iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IX **Month of publication:** September 2026

DOI: https://doi.org/10.22214/ijraset.2026.84927

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 14 Issue IX Sep 2026- Available at www.ijraset.com

Modeling Imbalanced Financial Transactions for Credit Card Fraud Detection Using Machine Learning and Deep Learning Techniques

Mansi Sharma[1], Amandeep Verma[2], Rajni Sobti[3]
[1, 2, 3]*Department of Information Technology University Institute of Engineering and Technology Panjab University* Chandigarh, India

Abstract: ***As the growth of electronic commerce and digital payment systems is increasing at a rapid pace, the menace of credit card fraud has surfaced as a highly advanced global threat with a huge financial loss of billions of dollars on a yearly basis. The conventional fraud detection systems using traditional rule-based systems or conventional machine learning techniques have become inadequate in dealing with the huge volume, velocity, and complex nonlinear characteristics of the transactions. This review aims at presenting a comprehensive review of the advanced techniques in the field of credit card fraud detection with special emphasis on the evolution of advanced deep learning techniques from conventional machine learning techniques in the time frame of 2023-2025. It highlights a critical review of conventional machine learning techniques such as Random Forest and Support Vector Machines with advanced deep learning techniques such as Convolutional Neural Network and Long Short-Term Memory networks. This demonstrates that the results of these individual models face difficulties in handling issues like class imbalance and the need for intensive feature engineering. On the other hand, recent hybrid models, such as the Deep Hybrid CLST model, have shown promising results in handling the problem of detecting financial fraud by integrating spatial feature learning and temporal sequence learning. Furthermore, the review has shown the increasing trend of data silos in the industry due to the enforcement of privacy policies and has introduced Federated Learning and Graph Neural Networks as possible solutions for collaborative learning in the detection of financial fraud. Lastly, the review has shown the difficulties in handling the problem of detecting financial fraud, including the interpretability of the model and scalability in real-time, and has shown the possible future direction of developing stronger and more efficient financial fraud detection systems by focusing on Explainable AI and distributed computing frameworks.***

Index Terms: Credit Card Fraud Detection, Deep Learning, Hybrid Models, Federated Learning, Graph Neural Networks, Class Imbalance

I. INTRODUCTION

In the 21st century, internet has become the integral part of our life. 59 % comment of the global populations were the active users of internet as of October 2020. That means the number of active users were 4.66 billion almost and this number is increasing rapidly. In 2020 we also saw the rapid use of internet on every sector of works. During the situation of Covid-19 people rely more on internet. So, with the increasing of the use of internet the rate of cyber-attack is also increasing. There were 80,000 cyber-attacks per day in 2018. According to 2020 Verizon Data Breach Investigations Report - 67% of data breaches for social engineering attack like phishing or email phishing attack [1]. Thus, information security is a crucial matter in everyone's daily life. Also, many organizations are interested in using technology services for working more efficiently, issue of protected information from risk must be concerned[2], [3]. Modern transactions happen through different channels, included international Card-Not-Present (CNP) transactions, online payment in various e-commerce platforms where no need of physical cards [4]. The Economic impact is intense; credit card fraud losses have escalated worldwide. For instance, the Nilson Report estimated these losses at roughly USD 31 billion in 2020. Likewise, a 2025 Reserve Bank of India report shows that total fraud across all categories in India had jumped sharply, reaching approximately Rs. 36,014 crore in FY 2024–25. These figures accelerating threat of digital financial fraud and highlight the urgent need for more sophisticated detection mechanism. Decision Trees and Random Forest were popular in this domain. These were able to improve the detection capabilities to a certain extent. However, these models have their own drawbacks as well. For instance, these models often do not perform well on imbalanced data sets, where the number of fraudulent transactions is relatively low[5][6].

