Credit Card Fraud Detection

Ravi pandey

1. INTRODUCTION

Nowdays, online payment methods have been used widely as 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 shape piece of plastic or metal issued by a bank or financial services company to a customer (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 users. Which the users can use to make a payments. With a card-based payments accounting for approximately 51% of transactions. [1], [2], [3]. Despite the advantages of electronic payments, credit card companies are experiences an increase in card fraud with the advent of many new technologies. Scammers are smart enough to takes advantage of loopholes and always try to steal data using new technologies like Skimming and phishing. There are occurrence when a website is designed to match a legitimate sites and victims enter personal information such as password, user name, and credit card informations The hustler send out a major number of emails 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 victims 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 reports, 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 credit card fraud worldwide in 2018 rose to $24.26 million‖[6] 2018 rose to $24.26 million‖ [6]. ―By 2019, the global frauds 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 frauds [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 cards frauds [9], [10]. This paper includes seven sections. Section II summarizes brief previous studies. Sections III the approaches by which the elementary studies were systematically chosen are offered. In sections IV. Several popular credit cards 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 acts of depriving another of ownerships 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 frauds occurs, fraudsters apply for a new card from the bank or provide it to companies that use false or other information. A customer can file multiple applications with a single usual of describes (named duplicate fraud), or a different customers with similar describes (named identity fraud). Instead, there are practically four main types of behavioural frauds: stolen/lost cards, mail thefts, fake cards, & ‗current cardholder does not exist' frauds. When a stolen / lost card fraud occurs, fraudsters steal a credit cards or get lost card. Mail theft frauds when a fraudster receives personal information from a bank in the mail before a credit card or original card holder. Fake & Card Holders Frauds & credit cards 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 cards data" explain more here [12].

1.2 Credit Card Fraud Detection

Service make electronic payments more easy, seamless, adequate, and simple to use; however, we must not overlooks the losse associated with electronic commerce. Organizations and banks to use them propose good security solutions. To address these issues, but fraudsters' subtle techniques evolves over time. As a result, it is critical to improving detections and preventions techniques [7]. It is critical to understand the mechanisms for carrying a frauds 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, provides the transactions details to the verification module, which will classify them as either fraud or non-fraud. If it classified as fraudulents, it will be rejected. Otherwise, the transaction is accepted [14]. Fraud detections techniques such as statistical data analysis and artificial intelligence can be used to distinguish between the two. AI techniques includes data mining that used to detects frauds, which can classify, group, and segment data to search through millions of transactions to find patterns and detect frauds. (Ml)Machine learning is a technique for automatically detecting fraud characteristics. One method of dealing with frauds is through both prevention and detections. Fraud detection and prevention's primary goal is to tell the difference between legitimate and fraudulent transactions and to prevents fraudulent activity. Using historical data, the user's pattern and behaviores are analysed to determine if a transaction is fraudulent or not. When the systems fails to detects and prevents 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 research have been conducted on severals methods to solve the problems of credit cards fraud detection. These approaches include, ANN, K-means Clustering, DT, etc.[16].

1.3 Frauds type in Card-based transactions

1) Physical Cards Fraud in most POS (point of sale) transactions, as it is essentials that the customer's must have to be physically presenting the cards to the merchants to carry out the transactions. There are chances that the cardholders cards can be stolen and misused by fraudsters without the cardholders 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 transactions. Fraudsters can steal this details 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 combinations of Luhn's and Hunt's algorithms. Luhn's algorithm is used to determine whether an incoming transactions is fraudulent or not. It validates credit card numbers via the input, which is the credit cards number. Address Mismatch and Degrees of Outlierness are used to assess the deviation of each incoming transactions from the customer’s normal profile. In the final step, the general belief is strengthened or weakened using Bayes Theorems, followed by recombinations of the calculated probability with the initial belief of frauds using an advanced combination heuristic. Vimala Devi. J et al. [19] To detect counterfeit transactions, three (ML)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 detections 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 cards fraud detections algorithms identify transactions that have a high probability of being fraudulents. We compared (ml)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, performances measures are computed. Dornadula and Geetha S. [5] Using the Sliding-Window method, the transactions were aggregated into respectives groups , some feature from the window were extracted to find customer’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 latest, have been considered. These include tree-based algorithms, classical and deep neural networks, hybrid algorithms and Bayesian approaches. The effectiveness of (ml)machine-learning algorithms in detecting credit card fraud has been assessed. On various metrics, a numbers of popular algorithms in the supervised, ensemble, and unsupervised categories were evaluated. It is concluded that unsupervised algorithms handle datasets skewness better and thus perform well across all metrics absolutely and in comparison to other techniques. Deepa and Akila [17] For frauds 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 severals techniques and predicted the best algorithms to detect deceitful transactions. To predict the fraud results, the systems used various instructions and algorithms to generate the Frauds score for that certain transactions. Xiaohan Yu et al. [23] have proposed a deep network algorithms for fraud detections A deep neural network algorithms for detecting credit cards frauds was described in the papers. It has described the neural network algorithms approach as well as deep neural network applications. The preprocessing methods and focal loss; for resolving data skew problems in the datasets. Siddhant. Bagga et al. [24] presented several techniques for determining whether a transactions is real or fraudulent Evaluated and compared the accomplishments of 9 techniques on data of credit cards fraud, including logistic regression, KNN, RF, quadrant discriminative

3. RESEARCH METHODOLOGY

Systematic literature review, for example, are a type of methodology, which conducts a literature reviews on a specific topic, could be used to detect frauds. A systematic reviews primary goal in this context is to identify, evaluate, and Interprets the available studies in the literature that address the Author's research questions. A secondary goal is to identify research gaps and opportunities in the area of interest. In this papers, 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 highlights primary research for selection, keywords were passed to the search engine, then they were chosen to enhance the developments of research that wishes to aid in answering the study question. The only Boolean factors that could be used were AND and OR. (‖machine-learning‖ OR

Artificial intelligenc) AND —fraud detection‖ were the search terms. IEEE Explore Digitals Library was one of the platforms looked into.

- Google Scholar
- Elsevier- Science Direct

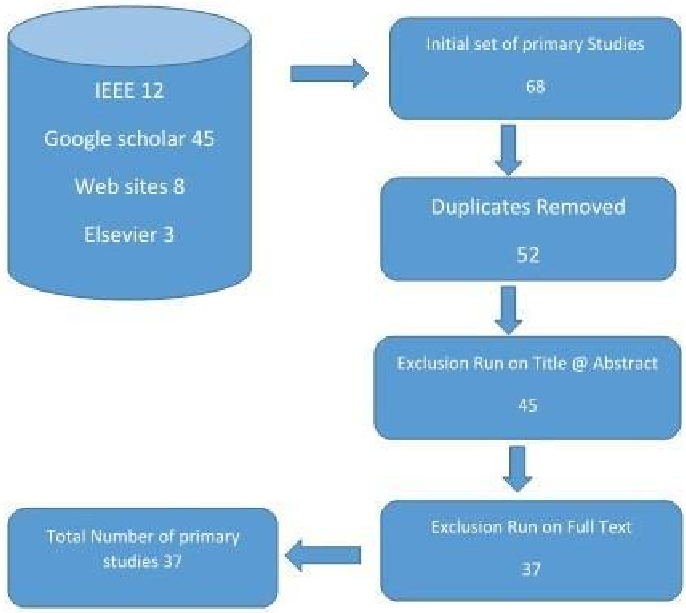
According on the search platforms, the title, keywords, and abstract were all searched for. On March 28, 2021, we conducted the searches, and we went over all of the previous studies. The outcome of these searches refined using the criteria described in Section 3.2, resulting in a collections of result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

3.2 Inclusion and Exclusion Criteria

Modern technological fraud detections, Case studies,research and comments on how to improves existing mechanisms by creating a hybrids approach could all be considered for inclusion in this SLR. Papers must be reads and writes 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 samples.

3.3 Selection Result

The primary keyword searches against the pick platforms yielded 68 studies. After duplicate studie were removed, this was reduced to 52. After the procedures 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 diagrams below:-

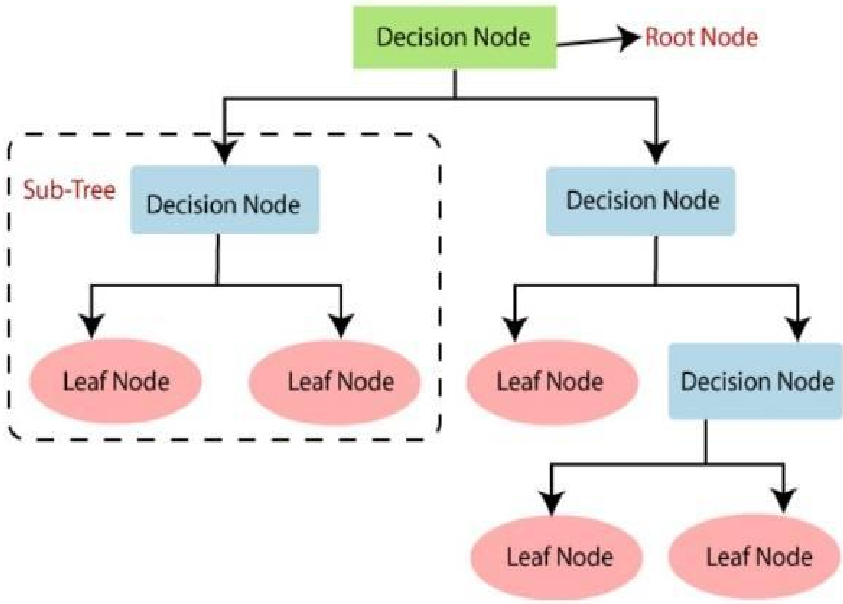


Paper Attrition during Processing

4. CREDIT CARD FRAUD DETECTION TECHNIQUES

4.1 Decision tree

A supervised learning methodology, graphical representations of possible solutions to a choice based on certain situations [29] As in Figure and it is a tree-structured classifier. It starts with a roots node where inside nodes represent the features of a datasets, branches symbolize the decision instructions and each leaf node represents the results. In a decision tree and they have the purposes of deciding and communicating respectively. A decision tree plainly asks a questions and then divide it into sub trees based on the answers. Although DT can solve classification and regression problems, it is most commonly used to solve classification problems. To find the datasets classes, the algorithm searches at the top of the tree. It compares the root Trait with the record attribute and follow the offshoot on way to the next node, which it calculate depending on the relations [30].



General structure working of DT

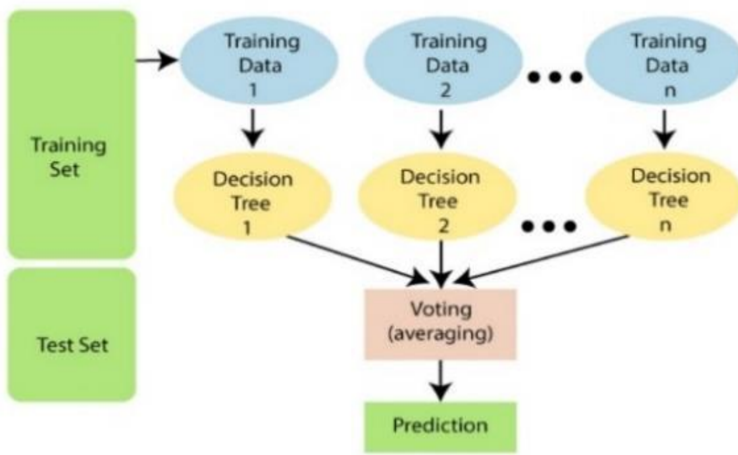
Step Working Of Decision Tree

In the first phase, starts with S, which is the root node and includes the entire datasets. Second, discovers the best Trait in the datasets 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 decisions node and one leaf node. In the end, the node is divided into two leaves .

4.2 Random Forest

Random Forest classifiers finds decision trees in a subsets of the data and then aggregates their details to that to get the full datasets predictive powers. Rather than relying on a single decision tree. The RF takes the predictions from each tree and forecasts the final outputs 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 precisions, and it runs efficiently even with large datasets. It can also keep accuracy when a large proportions of data is lost. Random Forest can handle both classification and regression task. It can handle large datasets with high dimensionality. It improves the models accuracy and avoids the over fitting problems. We use two-step training techniques in the process of tree-based Random

Forest: First, we generate the random forest by mixing N tree togethers, and then we estimate for each of the trees we generate in the first phase [31]. An ensemble algorithms employs the "random forest" artificial intelligence techniques. Because it averts over-fitting by averaging the results, this approach outperforms single decision tree. Random Forest is an ensemble of diverse tree, similar to Gradient Boosted Tree, but unlike GBT, RF tree grow in parallel. Random Forest have a lot of uncorrelated trees. Because various trees are trained in parallel, the overall model diminishes a large numbers of variances. Random Forest treat each trees as a separate classifiers that has been trained on resampled data. As a results of employing this this learn strategy and divide, the models overall learning ability are increased [10], [32].



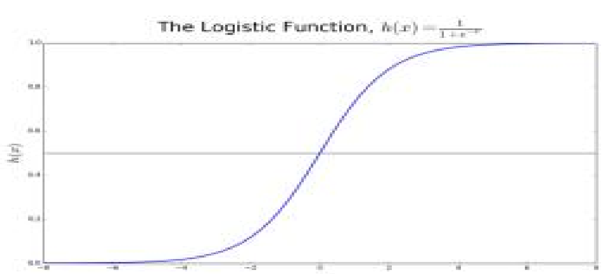
General structure working of the RF

The Random Forest Working Step

These step illustrate Figure above; in the first step, choose (K) as data points at random from the drill sets. 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 trees 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 datasets with a variety of fruites images. As outcome, RF classifiers will be given this datasets. Each decision tree is given a portion of the datasets to deal with. When a new data point occur’s, the Random Forest classifier predicts the conclusion based on the majority of outcome’s

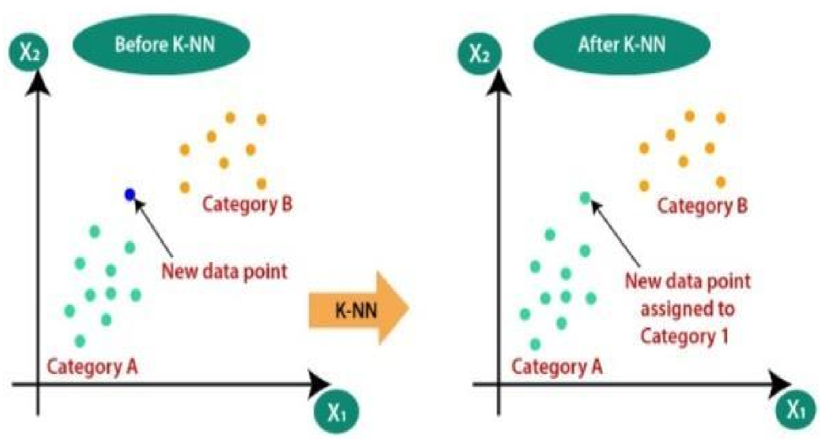
4.3 Logistic Regression

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 predicts 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 functions, this cost functions 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 variances within each groups, making it a less stringent statistical analysis procedure. As a results, logistic regression was used to predicts 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 malignants or not is y=1 (tumor= malignant), the x variable could be a measurement of the tumors, such as its size. The logistic function converts the x-values of the dataset's various instance's 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:



4.4 K -Nearest Neighbor

A simple, easy-to-implements supervised machine-learning technique that uses categorized input data to develop a function that gives a suitable output when given additional unlabelled data. Both classifications and regression problem's can be solved with the k-nearest neighbors (KNN) algorithms, which is quick and straight forward to apply. Uses labeled data to teach a functions that generates an acceptable performances for new data. In the K-Nearest Neighbor algorithms, the resemblance between the new cases 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 accessibles 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 algorithms get's significantly slower as predictors/independent variables increase [36]. As shown in the figure below:

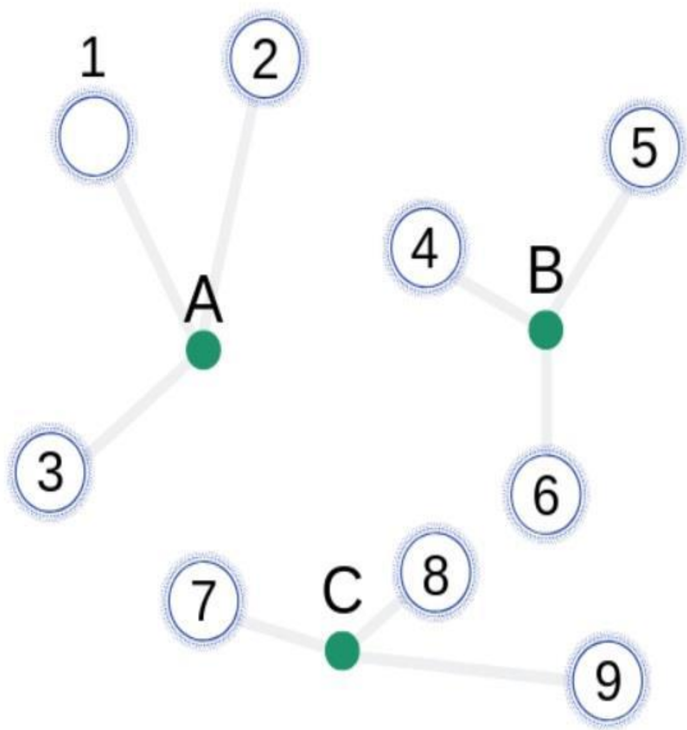


General structure working of the K-NN

Decide on the numbers 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 numbers of data points in every group between this KN in a subsequent phases, 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 methods for the definition because it is based on a likeness measures. Our KNN will look for similarities between the latests data set and the photos of animals, and classify it based on the most analogou's attributes.

4.5 K-means Clustering

Because of its simplicity and effectiveness, it is the most widely used unsupervised learning methodology. By calculating the mean distances 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 datasets.) In the following step: Assign each data point to the centroid that is closests to it, forming the preset K clusters. Then calculates the variance and reposition each cluster's centroid. Repeat the third step, reassigning each points 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.



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 establishs 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 results, the Emergency Units will be located at a minimum distance from all accident-prone places within a cluster.

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).