single decision tree. The RF takes the predictions from each tree and forecasts the final output based on the majority votes of forecasts. Using a huge number of trees in the forest improves precision and eliminates the issue of over fitting. It predicts output with high precision, and it runs efficiently even with large datasets. It can also keep accuracy when a large proportion of data is lost. Random Forest can handle both classification and regression tasks. It can handle large datasets with high dimensionality. It improves the model's accuracy and avoids the over fitting problem. We use two-step training techniques in the process of tree-based Random Forest: First, we generate the random forest by mixing N trees together, and then we estimate for each of the trees we generate in the first phase [31]. An ensemble algorithm employs the "random forest" artificial intelligence technique. Because it averts over-fitting by averaging the results, this approach outperforms single decision trees. Random Forest is an ensemble of diverse trees, similar to Gradient Boosted Trees, but unlike GBT, RF tree grow in parallel. Random Forests have a lot of uncorrelated trees. Because various trees are trained in parallel, the overall model diminishes a large number of variances. Random Forest treats each tree as a separate classifier that has been trained on resampled data. As a result of employing this this learn strategy and divide, the model's overall learning ability is increased [10], [32].

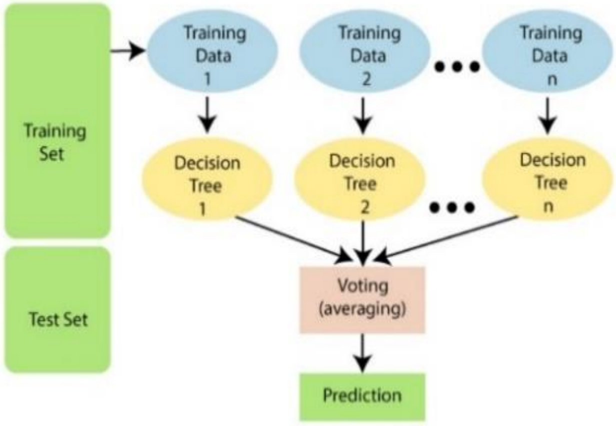

Fig. 3. General structure working of the RF

The Random Forest Working Steps

These steps illustrate Figure 3 above; in the first step, choose (K) as data points at random from the drill set. Second, construct the DT linked with the chosen data points (Subsets). Following that, select the digit (N) for the number of decision trees you wish to construct. Then, duplicate Steps 1 and 2. Finally, discover the predictions of each decision tree for new data points and assign the modern data points to the category that receives most votes. Clarify how RF works by using the following scenario: Assume you have a dataset with a variety of fruit images. As outcome, RF classifier will be given this dataset. Each decision tree is given a portion of the dataset to deal with. When a new data point occurs, the Random Forest classifier predicts the conclusion based on the majority of outcomes.

4.3 Logistic Regression

An algorithm that can be used for both regression and classification tasks, but it is most commonly used for classification.' 'Logistic Regression is used to predict categorical variables using dependent variables. Consider two classes, and a new data point is to be checked to see which class it belongs to. The algorithms then compute probability values ranging between (0) and (1). Logistic Regression employs a more complex cost function, this cost function is known as the Sigmoid Function or the Logistic Function.' [33]. LR also does not require independent variables to be linearly related, nor does it require equal variance within each group, making it a less stringent statistical analysis procedure. As a result, logistic regression was used to predict the likelihood of fraudulent credit cards [34]. Clarify the working of LR through the following scenario: The default variable for determining whether a tumor is malignant or not is y=1 (tumor= malignant); the x variable could be a measurement of the tumor, such as its size. The logistic function converts the x-values of the dataset's various instances into a range of 0 to 1. The tumor is classified as malignant if the probability exceeds 0.5. (As indicated by the horizontal line). As shown in the figure below:

