Journal of Theoretical and Applied Information Technology
31st October 2024. Vol.102. No. 20

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN INTELLIGENT APPROACH TO CREDIT CARD FRAUD DETECTION USING RANDOM FOREST

[1]Bhukya Dharma, [2]Dr.D. Latha
[1]Research Scholar , Department of Computer Science and Engineering, Adikavi Nannaya University, Rajamahendravaram, India
[2] Asst. Professor, Department of Computer Science and Engineering, Adikavi Nannaya University, Rajamahendravaram, India
Email: dharmaaknu9@rediffmail.com

ABSTRACT

Nowadays digitalization gaining popularity because of seamless, easy and convenience use of ecommerce. A credit card which remains a very widespread compensation method is accepted online & offline that provides cashless transactions. Credit card fraud is a critical issue for financial institutions and their customers. Credit card fraud is one of the most important threats that affect people as well as companies across the world, particularly with the growing volume of financial transactions using credit cards every day. Machine Learning algorithms have been applied for identifying fraudulent transactions efficiently. This paper presents, An Intelligent Approach to Credit Card Fraud Detection Using Random Forest (RF). The major issues in fraud detection on credit card transaction data are that they are huge and they exhibit huge imbalance levels. E-Commerce Sales Dataset is obtained from the Kaggle. In the dataset 85275 are the genuine transactions and 117 are fraud transactions. The results of the described model are based on Accuracy, Sensitivity, Specificity, and F1-score. Described model achieves Accuracy as 97.1%, Precision as 95.7%, Sensitivity as 95%, Specificity as 95.9%, and F1-Score as 97.5%. The investigational outcomes absolutely show the effectiveness of described model.
Keywords: *Credit card fraud, Machine Learning, Random Forest, Accuracy, Sensitivity, Specificity, and F1-score*

1. INTRODUCTION

Now a day's virtual companies and the internet are changing the scenario of traditional commerce. As the internet provide a global market, more flexibility and more competition in market, e-commerce value is increased. E-commerce also provides easier and wide range of innovation in the field of banking and payment. Online payment is the vital thing for Ecommerce or Digital market [1]. For online payment there are various payment mechanisms available in market. Users are using different types of payment mechanisms as per their need and choice. Various types of payment mechanisms are Credit card (CC), debit card (DC), net banking, e-wallet, etc [2].

Credit is the term used to describe the notion of conducting money transactions electronically without the need of real money [3]. Credit card is a plastic material card, issued by bank or payment organization. It gives credit to customer for purchase goods or services [4]. There is spending limit on card. The thin credit card carries customer and credit information. These cards are notable for their fast-growing e-banking services, used in online funds transfer and E-Commercial transactions [5]. Today, Credit Card Fraud is one of the leading and highest complications to the electronic business [6]. According to review or survey the highest fraudulent deal taken place by using credit card [7]. Some popular methods for online credit card frauds are phishing, identity theft, skimming, lost or stolen card use, card cloning, etc [8]. Apart from these methods some another mechanism that allow credit card scams such as, malware or key loggers who can hack credit card details while online transaction, scanning devices are used to read tour credit card details [9].
Fraudsters use a credit card for conducting unauthorized purchases, resulting in significant losses for consumers and institutions. The creation of bogus cards, on the alternate hand, has made it easier for fraudsters in executing transactions [10]. Credit Card Fraud is a fraudulent activity that is committed via payment card. When an attacker or hacker are using a victim's credit card for own gain or use, where the card holders are not aware from the circumstance that card is being used by third or illegal person. An illegitimate payment transaction

that is accomplish by criminal by using card and its sensitive details like card number, PIN, expiry date in order to buy something or personal gains [11].

As number of fraudsters are increasing and they are using the dark web technique. Dark web is completely inaccessible so far connected to the free Internet. The encoded side of the internet that cannot be followed to worked [12]. The software that supports it to remain hide while transferring out to frauds. Dark web is a portion of the web, that is non-indexed portion of Internet that cannot be used by search engines such as Google. It requires some encrypted techniques like Tor browser. Now a day's customer is become serious about their safety, besides all customers demand more security for online payment. There are many different types of credit card frauds performed by hacker. There are various methods and techniques are available in market to protect online transitions and recognize illegal transactions [13].

