iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** I **Month of publication:** January 2025

DOI: https://doi.org/10.22214/ijraset.2025.66733

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

A Review on Advanced Machine Learning Methods for Credit Card Fraud Detection

Shayna Bano[1], Dr. Pharindara Kumar Sharma[2]
[1]*M.Tech Scholar,* [2]*Associate Professor, Dept. of Computer Science and Engineering, Shriram College of Engineering and Management, College in Bamor, Madhya Pradesh, 476444.*

Abstract: ***This study looks at the serious problems associated with credit card theft and assesses how well machine learning methods detect and stop it. More sophisticated fraud has resulted from the rise in internet transactions, endangering both consumers and financial institutions. The growing use of credit cards necessitates the quick development of efficient fraud detection systems that can recognise and stop fraudulent transactions. This research looks at a range of machine learning methods, from more conventional ones like decision trees or logistic regression to more sophisticated ones like support vector algorithms, neural networks with artificial intelligence, randomly generated forests, and hybrid models. We analyse the advantages and disadvantages of each approach, focussing on its recall, accuracy, precision, and capacity to manage situations with unbalanced datasets. It may be possible to increase detection rates and reduce false positives by combining hybrid approaches with ensemble learning techniques. The Synthetic Minority Over-sampling Technique (SMOTE) improves the reliability of training machine learning models and successfully addresses class imbalance. This study emphasises how crucial it is to analyse data in real-time and employ state-of-the-art techniques like big data analytics and deep training in order to keep up with new fraud tactics. Industry-academia collaboration and ongoing research and development in the sector are essential for the successful deployment of fraud detection technologies. This study highlights the pressing need for cutting-edge machine learning methods to prevent credit card theft. By strengthening financial institutions' ability to identify fraud, these technical developments will protect and maintain consumer trust in online transactions. Improved fraud detection systems and a more secure economic environment for all stakeholders are the goals of the study's conclusions.***

I. INTRODUCTION

Given the volume and complexity of the ever-growing number of digital transactions, detecting credit card fraud is essential to financial security. Machine learning algorithms are crucial tools for spotting fraudulent transactions because of their capacity to evaluate enormous volumes of data and spot minute trends that point to fraud. Even though rule-based approaches frequently show limitations in their capacity to adapt to new fraudulent techniques, they have served as the foundation for the creation of fraud detection systems. However, machine learning (ML) provides a more flexible method that can improve over time by learning from past data. Credit card fraud detection systems work by using supervised learning methods and training the model with a labelled dataset that includes both fraudulent and valid transactions [1]–[3]. Decision trees, logistic regression, random forests, gradient boost computers (GBM), along with support vector machines (SVM) are all effective techniques. Researchers have occasionally examined sophisticated models, such as neural networks and deep training architectures, to see if they can understand intricate correlations in the data; in certain cases, these models frequently outperform simpler models. Since illicit transactions only make up a small portion of the whole information, the stark class discrepancy makes it extremely difficult to identify credit card fraud. This discrepancy can make it more difficult for the model to forecast successful transactions. Frequently employed in this context are specialised measures like as cost-sensitive learning, resampling, and the Area Underneath the Precision-Recall Curve (AUPRC). Unsupervised learning methods for spotting departures from typical transaction behaviour include clustering and anomaly detection systems. The isolation forest technique splits the data recursively in order to find anomalies. An alternative strategy is to use autoencoders, a kind of neural network that lowers dimensionality and identifies anomalies by identifying deviations as possible frauds and discovering typical transaction patterns. The employment of a hybrid approach that combines supervised and unsupervised techniques is also common to improve detection precision [4]–[6].

©IJRASET: All Rights are Reserved

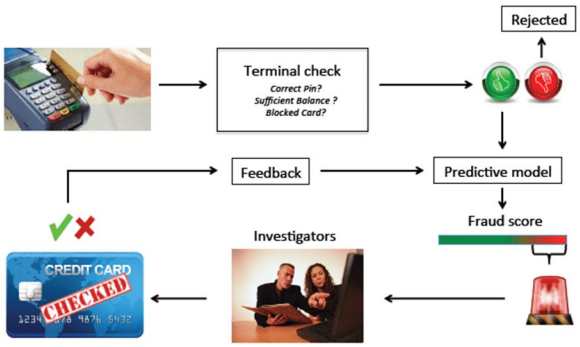


Fig. 1 Credit card fraud detection using ML [7]

