www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 06, June 2025, pp : 175-181

e-ISSN : 2583-1062
Impact Factor : 7.001

CREDIT CARD FRAUD DETECTION USING MACHINE LEARNING TECHNIQUES

Neeru Ahuja[1], Mandeep[2]

[1]Assistant Professor, DCSE CDLU Sirsa

[2]Student, DCSE CDLU Sirsa

Corresponding Email: neeru902@gmail.com

DOI: https://www.doi.org/10.58257/IJPREMS41819

ABSTRACT

The exponential growth of digital financial transactions has significantly increased the risk of online payment fraud, posing major challenges to the integrity and security of e-commerce systems. This research addresses the problem by exploring and evaluating deep learning models for the detection of fraudulent transactions. The study utilizes a large, real-world Kaggle dataset of online payments and applies advanced data pre-processing techniques to manage class imbalance and ensure data quality.

Three deep learning models Feedforward Neural Networks (FNN), Long Short-Term Memory (LSTM) networks, and Auto Encoders are implemented and evaluated using performance metrics such as accuracy, precision, recall and Mean Absolute Error (MAE). The FNN achieved the highest accuracy of 99.41%, followed closely by LSTM with 99.37%, while the Auto Encoder, though less accurate at 85.20%, demonstrated potential for unsupervised anomaly detection. The results reveal that supervised learning models (FNN and LSTM) outperform unsupervised models in binary fraud classification, with FNN proving most effective for real-time transaction analysis.

Keywords:-Feedforward Neural Networks (FNN), Long Short-Term Memory (LSTM) networks, Auto Encoders, accuracy, and Mean Absolute Error (MAE).

1. INTRODUCTION

Online fraud refers to illegal activities conducted through internet-based payment systems. With the rise of electronic payments since the 1990s, especially due to the growth of e-commerce, digital transactions have become common and convenient. However, this convenience has also made online platforms vulnerable to various forms of fraud. The increase in online fraud is mainly due to the ease of use, global access, fast transactions, and security gaps despite encryption and authentication technologies.[1]

There are several common types of online fraud. Advance payment fraud involves tricking users into paying upfront for goods or services they never receive[3]. Phishing uses fake emails or SMS to steal personal or financial information[4]. Online auction fraud occurs when sellers on auction sites either don't deliver items or misrepresent them[5]. Investment fraud persuades users to invest in fake businesses or stocks[8]. Identity theft includes using someone else's personal data to perform illegal actions, such as account takeovers or synthetic identity creation[8]. Card testing involves small test transactions on stolen cards before making big purchases. Clean fraud uses real stolen data to make purchases that seem legitimate, while chargeback fraud involves falsely claiming refunds after receiving goods[8]

Other types include triangulation fraud, where fake online shops collect card details,formjacking, which steals data through malicious code on payment pages; payment fraud, involving unauthorized card use; and interception fraud, where fraudsters reroute packages to steal them. These frauds continue to evolve with technology, posing serious challenges to online security and trust.

2. LITERATURE REVIEW

In her paper, Kanika studied fraud detection in online transactions by implementing various machine learning and deep learning techniques, including KNN, linear regression, decision trees, LightGBM, and random forests. She also examined the relationship between the decision threshold and the level of class imbalance. The proposed fraud detection system based on deep learning was found to be more efficient than the other machine learning techniques [2]

Bharne and Sumita Dinesh proposed an online social network scam detection system using machine learning models such as Naïve Bayes, Random Forest, Decision Tree, and Support Vector Machine. According to their research, the Random Forest model achieved the highest accuracy compared to the other machine learning models and demonstrated a lower False Positive Rate (FPR). The highest accuracy achieved by the Multi-Modal Scammer Detection model was 94.55%, with a low FPR of 0.01 and a False Negative Rate (FNR) of 0.119. The FNR indicates that approximately 11%

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 06, June 2025, pp : 175-181
e-ISSN : 2583-1062
Impact Factor : 7.001

of actual scammer profiles were incorrectly classified as genuine by the model, meaning a small portion of scammer profiles went undetected [9]