Classification, visualization, outlier detection, clustering, regression, and prediction, to mention a few, are six of the areas that predictive analytics might fall under and are frequently used for detecting financial crimes. Furthermore, it is claimed that one out of every three firms has been the subject of a large-scale fraud operation in the previous two years.

Artificial intelligence is a superset of machine learning. Computers acquire knowledge from the data provided in order to complete jobs. In machine learning, the computer creates training data based on the input, which aids in prediction and decision making. Fraud is identified via machine learning by examining past consumer behaviour and transactional methods [14]. It can assess these activities rapidly and effectively by identifying deviations from normal behaviour right away. This gives the user an ability to confirm a transaction in real time before it is finalized. Because human error in data collection and analysis is eliminated, machine learning delivers the extra benefit of increased accuracy. Furthermore, better predictions may be produced since machine learning algorithms can analyze enormous amounts of data [15].

For detecting and preventing the credit card fraud transaction various methods available in market. Some popular detecting techniques for credit card scams are HMM (Hidden Markov Model), Data mining, Biometrics, SVM, Bayesian Network, Neural Network, etc. The selection of an algorithm for the model is dependent on the performance of each algorithm under classification. The selection of the wrong algorithm can result in overfitting or under fitting. The balance of bias and variance are the driving forces behind the selection of the algorithm. The rest of the paper is organized as follows: Section II describes the literature survey. credit card detection process is described in Section III. Section IV demonstrates the performance analysis of credit card fraud detection and finally paper is concluded with Section V

2. LITERATURE SURVEY

Siva Parvathi.Nelluri, Shaik. Nagul, Dr. M. Kishorekumar, et. al. [16] modeled the sequence of operations in credit card transaction processing using a Hidden Markov Model (HMM) and shows how it can be used for the detection of frauds. There is also no benchmark data set available for experimentation. We have, therefore, performed large-scale simulation studies to test the efficacy of the system. A simulator is used to generate a mix of genuine and fraudulent transactions. An HMM is initially trained with the normal behavior of a cardholder. If an incoming credit card transaction is not accepted by the trained HMM with sufficiently high probability, it is considered to be fraudulent. At the same time, we try to ensure that genuine transactions are not rejected. Experimental results show the performance and effectiveness of our system and demonstrate the usefulness of learning the spending profile of the cardholders. Comparative studies reveal that the Accuracy of the system is 80 percent over a wide variation in the input data. The system is also scalable for handling large volumes of transactions.

A. Agrawal, S. Kumar and A. K. Mishra, et, al. [17] developed a technique for `Credit Card Fraud Detection'. Credit Card can be accepted for each online and offline in today's world. There are combinations of methods used. Firstly, Shopping Behavior is based on which type of products customer buys. Secondly, Spending Behavior in this the fraud is detected based on the maximum amount spent. Thirdly, Hidden Markov Model in this technique profiles are maintained and statistics of a particular user and statistics of different fraud scenarios are clustered. Genetic Algorithm is used for calculation of threshold and accurate frauds. Finally average is taken out by summing the result. The main task of this research work is to explore different views of the same problem and see what

can be learned from the application of each different technique. H. Wang, P. Zhu, X. Zou and S. Qin, et. al. [18] proposed an ensemble learning framework based on training set partitioning and clustering. It turns out that the proposed framework not only ensures the integrity of the sample features, but also solves the high imbalance of the dataset. A main feature of our framework is that every base estimator can be trained in parallel. This improves the efficiency of the framework. The average of AUC of RF based on partitioning and hierarchical clustering (RFPH) is about 0.965 and better than the average of RF based on random under-sampling (RFRU) which is about 0.947. The average of Savings of RFPH we constructed is about 68.0% and achieves improvement of 6% over RFRU. We show the effectiveness of our proposed ensemble framework by experimental results on a real credit card transaction dataset.

N. Nassar and G. Miller, et. al. [19] introduced a new approach to credit card security which takes the pardon and the risk away from all entities by securing the card number so that only the issuer and the reader know what it is. By securing those two end points and ensuring that card number is not known to any other entity between those two end points, the card itself would not hold any value even if it got lost or stolen. Technically this approach reduces the chances of card fraud by exponential magnitude.