To enhance pre-dictive capability Ileberi et al., later explored methods such as genetic algorithm–driven feature selection[7], however, these approaches often struggle to remain efficient as transaction volumes grows. More recent work in 2024, particularly studies leveraging distributed environments like PySpark, suggests that although models such as Random Forest and XGBoost deliver strong classification performance, maintaining real-time scalability across large-scale datasets remains a notable challenge[8]. The Nilson Report states that global credit card fraud losses hit USD 31 billion in 2020 and are expected to rise due to the increasing complexity of these kinds of scams [9]. The adoption of machine learning techniques that can learn discriminative patterns from data instead of depending on static rules was spurred by these difficulties [10].Machine Learning (ML) is a sub-field of Artificial Intelligence (AI) that allows computers to learn from previous experience (data) and to improve on their predictive abilities without explicitly being programmed to do so. Machine Learning (ML) methods for credit card fraud detection defined as a fraudulent transaction that is made using a credit or debit card by an unauthorized user. According to the Federal Trade Commission (FTC), there were about 1579 data breaches amounting to 179 million data points whereby credit card fraud activities were the most prevalent [11]. Concurrently, the sequential character of transaction behavior has inspired the application of long short-term memory (LSTM) models and recurrent neural networks (RNNs).Where the patterns in user behavior are informative, sequence models have always had a strong advantage over static classifiers. Jurgovsky et al. [12]redefined credit card fraud detection as a sequence classification problem and found that LSTM-based architectures produce better results in such scenarios. This has been followed up by further research, which has found that hybrid architectures that incorporate spatial feature extractors (such as CNNs) and LSTMs for modeling temporal patterns report higher accuracy than single networks [13]. and ensemble methods that combine LSTM and GRU cells with resampling strategies (such as SMOTE-ENN) improve detection accuracy and resistance to noise [14] More recent survey articles (2025) also reflect a paradigm shift in the literature from basic neural networks to more advanced Transformer architectures, which provide improved ability to model long-range dependencies in transaction sequences [15].At the same time, relational and graph-based approaches have moved to replace flat feature-based models in an in-creasing number of studies. Graph Neural Networks (GNNs) allow for the direct modeling of relations between entities such as cardholders, merchants, devices, and geolocations, thus revealing relational patterns that are not possible to discern in flat models. It is worth noting that a significant improvement in performance was achieved in 2024 using an encoder-decoder GNN architecture on large graphs of transactions, thus underlining the importance of relational modeling in fraud analysis [16]. Deep learning models can easily learn complex and non-linear transaction patterns. Several studies reported that neural networks outperform traditional machine learning models when large and high-dimensional datasets are used. However, these models often require more computational resources and lack interpretability, which can be a challenge for real-time fraud detection systems[7]. Finally, to address the critical need for collaborative detection without compromising user privacy, Federated Learning (FL) has emerged as a dominant trend. The FinGraphFL framework [17], integrates GNNs with federated learning, allowing multiple institutions to train a shared fraud detection model without ever exposing raw customer data. This paper is organized as follow: Section 2 presents the related work. Section 3 discusses the challenges in credit card fraud detection. Section 4 describes machine learning techniques for credit card fraud detection. Section 4 deep learning techniques for credit card fraud detection. Finally, the conclusion is presented in the section 6.

II. RELATED WORK

Research in the field of credit card/financial fraud detection using credit card data has progressed over the course of a few years, and this field can be divided into a handful of major di-rections, which are related to early statistical approaches, clas-sical machine learning, and recent deep learning and graph-based ones. These directions are related to the gradual shift in this field from a more rule-based approach to a data-driven one. In the early stages, this field was focused on statistical analysis, along with surveys that laid the groundwork for this field. In this regard, research by Bolton and Hand [2]described fraud detection in terms of anomaly detection and supervised learning, along with an emphasis on issues such as class imbalance and changes in data patterns over time. In the early stages, this field was focused on statistical analysis, along with surveys that laid the groundwork for this field. However, as the research progressed, there has been a significant shift towards the use of classical machine learning models, especially when features are well designed. In fact, there are many instances where the accuracy of the system has been improved not only by the choice of the model, but also the quality of the input data. Features like transaction history, patterns, and statistics have been found to significantly contribute to the accuracy of the system [4], [2]. Fraudulent transaction detection is a major challenge, especially because there is a huge imbalance between the number of legitimate and fraudulent transactions. Since the number of fraudulent transactions is less, the system can easily get biased towards legitimate transactions.