M. Valavan and S. Rita demonstrated financial fraud detection using a boosting classifier with the help of machine learning techniques, including Decision Tree, Logistic Regression, and Random Forest. According to their results, the Random Forest classifier achieved a prediction accuracy of 80%, while the Logistic Regression method provided an accuracy of 70%. The Random Forest model appeared to be a better option for this type of data. Additionally, one of the ensemble machine learning techniques, the Gradient Boosting algorithm, showed better results compared to the other methods, with accuracy exceeding 90% [18]

SaiVenktaJaswantKolupuri et al. studied scams and frauds in the digital age and implemented various machine learning techniques, including Naïve Bayes, Support Vector Machine (SVM), Random Forest, as well as deep learning methods such as Deep Neural Networks (DNN). In addition to these techniques, they explored concept drift handling methods, such as Dynamic Weight Majority Concept Drift Detection (DWM-CD) and Early Drift Detection Method (EDDM). Their work aimed to address the evolving nature of scams and frauds, leveraging both traditional machine learning algorithms and advanced methods to improve detection and adaptation to changing patterns in digital fraud [21]

KrishnadasNanath and Liting Olney conducted an investigation into crowdsourcing methods to enhance machine learning approaches for detecting online recruitment fraud. With the increasing use of analytics in research, several studies have applied machine learning (ML) algorithms to address the challenge of identifying fake content. These algorithms aim to differentiate between fake and non-fake content, which could lead to the development of automated and adaptive detection systems (Guzella&Caminhas, 2009).

These algorithms learn from available datasets and train classification models to identify fraudulent content. A majority of these studies have employed supervised learning techniques, such as Logistic Regression (LR), Support Vector Machines (SVM), Random Forests (RF), Decision Trees (DT), and Naïve Bayes (NB). These machine learning methods are commonly used to combat online recruitment fraud by effectively distinguishing between legitimate and fraudulent content based on historical data and patterns [19]

Manjeevan Seera et al.implemented both machine learning and deep learning techniques to detect online phishing scams using datasets from Germany and Australia. According to their findings, the Gradient Boosting Tree model performed most accurately on the Australian dataset, achieving an accuracy of 86.23%, which was higher than that of all other machine learning and deep learning models. However, when applied to the German dataset, the Gradient Boosting Tree model demonstrated lower accuracy compared to other machine learning and deep learning techniques. This highlighted the varying effectiveness of the models across different datasets and emphasized the need for tailored approaches depending on the regional characteristics of the data [20]

In their 2024 study, N Abid - Int. J. Innov. Sci. Res. Technol, explored the application of various machine learning and deep learning techniques on a "Fraudulent Transaction" dataset, which was sourced from the Kaggle repository. The study implemented several predefined algorithms, including Logistic Regression (LR), Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Convolutional Neural Networks (CNN), to detect fraudulent activities. To evaluate the performance of these models, the authors used standard classification metrics such as Accuracy, Precision, Recall, and F1-score. The results from each technique were systematically compared based on these metrics to determine the most effective approach for fraud detection [10]

Table1 Literature Review of Online Fraud

References	year	Used Algorithm	Result
Zhao et al.[14]	2016	Support Vector Machines (SVM)	SVM with non-linear kernels outperformed traditional models by classifying transactions accurately, even with imbalanced datasets, and subtle fraud patterns.
Gupta et al[12].	2017	Machine Learning (Decision Trees, Anomaly Detection)	Machine learning models, particularly decision trees and anomaly detection, were effective in identifying fraud in mobile payment systems, such as app-based fraud and SIM swap fraud.

Vermapardeep [17]	2022	LR(logistic regression), SVM(support vector machine)	Support Vector Machine (SVM) performs better than Logistic Regression (LR)
Kanika[2]	2022	KNN, LR, LGBM, DT, RF, DNN	LGBM offers better accuracy compared to other techniques
M.valavan and s.rita[18]	2023	GB(gradient boosting), LR(logistic regression),RF(random forest)	GB has the highest performance among the models, while LR has the lowest
KrishnadasNanath and Liting Olney[19]	2023	LR(logistic regression),RF(random forests),DT(decision trees),NB(naïve Bayes)	LR has better performed with high Auc score and RF has high precision rest algo has lowest performance
Afriyie et al. [16]	2023	Logistic Regression, Random Forest, Decision Trees	RF achieved maximum accuracy (96%) and AUC (98.9%), highlighted demographic and temporal fraud patterns.
Bharnesumita d [9]	2023	NB , RF, DT, SVM	Random Forest has the highest accuracy, while Naïve Bayes has the lowest accuracy.
Sharma and Babbar[15]	2023	XGBoost, AdaBoost, RF	XGBoost achieved the highest accuracy and RF achieved 67 lowest.
Manjeevanseeraand et.al[20]	2024	GBT(gradient boosting tree)	The model achieved an AUC of 0.967
Sharma and Sharma [13]	2024	RNN,CNN	RNN outperformed CNN with 95.8% accuracy, 93.7% sensitivity, 97.5% specificity, and robust performance across transactions.
Wahid et al. [11]	2024	Auto Encoder	All the metrics achieved high values

