

A Review On: Credit Card Fraud Detection Techniques Using ML

Aditya V. Belsare¹, Dr. R. R. Keole², Dr. A.B.Raut³

¹ PG Students, Dept. of Computer Science and Engineering, HVPM COET, Amravati, Maharashtra, India

² HOD, Dept. of Information and Technology, HVPM COET, Amravati, Maharashtra, India

³ HOD, Dept. of Computer Science and Engineering, HVPM COET, Amravati, Maharashtra, India

Abstract-Now a day's credit card frauds are easy and friendly targets. E-commerce and many other online sites have increased the online payment modes, increasing the risk for online frauds. Increase in fraud rates, researchers started using different machine learning methods to detect and analyses frauds in online transactions. Frauds are known to be dynamic and have no patterns, hence they are not easy to identify. Fraudsters use recent technological advancements to their advantage. They somehow bypass security checks, leading to the loss of millions of dollars. Analyzing and detecting unusual activities using data mining techniques is one way of tracing fraudulent transactions. In this paper the different proposed system developed by different researcher used in Credit Card Risk Detection Techniques Using Machine Learning is stated.

Key Words: credit card, fraud detection, machine learning, deep learning, random forest, k nearest neighbor, support vector machine, auto encoder, restricted Boltzmann machine, deep belief networks, convolutional neural networks

1. INTRODUCTION

A credit card is a thin handy plastic card that contains identification information such as a signature or picture, and authorizes the person named on it to charge purchases or services to his account - charges for which he will be billed periodically. Today, the information on the card is read by automated teller machines (ATMs), store readers, bank and is also used in online internet banking system. They have a unique card number which is of utmost importance. Its security relies on the physical security of the plastic card as well as the privacy of the credit card number. There is a rapid growth in the number of credit card transactions which has led to a substantial rise in fraudulent activities. Credit card fraud is a wide-ranging. Term for theft and fraud committed using a credit card as a fraudulent source of funds in a given transaction [1].

Fraud detection methods are continuously developed to defend criminals in adapting to their fraudulent strategies. These frauds are classified as [2]:

- Credit Card Frauds: Online and Offline
- Card Theft
- Account Bankruptcy

- Device Intrusion
- Application Fraud
- Counterfeit Card
- Telecommunication

Fraud Some of the currently used approaches to detection of such fraud are [2]:

- Artificial Neural Network
- Fuzzy Logic
- Genetic Algorithm
- Logistic Regression
- Decision tree
- Support Vector Machines
- Bayesian Networks
- Hidden Markov Model
- K-Nearest Neighbour

Science has presented human life much more accessible through technology. In this twentieth era, the entire world is in the time of big data. Machine learning can predict future data or can offer a desirable decision from a big dataset. It is commonly capable of guiding machines to perform tasks by regarding measures of pattern, whereby they should be done. Undoubtedly, machine learning is an enormously realistic technological application that operates with a big dataset. The contribution of machine learning in medical science is undeniable in many fields. Although, machine learning has developed many algorithms. Machine learning algorithms have succeeded in many oppressive things worldwide. Machine learning algorithms are generally mixed up with mathematics and logic that can easily predict from a given dataset. Machine learning algorithms are very accessible to diagnose complex diseases by applying machine learning algorithms. As there's loads of research performed about machine learning algorithms in healthcare for predicting diseases. All over the world thousands of researchers have

discovered a lot in predicting diagnosis applying machine learning algorithms. Since there is a lot of information scattered in many papers, whenever some researchers aspire to recognize about machine learning algorithms, what is the predicting accuracy of diagnosis and which algorithms are the best in all the papers, usually, they get exhausted of looking for papers. Since there are lots of diseases and lots of algorithms, it's extremely challenging to find out of the best algorithm for diagnosis most of the time they could not figure out of the exact paper. This paper purposed a literature survey with various machine learning algorithms predicting diseases with accuracy is explained by different papers information in one, a paper by using commonly used machine learning algorithms. This paper extensively presents as much information as possible can get, those can be kept. This work also focused to analyze the best algorithms which give the most reliable accuracy for the prediction of any disease based on the study from existing literature. This work will encourage practitioners and researchers to find the information easily while working in the healthcare sector. The remainder of the article is structured as follows. In the next section, the related work is described, followed by research methodology and data analysis. Then, discuss our work before conclude [3].