Real-time detection is crucial since fraud needs to be identified and stopped before money is lost. This is especially helpful for educational systems that gradually change their model in response to new information. It is also necessary to take into account feature engineering, which uses domain-specific knowledge to develop attributes like transaction time, location, or merchant type that better detect fraud tendencies. Two feature selection techniques that aim to improve model performance and decrease dataset dimensionality are principal component analysis, or PCA, & recursive elimination of features, or RFE. Graph-based techniques, which depict transactions as nodes and their relationships as edges, make it easier to identify fraudulent patterns in networks. To hide their activity, for example, criminals may spread fraudulent transactions throughout several accounts, which the transaction system can help detect [8]–[12]. The ROC (receiver operational characteristic) curve, F1-score, precision, and memory are among the metrics commonly employed to evaluate fraud detection systems because class imbalance makes a simple accuracy statistic inadequate. Interpretability is as important as model performance for financial firms that rely on easily understood models to meet regulatory obligations. Decision-making models of explainable artificial intelligence (XAI), like SHAP (Shapley a The additive Explanations) as well as LIME (Local Comprehensible Model-agnostic Explanations), aid in preventing false positives, which occur when legitimate purchases are inadvertently labelled as fraudulent, leading to unhappy customers. Since hostile attacks occur when scammers deliberately try to trick the detection system by giving false information, handling them is equally crucial. By strengthening machine learning models against such attacks, adversarial training makes them more resilient. Machine learning-powered credit card fraud detection systems integrate feature construction, unsupervised and supervised learning, real-time detection, and model interpretability to successfully fight fraud. In the end, this is a rapidly changing profession. Maintaining financial transactions in the face of growing fraud complexity calls for robustness, real-time processing power, and ongoing model development [13], [14], [14]–[16].

II. RELATED WORK

Sorour et al. 2024 has put in place banking procedures that protect clients, maintain adherence to the law, promote reputation building, and boost financial stability. Through algorithmic change and data assimilation, machine learning (ML) enables real-time fraud detection, facilitates data analysis, and permits the development of fraudulent schemes. Feature selection (FS) is crucial in machine learning to increase fraud detection and maximise model accuracy. This is because it makes it simpler to remove the negative impacts of unnecessary and extraneous components. The researchers tried with several factors to improve the dataset's precision. However, when used on datasets with additional feature dimensions, these methods may encounter issues with local optimality. However, the researchers are working to improve the efficacy of these medicines. This research presents a workable approach to improve the accurate identification of pertinent elements in financial CCF transactions using the Brown-Bear Optimisation (BBO) algorithm. BBO can reduce dimensionality and improve classification accuracy. Binary BBOA (BBBOA) is a binary variant of this idea since unexpected positional changes improve the capacity to investigate and exploit. The suggested methodology makes use of the machine learning classifiers Xgb-tree, Support Vector Machine (SVM), and k-nearest neighbour (k-NN). The Wilcoxon's rank-sum test (α=0.05) indicates that the suggested approach is better and significantly more effective on the dataset, attaining up to 91% classification accuracy and up to 67% attribute decrease length. The suggested method outperforms its rivals in well-known datasets in a number of performance metrics, according to further research on ten benchmark datasets. Finally, utilising five benchmark datasets from the UCI collection makes it easier to validate the proposed approach. In the majority of the evaluated datasets, it outperformed its rivals on a number of performance metrics [17].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Azim et al. 2024 have increased the frequency of fraudulent purchases daily. Every year, credit card theft costs many businesses and financial institutions billions of dollars. Because dishonest activity is so common, it can be challenging to distinguish it from honest behaviour. Another factor contributing to the discrepancy is the small percentage of fraudulent transactions. Therefore, a strong fraud-detection mechanism guarantees the payment system's dependability. An increasingly helpful method for identifying this type of fraud is machine learning. Machine learning techniques have low prediction accuracy when it comes to identifying fraud, despite the fact that unequal data has decreased misclassification costs. When faced with uneven data, this paper proposes a soft voting joint learning technique to identify credit card fraud. The suggested approach is assessed and contrasted with other sophisticated sampling strategies (such as hybrid sampling, undersampling, and oversampling) in order to address the problem of class imbalance. To combat credit card fraud, we use sampling and non-sampling techniques to create a number of classifiers. The results of the experiment show that the suggested soft-voting method works better than individual classifiers. The model attains an AUROC of 0.9936, an F1-score of 0.8764, an accuracy of 0.9870, a recall of 0.9694, and a false negative rate (FNR) of 0.0 [13].

Charizanos et al. 2024 has implemented fixes for security flaws that make financial institutions vulnerable. Class disparities, full separation issues in fraud data, and the dynamic nature of crime features make it more difficult to develop real-time algorithms for detection of fraud and accurately forecast fraudulent transactions. With a new online real-time fraud detection system, this work addresses issues caused by class imbalance, complete separation, and erratic changes in transaction and fraud characteristics. We offer a novel approach to dealing with non-stationary variations in fraudulent transaction trends. The more data there is, the better the model training is. We can lessen the challenges posed by the extremely low frequency of fraudulent transactions in the data set as well as the separation problems that arise from different transaction characteristics by using a robust fuzzy logistic regression method to handle the differences in classes and separation barriers. The performance-efficiency nexus of the methodology indicates that, even with small sample sizes, the suggested framework can differentiate between fraudulent and non-fraudulent transactions with an accuracy of greater than 0.99. The correlation coefficient for Matthew is above 0.80, while the sensitivity and certainty are also above 0.90. The suggested approach shows a higher percentage of recognising transactions that are not fraudulent and improved detection efficacy when compared to machine learning and other fraud detection techniques. Better classification performance reduces losses and increases customer satisfaction by more accurately detecting fraudulent activity while avoiding incorrectly classifying legal transactions [18].