Kazemi and H. Zarrabi, et. al. [20] proposed a deep autoencoder to extract best features from the information of the credit card transactions and then append a softmax network to determine the class labels. Regarding the effect of features in such data employing an overcomplete autoencoder can map data to a high dimensional space and using the sparse models leads to be in a discriminative space that is useful for classification aims. The benefit of this method is the generality virtues that we can use such networks in several realms e.g. national intelligence, cyber security, marketing, medical informatics and so on. Moreover gaining the high accuracy (84.1%), the low variance ($\pm$1.84) is noticeable. Results can reveal the advantages of proposed method comparing to the state of the arts.

Z. Li, G. Liu and C. Jiang, et al. [21] focus on obtaining deep feature representations of legal and fraud transactions from the aspect of the loss function of a deep neural network. We propose a new kind of loss function, full center loss (FCL), which considers both distances and angles among features and, thus, can comprehensively supervise the deep representation learning. We conduct lots of experiments on two big data sets of credit card transactions, one is private and another is public, to demonstrate the detection performance of our model by comparing FCL with other state-of-the-art loss functions. Area under precision–recall curve (AUC_PR) (87.7%), F1-Score (85.3%) is continuously improved obviously, which indicates the importance of intraclass compactness of learned representations. We also conduct experiments to show that FCL can ensure a more stable model than others.

A. C. Bahnsen, A. Stojanovic, D. Aouada and B. Ottersten, et. al. [22] presents a new comparison measure that realistically represents the monetary gains and losses due to fraud detection. Moreover, using the proposed cost measure a cost sensitive method based on Bayes minimum risk is presented. This method is compared with state of the art algorithms and shows improvements up to 23% measured by cost. The results of this paper are based on real life transactional data provided by a large European card processing company. H. Hormozi, M. K. Akbari, E. Hormozi and M. S. Javan, et al. [23] suggested a model for credit card fraud detection using AI. To do this, negative selection is parallelized using Apache Hadoop and MapReduce. Method uses three detectors. The results imply that implementing a fraud detection system on the cloud decreases algorithm training time. We designed one of the AIS (Artificial Immune System') algorithms and parallelized NSA (negative selection algorithm) in the cloud with several Mappers to decrease credit card fraud detection time. NSA provides Map and Reduce functions. Thus, training time (74s) has decreased. This means credit cards can identify fraud faster. A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi and G. Bontempi, et. al. [24] describes three major contributions. First, we propose, with the help of our industrial partner, a formalization of the fraud-detection problem that realistically describes the operating conditions of fraud-detection system (FDS) that everyday analyze massive streams of credit card transactions. Second, we design and assess a novel learning strategy that effectively addresses class imbalance, concept drift, and verification latency. Third, in our experiments, we demonstrate the impact of class unbalance and concept drift in a real-world data stream containing more than 75 million transactions, authorized over a time window of three years.

K. Randhawa, C. K. Loo, M. Seera, C. P. Lim and A. K. Nandi, et al. [25] used machine learning to detect credit card. Standard models are first used. Then, hybrid methods which use AdaBoost and majority voting methods are applied. To evaluate the model efficacy, a publicly available credit card data set is used. Then, a real-world credit card data set from a financial institution is analyzed. In addition, noise is added to the data samples to further assess the robustness of the algorithms. The experimental results positively indicate that the majority voting method achieves good accuracy rates 88% in detecting fraud cases in credit cards.

3. . AN INTELLIGENT APPROACH TO CREDIT CARD FRAUD DETECTION

The flow process of An Intelligent Approach to Credit Card Fraud Detection Using Random Forest (RF) is represented in below Fig. 1.