3. RESEARCH METHODOLOGY

This section outlines the research design, data collection methods, and analytical procedures used to develop and evaluate an online payment fraud detection system. Given the increasing prevalence of online financial transactions and the associated risks of fraud, the study focuses on leveraging deep learning techniques to identify fraudulent activities . The methodology consists of several key phases, including data collection, pre-processing, model development, and evaluation.

3.1 Dataset Description

This study employs a Kaggle dataset comprising 11,534,336 online transactions, including both fraudulent and legitimate entries. The dataset features critical attributes such as transaction type, amount, and account balances before and after each transaction. It enables comprehensive analysis of digital payment behaviors and supports the development of robust fraud detection systems by identifying patterns that distinguish fraudulent activities from legitimate ones.

3.2 Pre-Processing

In this study, pre-processing techniques are applied to the dataset to ensure it is clean and suitable for analysis. This process includes handling data imbalances, addressing missing values, and removing any erroneous or incorrect entries. Missing data is managed through imputation or by removing records where imputation is not appropriate. To correct class imbalances, techniques such as over-sampling the minority class using SMOTE (Synthetic Minority Over-sampling Technique) and under-sampling the majority class are employed. These pre-processing steps are essential to enhance data quality and ensure the development of a more accurate, fair, and reliable model for analysis and prediction.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 06, June 2025, pp : 175-181

e-ISSN : 2583-1062
Impact Factor : 7.001

3.3 Techniques

In this study deep learning techniques are apply to a pre-processed and clean dataset from Kaggle. After preparing the data, we will implement deep learning techniques and evaluate their performance using key metrics such as accuracy, precision and recall .We will then compare the results of both techniques to assess their effectiveness and determine which method performs best for the given problem

4. EXPERIMENTAL RESULTS

The results of predefined deep learning models for online payment fraud detection ,based online payment datasets, are presents in this section different deep learning model trained and evaluated The models were assessed based on performance metrics accuracy. The following subsections describe the evaluation results for each model.

4.1 FNN Model

The performance of the FNN models was evaluated based on their evaluation of the metrics. The table 2 summarizes these details.

Table 2 FNN Evaluation

Metrics	Result
Accuracy	99.41
Precision	99.15
Recall	99.67
M.A.E	0.0059

The Feedforward Neural Network (FNN) model exhibited exceptional performance in fraud detection tasks. It achieved an impressive accuracy of 99.41%, reflecting its ability to correctly classify both fraudulent and non-fraudulent transactions with high reliability. The precision was 99.15%, indicating that the model produced very few false positives when identifying fraud. Additionally, the recall reached 99.67%, demonstrating the model's effectiveness in capturing nearly all actual fraudulent cases. The mean absolute error (MAE) was remarkably low at 0.0059, signifying minimal average error between predicted and actual outcomes. These results underscore the FNN model's high precision, sensitivity, and overall accuracy in detecting fraudulent activity.