Ripa et al. [1] examine machine-learning approaches for detecting phishing attacks and demonstrating how feature choice and pre-processing are effectiveness in adversarial settings. At the same time, relational and graph-based approaches have moved to replace flat feature-based models in an increasing number of studies. Graph Neural Networks (GNNs) allow for the direct modeling of relations between entities such as cardholders, merchants, devices, and geolocations, thus revealing relational patterns that are not possible to discern in flat models. It is worth noting that a significant improvement in performance was achieved in 2024 using an encoder-decoder GNN archi-tecture on large graphs of transactions, thus underlining the importance of relational modeling in fraud analysis [5]. A common problem in these are strong class imbalance, many experimental comparisons have evaluated the use of undersam-pling, oversampling and cost-sensitive learning to counter it. Makki et al. [9] offer a thorough empirical comparison of these methods, showing that the resampling approach significantly affects the precision-recall trade-off and that hybrid methods can achieve more stable recall with less precision loss. In practice, resampling is often accompanied by score calibration methods to compensate for the bias caused by changes in class priors and to provide more accurate risk estimates [8], [6]. Feature selection and optimization techniques continue to play an important role in improving performance as well as efficiency. The work of Ileberi et al. [10] illustrates the use of Genetic Algorithms to select small sets of features that improve the accuracy of classifiers on noisy high-dimensional transaction data [9], [12]. Other techniques such as SVM-RFE and recursive feature elimination have been shown to improve the efficiency of training and the interpretability of results, where operationalization and regulatory compliance are major factor [6], [9]. However, in the recent past, a notable trend has been the use of deep learning models, which have the ability to automatically learn complex patterns from the data. In this case, the use of Recurrent Neural Networks, such as the Long Short-Term Memory and Gated Recurrent Unit, has been explored in relation to the sequence of transactions. In addition, the use of hybrid and ensemble methods, which involves the use of a combination of various deep learning methods and the use of resampling, has also been found to be effective in the experimental research [10]. Autoencoder-based [19] representation learning, often followed by supervised classification, has been demonstrated to outperform traditional dimensionality-reduction methods in many settings, making it a common choice for unsupervised pretraining or anomaly scoring Graph and relational models represent an important, emerging direction for capturing coordinated attacks and multi-entity fraud.

III. CHALLENGES IN CREDIT CARD FRAUD DETECTION

Despite the recent advancements, the problem of detecting fraudulent activities still poses a challenge. The majority of the problems stem directly from the nature of financial transaction data, which is highly imbalanced, dynamic, and often difficult to access.

A. Class Imbalance

The problem of class imbalance is one of the most critical problems faced during the process of detecting fraudulent activities. The percentage of fraudulent transactions in any financial transaction data set is extremely low, i.e., less than 0.5%. The majority of the models perform best for the majority class, thus achieving a higher accuracy rate but failing to detect actual fraudulent activities, As discussed in previous studies, the accuracy of the models, along with ROC-AUC, often creates a false impression of performance if the minority class is not well represented [10]. For this purpose, other evaluation metrics, i.e., precision recall curves, F1 score, Matthews correlation coefficient[14], [20] are often preferred.

B. Real-Time Detection and Computational Scalability

A fraud detection system is expected to handle a large num-ber of transactions in real-time [14]. This brings up an impor-tant trade-off between accuracy and efficiency. Sophisticated models, including deep learning ensembles and Graph Neural Networks, have been shown to deliver high accuracy. However, they are [16]often computationally expensive and difficult to deploy.recent research has indicated that distributed computing environments, including PySpark[8], can help address this issue by increasing efficiency. The ability to deliver results at high speed is as important as delivering high accuracy in a practical scenario.

C. Concept Drift and Evolving Attack Patterns

It has been observed that the nature of fraud behavior does not remain static. Attackers are constantly changing their methods of operation in an attempt to evade detection tools, and this phenomenon is referred to as concept drift. It has been suggested in a number of studies that, in order to effectively handle this problem, adaptive methods may be employed, and this has been shown to be effective in ensuring the efficacy of the model [9].

IV. MACHINE LEARNING TECHNIQUES FOR CREDIT CARD FRAUD DETECTION

A. *Traditional Machine Learning Algorithms*

1) *Support Vector Machines (SVM):* Support Vector Ma-chines are often used as a baseline method for solving the problem of detecting fraudulent transactions. The basic idea behind this method is to find a hyperplane that separates fraudulent from normal transactions. The advantage of this method lies in the fact that the data often has a large number of features, which makes this method effective. However, the disadvantage of this method lies in the fact that the model becomes slow and heavy as the data becomes large. As a result, many studies suggest that the number of features should be reduced to make the model easier to manage by Ngai et al [3].