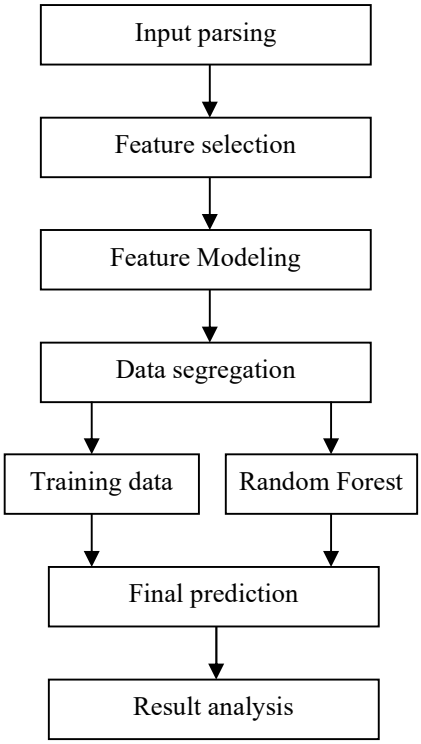

Fig. 1: Flow Process Of Intelligent Approach To Credit Card Fraud Detection

One of the most crucial jobs in the development of a machine learning model is data collection. It is the gathering of task- related data based on a set of targeted factors in order to analyze and provide a useful result. E-Commerce Sales Dataset is obtained from the Kaggle. In the dataset 85275 are the genuine transactions and 117 are fraud transaction detected. Its capacity to detect and prevent fraudulent transactions. Illicit activities are characterized by their uneven nature. The dataset have features from V1 to V28. Number of transactions and attributes are used in classification of credit card detection. In class attribute its shows zero fraud is not detected if it shows one the amount fraud has been detected.

The input preparation phase includes data parsing and data pre-processing. Data parsing is the process of modifying the data such that it becomes appropriate for consumption by the developed architecture. The streamed transaction data is usually in the form of comma separated values. However, the prediction architecture accepts input data in the form of data and labels. Parsing divides the input data into two components, data and labels. Pre-processing is performed by analyzing the input data for anomalous entries and missing entries. If present, such entries are filled with appropriate values, which are identified by finding instances with similar fields of the current instance. Further, nominal entries are normalized and converted to numerical entries and are passed to the next phase.

The memory and time constrain are too expensive when working on a large dataset. Sampling methods are used for subset selection is an important factor in dataset analysis. The linear discriminant analysis method is used for an optimal number of the feature with cross-validation and resampling method using imbalanced learn cluster centroids.

The data segregation phase performs a random division of data into training and test data. Train/Test is a technique for determining model's correctness. Total data is divided into two sets: one for training purposes and one for testing purposes. Training takes up eighty percent of budget, whereas testing consumes just twenty percent of total. Training set is used to train model. This process helps overcome the issue of data imbalance to a large extent.

Random forests are a combination of many decision trees through ensemble learning. If there was an input sample data, there might be N different classifiers that produce N different results in the random forest. Then the random forest combines these results and votes on them, with the most one being the desired output. This algorithm is better than the single decision trees because it reduces the

over-fitting by averaging the result. Random forest adds additional randomness to the model, while growing the trees. Instead of searching for the most important feature while splitting a node, it searches for the best feature among a random subset of features.

By using performance parameters as Accuracy, Precision, Sensitivity, Specificity, and F1-Score the evaluated model performance is calculated then fraudulent or normal transaction is identified.

4. RESULT ANALYSIS

The dataset, credit card fraud data is taken as E-Commerce Sales Dataset from Kaggle. In the dataset 85275 are the genuine transactions and 117 are fraud transaction detected. We split the entire dataset into 80% training set and 20% test set. To get performance analysis, we need to evaluate metrics like Accuracy, Precision, Sensitivity, Specificity, and F1-Score. Each metric reflects a different aspect of the model quality, and depending on the use case. Precision and recall are two evaluation metrics used to measure the performance of a classifier in binary and multiclass classification problems. Accuracy works best if false positives and false negatives have similar cost. If the cost of false positives and false negatives are very different, it's better to look at both Precision and Recall. In general, the evaluation can be accomplished using a confusion matrix which is formed from the following: True Positive (TP) False Positive (FP) True Negative (TN) False Negative (FN).