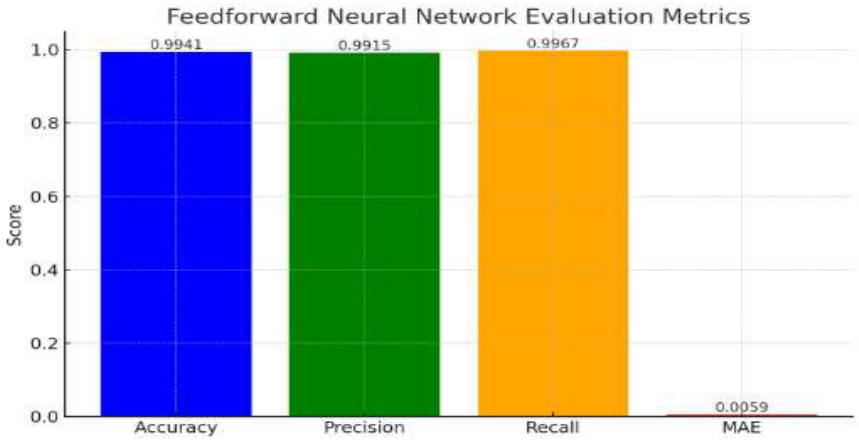

Fig1 FNN evaluation for different metrics

4.2 LSTM Model

The performance of the LSTM model was evaluated based on their evaluation of the metrics . The table 3 summarizes the metrics results for LSTM model.

Table 3 LSTM Evaluation

Metrics	Result
Accuracy	99.37
Precision	99.34
Recall	98.3
M.A.E	0.0063

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 06, June 2025, pp : 175-181
e-ISSN : 2583-1062
Impact Factor : 7.001

The LSTM (Long Short-Term Memory) model demonstrated strong performance in detecting fraudulent transactions. It achieved an accuracy of 99.37%, indicating a high rate of correct classifications across both fraud and non-fraud cases. The precision was 99.34%, suggesting that when the model flagged a transaction as fraudulent, it was accurate in the vast majority of cases. A recall of 99.39% highlights the model's ability to successfully identify most actual fraud cases, minimizing the number of missed detections. Furthermore, the mean absolute error (MAE) was 0.0063, signifying minimal deviation between predicted and actual values. These metrics collectively confirm the LSTM model's effectiveness and robustness in sequential pattern learning for fraud detection.

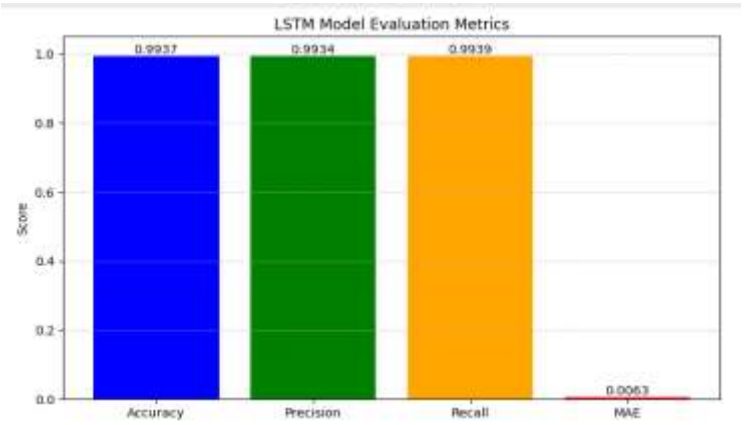

Fig 2 LSTM evaluation for different metrics

4.3 Auto Encoder

The performance of the Auto encoder model was evaluated based on their evaluation of the metrics as shown in table 4.

Table 4 Evaluation of Auto Encoder

Metrics	Result
Accuracy	85.20
Precision	93.78
Recall	75.40
M.A.E	0.14

The performance evaluation of the model was carried out using several key metrics. The accuracy of the model was recorded at 85.20%**,** indicating that the model correctly predicted the outcomes for the majority of the instances. A high precision value of 93.78% demonstrates that the model was highly effective in minimizing false positives, meaning that most of the instances it classified as positive were indeed correct. However, the recall was relatively lower at 75.40%,suggesting that while the model was precise, it missed a number of actual positive cases, highlighting potential room for improvement in identifying all relevant instances. Additionally, the Mean Absolute Error (MAE) was found to be 0.14, indicating that on average, the model's predictions deviated from the actual values by a small margin. Collectively, these metrics suggest that the model performs well, particularly in terms of precision, but could benefit from improvements in recall to ensure more comprehensive detection.