Yılmaz et al. 2024 The unpredictable and diverse tactics of scammers, who use technical advancements to get beyond security measures and cause large financial losses, put credit card transactions at serious risk. This article describes a method for identifying credit card fraud that is based on machine learning. Information normalisation, preparing the data, feature selection, and classification are the four main components of the suggested methodology. Artificial neural networks, including logistic regression, decision trees, naive Bayes, and random forests, use particle swarm optimisation for feature selection in classification. To test the suggested approach, we used a dataset of cards from all throughout Europe. The suggested approach outperforms all existing machine learning algorithms, according to experimental results, and has a high detection rate for accurately classifying fraud [19].

Detthamrong et al. 2024 the use of modern machine learning techniques to identify fraud in the financial sector. Using a large dataset of banking events, we tested a number of models, such as voting classifiers, LightGBM, which XGBoost, CatBoost, and neural networks. With its superior performance, the CatBoost model was able to detect fraudulent activity with greater accuracy. The use of different sampling and scaling techniques significantly improved the accuracy of detecting fraud, highlighting their crucial role in the procedure. Fraud detection was far more efficient thanks to the CatBoost ensemble technique. Our results demonstrate how well these cutting-edge machine-learning methods work to minimise monetary losses and guarantee safe transactions, which enhances the security and credibility of the banking sector. Future research will focus on adding real-time data, adjusting to new fraud trends, and fine-tuning the CatBoost model's hyperparameters for optimal performance. There will also be an attempt to make the model's decision-making more interpretable and a critical assessment of the model's capacity to increase confidence and broaden the scope of fraud detection techniques [20].

Table no. 1 Literature summary

Author/year	Methods	Findings	Research gap	Parameters
Zhu/2024 [21]	Neural Networks with SMOTE improve imbalanced credit card fraud	Neural Networks with SMOTE achieve better precision, recall, and F1-score.	Limited exploration of hybrid models addressing real-time fraud	Neural Networks with SMOTE significantly outperformed traditional fraud

	detection.		detection challenges.	detection models.
Aghware/2024 [22]	Random Forest with SMOTE improved fraud detection accuracy significantly over others.	Random Forest with SMOTE achieved highest accuracy, outperforming other algorithms.	Limited focus on real-time fraud detection using hybrid algorithms.	SMOTE improved Random Forest's accuracy, outperforming other machine learning models.
Tank/2024 [23]	Random Forest excels in fraud detection; Isolation Forest reduces false alarms.	Random Forest outperforms, Isolation Forest useful for minimizing false alarms.	Insufficient studies on combining multiple models for credit card fraud detection.	Random Forest showed highest performance; Isolation Forest reduced false positives.
Islam/2024 [24]	Rule-based model outperforms machine learning models in fraud detection accuracy.	Rule-based model achieves 0.99 accuracy and precision in fraud detection.	Limited exploration of rule-based models without resampling in fraud detection.	Rule-based model surpassed traditional methods, achieving 0.99 accuracy and precision.
Sani/2024 [25]	Logistic Regression applied to Kaggle data for fraud detection.	Model achieved 99.87% accuracy in detecting unseen fraudulent transactions.	Need for diverse algorithms beyond Logistic Regression for fraud detection.	Logistic Regression demonstrated high accuracy in detecting fraudulent transactions effectively.

III. IMPACT ON FINANCIAL INSTITUTIONS AND CONSUMERS

For those who create significant financial losses, mistrust, and operational challenges, credit card theft has a huge and varied impact on individuals and financial firms. Usually requiring payment to affected customers, direct financial losses from fraudulent transactions can be major for financial companies; these losses can strain resources and jeopardise profitability. Establishing sophisticated fraud detection systems, looking at claims, and adhering to regulatory standards helps to boost the financial weight. Apart from the direct financial repercussions, credit card fraud could erode customer confidence in financial services and reputation of financial companies. Those who become victims of fraud may be unwilling to make online purchases, thereby influencing the overall volume of transactions and the future expansion prospects for financial institutions. The trust component is very important; once a client's confidence is undermined, they may migrate to competitors believed to be more safe, therefore affecting long-term client retention. Credit card fraud—including illicit purchases, lost credit scores, and the labour-intensive procedure of fraud reporting and financial record corrections—may also cause considerable suffering to consumers. Those who find themselves in probable financial trouble may go through mental conflict and worry that might jeopardise their overall state of affairs. Besides, challenging false accusations can be taxing and make consumers feel helpless. Furthermore, there is more impact on society; if dishonest behaviour rises, general consumer purchasing can decrease, so hindering economic progress. Constant innovation in fraud detection and prevention defines the ongoing fight between financial institutions and criminals as both of them adjust their policies. This dynamic compels financial institutions to reconcile the need to preserve consumer confidence and loyalty with the cost of implementing strong fraud detection systems. Credit card fraud thus affects consumer behaviour as well as the bigger financial system and has far-reaching consequences going much beyond single transactions [26]–[29].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

Fig. 2 Financial institution [30]

IV. TYPES OF CREDIT CARD FRAUD

A. Card Not Present (CNP) Fraud:

The use of stolen credit card data by a fraudster for online or phone-based purchases without actually presenting the card is known as card not present (CNP) fraud Since e-commerce has expanded and helps criminals take advantage of the lack of physical validation during transactions, this form of fraud has exploded. Common techniques are phishing to gain card information, data breaches to pilfers private data, or using obtained card information bought on the dark web. Since traditional fraud detection methods could be less successful without physical card presence, CNP fraud poses serious challenges for stores and financial institutions.