One important infiltrate technique is recognized as “deep learning”, which includes a family of machine learning algorithms that attempt to mold high-level abstractions in data by utilizing deep architectures compiled of multiple non-linear transformations. Contrasting usual machine learning methods, deep learning imitates the human brain that is arranged in a deep architecture and processes information through multiple stages of transformation and representation. By exploring deep architectures to learn features at multiple level of abstracts from data automatically, deep learning methods permit a system to learn complex functions that directly map raw sensory input data to the output, without relying on human-crafted features using domain knowledge [4].

A Deep Neural Network is a type of discriminative feature learning technique, a neural network that contains multiple hidden layers. This is a simple conceptual extension of neural networks; however, it provides valuable advances with regard to the capability of these models and new challenges as to training them. The structure of deep neural networks causes them to be more sophisticated in design, and yet more complex in elements. There are two complexity aspects of a DNN model's architecture. Firstly, how wide, or narrow it is, in other words, how many neurons there are in each layer. Secondly, how deep it is, that is, how many layers of neurons there are. When dealing with the kind of data that has such deep architecture, Deep neural networks can be very beneficial, a deep neural network can fit the data more accurately with fewer parameters than a normal neural network, this is because more layers can be used for a more efficient and accurate representation. It is clear, that shallow

neural network models require far more parameters in achieving their tasks [5].

2. LITERATURE SURVEY

The following section describes the contribution of the various researchers in the area of credit card risk detection.

Esraa Faisal Malik, Khai Wah Khaw et al. [6] proposed the several hybrid machine learning models were developed and investigated based on the combination of supervised machine learning techniques as a part of a credit card fraud detection study. The hybridization of different models was found to have the ability to yield a major advantage over the state-of-the-art models. However, not all hybrid models worked well with the given dataset. Several experiments need to be conducted to examine various types of models to define which works the best. Comparing the performance of the hybrid model to the state-of-the-art and itself, conclude that Adaboost + LGBM is the champion model for this dataset. The result also illustrates that the use of hybrid methods has lowered the error rate. For future work, the hybrid models used in this study will be extended to other datasets in the credit card fraud detection domain. Future work may focus on different areas, starting by proposing data preprocessing techniques to overcome the drawback of the missing values. Additionally, different methods of feature selection and extraction should be investigated in the credit card domain and to determine its impact on prediction accuracy. An investigation of the most appropriate hybrid model among the state-of-the-art machine learning algorithms to determine the most accurate hybridized model in the previously mentioned domain should be the main concern for future studies.

Emmanuel Ileberi, Yanxia Sun et al. [7] has recommended the new technique for GA based feature selection method in conjunction with the RF, DT, ANN, NB, and LR was proposed. The GA was implemented with the RF in its fitness function. The GA was further applied to the European cardholder's credit card transactions dataset and 5 optimal feature vectors were generated. The experimental results that were achieved using the GA selected attributes demonstrated that the GA-RF (using v5) achieved an overall optimal accuracy of 99.98%. Furthermore, other classifiers such as the GA-DT achieved a remarkable accuracy of 99.92% using v1. The results obtained in this research were superior to those achieved by existing methods. Moreover, implemented our proposed framework on a synthetic credit card fraud dataset to validate the results that were obtained on the European credit card fraud dataset. The experimental outcomes showed that the GA-DT obtained an AUC of 1 and an accuracy of 100%. Seconded by the GA-ANN with an AUC of 0.94 and an accuracy of 100%. In future works, intend to use more datasets to validate our framework.

Najadat Hassan, Ola Adnan Altit et al. [8] accomplished a different performance technique by using several machine and deep learning models to detect whether an online transaction is legitimate or fraud on the IEEE-CIS Fraud Detection dataset as well built our model which is BiLSTM-MaxPooling-BiGRU MaxPooling that based on bidirectional LSTM and GRU. also tested several methods to deal with highly imbalanced datasets including under sampling, oversampling and SMOTE. Set of evaluation metrics used to evaluate the performance of the models. The results from machine learning classifiers show that the best AUC was 80% and 81% that achieved by hard voting with under sampling and oversampling technique. However, the results from machine learning classifiers were not promising compared with our model that achieved 91.37% AUC.