Table 1: Confusion Matrix For Evaluating Classification

Predicted	Actual	
	Normal	Fraud
Normal	TN	FN
Fraud	FP	TP

Performance parameters are expressed as follows:
Accuracy is the most intuitive performance measure and it is simply a ratio of correctly predicted observation to the total observations. One may think that, if we have high accuracy then our model is best.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FN} + \text{FP}} \ldots . (1)$$

Precision is the ratio of correctly predicted positive observations to the total predicted positive observations and will be the higher when the amount of false positives is low.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \ldots . (2)$$

Sensitivity is the ratio of correctly predicted positive observations to the all observations in actual class.

$$\text{Sensitivity/Recall} = \frac{\text{TP}}{(\text{TP} + \text{FN})} \ldots . (3)$$

Specificity measures the proportion of actual negatives that are correctly identified.

$$\text{Specificity} = \frac{\text{TN}}{\text{TN} + \text{FP}} \ldots . (4)$$

F1-score is also most elementary evaluation matrics, largely used for model evaluation.

$$\text{F1} - \text{Score} = 2 \times \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \ldots (5)$$

Where,
1. True Positive, which can be defined as the number of fraudulent transactions that are even classified by the system as fraudulent.
2. True Negative, which can be defined as the number of normal transactions that are even classified as normal by the system.
3. False Positive, which can be defined as a number of the normal transactions which are wrongly classified as fraud.
4. False Negative is defined as the transactions that are fraud but are wrongly classified as normal.

The comparative analysis of different classifiers as AdaBoost and Hidden Markov Model (HMM) based credit card fraud detection models with described An Intelligent Approach to Credit Card Fraud Detection Using Random Forest (RF) is represented in below Table 2.

Table 2: Comparative Performance Abnalysis

Parameters	HMM	AdaBoost	RF
Accuracy	84	88	97.1
Precision	83	87.8	95.7

Sensitivity	84.1	86	95
Specificity	83.6	86.1	95.9
F1-score	84.1	87.4	97.5

Fig. 2 shows the comparative graphical representation of accuracy and precision parameters for described An Intelligent Approach to Credit Card Fraud Detection Using Random Forest (RF) and other models. Fig. 3 shows the comparative graphical representation of Sensitivity, Specificity and F1-score parameters for different models.

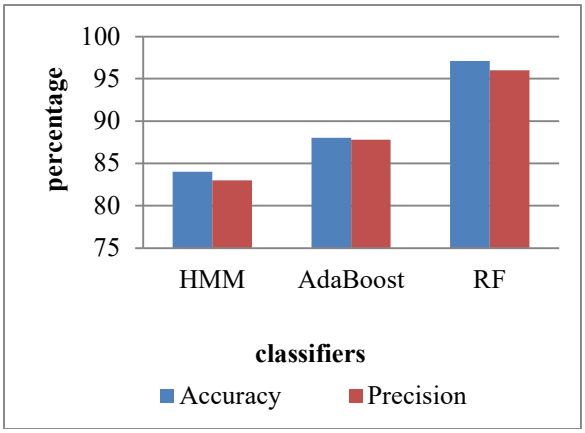

Fig. *2: Comparative Analysis Of Accuracy And Precision Parameters*

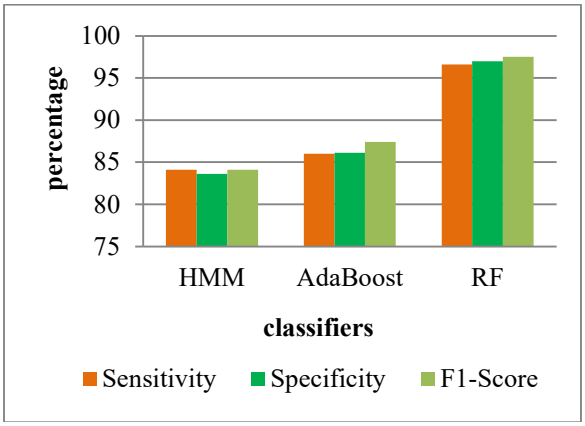

Fig. 3: Comparative Analysis Of Sensitivity, Specificity And F1-Score Parameters

From results it is clear that, described Intelligent Approach to Credit Card Fraud Detection Using Random Forest (RF) achieves better performance than other models in terms performance parameters. Described model achieves Accuracy as 97.1%, Precision as 95.7%, Sensitivity as 95%, Specificity as 95.9%, and F1-Score as 97.5%.

