Grenze International Journal of Engineering and Technology, June Issue

An Efficient Method for Credit Card Fraud Detection using Machine Learning

Ramakrishna Hegde[1], Basavaraju N.M[2], Ravi P[3], Soumyasri S M[4] and Nuthan Mourya N[5]
[1]Dept. of CSE, JSS Science and Technology University, Mysuru, India
Email: ramhegde111@gmail.com
[2]Department of ECE, JSS Academy of Technical Education (Affiliated to Visvesvaraya Technological University, Belagavi), Bengaluru, Karnataka, India
Email: basavarajunm@jssateb.ac.in
[3,5]Department of ISE, Maharaja Institute of Technology Mysore (Affiliated to Visvesvaraya Technological University, Belagavi), Mandya, Karnataka, India
Email: ravipbympr@gmail.com, nuthanmouryan2004@gmail.com
[4]Dept. of MCA, Vidya Vikas Institute of Engg. & Technology, Mysore, India
Email: drsoumyasrism@gmail.com

***Abstract*— In an era dominated by digital transactions, credit card fraud has become a pervasive threat, costing businesses billions annually. Traditional rule-based systems for fraud detection lack adaptability and struggle to keep pace with evolving fraudulent techniques. Consequently, there's a growing reliance on machine learning (ML) techniques to bolster fraud detection efforts. However, the imbalanced nature of fraud datasets, coupled with the dynamic and constantly evolving nature of fraudulent activities, presents significant challenges. This paper presents a comprehensive investigation into the efficacy of various supervised ML algorithms for credit card fraud detection. Specifically, we explore the performance of support vector machine (SVM), extreme Gradient Boosting (XGBOOST), and Adaptive Boosting (Adaboost).**

***Keywords*— Credit card, machine learning, support vector machine, extreme Gradient Boosting, Adaptive Boosting.**

I. Introduction

The surge in technological advancements and the proliferation of online transactions have significantly increased the vulnerability to credit card fraud, leading to substantial financial losses for businesses and financial institutions. As fraudulent activities continue to evolve, the urgency for effective fraud detection measures becomes paramount. In response to this pressing issue, numerous research endeavours have been undertaken to develop sophisticated fraud detection systems leveraging ML techniques.

Various ML algorithms, including Naive Bayes, SVM, ANN, Long Short-Term Memory- Recurrent Neural Network (LSTM-RNN), ensemble methods, and hybrid architectures, have been employed to address challenges such as class imbalance, categorical data handling, and model interpretability. This survey underscores the significance of feature selection techniques, uncertainty quantification methods, and the development of explainable ML models in enhancing fraud detection.

Grenze ID: 01.GIJET.12.2.446_21

It explores the utilization of genetic algorithms (GA) for feature selection, ensemble techniques for uncertainty quantification, and compares different black-box models for interpretability.
In essence, this survey encapsulates the collective efforts aimed at mitigating the adverse effects of credit card fraud through cutting-edge ML techniques. By synthesizing the findings of disparate studies, it provides insights into the current landscape of credit card fraud detection, highlights promising avenues for future research, and underscores the imperative of continuous innovation in combating fraudulent activities in online financial transactions.