2) *Genetic Algorithms (GA) for Feature Selection:* Genetic Algorithms (GA) for Feature Selection Feature selection has also gained a lot of research interest. Genetic Algorithm, for example, is often used to select a subset of useful features. Instead of considering everything, the model only concentrates on the most relevant features of the transactions. Not only does this help to remove noise, but it also improves the training process slightly [7].

B. *Ensemble Learning Methods*

1) *Random Forest:* An ensemble is a collection of multiple models, and the idea is to use these combined models to achieve a higher level of performance. One of the most common examples is the Random Forest algorithm. This algorithm is composed of a number of decision trees, and the combination is more stable and less susceptible to overfitting than a single decision tree. It is also more robust in handling variations in the dataset. It is also effective in dealing with large numbers of transactions, especially when distributed systems are used, although some tuning is still required [8].

TABLE I
CHALLENGES AND PROPOSED SOLUTIONS IN FRAUD DETECTION SYSTEMS

Ref	Category	Challenge	Description	Proposed Solution in Literature
[9], [11]	Data Quality	Class Imbalance	Fraud transactions are extremely rare, caus-ing models to favor majority classes and miss fraud cases.	• Resampling techniques such as SMOTE and Deep En-sembles with resampling [11]. • Cost-sensitive learning penalizing missed fraud cases more heavily [9].
[2], [12]	Data Quality	Verification Latency	Fraud labels are delayed, forcing models to train on outdated labels.	• Anomaly detection using unsupervised statistical methods [2]. • Continuous learning systems updating incrementally as labels arrive [12].
[7], [12]	Operational	Real-Time Scalability	Deep learning models such as GNN and LSTM are computationally expensive for real-time deployment.	• Distributed frameworks using PySpark clusters for parallel processing [7]. • Big data analytics using Hadoop ecosystems with XGBoost and Random Forest [7].
[6], [14]	Operational	False Positive Fatigue	High false positive rates block legitimate customers and reduce user satisfaction.	• Hybrid models such as CLST improving precision using spatial and temporal features [14]. • Pipeline op-timization through threshold tuning to reduce customer friction [6].
[1], [8]	Model	Concept Drift	Fraudsters continuously change attack pat-terns, making static models ineffective.	• Deep learning methods such as RNNs and LSTMs adapting to behavioral changes [8]. • Integration of phishing URL intelligence into fraud detection engines [1].
[10], [14]	Model	Feature Bottleneck	Manual feature engineering requires domain expertise and may miss hidden patterns.	• Genetic Algorithms for automated feature selection [10]. • CNN-based feature learning from raw transac-tion data [14].
[15]	Model	Cold Start Problem	New users or merchants lack transaction his-tory, reducing detection effectiveness.	• Graph Neural Networks analyzing interaction net-works rather than historical data [15].
[13]	Ethical/Legal	Data Privacy (Silos)	Regulations such as GDPR prevent institu-tions from sharing sensitive customer data.	• Federated Learning frameworks such as FinGraphFL enabling encrypted collaborative learning [13].
[14]	Ethical/Legal	Explainability	Advanced hybrid models lack interpretability, making regulatory explanations difficult.	• Current research prioritizes accuracy while identifying Explainable AI (XAI) as an important future direction [14].

2) *Logistic regression:* Logistic Regression algorithm and this is still a powerful algorithm. It is simple, quick, and easy to understand, and these are important considerations in a financial system. It is not effective in dealing with complex nonlinear relationships, but it is still useful as a comparison tool in some instances [5].

V. DEEP LEARNING TECHNIQUES FOR CREDIT CARD FRAUD DETECTION

A. *Convolutional Neural Networks (CNN)*

Although initially developed for image processing tasks, Convolutional Neural Networks have found application in credit card fraud detection, particularly when the data is structured. Such models have shown promising results, as studies indicate that CNNs could learn from the data without the need to manually specify features. However, one of the drawbacks of CNNs is that they cannot capture the evolution of transactions, which might be a problem in credit card fraud detection[9].

B. *Long Short-Term Memory (LSTM)*

While Long Short-Term Memory models are primarily de-signed to work with sequential data, they have shown promis-ing results in credit card fraud detection, where the behavior of users evolves over a period. Unlike other models, which try to learn from a single transaction, LSTM models learn from a sequence of transactions, which makes them highly effective in detecting fraudulent transactions. The ability of LSTM models to learn from a sequence of transactions makes them highly effective in detecting fraudulent transactions [14].