5.. CONCLUSION

This paper presents, An Intelligent Approach to Credit Card Fraud Detection Using Random Forest (RF) is described. Credit card fraud identification system has been an extreme requirement in recent times to protect against fraud problems by using the credit card for some type of online transactions. The use of machine learning in fraud detection has been an interesting topic now days. E-Commerce Sales Dataset is obtained from the Kaggle. In the dataset 85275 are the genuine transactions and 117 are fraud transactions. We split the entire dataset into 80% training set and 20% test set. To get performance analysis, we need to evaluate metrics like Accuracy, Precision, Sensitivity, Specificity, and F1-Score. From results it is clear that, described Intelligent Approach to Credit Card Fraud Detection Using Random Forest (RF) achieves better performance than other models in terms performance parameters. Described model achieves Accuracy as 97.1%, Precision as 95.7%, Sensitivity as 95%, Specificity as 95.9%, and F1-Score as 97.5%. In future we would like to include some fringe cases and error handler. For example, the case when the temporary card number expires prior to the vendor completely processes the transaction. We also expect to further increase the alert precision, that would be specifically designed to replace the linear aggregation of the posterior probabilities.

REFERENCES

[1] D. L. N, S. Guruswamy, V. Lalitha, M. Awasthy and P. K. Pareek, "A Powerful Algorithm for e-Commerce Credit Risk Analysis," *2023 International Conference on Data Science and Network Security (ICDSNS)*, Tiptur, India, 2023, pp. 1-7, doi: 10.1109/ICDSNS58469.2023.10245182.

[2] H. Zheng, Y. Tang and J. Zhang, "A Transition Transfer Mechanism in Payment Network," in *IEEE Access*, vol. 11, pp. 83983-83995, 2023, doi: 10.1109/ACCESS.2022.3227029.

[3] M. Du, P. Yang, W. Tian and Z. Han, "Anti-Collusion Multiparty Smart Contracts for Distributed Watchtowers in Payment Channel Networks," in *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 12, pp. 3600-3614, Dec. 2022, doi: 10.1109/JSAC.2022.3213355.

[4] N. K. Chahar, K. P. Singh and M. Hussain, "Simplified Micropayment Mechanism to Eliminate the Risk of Double Payment in E-Commerce," *2023 International Conference*

on Advances in Intelligent Computing and Applications (AICAPS), Kochi, India, 2023, pp. 1-6, doi: 10.1109/AICAPS57044.2023.10074490.

[5] B. Bavarsad, Z. Azizi, M. Saghaeian and A. A. Hozhabri, "Testing the relationship between service quality, overall e-banking service quality and customer satisfaction," *2015 9th International Conference on e-Commerce in Developing Countries: With focus on e-Business (ECDC)*, Isfahan, Iran, 2015, pp. 1-9, doi: 10.1109/ECDC.2015.7156323.

[6] S. Han, K. Zhu, M. Zhou and X. Cai, "Competition-Driven Multimodal Multiobjective Optimization and Its Application to Feature Selection for Credit Card Fraud Detection," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 12, pp. 7845-7857, Dec. 2022, doi: 10.1109/TSMC.2022.3171549.

[7] H. Tingfei, C. Guangquan and H. Kuihua, "Using Variational Auto Encoding in Credit Card Fraud Detection," in *IEEE Access*, vol. 8, pp. 149841-149853, 2020, doi: 10.1109/ACCESS.2020.3015600.

[8] C. Jiang, J. Song, G. Liu, L. Zheng and W. Luan, "Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism," in *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3637-3647, Oct. 2018, doi: 10.1109/JIOT.2018.2816007.

[9] B. Can, A. G. Yavuz, E. M. Karsligil and M. A. Guvensan, "A Closer Look Into the Characteristics of Fraudulent Card Transactions," in *IEEE Access*, vol. 8, pp. 166095-166109, 2020, doi: 10.1109/ACCESS.2020.3022315.

[10] L. Zheng, G. Liu, C. Yan and C. Jiang, "Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity," in *IEEE Transactions on Computational Social Systems*, vol. 5, no. 3, pp. 796-806, Sept. 2018, doi: 10.1109/TCSS.2018.2856910.