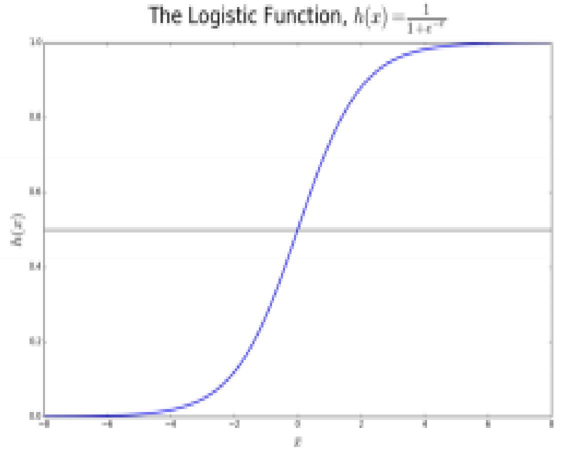

Fig. 4. Example of LR

4.4 Artificial Neural Networks

A sort of machine learning algorithm That uses a sophisticated interaction between outputs and inputs to uncover modern patterns. Also it a strategy for detecting fraudulent credit card activity. Because of their advanced predictive capabilities, ANNs can improve existing data analysis techniques. As shown in Figure 5 input Layers are the the first layer receives input information in the shape of different texts, audio files, image pixels, numbers, and so on. Hidden Layers are made up of units that transform the input into something that the output layer can use to perform various types of mathematical computations on the input data and recognize patterns. Layer of output: The result obtained by the middle layer's rigorous computations is obtained in the output layer [35], [2]. The weights w are multiplied by the inputs (x) obtained from the input layer. The Weighted Sum is formed by adding the multiplied values. After that, a related Activation Function is applied to the weighted sum of the inputs. The energizing assignment converts it into a corresponding output. If the network receives an input variable, the weight of that input is allocated at random. The importance of each input data point is indicated by its weight in terms of forecasting the result; the prejudice parameter, on the other hand, allows you to fine-tune the activation mission curve to achieve precise results. The produce of the input and the weight are calculated after the inputs have been given weight. We get the Weighted Sum by adding all of these products together. The summation function accomplishes this.

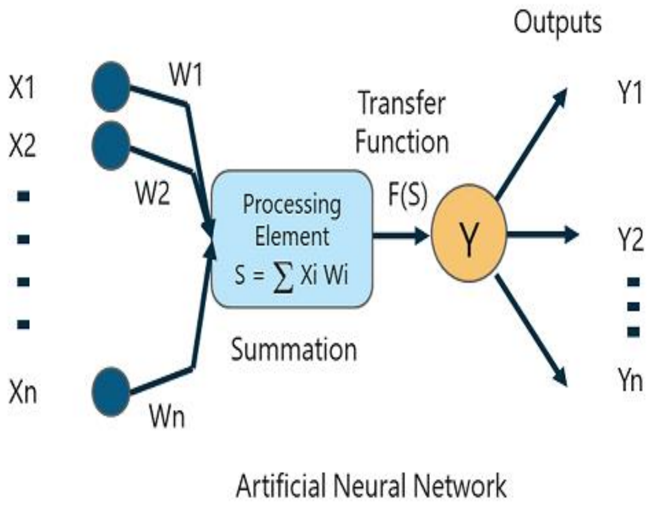

Fig. 5. General structure working of the ANN

Consider the following example to better understand how works: You're creating an Artificial Neural Network that categorizes photos into two groups to distinguish between infected and non-diseased crops: In Class A, you'll find photos of healthy leaves. In Class B, there are photos of sick leaves. Often, the process begins with the input being interpreted and transformed so that it can be facilely addressed. In this case, each paper picture is divided into pixels based on the size of the image. like, if the image's size is 30 * 30, the total number of pixels is 900. The total will be transformed into matrices and fed back into the system. An ANN's perceptrons receive entries and address them by moving them from the first layer to the secret layer and finally to the output layer, as Neurons in our brains help us create and connect thoughts. Each input is given an initial random weight as it passes from the input layer to the hidden layer. The inputs are then multiplied by their weights, and the sum is passed as data to the next hidden layer.Each perceptron is frequently activated or transformed, which determines whether or not it is active. A probability is calculated at the output layer to determine whether the data belongs to category A or category B.

4.5 K -Nearest Neighbors

A simple, easy-to-implement supervised machine-learning technique that uses categorized input data to develop a function that gives a suitable output when given additional unlabelled data. Both classification and regression problems can be solved with the k-nearest neighbors (KNN) algorithm, which is quick and straightforward to apply. Uses labeled data to teach a function that generates an acceptable performance for new data. In the K-Nearest Neighbor algorithm, the resemblance between the new case and the cases that are already categorized is calculated. Once the new case is placed in a category that is most comparable to the available ones, it is applied to all remaining cases in that group. In an analogous fashion, KNN organizes all accessible data and categorizes new points depending on how similar they are. This describes anytime new data emerges, it is just a matter of fitting a K-N classification scheme to it. The algorithm is very straightforward and uncomplicated to put into practice. If a model does not need to be built, so some parameters and expectations may be tuned, it is unnecessary. The algorithm gets significantly slower as predictors/independent variables increase [36]. As shown in the figure below:

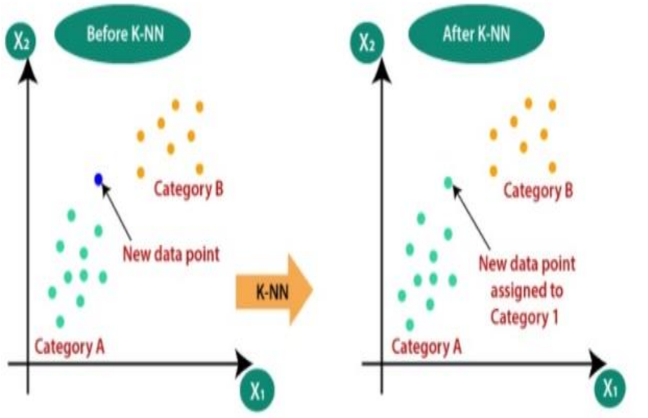

Fig. 6. General structure working of the K-NN

Decide on the number of neighbors in the first phase (K). Definethe Euclidean distance amidst K neighbors, then locate K closest neighbors using the measured Euclidean distance. Count the number of data points in every group between this KN in a subsequent phase, then assign the modern data points to the collection with the most neighbors. Finally, our paradigm is finished. Consider the following scenario: We have an image of two animals: a cat and a dog, and we want to identify which one the picture represents. As a result, the KNN can be utilized as a method for the definition because it is based on a likeness measure. Our KNN will look for similarities between the modern data set and the photos of animals, and classify it based on the most analogous attributes.

4.6 K-means Clustering

Because of its simplicity and effectiveness, it is the most widely used unsupervised learning methodology. By calculating the mean distance between data points, this method allocates points to groups. It then repeats this process in order to improve the accuracy of its categorizes over time [37]. The K-Means in the figure below are explained via the following steps: To determine the number of clusters, choose K. Then choose K locations or centroids at random. (It could be something different from the incoming dataset.) In the following step: Assign each data point to the centroid that is closest to it, forming the preset K clusters. Then calculate the variance and reposition each cluster's centroid. Repeat the third step, reassigning each point to the cluster's modern nearest centroid. Steps to finish: If there is a reassignment, go to step 4; otherwise, move to FINISH. The model is finished.

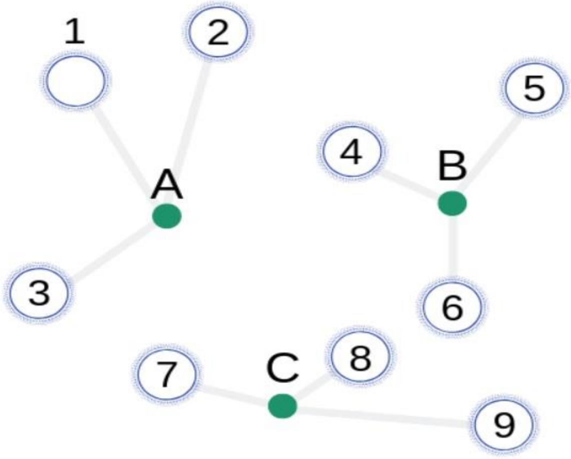

Fig. 7. General structure working of the K-MC

To explain how K-MC works. Consider the following situation: If a hospital wishes to establish Care Wards. K-means Clustering will divide these high-risk locations into clusters and establish a cluster centre for each cluster, which will be the location of the Emergency Units. These cluster centres are each cluster's centroids and are located at a minimum distance from all of the cluster's points; as a result, the Emergency Units will be located at a minimum distance from all accident-prone places within a cluster.

5. Comparison of various machine learning techniques

Table 1
COMPARISON ADVANTAGES AND DISADVANTAGES OF VARIOUS MACHIN-LEARNING TECHNIQUUES

Techniques	Strong Advantage	Weakness disadvantages
Decision Tree	It is simple to grasp and put into action. It can be extremely useful in resolving decision action problems. High adaptability, which aids in considering all potential solutions to a problem. There is minimal need for data cleaning.	This technique has many layers, making it difficulty. It may own an over fitting issue, which the RF algorithm mastery resolve. The DR Arithmetic intricacy may increase.
Random Forest	RF is capable of accomplishment both Classification and Regression tasks. It is able of handling large datasets with rise dimensionality. It promotes the thoroughness of the model and prevents over fitting problem.	Although RF can be applied for both classification and regression function, it is not more appropriate for Regression tasks.
Logistic Regression	Easier to implement, interpret, and very efficient to train. It makes no assumptions about distributions of classes in feature space.	The non-linear issue cannot be fixed with logistic regression because it has a linear decision surface.
Artificial Neural Networks	Storing information on the entire network. Ability to work with incomplete	The unexplained demeanor of the network.