B. Lost or Stolen Card Fraud:

Lost or stolen card fraud is the outcome of a credit card being physically lost or stolen from the cardholder letting unlawful users make purchases with it. This type of fraud can take numerous forms; lost or stolen card fraud results from a credit card taken without authorisation or lost, so enabling a criminal to use it illegally. Among the various ways this could happen are losing a card in public, having one snatched from a wallet, or becoming pickpocketed. Once in hand, fraudsters can make purchases—in-store and online—typically leading in significant financial losses for the victim. To help against this type of fraud, consumers should quickly report lost or stolen cards, routinely review account statements for unusual activity, and use transaction alerts from their banks. as when a card vanishes from a wallet or purse or is lost in public. Once in the hands of a thief, the card can be used for online and in-store purchases until the cardholder records it lost or stolen. To help to lower risks, consumers are recommended to routinely review their account statements, report any strange behaviour immediately, and apply transaction alerts [31]–[34].

C. Account Takeover Fraud:

Account Overhaul Usually by phishing, social engineering, or hacking, fraud comes from a fraudster acquiring illicit access to a credit card account. Once they get access, the fraudster can basically close the legal cardholder out by changing account data like passwords and contact information. This helps them build debt, make illicit purchases, or even file for victim-name new credit accounts. For victims, the impact could include stress of fraud resolution, credit score damage, and money losses. To help battle this, consumers should use secure passwords, enable two-factor authentication, and periodically review their accounts.

D. Card Skimming:

Illegal access to card data via the magnetic stripe is one type of credit card fraud frequently referred to as "card skimming." Usually found at gas stations or point-of-sale terminals, ATMs are targets for frauds using tiny, covert skimmers. The skimmer grabs card information without cardholder knowledge while a card is swiped. Then criminals might clone the card or use the information to make illegal purchases. This kind of fraud is quite advanced since it can occur without the victim aware. Consumers should regularly review their accounts and look for any unusual attachments on card readers in order to guard themselves.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

E. Application Fraud

Application fraud is the use of another name by credit card candidates using pilfers of personal information. Usually using phishing, data breaches, or social engineering techniques to get private information such Social Security numbers, addresses, and financial data, this kind of fraud usually once the fraudster has a new credit card, they can accumulate debt and make illegal purchases before the real cardholder finds out. Fallout for victims might include monetary losses and credit score deterioration. To fight this, people should guard their personal information, review their credit records, and promptly report any suspicious activity [35]–[37].

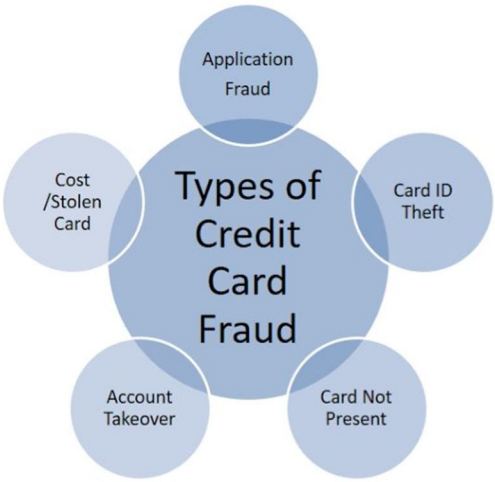


Fig. 3 Types of credit card fraud [30]

V. MACHINE LEARNING TECHNIQUES FOR FRAUD DETECTION

A. Supervised Learning Approaches

1) Logistic Regression: In binary classification, logistic regression is a statistical technique based on one or more predictor variables that projects the probability of an outcome. Using the logistic function, it generates values between 0 and 1 to show class membership and models the link between the dependent variable and independent factors.

2) Random Forests: For classification and regression problems, random forests is an ensemble learning approach. During training, it creates several decision trees and generates, for classification or regression, the average or mode of their predictions. By aggregating the strengths of individual trees, this method lowers overfitting, increases resilience, and improves accuracy.

3) Support Vector Machines: Regression and classification using supervised machine learning SVM stands for support vector machine. It divides data using the search for the best hyperplane. into multiple classes. For high-dimensional environments especially and for complex datasets with obvious margins of separation SVM is especially helpful.

4) Neural Networks: For applications including pattern recognition, regression, and classification, neural networks—computational models modelled after the human brain—are employed. Consisting of interconnected layers of nodes (neurones), they use training to modify the weights of connections in order to identify patterns in data. In big datasets, neural networks are excellent at managing intricate, non-linear interactions.