Vaishnavi Nath Dornadulaa , Geetha Sa [9] developed a novel method for fraud detection, where customers are grouped based on their transactions and extract behavioral patterns to develop a profile for every cardholder. Then different classifiers are applied on three different groups later rating scores are generated for every type of classifier. This dynamic changes in parameters lead the system to adapt to new cardholder's transaction behaviors timely. Followed by a feedback mechanism to solve the problem of concept drift. observed that the Matthews Correlation Coefficient was the better parameter to deal with imbalance dataset. MCC was not the only solution. By applying the SMOTE, tried balancing the dataset, where found that the classifiers were performing better than before. The other way of handling imbalance dataset is to use one-class classifiers like one-class SVM. finally observed that Logistic regression, decision tree and random forest are the algorithms that gave better results.

Masoumeh Zareapoor, PouryaShamsolmoalia,b [10] proposed the performance of three states of art data mining techniques, with bagging ensemble classifier based on decision tree algorithm which is a novel technique in area of credit card fraud detection system. A real-life dataset on credit card transactions is used for our evaluation. And found that, the bagging classifier based on decision tree works well with this kind of data since it is independent of attribute values. The second feature of this novel technique in credit card fraud detection is its ability to handle class imbalance. This is incorporated in the model by creating four sets of datasets (Df1, Df2, Df3, DF4) which the fraud rate in each of them were 20%, 15%, 10%, 3% respectively. Bagging classifier-based decision tree algorithm performance is found to be stable gradually during the evaluation. More over the bagging ensemble method takes very less time, which is also an important parameter of this real time application, because in fraud detection domain time is known one of the important parameters.

Salvatore J. Stolfo, David W. Fan et al. [11] proposed a new experiment tested using several machine learning algorithms as well as meta-learning strategies on real-world data. Unlike many reported experiments on "standard" data sets, the set up and the evaluation criteria of our experiments in this domain attempt to reflect the real-world context and its resultant challenges. The experiments reported here indicate: 50%/50% distribution of fraud/non-fraud training data will generate classifiers with the highest True Positive rate and low False Positive rate. Other researchers also reported similar findings. Meta-learning with BAYES as a meta-learner to combine base classifiers with the highest True Positive rates learned from 50%/50% fraud distribution is the best method found thus far.

Philip K. Chan, Salvatore J. Stolfo[12] has recommended the new technique to demonstrates that the training class distribution affects the performance of the learned classifiers and the natural distribution can be different from the desired training distribution that maximizes performance. Moreover, our empirical results indicate that our multi-classifier meta-learning approach using a 50:50 distribution in the data subsets for training can significantly reduce the amount of loss due to illegitimate transactions. The subsets are independent and can be processed in parallel. Training time can further be reduced by also using a 50:50 distribution in the validation set without degrading the cost performance. That is, this approach provides a means for efficiently handling learning tasks with skewed class distributions, non-uniform cost per error, and large amounts of data. Not only is our method efficient, it is also scalable to larger amounts of data. Although downscaling instances of the majority class is not new for handling skewed distributions (Breiman et al. 1984), our approach does not discard any data, allows parallelism for processing large amounts of data efficiently, and permits the usage of multiple "off-the-shelf" learning algorithms to increase diversity among the learned classifiers. Furthermore, how the data are sampled is based on the cost model, which might dictate down sampling instances of the minority class instead of the majority class. One limitation of our approach is the need of running preliminary experiments to determine the desired distribution based on a defined cost model. This process can be automated but it is unavoidable since the desired distribution is highly dependent on the cost model and the learning algorithm. Using four learning algorithms, our approach generates 128 classifiers from a 50:50 class distribution and eight months of data. might not need to keep all 128 classifiers since some of them could be highly correlated and hence redundant. Also, more classifiers are generated when the data set is more skewed or additional learning algorithms are incorporated. Metrics for analyzing an ensemble of classifiers (e.g., diversity, correlated error, and coverage) can be used in pruning unnecessary classifiers. Furthermore, the real distribution is more skewed than the 20:80 provided to us. Author intends to investigate our approach with more skewed distributions. As with a large

overhead, a highly skewed distribution can render fraud detection economically undesirable. More importantly, since thieves also learn and fraud patterns evolve over time, some classifiers are more relevant than others at a particular time. Therefore, an adaptive classifier selection method is essential. Unlike a monolithic approach of learning one classifier using incremental learning, our modular meta classifier approach facilitates adaptation over time and removal of out-of-date knowledge.