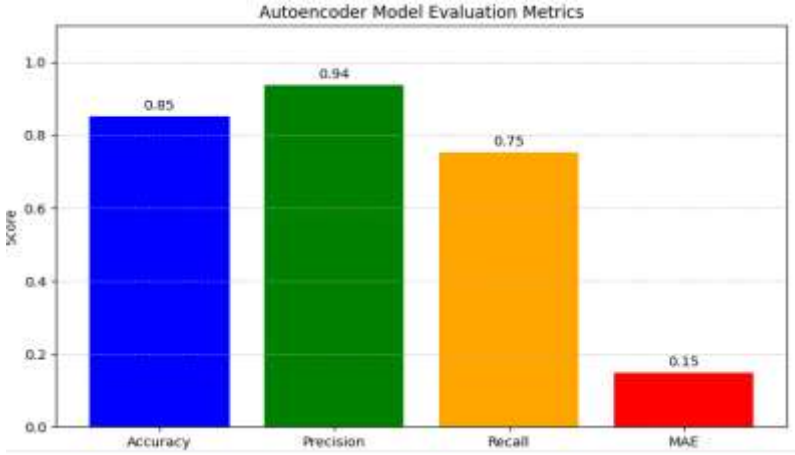

Fig 3 Auto Encoder evaluation for different metrics

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 06, June 2025, pp : 175-181
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

4.4 Evaluation of Models

The table 5 presents a comparison of three machine learning models—Feedforward Neural Network (FNN), Long Short-Term Memory (LSTM), and Auto encoder—using four key evaluation metrics: Accuracy, Precision, Recall, and Mean Absolute Error (M.A.E.).

FNN performs the best among the three models. With an accuracy of 99.41%, it classifies almost all samples correctly. It also demonstrates high precision (99.15%) and recall (99.67%), indicating that it is effective at minimizing both false positives and false negatives, a critical aspect of fraud detection. Additionally, its M.A.E. of 0.0059 is the lowest, showing that its predictions are very close to the actual values, which suggests a high level of prediction accuracy.

LSTM, while slightly behind FNN, also performs well with an accuracy of 99.37%, precision of 99.34%, and recall of 99.39%. These metrics indicate that LSTM is nearly as effective as FNN in identifying fraud cases. However, its M.A.E. of 0.0063 is slightly higher than FNN, but still shows good performance in prediction accuracy.

In contrast, the Auto encoder model falls behind both FNN and LSTM in terms of classification performance. Its accuracy is significantly lower at 85.20%, indicating that it fails to correctly 0classify many instances. Although its precision (93.78%) is relatively high, the recall of 75.40% shows that it misses a large number of true positive cases, which is a major drawback in fraud detection tasks where detecting as many fraudulent cases as possible is crucial. The Auto encoder also has a high M.A.E. of 0.14, suggesting that its predictions deviate significantly from the actual values.

Table 5 Evaluation of Models

Metrics	FNN	LSTM	Auto encoder
Accuracy	99.41	99.37	85.20
Precision	99.15	99.34	93.78
Recall	99.67	99.39	75.40
M.A.E	0.0059	0.0063	0.14

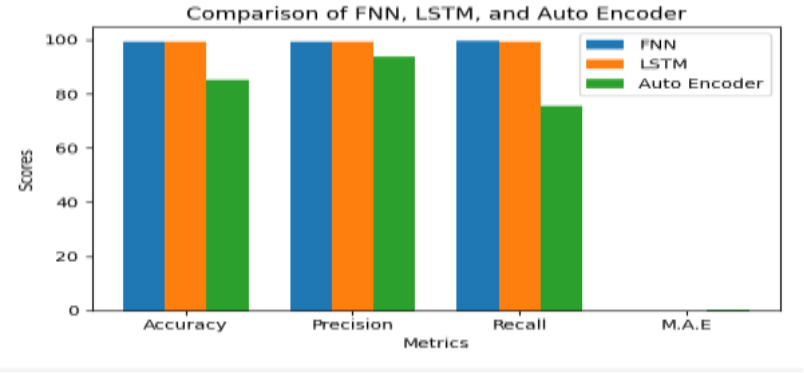

Fig 4 comparative analysis of each model

5. CONCLUSIONS

The growth of digital financial systems has improved transaction efficiency but also increased the risk of online payment fraud. This study explores the use of advanced deep learning models Feedforward Neural Networks (FNN), Long Short-Term Memory (LSTM) networks, and Auto encoders for detecting fraudulent transactions. A large-scale online transaction dataset from Kaggle was pre-processed and used to train and evaluate these models. The FNN model achieved the highest performance, with 99.41% accuracy, 99.15% precision, 99.67% recall, and a low mean absolute error (MAE) of 0.0059. The LSTM model also performed well, especially in identifying sequential fraud patterns. Although the Autoencoder was less effective for binary classification, it proved useful in detecting anomalies and unknown fraud types. The comparative analysis shows that FNNs are effective for static data, LSTMs for temporal patterns, and Autoencoders for unsupervised anomaly detection. The results confirm that deep learning significantly enhances real-time fraud detection in online payment systems.