II. Related Works

The paper by Roseline focuses on developing a credit card fraud detection system using machine learning techniques, particularly the Long Short-Term Memory- Recurrent Neural Network (LSTM-RNN). It addresses the challenge of class imbalance in fraud detection and proposes the use of statistical models and machine learning algorithms such as Naive Bayes, SVM, ANN, and LSTM-RNN to detect suspicious transactions. The study compares the proposed LSTM-RNN model with other classifiers and demonstrates its competitive performance. The paper also discusses the importance of understanding fraud detection technology, the challenges of dealing with categorical data, and the need for efficient fraud detection systems in the age of big data. Additionally, it outlines the structure of the paper, including related works, methodology, results, and conclusion. The proposed LSTM-RNN model is shown to outperform other methods, providing a competitive and alternative approach to existing fraud detection techniques. [1]
The paper by Palak Gupta presents a comprehensive study on credit card fraud detection using machine learning techniques, focusing on the impact of unbalanced data on the performance of classification algorithms. It discusses the experimental procedure, results, and findings, emphasizing the need for data balancing techniques to address biased outcomes. The study employs various machine learning algorithms, including Logistic Regression, Decision Tree, XGBoost, and Artificial Neural Network, to model credit card fraud detection. The findings reveal that the XGBoost classifier initially yielded biased results due to imbalanced data, prompting the implementation of data sampling techniques such as Random under Sampling, Random over Sampling, and Synthetic Minority Random Oversampling Technique (SMOTE) to balance the dataset. The results of the modified datasets show improved performance, with the XGBoost classifier demonstrating the best outcomes. The paper contributes to the field by highlighting the significance of data balancing techniques in achieving more accurate and unbiased fraud detection models, providing valuable insights for future research and development in this domain. [2]
The paper by Maryam Habibpour focuses on the application of uncertainty quantification (UQ) techniques in credit card fraud detection using deep neural networks. It addresses the challenges of fraud detection in modern e- commerce, particularly in the context of the COVID-19pandemic, which has led to an increase in online payment fraud. The study proposes and evaluates three UQ techniques
- Monte Carlo dropout, ensemble, and ensemble Monte Carlo dropout - to estimate uncertainty for transaction data. The research aims to improve the reliability and fairness of fraud detection models by quantifying uncertainty in predictions. The findings demonstrate that the ensemble method is more effective in capturing uncertainty in generated predictions. The paper also discusses the limitations of deep neural networks in fraud detection, such as overconfident predictions and the mismatch between training and test datasets, and emphasizes the importance of understanding and quantifying uncertainty in predictive models. Additionally, the document highlights the need for further research to address the challenges of fraud detection in dynamic and evolving environments and the limited number of samples available for training. [3]
The paper "Credit Card Fraud Detection Using a New Hybrid Machine Learning Architecture" investigates the development and evaluation of multiple hybrid machine learning models for detecting fraudulent activities in credit card transactions. The study focuses on the use of supervised machine learning techniques and real-world datasets to address the limitations of existing single and hybrid models in fraud detection. The research proposes and examines seven hybrid machine learning models, with the Adaboost + LGBM hybrid model identified as the champion model based on its superior performance. The study emphasizes the potential of hybrid models in improving fraud detection accuracy and lowering error rates. Additionally, the paper highlights the need for further research in exploring different types of hybridization and algorithms in the credit card fraud detection domain. The findings and methodology of the study are detailed across various sections, including model development, evaluation, results, and future work. The research contributes to the on-going efforts to enhance fraud detection methods in the financial sector, particularly in the domain of credit card fraud. [4]

The research paper "A machine learning based credit card fraud detection using the GA algorithm for feature selection" by Ileberi et al. focuses on addressing the challenges of credit card fraud detection using machine learning algorithms. The study proposes a credit card fraud detection engine that utilizes the genetic algorithm (GA) for feature selection and evaluates the performance using various supervised machine learning classifiers, including Decision Tree, Random Forest, Logistic Regression, Artificial Neural Network, and Naive Bayes. The research emphasizes the importance of feature selection in improving the accuracy of fraud detection models and highlights the challenges of highly imbalanced and confidential credit card fraud datasets. The proposed approach outperforms existing systems, achieving high accuracy scores in detecting fraudulent activities. The paper provides a comprehensive overview of the research methodology, dataset, feature selection, classifiers used, and performance metrics, demonstrating the effectiveness of the proposed machine learning-based approach for credit card fraud detection. [5]

The paper by Tanmay Srinath discusses the importance of explainable machine learning in identifying credit card defaulters, emphasizing the need for transparency and interpretability in machine learning models. It compares various black-box models, such as Support Vector Machine (SVM), Random Forest (RF), Neural Networks (NN), and XGBoost (XGB), in terms of performance metrics and provides explanations using a model-agnostic explainer called DALEX. The study concludes by proposing the XGBoost model with DALEX as the best model-explainer combo for identifying credit card defaulters, outperforming other models in terms of accuracy and specificity. The document also highlights the significance of variables such as bill amounts, paid amounts, payment delays, and personal information in predicting credit card defaulters, offering detailed insights into how different models interpret and prioritize these variables. [6]