Techniques	Strong Advantage	Weakness disadvantages
Decision Tree	It is simple to grasp and put into action. It can be extremely useful in resolving decision action problems. High adaptability, which aids in considering all potential solutions to a problem. There is minimal need for data cleaning.	This technique has many layers, making it difficulty. It may own an over fitting issue, which the RF algorithm mastery resolve. The DR Arithmetic intricacy may increase.
Random Forest	RF is capable of accomplishment both Classification and Regression tasks. It is able of handling large datasets with rise dimensionality. It promotes the thoroughness of the model and prevents over fitting problem.	Although RF can be applied for both classification and regression function, it is not more appropriate for Regression tasks.
	knowledge High accuracy. Having a distributed memory Ability to make machine learning. Parallel processing capability	Difficulty of showing the problem to the network. The duration of the network is unknown (High processing time for large neural networks
K -Nearest Neighbors	It is strong to the noisy coaching data. It is straightforward to implement. Speed of detection is good. If the training data is huge, it may be more efficient.	Always needs to define the value of K, which may be complex sometimes. The computation cost is high because of calculating the distance between the data points for all the training samples. Expensive
K-means Clustering	Efficient and Quick. Repeated technique. Works on categorized digital data.	Lots of recurrences. Have to select your possess k value. Must understand the case of your data well.

6. RESULTS AND DISCUSSION

We observe that while each technology has its advantages, there are disadvantages that affect its effectiveness and its ability to identify and detect fraudulent transactions. The unbalanced nature of the fraudulent activity (the percentage of fraud compared to the volume of transactions).

7. CONCLUSION AND FUTUREU SCOPE

Credit card fraud becomes a serious concern to the world. Fraud brings huge financial losses to the world. This urged Credit card companies have been invested money to create and develop techniques to reveal and reduce fraud. The prime goal of this study is to define algorithms that confer the appropriate, and can be adapted by credit card companies for identifying fraudulent transactions more accurately, in less time and cost. Different machine learning algorithms are compared, including Logistic Regression, Decision Trees, Random Forest, Artificial Neural Networks, Logistic Regression, K-Nearest Neighbors, and K-means clustering. Because not all scenarios are the same, a scenario-based algorithm can be used to determine which scenario is the best fit for that scenario. All of the fraud detection techniques discussed in this survey article have advantages and disadvantages. The researchers use different performance measures employed (techniques) and algorithms to predict and show transactions fraudulent. Studies are refreshed and encouraged to improve the fraud detection basis to determine the weight that is suitable with cost factors, the tested accuracy, and detection accuracy. Surveys of such kind will allow the researchers to build a hybrid approach most accurate for fraudulent credit card transaction detection.

ACKNOWLEDGMENT

The author wish to thank Palestine technical university-Kadoori (PTUK) for supporting this research work as part of PTUK research fund.

REFERENCES

[1] S. H. Projects and W. Lovo, “JMU Scholarly Commons Detecting credit card fraud : An analysis of fraud detection techniques,” 2020.

[2] S. G and J. R. R, “A Study on Credit Card Fraud Detection using Data Mining Techniques,” Int. J. Data Min. Tech. Appl., vol. 7, no. 1, pp. 21–24, 2018, doi: 10.20894/ijdmta.102.007.001.004.

[3] “Credit Card Definition.” https://www.investopedia.com/terms/c/creditcard.asp (accessed Apr. 03, 2021).

[4] K. J. Barker, J. D’Amato, and P. Sheridon, “Credit card fraud: awareness and prevention,” J. Financ. Crime, vol. 15, no. 4, pp. 398–410, 2008, doi: 10.1108/13590790810907236.

[5] V. N. Dornadula and S. Geetha, “Credit Card Fraud Detection using Machine Learning Algorithms,” Procedia Comput. Sci., vol. 165, pp. 631–641, 2019, doi: 10.1016/j.procs.2020.01.057.

[6] A. H. Alhazmi and N. Aljehane, “A Survey of Credit Card Fraud Detection Use Machine Learning,” 2020 Int. Conf. Comput. Inf. Technol. ICCIT 2020, pp. 10–15, 2020, doi: 10.1109/ICCIT-144147971.2020.9213809.

[7] B. Wickramanayake, D. K. Geeganage, C. Ouyang, and Y. Xu, “A survey of online card payment fraud detection using data mining-based methods,” arXiv, 2020.

[8] A. Agarwal, “Survey of Various Techniques used for Credit Card Fraud Detection,” Int. J. Res. Appl. Sci. Eng. Technol., vol. 8, no. 7, pp. 1642–1646, 2020, doi: 10.22214/ijraset.2020.30614.

[9] C. Reviews, “a Comparative Study : Credit Card Fraud,” vol. 7, no. 19, pp. 998–1011, 2020.

[10] R. Sailusha, V. Gnaneswar, R. Ramesh, and G. Ramakoteswara Rao, “Credit Card Fraud Detection Using Machine Learning,” Proc. Int. Conf. Intell. Comput. Control Syst. ICICCS 2020, no. Iciccs, pp. 1264–1270, 2020, doi: 10.1109/ICICCS48265.2020.9121114.

[11] I. Sadgali, N. Sael, and F. Benabbou, “Detection and prevention of credit card fraud: State of art,” MCCSIS 2018 - Multi Conf. Comput. Sci. Inf. Syst. Proc. Int. Conf. Big Data Anal. Data Min. Comput. Intell. 2018, Theory Pract. Mod. Comput. 2018 Connect. Sma, no. March 2019, pp. 129–136, 2018.

[12] R. Goyal and A. K. Manjhvar, “Review on Credit Card Fraud Detection using Data Mining Classification Techniques & Machine Learning Algorithms,” IJRAR-International J. Res. …, vol. 7, no. 1, pp. 972–975, 2020, [Online]. Available: http://www.ijrar.org/papers/IJRAR19K7539.pdf.

[13] M. Kanchana, V. Chadda, and H. Jain, “Credit card fraud detection,” Int. J. Adv. Sci. Technol., vol. 29, no. 6, pp. 2201–2215, 2020, doi: 10.17148/ijarcce.2016.5109.

[14] A. RB and S. K. KR, “Credit Card Fraud Detection Using Artificial Neural Network,” Glob. Transitions Proc., pp. 0–8, 2021, doi: 10.1016/j.gltp.2021.01.006.

[15] R. R. Popat and J. Chaudhary, “A Survey on Credit Card Fraud Detection Using Machine Learning,” Proc. 2nd Int. Conf. Trends Electron. Informatics, ICOEI 2018, vol. 25, no. 01, pp. 1120–1125, 2018, doi: 10.1109/ICOEI.2018.8553963.

[16] O. Adepoju, J. Wosowei, S. Lawte, and H. Jaiman, “Comparative Evaluation of Credit Card Fraud Detection Using Machine Learning Techniques,” 2019 Glob. Conf. Adv. Technol. GCAT 2019, pp. 1–6, 2019, doi: 10.1109/GCAT47503.2019.8978372.

[17] M. Deepa and D. Akila, “Survey Paper for Credit Card Fraud Detection Using Data Mining Techniques,” Int. J. Innov. Res. Appl. Sci. Eng., vol. 3, no. 6, p. 483, 2019, doi: 10.29027/ijirase.v3.i6.2019.483-489.

[18] P. Save, P. Tiwarekar, K. N., and N. Mahyavanshi, “A Novel Idea for Credit Card Fraud Detection using Decision Tree,” Int. J. Comput. Appl., vol. 161, no. 13, pp. 6–9, 2017, doi: 10.5120/ijca2017913413.

[19] J. Vimala Devi and K. S. Kavitha, “Fraud Detection in Credit Card Transactions by using Classification Algorithms,” Int. Conf. Curr. Trends Comput. Electr. Electron. Commun. CTCEEC 2017, pp. 125–131, 2018, doi: 10.1109/CTCEEC.2017.8455091.

[20] R. R. Popat and J. Chaudhary, “A Survey on Credit Card Fraud Detection Using Machine Learning,” Proc. 2nd Int. Conf. Trends Electron. Informatics, ICOEI 2018, no. Icoei, pp. 1120–1125, 2018, doi: 10.1109/ICOEI.2018.8553963.

[21] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, “Random forest for credit card fraud detection,” ICNSC 2018 - 15th IEEE Int. Conf. Networking, Sens. Control, pp. 1–6, 2018, doi: 10.1109/ICNSC.2018.8361343.

[22] S. Mittal and S. Tyagi, “Performance evaluation of machine learning algorithms for credit card fraud detection,” Proc. 9th Int. Conf. Cloud Comput. Data Sci. Eng. Conflu. 2019, pp. 320–324, 2019, doi: 10.1109/CONFLUENCE.2019.8776925.

[23] X. Yu, X. Li, Y. Dong, and R. Zheng, “A Deep Neural Network Algorithm for Detecting Credit Card Fraud,” Proc. - 2020 Int. Conf. Big Data, Artif. Intell. Internet Things Eng. ICBAIE 2020, pp. 181–183, 2020, doi: 10.1109/ICBAIE49996.2020.00045.

[24] S. Bagga, A. Goyal, N. Gupta, and A. Goyal, “Credit Card Fraud Detection using Pipeling and Ensemble Learning,” Procedia Comput. Sci., vol. 173, pp. 104–112, 2020, doi: 10.1016/j.procs.2020.06.014.

[25] R. San Miguel Carrasco and M.-A. Sicilia-Urban, “Evaluation of Deep Neural Networks for Reduction of Credit Card Fraud Alerts,” IEEE Access, vol. 8, pp. 186421–186432, 2020, doi: 10.1109/access.2020.3026222.

[26] G. Kibria and M. Sevkli, “Application of Deep Learning for Credit Card Approval : A Comparison with Application of Deep Learning for Credit Card Approval : A Comparison with Two Machine Learning Techniques,” no. January, pp. 0–5, 2021, doi: 10.18178/ijmlc.2021.11.4.1049.

[27] D. D. Borse, P. S. H. Patil, and S. Dhotre, “Credit Card Fraud Detection Using Naïve Bayes and C4,” vol. 10, no. 1, pp. 423–429, 2021.

[28] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, “A systematic literature review of blockchain cyber security,” Digit. Commun. Networks, vol. 6, no. 2, pp. 147–156, 2020, doi: 10.1016/j.dcan.2019.01.005.

[29] V. Patil and U. Kumar Lilhore, “A Survey on Different Data Mining & Machine Learning Methods for Credit Card Fraud Detection,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. © 2018 IJSRCSEIT, vol. 5, no. 10, pp. 320–325, 2018, doi: 10.13140/RG.2.2.22116.73608.

[30] “Machine Learning Decision Tree Classification Algorithm - Javatpoint.” https://www.javatpoint.com/machine-learning-decision-tree-classification-algorithm (accessed Apr. 03, 2021).

[31] “Machine Learning Random Forest Algorithm - Javatpoint.” https://www.javatpoint.com/machine-learning-random-forest-algorithm (accessed Apr. 03, 2021).

[32] A. Mishra and C. Ghorpade, “Credit Card Fraud Detection on the Skewed Data Using Various Classification and Ensemble Techniques,” 2018 IEEE Int. Students’ Conf. Electr. Electron. Comput. Sci. SCEECS 2018, pp. 1–5, 2018, doi: 10.1109/SCEECS.2018.8546939.

[33] “Introduction to Logistic Regression | by Ayush Pant | Towards Data Science.” https://towardsdatascience.com/introduction-to-logistic-regression-66248243c148 (accessed Apr. 03, 2021).

[34] S. Venkata Suryanarayana, G. N. Balaji, and G. Venkateswara Rao, “Machine learning approaches for credit card fraud detection,” Int. J. Eng. Technol., vol. 7, no. 2, pp. 917–920, 2018, doi: 10.14419/ijet.v7i2.9356.

[35] “Artificial Neural Networks for Machine Learning - Every aspect you need to know about - DataFlair.” https://data-flair.training/blogs/artificial-neural-networks-for-machine-learning (accessed Apr. 03, 2021).

[36] “K-Nearest Neighbor(KNN) Algorithm for Machine Learning - Javatpoint.” https://www.javatpoint.com/k-nearest-neighbor-algorithm-for-machine-learning (accessed Apr. 03, 2021).

[37] “K-Means Clustering Algorithm for Machine Learning | by Madison Schott | Capital One Tech | Medium.” https://medium.com/capital-one-tech/k-means-clustering-algorithm-for-machine-learning-d1d7dc5de882 (accessed Apr. 03, 2021).