6. REFERENCES

[1] O'Mahony, Donal, Michael Pierce, and Hitesh Tewari. Electronic payment systems for e-commerce. Artech, 2001.

[2] Kanika, and Jimmy Singla. "RETRACTED: A novel framework for online transaction fraud detection system based on deep neural network." Journal of Intelligent & Fuzzy Systems 43.1 (2022): 927-937.

[3] Chang, Joshua JS. "An analysis of advance fee fraud on the internet." Journal of Financial Crime 15.1 (2008): 71-81.
[4] Sahu, Krutika Rani, and JigyasuDubey. "A survey on phishing attacks." International Journal of Computer Applications 88.10 (2014).
[5] Yar, Majid, and Kevin F. Steinmetz. "Cybercrime and society." (2023): 1-100.
[6] Noufidali, V. M., Jobin S. Thomas, and Felix Arokya Jose. "E-auction frauds-a survey." International Journal of Computer Applications 61.14 (2013).
[7] Gragido, Will, and John Pirc. Cybercrime and espionage: An analysis of subversive multi-vector threats. Newnes, 2011.
[8] Brenner, Susan W. Cybercrime and the law: Challenges, issues, and outcomes. UPNE, 2012.
[9] Bharne, Smita, and PawanBhaladhare. "An enhanced scammer detection model for online social network frauds using machine learning." IJRITCC 11 (2023): 239-249.
[10] Abid, Noman. "Improving Accuracy and Efficiency of Online Payment Fraud Detection and Prevention with Machine Learning Models." Int. J. Innov. Sci. Res. Technol 9.12 (2024): 711-723.
[11] Wahid, Abdul, et al. "NFA: A neural factorization autoencoder based online telephony fraud detection." Digital Communications and Networks 10.1 (2024): 158-167.
[12] Gupta, P., and H. Lamba. "Machine Learning Techniques in Mobile Payment Fraud Detection." International Journal of Computer Applications, vol. 162, no. 3, 2017, pp. 10–15. https://doi.org/10.5120/ijca2017913003
[13] Sharma, Rishabh, and Ajay Sharma. "Combatting Digital Financial Fraud through Strategic Deep Learning Approaches." 2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS). IEEE, 2024.
[14] Zhou, Xiaohui, Shuo Wang, and Shuang Wu. "Hybrid Machine Learning Models for Real-Time Fraud Detection in E-Commerce Payments." E-Commerce Research and Applications, vol. 27, 2018, pp. 33–42. https://doi.org/10.1016/j.elerap.2017.12.002
[15] Sharma, Anshika, and HimanshiBabbar. "Machine learning-driven detection and prevention of cryptocurrency fraud." 2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE). IEEE, 2023.
[16] Afriyie, Jonathan Kwaku, et al. "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions." Decision Analytics Journal 6 (2023): 100163.
[17] Verma, Pradeep, and PoornimaTyagi. "Credit Card Fraud Transaction Classification Using Improved Class Balancing and Support Vector Machines." Recent Innovations in Computing: Proceedings of ICRIC 2021, Volume 2. Singapore: Springer Singapore, 2022. 477-488.
[18] Valavan, M., and S. Rita. "Predictive-Analysis-based Machine Learning Model for Fraud Detection with Boosting Classifiers." Computer Systems Science & Engineering 45.1 (2023).
[19] Nanath, Krishnadas, and Liting Olney. "An investigation of crowdsourcing methods in enhancing the machine learning approach for detecting online recruitment fraud." International Journal of Information Management Data Insights 3.1 (2023): 100167.
[20] Seera, Manjeevan, et al. "An intelligent payment card fraud detection system." Annals of operations research 334.1 (2024): 445-467.
[21] Kolupuri, SaiVenkataJaswant, et al. "Scams and Frauds in the Digital Age: ML-Based Detection and Prevention Strategies." Proceedings of the 26th International Conference on Distributed Computing and Networking. 2025.