C. *Graph Neural Networks (GNN)*

A new perspective has been introduced with Graph Neu-ral Networks, which focus on relationships between users, merchants, and devices. Instead of analyzing transactions individually, GNNs analyze relationships between them. Such an approach enables the detection of coordinated fraudulent activities, i.e., fraud rings, which cannot be detected through conventional models. Recent studies have shown that graph-based models improve the performance of fraud detection systems.Graph Neural Networks bring a relational view to the task by modeling interactions between entities such as cardholders, merchants, and devices. Cherif et al. (2024) developed an encoder-decoder GNN architecture to model transaction ecosystems as graphs, facilitating the detection of fraudulent activities that could be hidden from transaction-level models, such as fraud rings [16].

VI. CONCLUSION

This review demonstrates the evolution of the detection of credit card fraud using machine learning techniques. Previ-ously, statistical approaches and basic machine learning tech-niques were used. Although these techniques are still valid in some cases, especially when interpretability and efficiency are key factors in the approach. However, more recent approaches have focused on the use of deep learning and the combination of machine learning techniques in the detection of fraud. The combination of these techniques has shown a significant improvement in the performance of the systems. Despite the improvements in the detection of fraud using machine learning techniques, there is a gap between the results of the

TABLE II
MACHINE LEARNING TECHNIQUES USED IN FRAUD DETECTION STUDIES

Reference	ML Technique Used	Dataset	Key Challenges Addressed	Remarks
[1]	ML Classifiers	Phishing and Transaction Data	Evolving attack patterns	Extended machine learning techniques to phishing-based fraud detection.
[3]	Data Mining Review	Literature Survey	Classification framework	Foundational review identifying stan-dard data mining stages in fraud detec-tion.
[4]	Statistical Methods	Literature Survey	Unsupervised detection	Early baseline study establishing statis-tical anomaly detection methods.
[5], [6]	LR, RF, SVM	Kaggle Credit Card Dataset	Generalization and class imbalance	Empirical benchmarking of traditional machine learning methods.
[6]	Rule-Based + ML Pipeline	Credit Card Datasets	Real-time detection	Implementation-focused fraud detection pipeline.
[10]	RF, SVM, DT with Sampling	Europea Credit Card n Dataset	Severe class imbalance	Benchmark study addressing imbalance problems in fraud detection.
[7]	GA-Based Feature Selection	Europea Credit Card n Dataset	High dimensionality	Optimized feature subset selection using Genetic Algorithms.

TABLE III
DEEP LEARNING TECHNIQUES USED IN FRAUD DETECTION STUDIES

Ref.	Year	DL Technique Used	Dataset	Key Challenges Addressed	Accuracy / Performance
[14]	2025	Deep Hybrid CLST (CNN + LSTM)	European Credit Card	Capturing both transaction details (spatial) and user history (temporal).	Accuracy: 99.95%
[17]	2025	Federated Transfer Learning	Heterogeneous Data	Handling Non-IID data and enabling knowl-edge transfer between banks.	High cross-domain robustness
[13]	2025	FinGraphFL (Federated Learn-ing + GNN)	Partitioned Financ ial Data	Privacy-preserving collaborative learning without sharing raw data.	Accuracy: 99%
[8]	2025	DL Survey (CNN, RNN, Au-toencoders)	Multiple Benchmarks	Review of the transition from traditional ML to advanced DL architectures.	Accuracy: 99.2%
[12]	2025	Systematic Review (Transform-ers/DL)	Literature Review	Analysis of Transformer and attention-based fraud detection trends.	ROC-AUC: 0.9733, F1: 76%
[15]	2024	Encoder–Decoder GNN	Real Transaction Graphs	Detecting coordinated fraud rings using graph relationships.	Significant improvement over static ML
[11]	2023	Deep Learning Ensemble (Stacked Autoencoder)	European Credit Card	Addressing class imbalance using resampling and deep ensembles.	Accuracy: 98.0%, High sensi-tivity
[9]	2019	Experimental DL/ML (Resam-pling + Classifiers)	European Credit Card	Benchmarking SMOTE and cost-sensitive learning methods.	Recall varied by sampling method

research and the practical application of the systems. There is a problem with the interpretability of the results of the systems. Future work should be focus on developing efficient, scalable detection using advanced Transformers based architectures, Graph based learning and AI techniques. Transformer models, due to their ability to capture long range transaction they can improve the accuracy and detections in the system.