The paper by M J Madhurya presents an in-depth exploration of credit card fraud detection using machine learning techniques, focusing on the performance, accuracy, and efficiency of various classifiers. It discusses the use of clustering and classification methods in machine learning, as well as the implementation of supervised learning techniques for fraud detection. The study compares the effectiveness of different algorithms, such as Naive Bayes, K-Nearest Neighbour, Logistic Regression, Random Forest Classifiers, and Decision Trees, in detecting fraudulent activities in credit card transactions. Additionally, the paper delves into the use of support vector machines and artificial neural networks for fraud detection. It emphasizes the importance of data analysis, pre-processing, and performance metrics in evaluating the classifiers' efficiency. The document also highlights the need for adaptive and universal data mining techniques to increase prediction accuracy and addresses the limitations and future scope of the study. Overall, the paper provides a comprehensive overview of the challenges and solutions in credit card fraud detection, emphasizing the role of machine learning algorithms and the need for continuous advancements in this domain to address the evolving nature of fraudulent activities. [7]

The research paper "Performance Evaluation of ML Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost" presents a comprehensive study on implementing ML algorithms for credit card fraud detection. The study focuses on addressing the issue of class imbalance in credit card fraud datasets and evaluates the effectiveness of various ML methods, such as SVM, Logistic Regression (LR), Random Forest (RF), XGBoost, Decision Tree (DT), and Extra Tree (ET), coupled with the Adaptive Boosting (AdaBoost) technique. The research utilizes the SMOTE to address class imbalance and evaluates the performance of the proposed framework using metrics such as accuracy, recall, precision, Matthews Correlation Coefficient (MCC), and Area under the Curve (AUC).

The study also compares the proposed methods with existing ML-based credit card fraud detection frameworks, demonstrating the superior performance of the proposed methods. Additionally, the paper provides a detailed analysis of the experimental results and discusses the impact of AdaBoost on the performance of the ML methods. Overall, the research contributes a scalable credit card fraud detection framework and validates its effectiveness on real-world and synthetic datasets. [8]. In order to promote mental wellbeing and create a safer and more positive online environment, machine learning can be a valuable tool for identifying mental health concerns and providing solutions to online toxicity[17]. This study [18]summarizes the findings from the pre-processing of each model's data, feature extraction, and model creation. The findings are then utilized to assess state-of-the-art machine learning algorithms for thoroughly recognizing URL-based and phishing attacks.

III. METHODOLOGY

A. Long Short-Term Memory

The Long Short-Term Memory technique, an advancement of Recurrent Neural Networks (RNNs), is utilized in this study to develop a deep learning intrusion detection model, offering computational efficiency and adept memory handling. Particularly suited for forecasting tasks, LSTM leverages past input parameters to predict future outputs effectively, accommodating long-term dependencies and patterns. [4] Functioning within the RNN framework, LSTM maintains an internal hidden state model through cyclic connections, incorporating a hidden Markov model extension for modeling long-term temporal dependencies via non-linear transition functions. The addition of three gated layers—forget gate, input gate, and output gate—extends LSTM's capabilities, enabling effective control over information retention, output generation, and input processing. These gated mechanisms facilitate the learning of sequence-based long-term dependencies without compromising output accuracy, enhancing the effectiveness of the recurrent hidden layer within the neural network architecture. [1]