Abhishek Shivanna, SujanRay et al. [13] has recommended the new technique for credit cards, online transactions is increasing very rapidly. In this day and age, it is very critical to correctly identify online credit card fraudulent transactions. In conclusion, have proposed a credit card fraudulence detection method which identifies online credit card fraudulent transactions. Decision Jungle algorithm has shown promising results to be adapted in any fraudulence detection system. will extend our work in the future by using neural networks to build more advanced fraudulence detection system.

Yiheng Wei, Yu Qi et al. [14] proposed machine learning techniques which is used to identify potential fraud cases. The first step was data description and data cleaning, where this work located and cleaned all frivolous values and replace them with the record number. The second step was the variable creation. More than 600 variables were created using a different method. Then the third step was to select the most relevant features among all the variables that this work had created. Finally, this work trained several models using the features that this work has selected: logistic regression, support vector machine, boosted trees, random forest, and neural network. The best model turns out to be Boosted Tree, with a 54.3% FDR at 3% cutoff for testing and a 54% FDR at 3% cutoff for OOT. This article has very important research significance and explains how to use different machine learning methods to monitor credit card fraud in real time. Finally, this work hopes to improve the optimization of these methods in dealing with unbalanced data sets in the future.

Mohammed Azhan, ShazliMeraj [15] has recommended the new technique for Machine learning techniques have shown to be more competent in handling class imbalance problem as compared to a shallow neural network. Distribution of class weights in neural networks make minor contribution towards handling the class imbalance. Additional techniques like using Cost sensitive loss functions, over-sampling, under-sampling can also be used. It must also be noted that, a better-balanced dataset would provide a much better insight into the problem.

Anu Maria Babu, Dr. Anju Pratap [16] proposed new technique based on the feature rearrangement developed in this paper, the CNN model has an excellent experimental performance with good stability. The model does not require high-dimensional input features or derivative variables, and

can consider a fairly good ordered input arrangement within a number of times. Compared to most current CNN models, this model saves significant calculation time for the derived variables, making the model's design and adjustment process fast and simple. And in an environment where online transactions require rapid response and accurate identification, there's a higher level of availability. From the above model can conclude that when the max pooling layer had added to the model the accuracy level will be decreases as max pooling layer is the part of the network without taking into account other factors: the dimensionality curse, the network size and the problem of over fitting. And also max pooling preserves the most important details that can be used to create a powerful multilayer completely linked network at the edge. When the max pooling layer is not added to the model the accuracy level has been increased.

RuttalaSailusha, V. Gnaneswar et al. [17] has recommended the new technique for fraud detection techniques. From author analysis, author can conclude that the accuracy is the same for both the Random Forest and the Adaboost algorithms. When author consider the precision, recall, and the F1-score the Random Forest algorithm has the highest value than the Adaboost algorithm. Henceauthor conclude that the Random Forest Algorithm works best than the Adaboost algorithm to detect credit card fraud. From the above analysis, it is clear that many machine learning algorithms are used to detect the fraud but can observe that the results are not satisfactory. So, would like to implement deep learning algorithms to detect credit card fraud accurately.

Anuruddha Thennakoon, Chee Bhagyani et al. [18] has recommended the new technique for Credit card fraud detection. Credit card fraud has been a keen area of research for the researchers for years and will be an intriguing area of research in the coming future. This happens majorly due to continuous change of patterns in frauds. In this paper, propose a novel credit-card fraud detection system by detecting four different patterns of fraudulent transactions using best suiting algorithms and by addressing the related problems identified by past researchers in credit card fraud detection. By addressing real time credit-card fraud detection by using predictive analytics and an API module the end user is notified over the GUI the second a fraudulent transaction is taken place. This part of our system can allow the fraud investigation team to make their decision to move to the next step as soon as a suspicious transaction is detected. Optimal algorithms that address four main types of frauds were selected through literature, experimenting and parameter tuning as shown in the methodology. also assess sampling methods that effectively address the skewed distribution of data. Therefore, can conclude that there is a major impact of using resampling techniques for obtaining a comparatively higher performance from the classifier. The machine learning models that captured the four fraud patterns (Risky MCC, Unknown web address, ISOResponse Code, Transaction

above 100\$) with the highest accuracy rates are LR, NB, LR and SVM. Further the models indicated 74%, 83%, 72% and 91% accuracy rates respectively. As the developed machine learning models present an average level of accuracy, hope to focus on improving the prediction levels to acquire a better prediction. Also, the future extensions aim to focus on location-based frauds.

Greeshma N Pai, Kirana R [19] has recommended the new technique for CCRD(CREDIT CARD RISK DETECTION). A limitation of this study is however that it only deals with detecting fraud in a supervised learning context. Although supervised learning KNN, Random Forest seem attractive and produce good results, they do not work well for dynamic environments. Fraud patterns typically change over time and would be hard to catch. New data sets would need to be collected and machine learning models need to be retained. In this paper, studied applications of machine learning like Naïve Bayes, Logistic regression, Random forest with boosting and shows that it proves accurate in deducting fraudulent transaction and minimizing the number of false alerts. Supervised learning algorithms are novel one in this literature in terms of application domain. If these algorithms are applied into bank credit card fraud detection system, the probability of fraud transactions can be predicted soon after credit card transactions. And a series of anti-fraud strategies can be adopted to prevent banks from great losses and reduce risks. Our study reveals that to detect fraud, the best methods with larger datasets would be using SVMs, potentially combined with CNNs to get a more reliable performance. For the smaller datasets, ensemble approaches of SVM, Random Forest and KNNs can provide good enhancements. Convolution Neural Networks (CNN) usually, outperforms other deep learning methods such as Auto encoders, RBM and DBN methods such as CNN.

DejanVarmedja, Mirjana Karanovic [20] proposed a technique for credit card frauds detection which is a very serious business problem. These frauds can lead to huge losses, both business and personal. Because of that, companies invest more and more money in developing new ideas and ways that will help to detect and prevent frauds. The main goal of this paper was to compare certain machine learning algorithms for detection of fraudulent transactions. Hence, comparison was made and it was established that Random Forest algorithm gives the best results i.e. best classifies whether transactions are fraud or not. This was established using different metrics, such as recall, accuracy and precision. For this kind of problem, it is important to have recall with high value. Feature selection and balancing of the dataset have shown to be extremely important in achieving significant results. Further research should focus on different machine learning algorithms such as genetic algorithms, and different types of stacked classifiers, alongside with extensive feature selection to get better results.

Thulasyammal Ramiah Pillai et al. [21] has recommended the new technique which is MLP algorithm. In this paper, the highest sensitivity is only 83% due to very limited combination of number of hidden layers and number of nodes. In the future study should use multiple number of hidden layers and various number of nodes in the hidden layers to obtain the optimum results. can conclude that MLP with logistic activation function gives the best result followed by the tan. can also observe that identity activation function gives the lowest sensitivity value due to its nature. It does not perform any transformation. In our future study, should use a balanced data. In the future, more advanced deep learning algorithms can be used to detect credit card fraud. Moreover, will try using new activation functions in our future study.

John O. Awoyemi et al. [22] proposed technique which investigates the comparative performance of Naïve Bayes, K-nearest neighbor and Logistic regression models in binary classification of imbalanced credit card fraud data. The rationale for investigating these three techniques is due to less comparison they have attracted in past literature. However, a subsequent study to compare other single and ensemble techniques using our approach is underway. The contribution of the paper is summarized in the following: 1. Three classifiers based on different machine learning techniques (Naïve Bayes, K-nearest neighbors and Logistic Regression) are trained on real life of credit card transactions data and their performances on credit card fraud detection evaluated and compared based on several relevant metrics. 2. The highly imbalanced dataset is sampled in a hybrid approach where the positive class is oversampled and the negative class under-sampled, achieving two sets of data distributions. 3. The performances of the three classifiers are examined on the two sets of data distributions using accuracy, sensitivity, specificity, precision, balanced classification rate and Matthews Correlation coefficient metrics. Performance of classifiers varies across different evaluation metrics. Results from the experiment shows that the kNN shows significant performance for all metrics evaluated except for accuracy in the 10:90 data distribution. This study shows the effect of hybrid sampling on the performance of binary classification of imbalanced data. Expected future areas of research could be in examining meta-classifiers and meta learning approaches in handling highly imbalanced credit card fraud data. Also effects of other sampling approaches can be investigated.

D. Tanouz, R Raja Subramanian et al. [23] has recommended the new technique for credit card risk detection is algorithms decision tree, Random forest, logistic regression, naive bayes classification machine learning algorithms, results shows that Random forest classifier performs best with having 96.7741% accuracy, 100% precision, 91.1111% recall, 95.3488% f1 scores and 95.5555 ROU-AUC score and still there are 4 False Negative values and when use data without Random Under Sampling will get accuracy of 99.98% due to heavily imbalance and results many false output. After cleaning data

and applying algorithms got random forest as best algorithm still can see there is much less difference between all four algorithms but based on the decisions for transactions whether fraud or not by making a particular feature as root and gaining information from all trees predicting the outcome. All the algorithms performed almost same with less difference, but can consider that If these algorithms are trained with some more real-world data then the efficiency and prediction will increase As could not reach 100% accuracy even after making many data mining techniques, but are trying to get more accuracy will work on combining different algorithms which can give us better accuracy and with respect to data also if get more data and that is by bank officially, can gain more accuracy as learning increases, will try to decrease False Negatives. can be still able to get better results if train models with more data and use genetic algorithms which will test in our future work.

Gaurav Mhatre , Oshan Almeida et al .[24] has recommended the new technique for Credit card fraudulent detection which is done using HMM (Hidden Markov Model).This technique is used to detect various suspicious activities on credit card. It maintains a database, where past records of transactions are saved and any unusual transaction if carried out, which differs too much from the previous records, it tracks it. Let the user know by sending the details of the transaction on his mobile and hence prevent fraud. After evaluation of well-known Hidden Markov Model it is clearly shown the various methods which can detect the Fraud efficiently and provide accurate security. Speed of the software can be enhanced by implementation of algorithms of less complexity. Inter mail server can be implemented using the same concept. Proper security provisions are made from malicious threats and hacking tools so that user account cannot be harmed intentionally or non-intentionally from frauds. Proper hierarchy of the users is maintained as per authority to access the data and use the services provided by the authority. Track all the necessary details during transaction process.

3. CONCLUSION

This paper studies the work proposed by various researchers in the area of credit card risk detection based upon Deep learning, machine learning and different algorithms. These learning methods resolve the challenges in credit card risk detection system to solve modeling past credit card transactions with the knowledge of the ones that turned out to be a fraud. This model is then used to identify whether a new transaction is fraudulent or not. These techniques show how to reduce not just the computational time but also cost. In this paper each technique can be improve in future by combining various technique as stated in the paper.

REFERENCES

- [1] Munira Ansari, Hashim Malik, Siddhesh Jadhav, Zaiyyan Khan, "Credit Card Fraud Detection", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Special Issue - 2021
- [2] S P Maniraj, Aditya Saini, Swarna Deep Sarkar Shadab Ahmed," Credit Card Fraud Detection using Machine Learning and Data Science", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 8 Issue 09, September-2019
- [3] Munira Ferdous, Jui Debnath† and Narayan Ranjan Chakraborty," Machine Learning Algorithms in Healthcare: A Literature Survey", 11th ICCCNT 2020 July 1-3, 2020 - IIT-Kharagpur Authorized licensed use limited to: Carleton University.
- [4] Sakshi Makwane, V S Mahalle , Dr. D R Dhotre," A Review On: Content Based Image Retrieval Using Intelligence Techniques", International Journal of Innovative Research in Computer and Communication Engineering ,Volume 8, Issue 8, August 2020
- [5] Katleho L Masita, Ali N Hasan, Thokozani Shongwe," Deep Learning in Object Detection: a Review", Authorized licensed use limited to: Cornell University Library @2020 IEEE.
- [6] Esraa Faisal Malik ,Khai Wah Khaw , Bahari Belaton , Wai Peng Wong and XinYing Chew ,"Credit Card Fraud Detection Using a New Hybrid Machine Learning Architecture", Mathematics 2022.
- [7] Emmanuel Ileberi ,Yanxia Sun and Zenghui Wang," A machine learning based credit card fraud detection using the GA algorithm for feature selection", Journal of Big Data (2022).
- [8] Najadat Hassan, Ola Adnan Aliti,Ayah Abu Aqouleh,Mutaz Younes," Credit Card Fraud Detection Based on Machine and Deep Learning", Conference: 2020 11th International Conference on Information and Communication Systems (ICICS)
- [9] Vaishnavi Nath Dornadulaa , Geetha Sa," Credit Card Fraud Detection using Machine Learning Algorithms", INTERNATIONAL CONFERENCE ON RECENT TRENDS IN ADVANCED COMPUTING 2019, ICRTAC 2019.
- [10] Masoumeh Zareapoor ,Pouya Shamsolmoali," Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier", International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014) Conference Organized by Interscience Institute of Management and Technology, Bhubaneswar, Odisha, India