REFERENCES

[1] S. P. Ripa, F. Islam, and M. Arifuzzaman, "The emergence threat of phishing attack and the detection techniques using machine learning models," in 2021 International Conference on Automa-tion, Control and Mechatronics for Industry 4.0 (ACMI), Insti-tute of Electrical and Electronics Engineers Inc., Jul. 2021, doi: 10.1109/ACMI53878.2021.9528204.
[2] R. J. Bolton and D. J. Hand, "Statistical Fraud Detection: A Review," 2002.
[3] E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," Decision Support Sys-tems, vol. 50, no. 3, pp. 559–569, 2011, doi: 10.1016/j.dss.2010.08.006.
[4] "A Comprehensive Survey of Data Mining-based Fraud Detection Re-search."
[5] R. Qi, "An Empirical Study on Credit Risk Assessment Using Machine Learning: Evidence from the Kaggle Credit Card Fraud Detection Dataset," Journal of Computer, Signal, and System Research, vol. 2, no. 5, p. 48, 2025, doi: 10.71222/7mn4wp34.
[6] B. Mehar Sri Satya Teja, B. Munendra, and S. Gokulkrishnan, "A Research Paper on Credit Card Fraud Detection," International Research Journal of Engineering and Technology, 2022.
[7] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," Journal of Big Data, vol. 9, no. 1, Dec. 2022, doi: 10.1186/s40537-022-00573-8.
[8] L. Theodorakopoulos, A. Theodoropoulou, F. Zakka, and C. Halkiopou-los, "Credit Card Fraud Detection with Machine Learning and Big Data Analytics: A PySpark Framework Implementation," Jul. 2024, doi: 10.20944/preprints202407.0022.v1.
[9] R. Jayalakshmi, R. G. Suresh Kumar, and T. Thanushree, "A Survey on Credit Card Fraud Detection using Deep Learning Model," International Research Journal on Advanced Engineering and Management, vol. 3, no. 4, pp. 1325–1334, Apr. 2025, doi: 10.47392/irjaem.2025.0216.

[10] 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," IEEE Access, vol. 7, pp. 93010–93022, 2019, doi: 10.1109/ACCESS.2019.2927266.

[11] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," Journal of Big Data, vol. 9, no. 1, Dec. 2022, doi: 10.1186/s40537-022-00573-8.

[12] J. Jurgovsky et al., "Sequence classification for credit-card fraud de-tection," Expert Systems with Applications, vol. 100, pp. 234–245, Jun. 2018, doi: 10.1016/j.eswa.2018.01.037.

[13] M. Jabeen, S. Ramzan, A. Raza, N. L. Fitriyani, M. Syafrudin, and S. W. Lee, "Enhanced Credit Card Fraud Detection Using Deep Hy-brid CLST Model," Mathematics, vol. 13, no. 12, Jun. 2025, doi: 10.3390/math13121950.

[14] I. D. Mienye and Y. Sun, "A Deep Learning Ensemble With Data Resampling for Credit Card Fraud Detection," IEEE Access, vol. 11, pp. 30628–30638, 2023, doi: 10.1109/ACCESS.2023.3262020.

[15] Y. Chen, C. Zhao, Y. Xu, C. Nie, and Y. Zhang, "Year-over-Year Developments in Financial Fraud Detection via Deep Learning: A Systematic Literature Review," Jul. 2025.