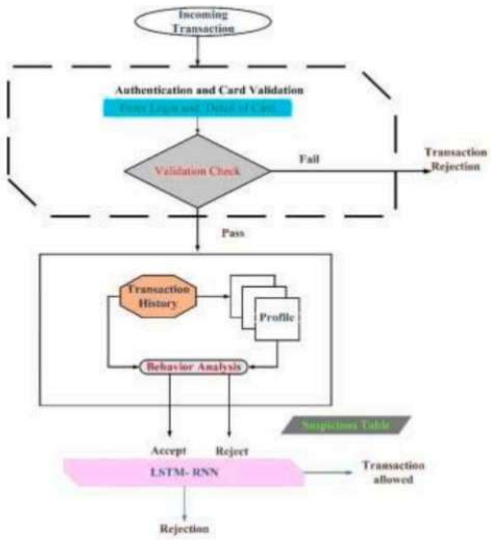

Fig 1: Credit card fraud detection using LSTM-RNN

B. XGBoost

XGBoost, an abbreviation for "Extreme Gradient Boosting," stands out as a highly favored machine learning algorithm recognized for its exceptional predictive accuracy and computational efficiency. Operating as an ensemble learning technique rooted in decision trees, XGBoost amalgamates numerous weak classifiers to form a potent classifier. [4] This algorithm has garnered widespread adoption across diverse domains spanning finance, healthcare, and natural language processing. XGBoost progressively integrates decision trees into its model while fine-tuning the weights of misclassified samples. To enhance its robustness and prevent overfitting, XGBoost incorporates regularization methods like L1 and L2 regularization. Furthermore, it leverages distributed computing systems to parallelize the training process, rendering it highly scalable and proficient in handling extensive datasets. [2]

C. SMOTE

Synthetic Minority Over-sampling Technique stands out as a potent algorithm for mitigating imbalanced class problems by rebalancing datasets through a combination of over-sampling the minority class and under-sampling the majority class [4]. This method operates by leveraging k- nearest neighbours to select neighbouring points randomly for interpolation, with a tuneable threshold ranging between 0 and 1. Unlike conventional sampling methods, SMOTE conducts sampling in feature space rather than data space, leading to more precise outcomes. The versatility of SMOTE is evidenced by its successful deployment across a myriad of application domains, including bioinformatics, fault detection, high-dimensional gene expression datasets, and video surveillance. Notable variants of SMOTE include Borderline-SMOTE, SVM-SMOTE, KMeans-SMOTE, alongside the traditional SMOTE approach. [2][8]

D. Naive Bayes

This supervised machine learning classifier is adept at forecasting future instances of the target class. Known as NB, it harnesses feature and class information within the dataset, leveraging probabilistic methods for prediction. The term "naïve" reflects its approach of treating attributes independently based on the presence or absence of the class variable, while "Bayes" signifies its calculation of class probability. Despite its simplistic mechanism, NB consistently delivers robust results across complex real- world scenarios, showcasing its effectiveness in various problem domains. [4]

E. GA Algorithm

Genetic algorithms, rooted in evolutionary principles since their inception by Holland, have demonstrated wide applicability across diverse domains such as astronomy, sports, optimization, and computer science. Their utilization extends to data mining, particularly in variable selection tasks, often integrated with other algorithms.[4] In the context of fraud detection in transactions, genetic algorithms offer a potent solution, aiming to iteratively refine solutions towards improved performance over time. By navigating complex and vast search spaces, they effectively converge towards optimal solutions, making them suitable for scenarios like black box testing where the objective is to identify optimal inputs within defined ranges, such as the boundary value testing criteria where values within the range of 0 to 8 are assessed. This underscores the adaptability and effectiveness of genetic algorithms in tackling multifaceted problems across various domains, showcasing their capacity to address challenges and enhance decision-making processes. [5]

F. Support Vector Machine

The support vector machine is a generalization of the maximal margin classifier. SVM works by using kernels to enlarge the feature space in a specific way. Most SVM models trained today use non-linear kernels. It is a robust algorithm renowned for its efficacy in addressing classification and regression challenges in supervised machine learning. It excels in scenarios where data segregation into classes isn't achievable via linear boundaries. By pinpointing crucial data points termed support vectors, SVM constructs a hyperplane that effectively separates data classes. It employs the kernel trick to elevate data dimensionality, rendering it linearly separable when conventional linear boundaries fail. This strategy enables SVM to discern optimal decision boundaries, facilitating accurate classification or regression outcomes even in complex data landscapes. [6] [9] [4]

G. Artificial Neural Networks

Artificial neural networks have evolved through inspiration from biological neural networks, with scientists continually refining their design and functionality. These networks serve to approximate functions or relationships influenced by input variables whose exact determinants are obscured. Constructed through a sequential node-by-node stacking process, ANNs interface between the feature vector and target vector layers. Emulating aspects of human brain interpretation and learning, ANNs have found widespread success across diverse models and applications, showcasing their adaptability and effectiveness in various domains. [7][4]

H. AdaBoost

Boosting, a machine learning methodology, focuses on enhancing model accuracy by amalgamating multiple simple or less accurate models. This study applies the AdaBoost algorithm alongside other machine learning techniques to enhance classification performance. AdaBoost produces a weighted sum output achieved through the aggregation of predictions from individual boosted models, thereby refining the overall predictive capability. [8]

