IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, May 2022
Impact Factor: 6.252

Analysis of Credit Card Fraud Detection Using Machine Learning Algorithms

D. Harish Kumar[1] and S. Arumugam[2]
Student, Department of Computer Science and Applications[1]
Assistant Professor, Department of Computer Science and Applications[2]
Periyar Maniammai Institute of Science and Technology, Thanjavur, India

Abstract: *For the past decade of year's credit card holders are facing a problem that the card had been swiped and cash has been withdrawn in an ATM (Automatic Teller Machine) or it has been swiped in a shopping mall by purchasing a product as creating a fake credit card. These transactions are considered as illegal activity, it is also one of the cybercrime theft activities. Credit card fraud detection has been increasing highly in the world. Fake credit cards can be tackled by applying data science along various machine learning algorithms. This research work focus on analysis of various credit card fraud transaction using machine learning algorithms. Also, this research focuses on detecting the fake credit cards by approaching Artificial Intelligence (AI), Data mining and Big data analytics etc. by using machine learning algorithms. Machine learning algorithms are applied by training the dataset which are collected from the fake credit dataset and original credit card dataset. Computer operations are handled by the data as data's are ruling the world. Predicted card details are stored on the server of the banker. From the server information has been passed to the cybercrime in order to catch the culprit. Different kinds of machine learning algorithms that has been used for credit card fraud detection has been studied on which it gives the more precision.*

Keywords: Credit card fraud detection, identifying illegal transaction, detecting fake credit cards by approaching Artificial Intelligence (AI), Data mining, Big data analytics etc..., and comparison of accuracy level.

I. INTRODUCTION

In this 21st century digital transactions has reached a larger wide around the world. Credit card transactions such as cash can be withdrawn at anywhere in a card swiper machine or in an Automatic Teller Machine (ATM). Withdrawing cash by using a credit card can be easily done by inserting the card in Automatic Teller Machine (ATM) or in a card swiper. Credit card can be classified into two categories. They are physical card and virtual card. Physical cards allows user to purchase articles either in the store or in an online shopping by entering the personal PIN (Personal Identification Number) code. Virtual cards are those whom needed to purchase on a limitations of spending amount for a certain period of time provided by the admin [5]. These credit card transactions had opened as a gateway for ease of business. Credit card fraud transactions can be termed as thefting the cash of someone by using electronic gadgets which are programmed for their desire needs. Withdrawing cash using fake credit card is the recent problem occurring in the world [1]. Statistical properties can be varied in due course of time. To make a secure transaction machine learning algorithms are used in which it checks for the optimized datasets which are trained by confirming it is a fraudulent transaction or genuine transaction. Numerous ways to occur a credit card fraud. By stealing a card or a card lost by someone can helps to give a way for the fraudsters as cloning the cards from their original site or altering the magnetic strips which are presented on the card such as user information and card pinhole number. From the merchant side these stolen credit cards user information are obtained either skimming or phishing. Increasing the advancement of technologies effective models are developed for preventing the credit card fraud activities. Challenging situation is finding the total number of fraud transactions is quite low while comparing to the clear transactions [2]. Data's are increasing in a higher demand rate as much as large as to Peta Bytes (PB) it is also a major fault on transactions for pertaining in which it satisfies on performing on an analytical server, so that building a model for server is also important to enhance machine learning algorithms. This research paper focus on various types of credit card fraudulent transactions and how to safeguard the cash by using

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, May 2022
Impact Factor: 6.252

machine learning algorithms so, that the fraudulent transactions is easily detected as soon as possible for the purpose of saving the cash.

II. MOTIVATION

Machine learning is an emerging technology as it is a subset of AI. Using machine learning researchers have proposed various methods and introduced many innovative things which will be help full for mankind in various domains. Fraud detection is a wide research area however, in that fraud detection I had particular focussed on credit card fraud detection in which transaction can be made via online and offline. Identifying the fraudsters and saving the cash is a challenging task. Using machine learning algorithms various researchers have analyzed and produced various methods by the way of different machine learning algorithms. This research paper will be able to learn for researchers who are working on credit card fraud detection. As, in this paper shows types of credit card fraud and various algorithms shown by the researcher is discussed.

III. LITERATURE REVIEW

Yashvi Jain et al. has made an analysis by comparing of various credit card fraud transaction by either the possibilities of chances to occur and also stated that various techniques such as using machine learning and deep algorithms such as artificial neural network, decision tree, fuzzy logic, support vector machines, bayesian network, K-nearest neighbour, hidden markov model and logistic regression [2]. N. Malini et al. proposed and build a new model by using classification logistic regression algorithm for classifying the data and the data prediction is carried through the streams Map R and Map R-FS in which supports the Hadoop Distributed File System (HDFS) for storing the credit and profile details. C. Sudha et al. had made discriminative and multivariant analysis to offering truth making information by designing user interface and uploading the data [8]. A. Singh et al. had identified various credit card frauds and concluded that most of the transaction frauds are held by card not present and skimming techniques by the fraudster and the research work also compared the accuracy of every method with the existing proposed work by giving a higher accuracy rate [9]. Andrea Dal Pozollo et al. addressed a major challenging occurring of the credit card for real world FDS (Fraud Detection System) by considering two vast datasets for real-world in order for getting precise alerts. Also, solution is provided for lowering the instance of feedbacks. Framework is designed reproducing the working instances by collecting and analyzing the feedback [15, 21]. M. Deepa et al. discussed with various credit card fraud techniques on data mining by detecting the type of anomalies as the name specifying the anomalies behaviour for an abnormal suspicious. Harshat bargat et al. proposed on detecting the credit card fraud by applying various machine learning algorithms [30]. Vaka Sravani et al. proposed and concluded that decision tree and neural network provides a high accuracy. It also base on feature engineering extraction analyzing from the existing information [11]. S.P. Maniraj et al. highly analyzed and focused on local outlier factor and isolation forest algorithm by detecting the anomalies activities on fraud transactions [1]. Alejandro Correo Bahensen et al. implemented on an intersecting example of cost effective dependent for over-sampling the data tends to a large data storage space in server. Traditional statistics cannot be explained on misclassification rate on credit card creating companies for producing new credit cards [12, 22]. Andrea Dol Pozollo et al. given a practioner's learning methodology in a perspective manner such as unbalancing, nonstationary and assessment by creating a strategy that can be used for a constant getting rate in a fixed window for the recent observations for retaining the model. So, that it can take of already in the existing techniques filled out in the dataset [24]. Sanjana Jagdish et al. insists on frauds can be categorized as behavioural frauds and application frauds. By, categorizing them supervised learning is more efficient in which boundaries of inputs can be classified as decision surface. Modified Fisher Discriminant Analysis (MFDA) algorithm gives an high accuracy result by performing the analysis based on supervised learning [3]. Y. Sahin et al. mentioned the credit card fraud types and used the classification algorithms such as decision trees and support vector machines. As, classification algorithms is used accuracy is more important for every individual process for extracting the future result [28]. Harshat Jayant Jagtup builded a scalable fraud detection system with an solution of high performance for predicting the fault tolerance [13]. Dipti D. Patel efficient scalable multilevel classifier algorithm is developed to scalable the large credit card dataset, fraud detecting rules are shared within the interconnecting banks to overcome the threat. Main feature of efficient scalable multilevel is scalability as it is one of the features as database are spread around the world whereas decision for classifying the data is low [29]. Tammay Kumar Behra et al. proposed an hybrid approach

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, May 2022
Impact Factor: 6.252

by clustering using fuzzy methods and evaluated using neural network. As soon as, the transaction is founded is suspicious the neural network mechanisms are applied for detecting whether it is fraudulent activity or occasionally deviated by a genuine user [17]. K.R. Seeja experimental works on handling imbalance class independent and performance evaluated with an anonymous dataset may changes over a long period of time for gradual behavioural appearance [23]. Joseph Pun et al. research insisted by using meta learning strategy so that meta-classifier probability is obtained by generating the neural networks [26]. M. Sathyapriya et al. proposed by big data analytics in forensic integrating various context such as processing speed, fault tolerance, latency and performance [7]. Khyati Chaudary et al. Obtaining a high fraud coverage with low or high false alarm rate by a hybrid approach. Supervised methods or unsupervised methods for fraud detection methods neural networks specifies the user to create number of hidden layer so that the hidden layer tries to create a multiple nodes associated within the hidden layer. Building a precise and simple handled credit card monitoring system is a major challenging task for the merchant and organization to improve the merchant risk management level based on automatic as well as in a scientific way [27]. Suresh K Shirgave et al. reviewed machine learning algorithms based on the accuracy for detecting the fraud methods by using Random forest algorithm as classifying the trained model from the feedback system [10]. Sanaz name et al. proposed work is made up of a cost semsitive payment by storing the original profile creditcardholders by comparing with the primary data extracted from the original transaction. Then, the fake transaction is to be identified by using KNN and dynamic random forest algorithm [14]. Anika Nahar et al. found's anti – fraud strategy are to be followed by finding the probability of the credit transaction so that it helps to maximize the genuine transaction [16]. Ayahiko Niimi concluded that in the imbalanced distribution data stream is to be satisfied on the statistical criterion by verifying the imbalanced data with the effectiveness of verified decision tree algorithm [25].

IV. Related Works

Detecting the anomalous activities is known as outliers by using latest machine learning algorithms and datasets can be obtained from the Kaggle (Kaggle is a data analysis website created by a team for providing the datasets) [1]. Decision tree algorithm can be used to make decisions by organizing in a tree like structure in which name of the attributes represent to the connecting nodes and values of the attributes representing to the edges of branches. Training the data model to work K – nearest neighbours can be used in a predetermined data [4]. Sapna gupta et al. research works for a hybrid approach based prediction pre-processing the data is more important as anonymous transactions are to be removed and in the ending stage process using support vector machine (SVM) classification is applied to categorize the datasets. It is also can be easily determined that comparing the K-nearest neighbour with SVM, SVM produced a higher accuracy [20]. Performance evaluation can be increased by using meta classifier system [26]. To gather the original data from the massive data as structured or unstructured data hinges on influencing the selection and performing on forensic techniques [7]. Class imbalance handling legitmate transactions for particular fraudelnt's by alerting analyzed from the feedback. Two main factors evolved suckle transactions mode for genuine purpose and frauds varying on time to time by dominating the aggregated amount of delayed supervised samplings [15, 21]. Advanced encryption standard algorithm is used to execute the operation works on bytes instead of bits. AES algorithm creates and advanced encryption structure tending for designing the user interface and uploading the data. Generating the key and to add in the spherical body takes a large amount of time [8]. Random forest algorithm yields a better result for detecting the fraud when it is compared to the classifier [30]. Comparison is to be made for existing techniques based on the performance of sensitivity, specificity and accuracy as the performance depends on the datasets. Datasets can be in the form of primary attributes such as grouped transactions for the card identification number, to select the transactions from the previous period of time and then the primary feature is to be made standing as a basis from the group selected transactions [9]. Application is useful for interconnecting the banks while sharing the fraud issues raised within them. To develop a novel model meta decision trees are useful. Task of constructing ensembles, the task is broken into two sub-tasks in initial stage classifies the base set of level by classifiers. At second, stage to combine the predictions for handling. System has to be dealt with different local sites by the credit database of a individual bank. Avoiding the unwanted and meaningless data in decision trees as the tree grows is called as over-fitting. For giving a better classification in decision trees, the generation of tree is stopped at a particular level [29]. Fuzzy darawanian fraud detection system has improved the accuracy in terms of true positive and also presented a good result for detecting the fraud transactions. Down sampling data and upsampling data methods are applied up sampling methods can gives a better result of accuracy whereas down sampling method gives a lower

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, May 2022
Impact Factor: 6.252

accuracy result with a loss of information [11]. Bayes minimum risk classifier, leads a better result while it is used for estimating probability in which it beliefs model is needed only if it has to incorporate the real financial status [12, 22]. Aiming to a fusion of detecting the algorithms in need of improving the accuracy by using a designing a two-layer authentication for handling the storage of data, rained modeling and data sharing for an online detection can be made [13]. Vaishnavve Jonnalagadee. et. al. proposed and achieved a higher accuracy result of fraud detection in credit card transactions by using random forest algorithm [31].

V. TYPES OF CREDIT CARD FRAUD

Different kinds of credit card frauds are analyzed in which type the fake card occurs not only fake credit card by also how the information is stealed from the user is listed below.

5.1. Application Fraud

Application based frauds are happened by knowing the user's sensitive details to the fraudster like username and password which helps them to create a fake account. It can be termed as identity theft. Sustainable application is made for stealing the documents.

5.2. Electronic or Mail Card Imprints

Skimming the information is the main objective of the fraudster placed on a magnetic strip. These skimmed information can helps the fraudsters in future for purchasing the products in online as skimmed information is maintained very confidential.

5.3. CNP (Card Not Present)

In this type of transaction the fraudsters doesn't need the card. If they just know the account number of the card and expiry date cash amount can be easily taken from the original cardholder.

5.4. Counterfeit Card Fraud

Counterfeit Card Fraud attacks are helded by placing a skimmer device in which the skimmer device stores the original cardholder's information such as account number, name, and personal details so on. These stored information in skimmer helps the fraudsters to create a fake card as same as the original card. Such a skimmer device is placed on ATM centre and on devices where the card can be swiped.

5.5. Lost and Stolen Card

If an user has lost his original card or the user had misplaced his card at any public places the card may get to the hands of the fraudsters so that they can easily make payments on online however, the PIN number is not such that enough for the fraudsters.

5.6. Card ID Theft

It is one of the biggest challenges to identify the fraudster in which it replaces a new account but the account credentials are same. Creating a new account with the same details such as card number and account number is not easy to identify.

5.7. Mail Non – Receipt Card Fraud

This type of fraud occurs when a user is applying for a credit card it takes some duration or a certain period of time for fulfilling the formalities. This gap is sometimes used by the fraudsters to intercept they are the original owner by making their card name as their desire in order to make online payments. This type of fraud can be termed as card not received but money has taken by the way of card.

5.8. Account Takeover

This type of fraud can be described as taking over the user's account by knowing the account number and user's details of the original card holder. By knowing these information they approach for a credit card company as acting like they are

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, May 2022
Impact Factor: 6.252

the original cardholder and may ask them for a new card as the fraudster is changing the hometown by submitting the documents which was taken from the original user by misusing them or by obtaining the documents by hacking their communicating devices. By, using the information the criminal can easily get a new card from the card company.

5.9. False Merchant Sites

When a user is searching for something it can be directed to the phishing websites in which it instructs the user to buy some products by offering a discount and looking like well attractive. As soon as, the transaction is made the details are fetched and it is taken to withdraw the cash.

5.10. Merchant Collusion

Merchant collusion is a kind of credit card fraud in which the details of the user is transferred by the merchant to the criminals without the card holder knowing.

5.11. Localizing Data Theft on ATM attack

Mostly, these type of credit card fraud occurs in a particular locality based region. When a user swipes a card in an ATM machine the card number details and the cardholder's information are automatically sent to the fraudester however the card information will be attacked similar to a phishing after swiping in an ATM center phished card will start to attack on that ATM. If a user come and inserts the card in the ATM that card's information also will be sent to the fraudster.

VI. Machine Learning Algorithms for Credit Card Fraud Detection

6.1 Random Forest Algorithm

Random forest algorithm is an ensemble decision model algorithm which is most precisely used for many real time applications for producing the result without hyper-parameter tuning that can be used for the classification and regression purposes for a labelled and unlabelled datasets. Output produced is not only made from the single decision tree it further iterates and produces the output from multiple decision trees. Main advantage of this algorithm it does not get biased and it will separately trains the tree based upon their branches and leaf nodes. It can be considered as a standardized and stabled algorithm in which it will enhances to work on the missing values in the datasets. It is easy to add a new dataset in a single decision tree and it does not affect the whole multiple decision trees for the purpose of predicting the output results. For identifying the credit card transaction is normal or abnormal transaction random forest algorithm is widely used by a confusion matrix by a representation of trained data and testing data by a process of feature extraction.

6.2 Artificial Neural Networks

Artificial Neural Networks works on the process of human brain neurons by analyzing and processing the information. Decision can be made with the neurons between the edges in the previous layer of the decision and the result will be shown on the current neuron. When it comes under credit card fraud detection datasets collected from the previous transactions are processed, from the processed dataset it easy to find the occurring transaction is a genuine transaction or a fraud transaction if the transaction is made for online purchases or credit card is swipped in an ATM machine.

6.3 Local Outling Factor

Local Outling Factor works on the basis of identifying the density which is calculated with the help of the nearest regional objects. In, the initial stage Local Outling Factor algorithm identifies the regions of similar local densities. To identify the fraudulent credit card transaction it is necessary to import the sampling data from the clustered regions of sampling. From these sampling datasets it is able to make up the system is functioning on a localized region. From this region it is capable to identify the transaction may proceeds for cash withdrawal or not.

6.4 Support Vector Machines (SVM)

Support Vector Machines is normally used for classifying the given data. It comes under the category of supervised machine learning technique. Support Vector Machines separates the data into different classes of n-dimensional Euclidean space. The n-dimensional Euclidean spaces are known as support vectors in which it is easy to predict and classify the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, May 2022
Impact Factor: 6.252

upcoming data points from the datasets. While it comes under for credit fraud detection upcoming data points are measured by the level of past dataset transaction which it will be more helpful for the bankers whether the transaction is legal or not.

6.5 Bayesian networks

Bayesian networks on the theorem of conditional probability. However, Bayes theorem stands as a basis for Bayesian networks algorithm. Correspondingly, Bayesian network can be depicted by a acyclic graph. In which a graph consists of edges and nodes. Nodes corresponds to the randomized unique variables of a dependency and the edges corresponds to the behavioural pattern of relationship lying between the randomized unique variables and the probabilistic distribution of possible chances. This relationship tends to the genuine transaction if it is less than the minimum reached value whereas if it is greater than the maximum reached value it will be termed as fraudulent transaction.

6.6 K-Nearest Neighbour

K-Nearest Neighbour is a distance based machine learning algorithm. It is used for both the classification and regression purpose. It is termed as distance based machine learning algorithm because of calculating or measuring the distance between the datasets such as sampling dataset and the training dataset. K-nearest neighbour algorithm characteristics is measured by the performance of distance metrics, decision rule for classification and the number of neighbours. Distance metrics is used to predict the measurement of the data scale level. Decision rule for classification is used to categorize the data scale level by itself making a comparison by obtaining the feature datasets pointing to the neighbourhood. Number of neighbours is used for the purpose of classifying the data point levels from the past datasets. Based on these performance characteristics it is used to identify the fraudulent credit card transaction as the distance metrics measures the level of possibility of data level either the transaction is legal or illegal. However, decision rule classifies the data by making a comparison for the chances of legal or illegal transaction. Similarly, the number of neighbours classifies the example of transactions from the past experience.

6.7 Fuzzy logic based system

Fuzzy logic works on the degrees of truth values apart from the Boolean logic such ‘0’ or ‘1’ which means identifying the degree values not simply telling the values ‘false’ or ‘true’. Architectural design for fuzzy logic consists of four parts such as rules, fuzzification, inference engine and defuzzification. Rules can be described as the decision making expertise system offered by the controllers of the fuzzy system. Fuzzification is a process of converting the crispy numbers into the input for the controlling system that proceeds the process for the another actions. Inference engine searches for the degrees of the match which had been obtained between the fuzzy inputs and the rules. Defuzzification can be described as converting the fuzzy sets to the crispy values. For a credit card fraud detection using fuzzy logic based system can be performed using threes step order such as rules, fuzzification and defuzzification. Rules will work on the process of drafting system that has been founded from the customer’s characteristics pattern. Fuzzification is used to classify the transaction based upon the levels of low level transaction, middle level transaction and high level transaction. Defuzzification checks the predefined set of rules in a iterative manner as if a transaction is found to be fraud it will immediately stops that transaction and attribute sets of the will again cross checks the transaction by an iterative procedural manner neither the transaction to be proceeded nor not.

6.8 Decision Trees

Decision tree algorithm has a tree-like structure consisting of root nodes and branch nodes as a tree-like structure. Each root nodes points to the branch nodes and the branching nodes points to the leaves node. Techniques used by the decision trees are the ID3 (Iterative Dichotomiser) technique. ID3 technique helps to create the decision trees by a constant set of data samples. Output of the samples helps to classify the future samplings. Each decision leaf nodes corresponds to the trained samples. It may differs based on the trained samples of the entropy datasets. Each entropy of the datasets will be calculated again and again for every decision process. When it comes to the fraud detection of credit card transactions it act as a computing tool for both the classifying transactions as well as the predicting the transactions whether it is a legal or illegal. However, it makes decision of an optimal result by the approachment of the breadth-first search and the depth-first search greedy optimization algorithms.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, May 2022
Impact Factor: 6.252

6.9 Modified Fisher Discriminant Analysis

Modifies fisher discriminant analysis works on the basis of the fisher discirminant analysis algorithm however it comes under the category of supervised learning method as the given input values performs the operations of grouping the regions surrounded by the decision surface. For finding the credit card transaction is made by a genuine user or abnormal user it calculates the difference between mean values and the arithmetic mean value of the labeled input classes of the fisher criterion.

VII. Comparison of Accuracy Level

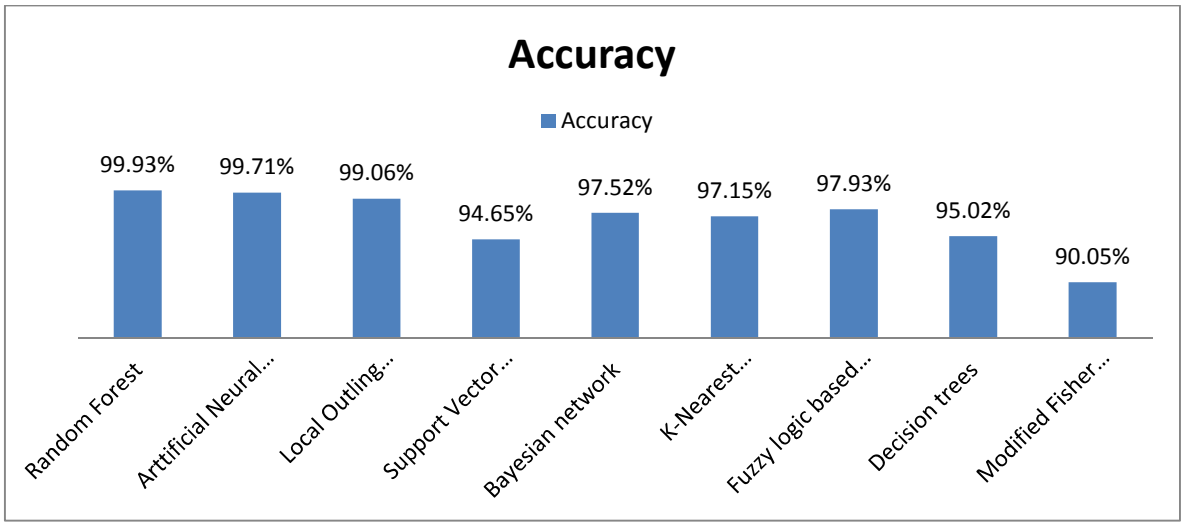

Figure: Comparison of accuracy level for various machine learning algorithms detecting credit card frauds.

VIII. Conclusion

Thus, various techniques credit card fraud detection is analyzed and how to identify the credit card transaction is a fraudulent transaction or a genuine transaction using machine learning algorithms developed by the researchers has made an comparative study with the obtained accuracy results.

IX. Future Scope

Thus, to make a secure credit card transaction by preventing the cash from fraudster had been made a comparative analysis of various machine learning algorithms it is clear that Random forest algorithm gives an higher accuracy of result as well as Artificial Neural Network algorithm also produces an excellent accuracy result whereas it is expensive to implement in real time. Classifying the datasets such as genuine transaction and fraudulent transaction SVM algorithm is very much powerful. From these analyzed algorithms in future combining these algorithms such as Random Forest, Aritificial Neural Network and SVM by using any optimization techniques will be more helpful by minimizing the inputs and maximizing the output results.

References

[1]. S.P. Maniraj et.al. - "Credit card fraud detection using machine learning and data science." International Journal of Engineering and Technical Research (September - 2019).

[2]. Yashvi Jain et. al. - "A comparative analysis of various credit card fraud detection techniques." - International Journal of Recent Technology and Engineering (January – 2019).

[3]. Sanjana Jagdish. et. al. – "Credit Card Fraud Detection System: A Survey.." - Journal of Xidian University (May - 2020).

[4]. M.Deepa and Dr.D.Akila – "Survey Paper for Credit Card Fraud Detection Using Data Mining Techniques." - International Journal of Innovative Research in Applied Sciences and Engineering (December - 2019).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, May 2022
Impact Factor: 6.252

[5]. N. Malini et. al. - "Analysis on credit card fraud detection techniques by data mining and big data approach."- International Journal of Research in Computer Applications And Robotics (May - 2017).

[6]. Suraj Patil et. al. – "Predictive Modelling For Credit Card Fraud Detection Using Data Analytics." - International Conference on Computational Intelligence and Data Science (2018).

[7]. M. Sathyapriya and Dr. V. Thiagarasu – "Big Data Analytics Techniques for Credit Card Fraud Detection: A Review." - International Journal of Science and Research (May - 2017).

[8]. C. Sudha and D. Akila - "Credit card fraud detection using AES technique." - Intelligent Computing and Innovation on Data Science (January - 2020).

[9]. A. Singh and A. Jain. - "An empirical study of AML approach for credit card fraud detection–financial transactions." - International Journal of Computers, Communications & Control (November - 2019).

[10]. Suresh K Shirgave et. al. – "A Review On Credit Card Fraud Detection Using Machine Learning." - International Journal Of Scientific & Technology Research (October - 2019).

[11]. Vaka Sravan and Dr. V. Murali Krishna – "Credit Card Duplicity Reduction System Using Classification Metrics." - International Journal for Research in Applied Science & Engineering Technology (May - 2019).

[12]. Alejandro Correa Bahnsen et. al. – "Example-Dependent Cost-Sensitive Decision Trees" – Elsevier (November - 2015).

[13]. Harshal Jayant Jagtap et. al. – "Fraud recognition and uniquely designed system (F.R.A.U.D.S)." - International Journal of Engineering Development and Research (September - 2018).

[14]. Sanaz Nami and Mehdi Shajari – "Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors" - Elsevier (November - 2015).

[15]. Andrea Dal Pozzolo. et. al. – "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy" - IEEE Transactions on Neural Networks and Learning Systems (August - 2018).

[16]. Anika Nahar et. al. – "A Survey on Different Approaches used for Credit Card Fraud Detection" - International Journal of Applied Information Systems (January - 2016).

[17]. Tanmay Kumar Behera and Suvasini Panigrahi – "Credit Card Fraud Detection: A Hybrid Approach Using Fuzzy Clustering & Neural Network" - Second International Conference on Advances in Computing and Communication Engineering (May - 2015).

[18]. R. Rajamani and M.Rathika – "Credit Card Fraud Detection using Hidden Morkov Model and Neural Networks." - Proceedings of the UGC Sponsored National Conference on Advanced Networking and Applications (March - 2015).

[19]. Alejandro Correa Bahnsen et. al. - "Feature engineering strategies for credit card fraud detection." - Expert Systems with Applications (January - 2016).

[20]. Sapna Gupta – "Deep Learning vs. traditional Machine Learning algorithms used in Credit Card Fraud Detection" – Semantic scholar (December - 2016).

[21]. Andrea Dal Pozzolo et. al. – "Credit Card Fraud Detection and Concept-Drift Adaptation with Delayed Supervised Information." - International Joint Conference on Neural Networks (October - 2015).

[22]. Alejandro Correa Bahnsen et. al. – "Example-Dependent Cost-Sensitive Logistic Regression for Credit Scoring" - International Conference on Machine Learning and Applications (December - 2014).

[23]. K. R. Seeja and Masoumeh Zareapoor - "Fraud miner: A novel credit card fraud detection model based on frequent itemset mining." – Hindawi Journal (September - 2014).

[24]. Andrea Dal Pozollo et. al. – "Learned lessons in credit card detection from a practitioner perspective." - Expert Systems with Applications (August - 2014).

[25]. Tatsuya Minegishi and Ayahiko Niimi – "Proposal of Credit Card Fraudulent Use Detection by Online-type Decision Tree Construction and Verification of Generality." - International Journal for Information Security Research (December - 2011).

[26]. Joseph Pun and Yuri Lawryshyn – "Improving Credit Card Fraud Detection using a Meta Classification Strategy." - International Journal of Computer Applications (October - 2012).

[27]. Khyati Chaudhary. et. al. - "A review of Fraud Detection Techniques: Credit Card" - International Journal of Computer Applications (May - 2012).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, May 2022
Impact Factor: 6.252

[28]. Raghavendra Patidar and Lokesh Sharma – "Credit Card Fraud Detection Using Neural Network" - International Journal of Soft Computing and Engineering (June - 2011).

[29]. Dipti D.Patil. – "Efficient Scalable Multi-Level Classification Scheme for Credit Card Fraud Detection." - International Journal of Computer Science and Network Security (August - 2010).

[30]. Harshit Bagra and Harshit Arora – "Credit Card Fraud Detection."

[31]. Vaishnave Jonnalagadda et. al. – "Credit card fraud detection using Random Forest Algorithm." - International Journal of Advance Research, Ideas and Innovations in Technology (2019).