B. Unsupervised Learning Approaches

1) Clustering Techniques: Clustering methods are unsupervised learning methods employed to cluster similar data points depending on shared attributes. Common techniques consist in DBSCAN, hierarchical clustering, and K-Means. These techniques uncover natural groups inside datasets, so helping activities including market segmentation, picture analysis, and anomaly identification.

2) Anomaly Detection: Often used in quality control, cybersecurity, and fraud detection, anomaly detection searches data points that differ greatly from the norm. Techniques call for statistical methods, one-class SVM and isolated forest machine learning models, and neural networks. Finding anomalies in large datasets helps identify unusual trends, errors, or rare events.

3) Isolation Forest: Exclusion forest is an unsupervised machine learning approach meant for anomaly detection. It isolates anomalies by use of random tree structural data point splitting. This method works well for identifying outliers in large datasets since anomalies are less prevalent and easier to separate from the majority [38]–[41].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

C. Hybrid Approaches

In machine learning, hybrid methods integrate two or more algorithms or techniques to leverage their advantages and offset personal constraints. A hybrid model might combine machine learning classifiers with anomaly detection techniques like Isolation Forest and Random Forests in fraud detection. Combining the sensitivity of unsupervised methods with the prediction power of supervised learning yields more exact and strong findings. Particularly in sectors like healthcare, cybersecurity, and recommendation systems delivering superior performance, adaptability, and precision over solo algorithms, hybrid models are also employed in fields including complicated, imbalanced, or noisy datasets.

D. Ensemble Learning Techniques

Combining numerous machine learning models under ensemble learning techniques helps to improve performance, accuracy, and resilience. Combining numerous models lets ensemble methods reduce variance and error relative to single models. Key methods are bagging, in which models such as Random Forests use several decision trees trained on random subsets of data to improve stability; boosting, in which successive models are trained to correct past errors for increased precision; and stacking, in which the outputs of several models are combined. Widely used in applications including anomaly detection, classification, and regression, ensemble methods yield better results than single models [41], [42].

VI. CONCLUSION

For both customers and financial institutions, credit card theft is a serious problem that necessitates the creation of efficient detection systems in order to protect money and private data. This study examines the benefits and drawbacks of various machine learning techniques for identifying credit card fraud. Basic concepts like logistic regression and decision trees are part of traditional techniques, however high-dimensional data as well as unbalanced datasets can occasionally pose problems. Nonetheless, contemporary methods such as random forest analysis, neural networks, and support vector machines show greater accuracy and reliability in detecting fraudulent activity. By combining the advantages of multiple algorithms, hybrid methods and ensemble learning-based techniques have shown great promise in increasing detection rates and reducing false positives. Using anomaly detection methods like Isolation Forest in conjunction with conventional classifiers allows for a more thorough examination and regulation of intricate fraud patterns. Synthetic Minority Oversampling Technique (SMOTE) is a widely used method to improve machine learning model training on under-represented fraudulent events and address class imbalance. Additionally, the rapid advancement of technology and the growing complexity of fraudulent strategies necessitate constant improvement and modification of detection mechanisms. To improve fraud detection capabilities, researchers and professionals must be proactive and watchful while analysing new technologies and incorporating real-time data analysis. Continuous improvements to machine learning algorithms for credit card fraud detection are necessary to safeguard consumers and financial institutions. Future research opportunities in deep learning, natural language processing, and big data analytics are intriguing. To build a more secure and robust financial ecosystem, stakeholders may employ cutting-edge technologies and foresee new risks. In order to lessen the negative effects of credit card fraud on society, this study emphasises the necessity of cooperative research and development.

REFERENCES

[1] S. Sruthi, S. Emadaboina, and C. Jyotsna, “Enhancing Credit Card Fraud Detection with Light Gradient-Boosting Machine: An Advanced Machine Learning Approach,” 2024 Int. Conf. Knowl. Eng. Commun. Syst. ICKECS 2024, 2024, doi: 10.1109/ICKECS61492.2024.10616809.
[2] T. Xu, “Fraud Detection in Credit Risk Assessment Using Supervised Learning Algorithms,” Comput. Life, vol. 12, no. 2, pp. 30–36, 2024, doi: 10.54097/qw9j1892.
[3] D. Planinic and V. Popovic-Bugarin, “Credit Card Fraud Detection Using Supervised Learning Algorithms,” 2024 28th Int. Conf. Inf. Technol. IT 2024, vol. 9, no. 10, pp. 2–5, 2024, doi: 10.1109/IT61232.2024.10475768.
[4] I. D. Mienye and N. Jere, “Deep Learning for Credit Card Fraud Detection: A Review of Algorithms, Challenges, and Solutions,” IEEE Access, vol. 12, no. June, pp. 96893–96910, 2024, doi: 10.1109/ACCESS.2024.3426955.
[5] MD RASHED MOHAIMIN, Md Sumsuzoha, Md Amran Hossen Pabel, and Farhan Nasrullah, “Detecting Financial Fraud Using Anomaly Detection Techniques: A Comparative Study of Machine Learning Algorithms,” J. Comput. Sci. Technol. Stud., vol. 6, no. 3, pp. 01–14, 2024, doi: 10.32996/jcsts.2024.6.3.1.
[6] C. Yan, J. Wang, Y. Zou, Y. Weng, Y. Zhao, and Z. Li, “Enhancing Credit Card Fraud Detection Through Adaptive Model Optimization,” no. June, 2024, doi: 10.13140/RG.2.2.12274.52166.
[7] Y. Y. Dayyabu, D. Arumugam, and S. Balasingam, “The application of artificial intelligence techniques in credit card fraud detection: A quantitative study,” E3S Web Conf., vol. 389, 2023, doi: 10.1051/e3sconf/202338907023.
[8] G. Airlangga, “Evaluating the Efficacy of Machine Learning Models in Credit Card Fraud Detection Journal of Computer Networks , Architecture and High Performance Computing,” J. Comput. Networks, Archit. High Perform. Comput., vol. 6, no. 2, pp. 829–837, 2024.