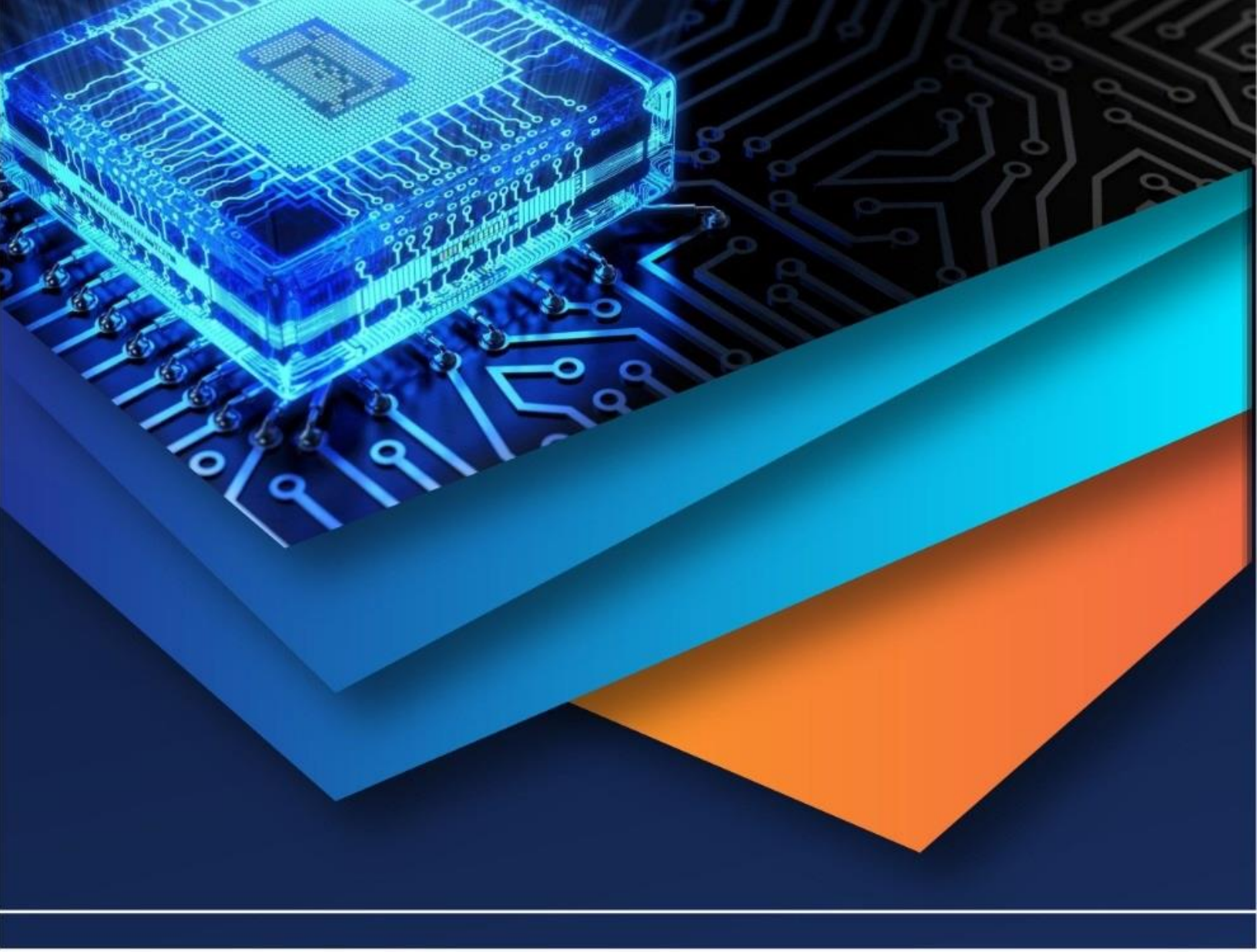
[16] A. Cherif, H. Ammar, M. Kalkatawi, S. Alshehri, and A. Imine, "Encoder–decoder graph neural network for credit card fraud detection," Journal of King Saud University - Computer and Information Sciences, vol. 36, no. 3, Mar. 2024, doi: 10.1016/j.jksuci.2024.102003.

[17] Z. Xia and S. C. Saha, "FinGraphFL: Financial Graph-Based Federated Learning for Enhanced Credit Card Fraud Detection," Mathematics, vol. 13, no. 9, May 2025, doi: 10.3390/math13091396.

[18] Y. Chen, K. Zhang, H. Zhu, and Z. Qiu, "A Novel Federated Transfer Learning Framework for Credit Card Fraud Detection Under Hetero-geneous Data Conditions," Risks, vol. 13, no. 11, Nov. 2025, doi: 10.3390/risks13110208.

[19] M. T. Singh, R. K. Prasad, G. R. Michael, N. K. Kaphungkui, and N. H. Singh, "Heterogeneous Graph Auto-Encoder for Credit Card Fraud Detection," Oct. 2024.

[20] I. D. Mienye and N. Jere, "Deep Learning for Credit Card Fraud Detec-tion: A Review of Algorithms, Challenges, and Solutions," IEEE Access, vol. 12, pp. 96893–96910, 2024, doi: 10.1109/ACCESS.2024.3426955.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY