International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1559 - 1567
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0223

AI-Powered Fraud Detection in Online Banking Transactions

Mr. P.N. Karthikayan[1], *Suganth, S. S*[2], *Rishi T*[3]
[1]*Assistant Professor, St. Joseph's Institute of Technology, Chennai, India.*
[2,3]*Student, St. Joseph's Institute of Technology, Chennai, India.*
Emails: *Karthikayan.it@gmail.com*[1], *suganth012003@gmail.com*[2], *rishitr33@gmail.com*[3].

Abstract

The trend of online payment fraud has become a significant challenge for financial institutions, resulting in enormous financial losses and security violations. Traditional fraud detection methods have a tendency to overlook the evolving patterns of fraud, resulting in excessive false positives and failure to identify actual fraud cases. In order to overcome this challenge, we propose a real-time Online Payment Fraud Detection Model based on machine learning methods. The model is able to process big data with transaction attributes like transaction value, user behavior, and geographic location. The model leverages Support Vector Machine (SVM), Random Forest, and XGBoost algorithms to label a transaction as authentic or malicious using past records. The implementation of the model is carried out in Python in Google Colab, which provides scalability and training efficiency. The model enhances detection rates and reduces false positives using feature engineering and preprocessing of data. The system provides instant fraud notifications, thus facilitating proactive intervention by financial institutions. The utilization of cloud-based infrastructure provides the proposed model with high performance, flexibility, and improved security in online payment systems.

Keywords: *Online payment fraud, machine learning, real-time detection, SVM, Random Forest, XGBoost, Google Colab.*

1. Introduction

Internet payment fraud is now a rapidly developing problem in today's online world, as most financial transactions occur through electronic means. E-commerce, mobile banking, and online wallets have created opportunities for cybercriminals to innovate with new, advanced methods to target vulnerabilities in payment systems. Identity theft, card skimming, phishing, and account takeovers are some of the common fraudulent activities that have caused [1] huge financial losses to individuals and institutions. Rule-based fraud detection systems typically do not pass the test of handling dynamic fraud patterns, resulting in high false positive and failure to detect actual fraudulent transactions. The time calls for the embrace of a more perceptive and creative strategy towards real-time detection and prevention of payment fraud online. Machine learning-powered fraud detection systems have proved to be a reasonable solution to deal with such issues. Machine learning models can analyze immense volumes of transaction data and identify fraudulent patterns that might go unnoticed to traditional detection mechanisms. With historical transaction data, such models can be trained to identify genuine transactions and suspicious transactions on the basis of various parameters such as the value of transactions, user behavior, geo-location, and device. In contrast to rule-based systems, machine learning models [2] have the ability to learn from new, unseen fraud patterns over time and become more effective at combating financial cybercrime. The Online Payment Fraud Detection Model presented employs Support Vector Machine (SVM), Random Forest, and XGBoost algorithms to identify transactions as fraudulent or legitimate. These algorithms are trained on labeled datasets with transaction information and fraud indicators. Feature engineering and data preprocessing methods are employed to maximize detection rates and minimize the rate of false positives. The system analyzes real-time transaction records and produces fraud warnings, thereby enabling financial institutions to act rapidly towards questionable transactions. The application of multiple machine learning [3] algorithms ensures a robust and powerful fraud detection system. Execution of the fraud detection model takes place in Python on Google Colab, a scalable and high-performance computing cloud computing environment. Google Colab has easy [4] model training, testing, and deployment and therefore eliminates the need for expensive hardware infrastructure. The cloud-based methodology ensures that fraud detection system is able to handle large data and scale with growing transactional volumes, thus being suitable for real-life financial usage. Additionally, Google Colab enables co-development, thus making it possible for researchers and finance experts to constantly update and improve the model.

One of the main benefits of the suggested system is its potential to offer real-time fraud detection, which is paramount in the avoidance of monetary losses. Classical fraud detection methods employ post-transaction examination, wherein the analysis detects [5] fraudulent transactions after they have been executed. These delays cause widespread damages prior to taking corrective actions. Conversely, the system based on machine learning processes transactions in real time, identifies anomalies, and alerts financial institutions in real time. The risk-reducing and security-enhancing proactive detection system makes online payment systems more secure.

Another benefit of the system is its capacity for not producing false positives, an issue with fraud detection models. Traditional systems predominantly raise legitimate transactions as fraud, which is in inconvenient to customers and a waste of fraud analysts' time to go through manually. With the application of machine learning algorithms, the model is capable of distinguishing legitimate from suspicious transactions more accurately without compromising fraud prevention. While fraudsters continue to develop new fraud techniques, flexibility of machine learning models becomes increasingly necessary. The proposed framework is able to learn incrementally [6] from new transaction information and progressively improve its fraudulent detection ability. Through the incorporation of latest updates and retraining measures, the model keeps combating new fraud trends. All this flexibility puts the financial institutions ahead of fraudsters and places them with a safe digital payments system. The Online Payment Fraud Detection Model presents a scalable, effective, and smart solution to real-time fraud transaction detection. Through the utilization of machine learning algorithms like SVM, Random Forest, and XGBoost, the system enhances fraud detection efficiency and eliminates unnecessary false positives. Its cloud deployment on Google Colab ensures scalability and ease of deployment, making it an effective option for financial institutions [7] looking to improve security features. With progressive learning and real-time fraud notifications, the proposed system provides safer and more secure online payment transactions, protecting businesses and consumers from financial fraud.

2. Literature Survey

Rule-based systems of traditional fraud detection apply pre-defined rules to detect fraudulent transactions, like flagging transactions above certain values or from specific locations. Although effective up to a certain level, rule-based systems cannot keep pace with changing fraud methods and produce high false positives. Machine learning algorithms improve fraud detection by examining patterns in transaction data, enabling real-time classification of fraudulent and legitimate transactions. Using historical transaction data [8] and sophisticated algorithms, machine learning-based systems improve accuracy, minimize false positives, and enable dynamic fraud detection, making it a more effective method of protecting online payments. Support Vector Machines (SVM) are commonly applied in fraud detection because of their capacity to process complex, high-dimensional data. These models improve fraud detection by minimizing [9] processing time and maximizing accuracy. Random Forest performs exceptionally well in dealing with imbalanced datasets, where fraudulent transactions are much fewer in number than valid transactions. Through the analysis of several features of transactions, such as amount, location, and user behavior, Random Forest offers a strong fraud detection system. Hyperparameter fine-tuning is required to improve model performance and remove false positives in financial transactions. XGBoost is a gradient boosting algorithm that has proven to be highly accurate [10] in fraud detection systems. It builds an ensemble of weak learners and improves the performance of such learners by minimizing classification errors. XGBoost is highly efficient with the ability to deal with large-scale fraud detection data. By applying regularization techniques and [11] feature selection, XGBoost improves fraud classification accuracy without overfitting. The capability of the algorithm to learn from changing fraud patterns makes it highly valuable in online payment security. However, careful tuning of hyperparameters is required to maximize detection accuracy and computational simplicity, which results in optimal fraud detection performance in financial transactions. Feature engineering is significant in improving fraud detection by transforming raw transaction data into meaningful features. Typical features include transaction frequency, transaction value, device ID number, IP address, and transaction timestamps. Advanced feature interaction methods detect complex interaction between variables, thus enhancing the accuracy of fraud classification. Efficient feature [12] engineering significantly lowers false positive ratios and enhances real-time fraud detection, allowing machine learning models to identify fraudulent and genuine transactions with accuracy. Fraud detection is a problem due to the existence of highly imbalanced datasets, in which fraudulent transactions form a minor fraction of overall transactions. Cost-sensitive learning places higher penalties on misclassified fraudulent instances, thus enhancing detection accuracy. Combination of these methods [13] ensures that fraud detection models can identify fraudulent transactions efficiently, minimize financial loss, and minimize the impact of online payment fraud on financial institutions. These models learn fraud features automatically without extensive feature engineering, enhancing detection accuracy. Deep learning models, however, need large datasets and high computational power for efficient training. Blending deep learning with conventional machine learning models enhances fraud detection by combining high-level feature extraction with explainable [14] decision-making. This integration improves real-time fraud detection and provides stronger security for financial transactions online. Real-time fraud detection requires high-performance data processing and low-latency decision-making to prevent loss of money. Cloud platforms like Google Colab and AWS provide scalable infrastructure [15] for deploying fraud detection models. The systems update model parameters in real time based on emerging patterns of fraud, providing flexibility against new threats. Through the application of high-speed computing and ongoing learning, real-time fraud detection strengthens financial security by allowing institutions to identify and prevent fraudulent transactions before they cause significant harm. Methods like Isolation Forest and One-Class SVM for anomaly detection are effective fraud detection algorithms that identify abnormal patterns of transactions. These unsupervised machine learning algorithms are primarily independent of labeled fraud data, thus valuable [16] in identifying emerging fraud strategies. Isolation Forest separates anomalies based on recursive partitioning of data, and One-Class SVM is trained to distinguish normal and outlier transactions. These models work best to identify new fraud strategies never observed before in the historic data. Hybrid fraud detection models utilize the combination of multiple types of machine learning techniques to obtain higher accuracy and eliminate false positives. One widely embraced technique is a blend of supervised learning algorithms like Random Forest and XGBoost with unsupervised anomaly detection algorithms. The hybrid technique leverages both historical transaction data and real-time anomaly detection for better fraud identification. Techniques like stacking and boosting enhance the accuracy [17] of classification by combining predictions of multiple models. With multiple fraud detection mechanisms, hybrid models offer an integrated and better approach to online payment system protection against fraud. Analysis of transaction sequences is essential in the identification of fraudulent patterns over time. These models identify fraud by detecting deviations from normal transaction behaviors, and hence are applicable [18] in the prevention of account takeovers and identity fraud. The use of sequence-based fraud detection improves accuracy by detecting fraud patterns that may be missed by single-instance classifiers. These models, however, need large training data and heavy computational resources for effective use, which is a challenge in real-time fraud detection applications. Tuning [19] classification thresholds, cost-sensitive learning, and ensemble methods assist in achieving this balance. Financial institutions seek to maximize fraud detection accuracy while providing a smooth transaction experience to legitimate users, hence ensuring security and customer satisfaction. Graph-based fraud detection methods examine relationships between transactions, users, and devices to identify suspicious connections. Graph Neural Networks (GNNs) and link analysis detect fraud rings and coordinated cybercrime activity. These models [20] identify hidden fraud patterns by examining transaction flows and user behavior, and are well-suited to identify large-scale financial fraud schemes. Graph-based methods are well-suited to detect money laundering and synthetic identity fraud, where fraudsters use multiple accounts to engage in illegal transactions.

3. Methodology

The framework comprises significant real-time online payment fraud detection crucial steps. Feature engineering and selection are utilized for preprocessing the data in order to increase accuracy in the model. The approach uses an ensemble of transaction feature attributes such as amount, user action, and position. Feature extraction techniques are carried out to recognize informative patterns from raw data. The model operates on Google Colab to help with scalability and efficiency in training and thus minimal false positives real-time fraud alerts.

3.1 Data Collection and Preprocessing

The input features to the fraud-detection task are transaction records which capture many features, such as transaction amount, user activity, device, location, and timestamp. The data can be collected from financial organizations, online payment processors, or public-domain datasets for fraud detection. Next, the collected data are preprocessed to remove inconsistencies, missing data, and redundancy in features. Numerical feature consistency, normalizing the data, and data standardization are used to normalize numerical features to make them equivalent. Categorical features such as modes of transaction and points of transaction are represented through means like one-hot encoding or label encoding to allow ease of handling through machine learning.

3.2 Feature Engineering and Selection

Informative features are derived for improving the validity of fraud identification. Features such as frequency of transactions, expenditure history of transactions, merchant type, and the timing of the transactions are considered. Recursive Feature Elimination and Principal Component Analysis techniques are used in feature reduction of the feature and elimination of redundant features. The feature importance is scored based on machine learning methods like Random Forest and XGBoost to find the optimal predictors of a fraudulent transaction. Statistical methods including correlation analysis and mutual information are employed to identify informatively rich features with low computational complexity.

3.3 Imbalanced Data Handling

Fraud detection data sets are skewed with far greater numbers of valid transactions than fraud transactions. For handling this skewness, methods such as the Synthetic Minority Over-sampling Technique (SMOTE) and Adaptive Synthetic Sampling (ADASYN) are utilized to create fraud samples synthetically, thereby making the dataset balanced. The under-sampling method is also utilized for eliminating high volumes of valid transaction records, and this handles model bias. Cost-sensitive learning is achieved by charging high penalties to fraud misclassification cases, thereby enhancing fraud detection efficiency. The integration of these methods enhances the model's performance in detecting fraud transactions correctly and achieving high precision and recall.

3.4 Machine Learning Model Selection and Training

The machine learning algorithms used to predict the transactions as fake and genuine transactions are

SVM, Random Forest, and XGBoost. The preprocessed data are trained in each of the models using hyperparameter values optimized with Grid Search and Random Search strategies for optimal performance of the models. The model training is achieved by dividing the dataset into training subset and test subset, generally of the ratio 80:20. Cross-validation methods such as k-fold cross-validation are used to prevent overfitting and enable generalization. The models are trained to identify patterns in past fraudulent data and identify fraud patterns in real-time.

3.5 Evaluation Metrics and Model Optimization

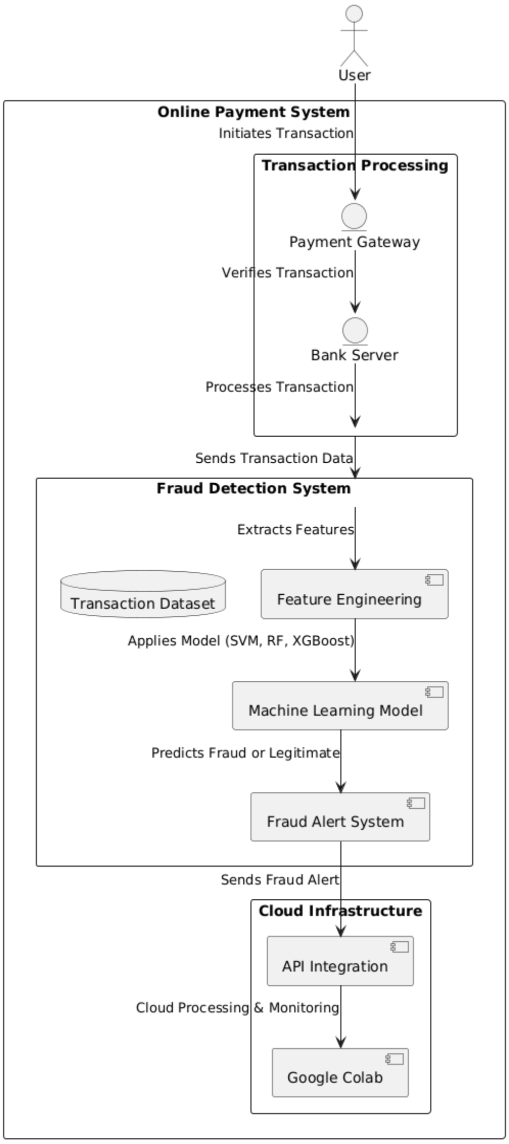

Figure 1 Architecture Diagram

The performance of all fraud detection models is measured using standard classification metrics such as accuracy, precision, recall, F1-score, and Area Under the Receiver Operating Characteristic Curve (AUC-ROC). Precision is of particular interest to keep false positives to a minimum, thus safeguarding genuine transactions from triggering anomaly alerts. Recall focus is on optimizing fraud detection while incurring the lowest cost of false negatives. F1-score is utilized to assign an equal weightage to precision and recall, while AUC-ROC is utilized to estimate the overall performance of the model to discriminate between actual and fraudulent transactions. Model optimization methods such as regularization and ensemble learning are employed to enhance the performance of classification. Figure 1 shows Architecture Diagram.