[11] Z. Zhang, L. Chen, Q. Liu and P. Wang, "A Fraud Detection Method for Low-Frequency Transaction," in *IEEE Access*, vol. 8, pp. 25210-25220, 2020, doi: 10.1109/ACCESS.2020.2970614.

[12] S. A. A. Shah, M. Ali Masood and A. Yasin, "Dark Web: E-Commerce Information Extraction Based on Name Entity Recognition Using Bidirectional-LSTM," in *IEEE Access*, vol. 10, pp. 99633-99645, 2022, doi: 10.1109/ACCESS.2022.3206539.

[13] M. Wang, Z. Ding and P. Zhao, "Vulnerability Evaluation Method for E-Commerce Transaction Systems With Unobservable Transitions," in *IEEE Access*, vol. 8, pp. 101035-101048, 2020, doi: 10.1109/ACCESS.2020.2998132.

[14] E. A. E. Dawood, E. Elfakhrany and F. A. Maghraby, "Improve Profiling Bank Customer's Behavior Using Machine Learning," in *IEEE Access*, vol. 7, pp. 109320-109327, 2019, doi: 10.1109/ACCESS.2019.2934644.

[15] S. Makki, Z. Assaghir, Y. Taher, R. Haque, M. -S. Hacid and H. Zeineddine, "An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection," in *IEEE Access*, vol. 7, pp. 93010-93022, 2019, doi: 10.1109/ACCESS.2019.2927266.

[16] Siva Parvathi.Nelluri, Shaik. Nagul, Dr. M. Kishorekumar, "Credit Card Fraud Detection Using Hidden Markov Model", International Journal Of Engineering Research & Technology (IJERT), Volume 01, Issue 05 (July 2012), **DOI : 10.17577/IJERTV1IS5339**

[17] A. Agrawal, S. Kumar and A. K. Mishra, "Implementation of Novel Approach for Credit Card Fraud Detection," *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, 2015, pp. 1-4

[18] H. Wang, P. Zhu, X. Zou and S. Qin, "An Ensemble Learning Framework for Credit Card Fraud Detection Based on Training Set Partitioning and Clustering," *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/ IOP/SCI)*, Guangzhou, China, 2018, pp. 94-98, doi: 10.1109/SmartWorld.2018.00051.

[19] N. Nassar and G. Miller, "Method for secure credit card transaction," *2013 International Conference on Collaboration Technologies and Systems (CTS)*, San Diego, CA, USA, 2013, pp. 180-184, doi: 10.1109/CTS.2013.6567226.

[20] Z. Kazemi and H. Zarrabi, "Using deep networks for fraud detection in the credit card transactions," *2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI)*, Tehran, Iran, 2017,

pp. 0630-0633, doi: 10.1109/KBEI.2017.8324876.

[21] Z. Li, G. Liu and C. Jiang, "Deep Representation Learning With Full Center Loss for Credit Card Fraud Detection," in *IEEE Transactions on Computational Social Systems*, vol. 7, no. 2, pp. 569-579, April 2020, doi: 10.1109/TCSS.2020.2970805.

[22] A. C. Bahnsen, A. Stojanovic, D. Aouada and B. Ottersten, "Cost Sensitive Credit Card Fraud Detection Using Bayes Minimum Risk," *2013 12th International Conference on Machine Learning and Applications*, Miami, FL, USA, 2013, pp. 333-338, doi: 10.1109/ICMLA.2013.68.

[23] H. Hormozi, M. K. Akbari, E. Hormozi and M. S. Javan, "Credit cards fraud detection by negative selection algorithm on hadoop (To reduce the training time)," *The 5th Conference on Information and Knowledge Technology*, Shiraz, Iran, 2013, pp. 40-43, doi: 10.1109/IKT.2013.6620035.

[24] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi and G. Bontempi, "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy," in *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 8, pp. 3784-3797, Aug. 2018, doi: 10.1109/TNNLS.2017.2736643.

[25] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim and A. K. Nandi, "Credit Card Fraud Detection Using AdaBoost and Majority Voting," in *IEEE Access*, vol. 6, pp. 14277-14284, 2018, doi: 10.1109/ACCESS.2018.2806420.

.