[9] E. Rawashdeh, N. Al-Ramahi, H. Ahmad, and R. Zaghloul, "Efficient credit card fraud detection using evolutionary hybrid feature selection and random weight networks," Int. J. Data Netw. Sci., vol. 8, no. 1, pp. 463–472, 2024, doi: 10.5267/j.ijdns.2023.9.009.
[10] Md Rokibul Hasan, Md Sumon Gazi, and Nisha Gurung, "Explainable AI in Credit Card Fraud Detection: Interpretable Models and Transparent Decision-making for Enhanced Trust and Compliance in the USA," J. Comput. Sci. Technol. Stud., vol. 6, no. 2, pp. 01–12, 2024, doi: 10.32996/jcsts.2024.6.2.1.
[11] A. Qayoom et al., "A novel approach for credit card fraud transaction detection using deep reinforcement learning scheme," PeerJ Comput. Sci., vol. 10, pp. 1–21, 2024, doi: 10.7717/PEERJ-CS.1998.
[12] R. Ming, O. Abdelrahman, N. Innab, and M. H. K. Ibrahim, "Enhancing fraud detection in auto insurance and credit card transactions: a novel approach integrating CNNs and machine learning algorithms," PeerJ Comput. Sci., vol. 10, pp. 1–35, 2024, doi: 10.7717/peerj-cs.2088.
[13] M. Azim Mim, N. Majadi, and P. Mazumder, "A soft voting ensemble learning approach for credit card fraud detection," Heliyon, vol. 10, no. 3, p. e25466, 2024, doi: 10.1016/j.heliyon.2024.e25466.
[14] M. Abdul Salam, K. M. Fouad, D. L. Elbably, and S. M. Elsayed, "Federated learning model for credit card fraud detection with data balancing techniques," Neural Comput. Appl., vol. 36, no. 11, pp. 6231–6256, 2024, doi: 10.1007/s00521-023-09410-2.
[15] M. Seera, C. P. Lim, A. Kumar, L. Dhamotharan, and K. H. Tan, "An intelligent payment card fraud detection system," Ann. Oper. Res., vol. 334, no. 1–3, pp. 445–467, 2024, doi: 10.1007/s10479-021-04149-2.
[16] G. M. Paldino et al., "The role of diversity and ensemble learning in credit card fraud detection," Adv. Data Anal. Classif., vol. 18, no. 1, pp. 193–217, 2024, doi: 10.1007/s11634-022-00515-5.
[17] S. E. Sorour, K. M. AlBarrak, A. A. Abohany, and A. A. A. El-Mageed, "Credit card fraud detection using the brown bear optimization algorithm," Alexandria Eng. J., vol. 104, no. June, pp. 171–192, 2024, doi: 10.1016/j.aej.2024.06.040.
[18] G. Charizanos, H. Demirhan, and D. İçen, "An online fuzzy fraud detection framework for credit card transactions," Expert Syst. Appl., vol. 252, no. April, 2024, doi: 10.1016/j.eswa.2024.124127.
[19] A. A. Yılmaz, "A machine learning-based framework using the particle swarm optimization algorithm for credit card fraud detection," Commun. Fac. Sci. Univ. Ankara Ser. A2-A3 Phys. Sci. Eng., vol. 66, no. 1, pp. 82–94, 2024, doi: 10.33769/aupse.1361266.
[20] U. Detthamrong, W. Chansanam, T. Boongoen, and N. Iam-On, "Enhancing Fraud Detection in Banking using Advanced Machine Learning Techniques," Int. J. Econ. Financ. Issues, vol. 14, no. 5, pp. 177–184, 2024, doi: 10.32479/ijefi.16613.
[21] M. Zhu, Y. Zhang, Y. Gong, C. Xu, and Y. Xiang, "Enhancing Credit Card Fraud Detection: A Neural Network and SMOTE Integrated Approach," J. Theory Pract. Eng. Sci., vol. 4, no. 02, pp. 23–30, 2024, doi: 10.53469/jtpes.2024.04(02).04.
[22] F. O. Aghware et al., "Enhancing the Random Forest Model via Synthetic Minority Oversampling Technique for Credit-Card Fraud Detection," J. Comput. Theor. Appl., vol. 1, no. 4, pp. 407–420, 2024, doi: 10.62411/jcta.10323.
[23] E. Tank and M. Das, "On Credit Card Fraud Detection Using Machine Learning Techniques," Lect. Notes Networks Syst., vol. 966 LNNS, no. September, pp. 293–303, 2024, doi: 10.1007/978-981-97-2004-0_21.
[24] S. Islam, M. M. Haque, and A. N. M. R. Karim, "A rule-based machine learning model for financial fraud detection," Int. J. Electr. Comput. Eng., vol. 14, no. 1, pp. 759–771, 2024, doi: 10.11591/ijece.v14i1.pp759-771.
[25] A. Sani, Z. L. Hassan, and A. T. Balarabe, "A Logistic Regression-based Model for Identifying Credit Card Fraudulent Transactions," Asian J. Res. Comput. Sci., vol. 17, no. 7, pp. 41–54, 2024, doi: 10.9734/ajrcos/2024/v17i7476.
[26] A. Aslam and A. Hussain, "A Performance Analysis of Machine Learning Techniques for Credit Card Fraud Detection," J. Artif. Intell., vol. 6, no. 1, pp. 1–21, 2024, doi: 10.32604/jai.2024.047226.
[27] J. K. Afriyie et al., "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," Decis. Anal. J., vol. 6, no. January, p. 100163, 2023, doi: 10.1016/j.dajour.2023.100163.
[28] M. A. Islam, M. A. Uddin, S. Aryal, and G. Stea, "An ensemble learning approach for anomaly detection in credit card data with imbalanced and overlapped classes," J. Inf. Secur. Appl., vol. 78, no. October, p. 103618, 2023, doi: 10.1016/j.jisa.2023.103618.
[29] A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic review," J. King Saud Univ. - Comput. Inf. Sci., vol. 35, no. 1, pp. 145–174, 2023, doi: 10.1016/j.jksuci.2022.11.008.
[30] F. A. Ghaleb, F. Saeed, M. Al-Sarem, S. N. Qasem, and T. Al-Hadhrami, "Ensemble Synthesized Minority Oversampling-Based Generative Adversarial Networks and Random Forest Algorithm for Credit Card Fraud Detection," IEEE Access, vol. 11, no. July, pp. 89694–89710, 2023, doi: 10.1109/ACCESS.2023.3306621.
[31] B. A. Raphael, B. G. Adashu, and A. I. Wreford, "Card fraud detection using artificial neural network and multilayer perception algorithm," Int. J. Algorithms Des. Anal. Rev., vol. 1, no. 1, pp. 21-30p, 2023, doi: 10.37591/IJADAR.
[32] M. A. Gill, M. Quresh, A. Rasool, and M. M. Hassan, "Detection of Credit Card Fraud Through Machine Learning In Banking Industry," vol. 05, no. 01, pp. 1–10, 2023, [Online]. Available: https://doi.org/10.56979/501/2023
[33] N. R. Palakurti, "Data Visualization in Financial Crime Detection: Applications in Credit Card Fraud and Money Laundering," Int. J. Manag. Educ. …, vol. 6, no. 6, 2023, [Online]. Available: https://ijsdcs.com/index.php/IJMESD/article/view/466%0Ahttps://ijsdcs.com/index.php/IJMESD/article/download/466/186
[34] S. Al Balawi and N. Aljohani, "Credit-card Fraud Detection System using Neural Networks," Int. Arab J. Inf. Technol., vol. 20, no. 2, pp. 234–241, 2023, doi: 10.34028/iajit/20/2/10.
[35] V. R. Ganji, A. Chaparala, and R. Sajja, "Shuffled shepherd political optimization-based deep learning method for credit card fraud detection," Concurr. Comput. Pract. Exp., vol. 35, no. 10, 2023, doi: 10.1002/cpe.7666.
[36] E. Strelcenia and S. Prakoonwit, "Improving Classification Performance in Credit Card Fraud Detection by Using New Data Augmentation," AI, vol. 4, no. 1, pp. 172–198, 2023, doi: 10.3390/ai4010008.
[37] A. Malaker, A. H. Miad, F. K. Mim, W. Bin Wahid Badhan, and M. I. HOSSEN, "An Approach to Detect Credit Card Fraud Utilizing Machine Learning," Int. J. Adv. Netw. Appl., vol. 14, no. 05, pp. 5619–5625, 2023, doi: 10.35444/ijana.2023.14506.
[38] I. D. Mienye and Y. Sun, "A Machine Learning Method with Hybrid Feature Selection for Improved Credit Card Fraud Detection," Appl. Sci., vol. 13, no. 12, 2023, doi: 10.3390/app13127254.