- [11] Salvatore J. Stolfo, David W. Fan, Wenke Lee and Andreas L. Prodromidis, Philip K. Chan, "Credit Card Fraud Detection Using Meta-Learning: Issues 1 and Initial Results", from DARPA (F30602-96-1-0311), NSF (IRI-96-32225 and CDA-96-25374), and NYSSTF (423115-445).
- [12] Philip K. Chan, Salvatore J. Stolfo, "Toward Scalable Learning with Non-uniform Class and Cost Distributions: A Case Study in Credit Card Fraud Detection", American Association for Artificial Intelligence
- [13] Abhishek Shivanna, Sujan Ray, Khaldoon Alshouli, Dharma P Agrawal, "Detection of Fraudulence in Credit Card Transactions using Machine Learning on Azure ML" ©2020 IEEE
- [14] Yiheng Wei, Yu Qi, Qianyu Ma, Zhangchi Liu, Chengyang Shen, Chen Fang, "Fraud Detection by Machine Learning", 2020 2nd International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI) ©2020 IEEE
- [15] Mohammed Azhan, Shazli Meraj, "Credit Card Fraud Detection using Machine Learning and Deep Learning Techniques", Proceedings of the Third International Conference on Intelligent Sustainable Systems [ICISS 2020] IEEE Xplore.
- [16] Anu Maria Babu, Dr. Anju Pratap, "Credit Card Fraud Detection Using Deep Learning", 2020 IEEE Recent Advances in Intelligent Computational Systems (RAICS).
- [17] Ruttala Sailusha, R. Ramesh, V. Gnaneswar, G. Ramakoteswara Rao, "Credit Card Fraud Detection Using Machine Learning", Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS 2020) IEEE.
- [18] Anuruddha Thennakoon, Chee Bhagyan, Sasitha Premadasa, Shalitha Mihiranga, Nuwan Kuruwitaarachchi, "Real-time Credit Card Fraud Detection Using Machine Learning", @2019 IEEE. 7
- [19] Greeshma N Pai, Kirana R, Likhitha, Madhushree N, "Credit Card Fraud Detection Techniques", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 07 Issue: 11 | Nov 2020
- [20] Dejan Varmedja, Mirjana Karanovic, Srdjan Sladojevic, Marko Arsenovic, Andras Anderla, "Credit Card Fraud Detection - Machine Learning methods", 18th International Symposium INFOTEH-JAHORINA, 20-22 March 2019
- [21] Thulasyammal Ramiah Pillai, Ibrahim Abaker Targio Hashem, Sarfraz Nawaz Brohi, Sukhminder Kaur, Mohsen Marjani, "Credit Card Fraud Detection Using Deep Learning Technique", ©2018 IEEE
- [22] John O. Awoyemi, Adebayo O. Adetunmbi, Samuel A. Oluwadare, "Credit card fraud detection using Machine Learning Techniques: A Comparative Analysis", ©2017 IEEE
- [23] D. Tanouz, R Raja Subramanian, D. Eswar, G V Parameswara Reddy, A. Ranjith kumar, CH V N M praneeth, "Credit Card Fraud Detection Using Machine Learning", Proceedings of the Fifth International Conference on Intelligent Computing and Control Systems (ICICCS 2021) IEEE
- [24] Gaurav Mhatre, Oshan Almeida, Dhiraj Mhatre, Poonam Joshi, "Credit Card Fraud Detection Using Hidden Markov Model", Gaurav Mhatre et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014