IV. RESULT

The study by Palak gupta employed the Fraudulent Transactions Detection dataset classifies transactions as fraudulent or legitimate by giving them a binary value: 1 means fraudulent and 0 means legitimate. This dataset has 31 features and 284,807 records in total. Each row shows one transaction. The dataset includes 284,315 real transactions and 492 fake ones, which means just 0.17% of the transactions are fake [2]. Faisal Malik suggests an approach to develop and test hybrid models by comparing how well they work against several top machine learning algorithms. These algorithms include Logistic Regression (LR), Random Forest (RF), Decision Trees (DT) XGBoost, Support Vector Machines (SVM), Naive Bayes (NB), AdaBoost, and LightGBM (LGBM). He assessed these individual algorithms based on their AUROC scores to find the best candidates to create hybrid models. NB didn't work well scoring 0.56 AUROC because it assumes independence. All other single models got similar AUROC scores between 0.66 and 0.71, with AdaBoost scoring the highest at 0.71. AdaBoost worked the best, as shown by its high true positive rate (TPR) and low false positive rate (FPR) so it was picked as the starting point to make hybrid models. After that, researchers combined AdaBoost with other algorithms to make seven hybrid models. The AdaBoost + LGBM hybrid stood out in AUROC, precision, and misclassification rate becoming the top performer. This model got an AUROC score of 0.82 and a precision of 0.97, which means it

spotted positive cases 97% of the time, while keeping a decent recall rate of 0.64. Even though some hybrid models had high Type-II error rates, they cut
down on Type-I error, which matters more in catching financial fraud. This suggests that the hybrid models give a big advantage. In particular, AdaBoost + XGBoost and AdaBoost + LGBM were good at finding fraudulent activities. The AdaBoost + LGBM model had the best mix of precision, recall, and F1-measure making it the best hybrid model for the dataset in this study[4].

TABLE I: COMPARISON OF THE STATE-OF-THE-ART MACHINE LEARNING ALGORITHMS AND THE HYBRID MODELS [4]

	ROC	Recall (TPR)	Precision	F-Measure	Misclassification Rate	TNR	Type-I Error	Type-II Error
state-of-the-Art								
LR	0.70	0.71	0.08	0.14	0.30	0.68	0.31	0.28
RF	0.66	0.38	0.19	0.25	0.07	0.93	0.06	0.59
DT	0.66	0.41	0.15	0.22	0.10	0.91	0.08	0.57
XGBOOST	0.69	0.44	0.23	0.30	0.07	0.93	0.06	0.52
NB	0.56	0.97	0.04	0.08	0.81	0.15	0.84	0.03
SVM	0.70	0.62	0.09	0.16	0.23	0.74	0.25	0.35
Adaboost	0.71	0.58	0.11	0.18	0.17	0.82	0.17	0.41
LGBM	0.70	0.47	0.21	0.29	0.07	0.92	0.07	0.52
Hybrid Models								
Adaboost+LR	0.67	0.36	0.83	0.50	0.004	0.999	0.0004	0.52
Adaboost+RF	0.74	0.50	0.97	0.66	0.003	0.999	0.0004	0.33
Adaboost+DT	0.76	0.54	0.51	0.52	0.006	0.990	0.0099	0.29
Adaboost+XGBOOST	0.79	0.59	0.94	0.73	0.002	0.996	0.0031	0.31
Adaboost+NB	0.76	0.96	0.05	0.10	0.105	0.579	0.5791	0.05
Adaboost+SVM	0.58	0.18	0.91	0.30	0.005	1.0	0.0000	0.66
Adaboost+LGBM	0.82	0.64	0.97	0.77	0.002	0.998	0.0018	0.25