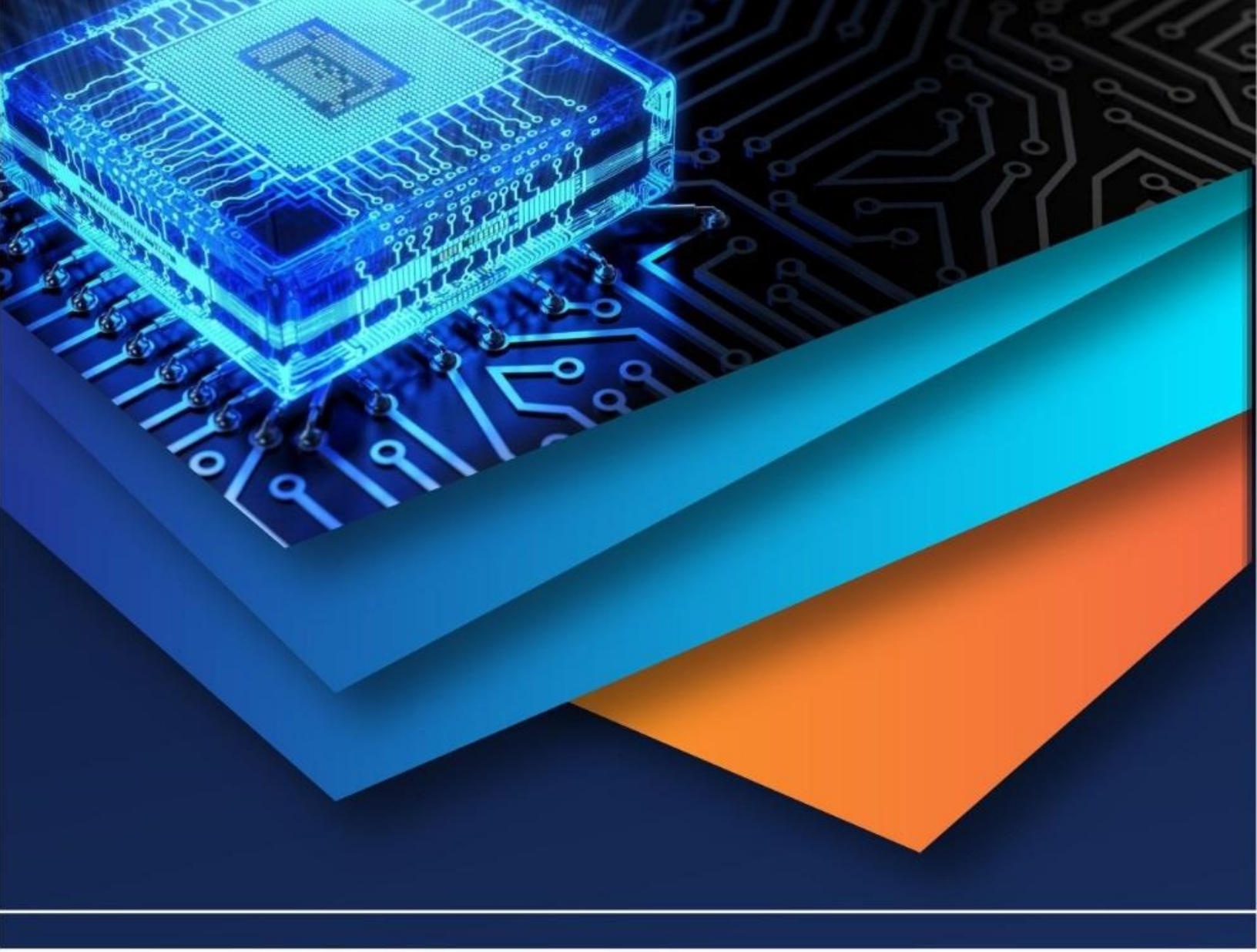
[39] J. Soni et al., "Deep Learning Approach for Detection of Fraudulent Credit Card Transactions," Intell. Syst. Ref. Libr., vol. 240, no. October, pp. 125–138, 2023, doi: 10.1007/978-3-031-28581-3_13.

[40] T. S. Anagha, A. Fathima, A. D. Naik, C. Goenka, S. B. Devamane, and A. R. Thimmapurmath, "Credit Card Fraud Detection Using Machine Learning Algorithms," Proc. - 2023 Int. Conf. Comput. Intell. Information, Secur. Commun. Appl. CIISCA 2023, vol. 8, no. 2, pp. 419–424, 2023, doi: 10.1109/CIISCA59740.2023.00085.

[41] et al., "Fraud Detection of Credit Cards Using Supervised Machine Learning Techniques," Pakistan J. Emerg. Sci. Technol., vol. 4, no. 3, pp. 38–51, 2023, doi: 10.58619/pjest.v4i3.114.

[42] R. Van Belle, B. Baesens, and J. De Weerdt, "CATCHM: A novel network-based credit card fraud detection method using node representation learning," Decis. Support Syst., vol. 164, 2023, doi: 10.1016/j.dss.2022.113866.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)