Ileberi and colleagues [5] carried out their experiments in two stages. The first stage involved classifying data using a set of features called F = {v1, v2, v3, v4 v5}. They trained and tested several machine learning methods for each feature vector in F. These methods included Random Forest (RF), Decision Trees (DT), Artificial Neural Networks (ANN), Naive Bayes (NB), and Logistic Regression (LR). ANN and RF reached the highest test accuracy (TAC) of 99.94% with the v1 feature vector. RF however, beat ANN in precision. RF again came out on top when using the v2 feature vector, with an accuracy of 99.93%. The story was similar with the v3 feature vector where RF spotted fraud with 99.94% accuracy. DT showed an accuracy of 99.1% and a precision of 81.17% for the v4 feature vector. But the v5 feature vector led to the best results. RF detected fraud with 99.98% accuracy and 95.34% precision. This comparison shows how well the Genetic Algorithm (GA) feature selection approach works. It also proves that the machine learning methods used in this paper perform better than others. Specifically, the GA-RF model developed in this research achieved an accuracy of 2.28% higher than the LR model which was previously developed, while the GA- DT model showed a 4.42% improvement in fraud detection accuracy over the standard DT model developed earlier. Additionally, the GA-LR model achieved an accuracy 2.41% higher than the SVM model compared to the model developed earlier, and the GA-NB model outperformed the K-Nearest Neighbors (KNN) model by 1.75% in accuracy. Notably, the GA-DT model presented in this study achieved an overall accuracy improvement of 17.23%. In terms of classification accuracy, the RF model, particularly when implemented with the v5 feature vector, proved to be the most optimal classifier, achieving a remarkable credit card fraud detection accuracy of 99.98%. [7] Indicates that the K-Nearest Neighbor (KNN) algorithm outperforms other algorithms in detecting fraudulent transactions. The KNN algorithm shows high accuracy, sensitivity, and specificity
across different folds. Logistic Regression also demonstrates high accuracy, but the KNN algorithm is identified as the better classifier for fraud detection due to its learning ability.

[1] Research shows that the K-Nearest Neighbor (KNN) algorithm has the highest accuracy for different fraud rates, with accuracy from 96.50% to 96.71%. KNN also has high sensitivity and specificity, which matter a lot in spotting fraud. The Neural Network algorithm comes next with accuracy from 95.70% to 99.30%. But its sensitivity changes a lot, which could make it hard to spot fake transactions. Logistic Regression does well too, with accuracy from 96.80% to 96.90%, but it's a bit less accurate than KNN. The Decision Tree algorithm is the least accurate of the ones tested, with accuracy from 94.03% to 94.94%.

The ensemble method is much better at quantifying uncertainty as compared to MCD and EMCD. Especially at a threshold of 0.4, the ensemble method achieved a UAcc of 0.85, against 0.82 for MCD and 0.84 for EMCD. It means that the ensemble model has some advantages in the correct identification of uncertain predictions. [3] has the finding that the method of ensembling is more robust in capturing the uncertainties corresponding to the predictions. This paper has also discussed how to set appropriately the value of the threshold as it controls the tradeoff between flagging the incorrect predictions as uncertain and keeping at a low false positive rate. In [6] four models were compared XGBoost, Support Vector Machine, Random Forest, and Neural Network. The models were evaluated using a dataset obtained from the UCI Machine Learning Laboratory with respect to accuracy, sensitivity, and specificity. Concretely, this study shows that among these four models, XGBoost performed better, since it gave an accuracy of 0.7978 as compared with the other models: SVM indicated an accuracy of 0.7916, RF of 0.7928, and NN of 0.7531. Moreover, high specificity of 0.7057 was achieved with XGBoost, making it effective at identifying the true negatives, that is, non-defaulters. They have also checked for explainability of these models using DALEX tools, and though it is reported that when used with DALEX, not only does XBoost provide accurate predictions, but with DALEX, this gives a logical chain of reasoning; it is quite robust and interpretable.

V. Conclusion

The XGBoost Classification model demonstrates impressive performance metrics with an F1-score of 0.856, precision score of 0.913, recall of 0.805, and an accuracy score of 0.99. The study delves into a thorough exploration of hybrid machine learning models tailored for credit card fraud detection, employing a two-stage approach. Initially, nine algorithms spanning from Logistic Regression to Gradient Boosting Machines were scrutinized, followed by the integration of the top three algorithms with nineteen resampling techniques. This exhaustive evaluation process, encompassing 66 models, culminated in the identification of KNN-CatBoost as the pinnacle model, showcasing superior metrics including AUC, Recall, and F1-Score compared to conventional methodologies. Additionally, the study juxtaposes traditional methods such as Naive Bayes, SVM, and ANN with a novel approach harnessing Long Short- Term Memory (LSTM) techniques. This LSTM-based model, fortified with boosting strategies, surpassed traditional methods, highlighting its prowess in detecting intricate fraud patterns amidst the complexities of big data. Thus, it presents a promising avenue for elevating fraud detection accuracy in the era of expansive data volumes.

References

[1] Roseline, J. Femila, G. B. S. R. Naidu, V. Samuthira Pandi, S. Alamelu alias Rajasree, and N. Mageswari. "Autonomous credit card fraud detection using machine learning approach." Computers and Electrical Engineering 102 (2022): 108132.

[2] Palak Gupta, Anmol Varshney, Mohammad Rafeek Khan, Rafeeq Ahmed, Mohammed Shuaib, Shadab Alam, Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques, Procedia Computer Science, Volume 218, 2023

[3] Maryam Habibpour, Hassan Gharoun, Mohammadreza Mehdipour, AmirReza Tajally, Hamzeh Asgharnezhad, Afshar Shamsi, Abbas Khosravi, Saeid Nahavandi, Uncertainty-aware credit card fraud detection using deep learning, Engineering Applications of Artificial Intelligence, Volume 123, Part A, 2023.

[4] Malik, Esraa & Khaw, Kw & Belaton, Bahari & Wong, Wai & Chew, Xinying. (2022). Credit Card Fraud Detection Using a New Hybrid Machine Learning Architecture. Mathematics.

[5] Ileberi, E., Sun, Y. & Wang, Z. A machine learning based credit card fraud detection using the GA algorithm for feature selection. J Big Data 9, 24 (2022).

[6] Tanmay Srinath, Gururaja H.S., Explainable machine learning in identifying credit card defaulters, Global Transitions Proceedings, Volume 3, Issue 1, 2022.

[7] M J Madhurya, H L Gururaj, B C Soundarya, K P Vidyashree, A B Rajendra, Exploratory analysis of credit card fraud detection using machine learning techniques, Global Transitions Proceedings, Volume 3, Issue 1, 2022.

[8] Ileberi, E., Sun, Y. and Wang, Z., 2021. Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost.

[9] Sushant Kumbhar , Ashish Lade , Abhishek Patil , Jaykishan Pandey, A. B. Ghandat, 2023, Support Vector Machine based Credit Card Fraud Detection, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 12, Issue 03 (March 2023).

[10] RB, Asha & K R, Suresh. (2021). Credit Card Fraud Detection Using Artificial Neural Network. Global Transitions Proceedings.

[11] Osegi, Emmanuel & Jumbo, E.F.(2021). Comparative analysis of credit card fraud detection in Simulated Annealing trained Artificial Neural Network and Hierarchical Temporal Memory. Machine Learning with Applications.

[12] VOICAN, Oona. (2021). Credit Card Fraud Detection using Deep Learning Techniques. Informatica Economica.

[13] R. Sailusha, V. Gnaneswar, R. Ramesh and G. R. Rao, "Credit Card Fraud Detection Using Machine Learning," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2020.

[14] Bin Sulaiman, R., Schetinin, V. & Sant, P. Review of Machine Learning Approach on Credit Card Fraud Detection. Hum-Cent Intell Syst 2, 55–68 (2022).

[15] Lucas, Yvan & Jurgovsky, Johannes. (2020). Credit card fraud detection using machine learning: A survey.

[16] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan and M. Ahmed, (2022). "Credit Card Fraud Detection Using State-of-the- Art Machine Learning and Deep Learning Algorithms".
[17] P. H K, R. Hegde, N. K. Mishra, A. Kumar Sandliya, A. Singh and S. S M, "Detection of Mental Health Issues and Solution to Online Toxicity using Machine Learning," 2023 IEEE 3rd Mysore Sub Section International Conference (MysuruCon), HASSAN, India, 2023, pp. 1-7, doi: 10.1109/MysuruCon59703.2023.10396981.
[18] S. M, R. Hegde and S. S M, "Social Engineering Threat: Phishing Detection using Machine Learning Approach," 2023 IEEE 3rd Mysore Sub Section International Conference (MysuruCon), HASSAN, India, 2023, pp. 1-7, doi:10.1109/MysuruCon59703.2023.10397016