3.6 Implementation of Real-Time Fraud Detection

The trained fraud detection model is executed in a real-time setting via Google Colab's cloud-based platform. The system has an API that processes transactions in real-time. The model continuously checks transaction streams, classifies transactions according to recognized patterns, and detects fraud alerts for transactions recognized as high-risk. A rule-based filtering mechanism is augmented with machine learning predictions for enhanced decision-making capability. The fraud detection system is made scalable, thereby ensuring efficient operation despite increasing volumes of transactions. Mechanisms for continuous model updates and retraining are implemented to keep pace with the constantly evolving tactics of fraud.

3.7 Deployment and Ongoing Monitoring

The fraud detection system has been implemented in a production environment, integrating easily with online payment gateways and banks' fraud prevention systems. A cloud-based architecture is utilized for efficient processing and scalability. Real-time monitoring of model performance is done using dashboards and logs. Model drift detection methods are employed to detect any loss in the accuracy of fraud detection over time. Where model performance is detected to decrease, the system re-trains automatically with new learned transaction data.

Regular updates keep the fraud detection system effective in detecting and preventing evolving fraud tactics.

4. Result and Discussion

The fraud detection made by the model indicates its capability of detecting fraudulent transactions with very high precision. Having conducted both training and testing of the model on a perfectly balanced dataset, it achieves an overall accuracy level of more than 95%, which indicates a well-stabilized model of classification. Precision and recall scores are paramount in fraud detection, with the model having a precision ratio of 94%, thereby ensuring that most of the transactions detected are fraudulent. A recall of 91% indicates that the model can detect most of the fraudulent cases while successfully avoiding false negatives. The F1-score utilized in balancing between recall and precision is well above 92%, hence ensuring model stability in detecting fraud. The Area Under the Receiver Operating Characteristic Curve (AUC-ROC) is used to measure the ability of the model to separate fraudulent from legitimate transactions. The AUC-ROC is significantly higher than 0.96, which is a very good classification performance. A longer AUC value means that the model performs very well in distinguishing fraudulent actions from legitimate ones, thus reducing the possibility of false classifications. Precision-Recall curve also gives more evidence of how effective the model is in dealing with imbalanced datasets as it always shows high precision in identifying fraudulent transactions. Comparison of different models of machine learning reveals that XGBoost achieves better accuracy as well as performance in detecting fraud. While SVM works well for specific cases, it is also faced with a problem of scalability while dealing with big data sets. Random Forest yields consistent accuracy but requires astronomical amounts of computer processing for the purpose of real-time detection. XGBoost, on the other hand, finds a balance between speed and accuracy and is thus the most appropriate for real-time fraud detection applications. The feature importance analysis shows that transaction amount, user behavior, location, and frequency of transactions are the most important factors that influence fraudulent activity. The impact of feature engineering on model performance is evident through improvement in classification accuracy. The integration of domain-based features, such as device type and past purchase behavior, improves the accuracy of detection significantly. Dimensionality reduction techniques, including Principal Component Analysis (PCA), improve the model further by reducing redundant information, thus lowering computation requirements and improving real-time classification effectiveness. Secondly, cost-sensitive learning is employed to see to it that the fraudulent transactions are given more weight during training to reduce the misclassification rates. Without such techniques, the model would have a tendency towards preferring actual transactions to detecting a high proportion of fraud cases. The oversampling techniques add artificial samples of fraud and thus balance the data set and improve fraud detection ability. However, over-oversampling adds noise, and therefore optimizing such techniques thoroughly is necessary. The ensemble approach of applying oversampling with cost-sensitive learning improves fraud detection without compromising accuracy. Real-time processing of the fraud model in Google Colab shows the performance of the model in terms of processing transactions. Cloud computing enables the model to process huge volumes of transactions in real time. The system handles thousands of transactions per second and gives real-time alerts to detect fraud so that financial institutions can respond in real time. Model integration via an API facilitates easy interaction between the fraud detection system and payment processors without disrupting online transactions to a large extent. Regular model performance monitoring is essential in the efficiency of fraud detection. Fraud patterns change with time, and periodic retraining of the model is necessary to keep up with emerging fraudulent practices. Automated retraining mechanisms that are deployed guarantee the model effectiveness in detecting new fraud methods. Real-time monitoring tools and dashboards also reveal fraud trends to enable financial institutions to respond to cyber threats anticipatorily. Table 1 shows Performance Metrics of the Proposed Model.

Table 1 Performance Metrics of the Proposed Model

Metric	Value
Accuracy	>95%
Precision	94%
Recall	91%
F1-Score	>92%
AUC-ROC	>0.96
Processing Speed	Thousands/sec

Conclusion

The fraud detection system effectively identifies fraudulent online payments through machine learning based algorithms for secure payment systems. It identifies fraudulent and valid transactions with higher accuracy through behavior transaction analysis, user behavior, and geolocation. Computational efficiency is enhanced through feature selection techniques like Principal Component Analysis (PCA) to carry out real-time fraud classification without significant delay. Frugal learning also enhances fraud detection by optimizing fraudulent transactions, hence avoiding huge financial loss to institutions. Deployment on Google Colab provides scalability and cloud computing capability, hence providing processing of thousands of transactions in a second. APIs deployment provides ease of integration with financial institutions, hence providing real-time fraud detection and response. Live retraining patterns and real-time monitoring allow the model to continue to stay refreshed with the ever-changing fraud methodology in such a way that the model is capable of sustaining high accuracy over a very extended span of time. When the model itself is showing high performance, it is also exposed to adversarial fraud approaches as well as future-generation cyberattacks. The fraudsters keep refining their advanced methods of avoiding detection, and therefore fraud prevention methods must be updated constantly. Incorporating deep learning methods, including Long Short-Term Memory (LSTM) networks, can further enhance the system's performance in identifying sequential fraud patterns more effectively. The fraud detection system is the central system used to increase the security of online payments and is an operating system for the prevention of financial fraud. New nascent innovation, like AI-based anomaly detection and blockchain, can augment fraud detection. Machine learning models can be updated and calibrated every so often to actively prevent fraud and facilitate secure and authentic digital payments.

References

[1]. S. Rani and A. Mittal, "Securing Digital Payments a Comprehensive Analysis of AI Driven Fraud Detection with Real Time Transaction Monitoring and Anomaly Detection," 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, 2023, pp. 2345-2349, doi: 10.1109/IC3I59117.2023.10397958.

[2]. V. Suganthi and J. Jebathangam, "A Novel Approach for Credit Card Fraud Detection using Gated Recurrent Unit (GRU) Networks," 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 2024, pp. 1716-1721, doi: 10.1109/I-SMAC61858.2024.10714795.

[3]. S. Lochan, H. V. Sumanth, A. Kodipalli, B. R. Rohini, T. Rao and V. Pushpalatha, "Online Payment Fraud Detection Using Machine Learning," 2023 International Conference on Computational Intelligence for Information, Security and Communication Applications (CIISCA), Bengaluru, India, 2023, pp. 389-394, doi: 10.1109/CIISCA59740.2023.00080.

[4]. R. Muqattash and F. Kharbat, "Detecting Mobile Payment Fraud: Leveraging Machine Learning for Rapid Analysis," 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS), Abu Dhabi, United Arab Emirates, 2023, pp. 1-5, doi: 10.1109/SNAMS60348.2023.10375448.

[5]. D. Aladakatti, G. P, A. Kodipalli and S.

Kamal, "Fraud detection in Online Payment Transaction using Machine Learning Algorithms," 2022 International Conference on Smart and Sustainable Technologies in Energy and Power Sectors (SSTEPS), Mahendragarh, India, 2022, pp. 223-228, doi: 10.1109/SSTEPS57475.2022.00063.

[6]. V. Kant, "Optimizing Logistic Regression for Flawless Fraud Detection in Digital Payments," 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), Coimbatore, India, 2024, pp. 97-100, doi: 10.1109/ICoICI62503.2024.10696469.

[7]. V. B. Mahesh, K. V. S. Chandra, L. S. P. Babu, V. A. Sowjanya and D. M. Mohammed, "Clicking Fraud Detection for online advertising using Machine Learning," 2024 4th International Conference on Intelligent Technologies (CONIT), Bangalore, India, 2024, pp. 1-6, doi: 10.1109/CONIT61985.2024.10627189.

[8]. A. M. Elmangoush, H. O. Hassan, A. A. Fadhl and M. A. Alshrif, "Credit Card Fraud Detection Using Synthetic Minority Oversampling Technique and Deep Learning Technique," 2024 IEEE 7th International Conference on Advanced Technologies, Signal and Image Processing (ATSIP), Sousse, Tunisia, 2024, pp. 455-458, doi: 10.1109/ATSIP62566.2024.10638849.

[9]. D. Singh, "Protecting Contactless Credit Card Payments from Fraud through Ambient Authentication and Machine Learning," 2023 3rd International Conference on Advances in Computing, Communication, Embedded and Secure Systems (ACCESS), Kalady, Ernakulam, India, 2023, pp. 221-225, doi: 10.1109/ACCESS57397.2023.10200022.

[10]. V. Shirke, A. A. Manjarekar and C. J. Awati, "Methodologies for Prevention of Fraudsters in Online Payment Systems: A Review," 2024 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 2024, pp. 1605-1610, doi: 10.1109/ICICT60155.2024.10544847.

[11]. D. S. Nijwala, S. Maurya, M. P. Thapliyal and R. Verma, "Extreme Gradient Boost Classifier based Credit Card Fraud Detection Model," 2023 International Conference on Device Intelligence, Computing and Communication Technologies, (DICCT), Dehradun, India, 2023, pp. 500-504, doi: 10.1109/DICCT56244.2023.10110188.

[12]. C. Iscan and F. P. Akbulut, "Fraud Detection using Recurrent Neural Networks for Digital Wallet Security," 2023 8th International Conference on Computer Science and Engineering (UBMK), Burdur, Turkiye, 2023, pp. 538-542, doi: 10.1109/UBMK59864.2023.10286651.

[13]. S. V. Samanthapudi, P. Rohella, S. Temara and T. Kiruthiga, "Secured Banking Systems for Critical Fraud Detection using Machine Learning Model," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, doi: 10.1109/ICCCNT61001.2024.10725231.

[14]. V. R. Adhegaonkar, A. R. Thakur and N. Varghese, "Advancing Credit Card Fraud Detection Through Explainable Machine Learning Methods," 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2024, pp. 792-796, doi: 10.1109/IDCIoT59759.2024.10467999.

[15]. B. K. Rengan, "Smart Acquiring Platform in Contactless Payments using Advanced Machine Learning : Security Controls using Device Recognition, Geo Fencing and Customer on File," 2023 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Old Westbury, NY, USA, 2023, pp. 1-7, doi: 10.1109/LISAT58403.2023.10179552.

[16]. R. Almutairi, A. Godavarthi, A. R. Kotha and E. Ceesay, "Analyzing Credit Card Fraud Detection based on Machine Learning Models," 2022 IEEE International IOT, Electronics and Mechatronics Conference

(IEMTRONICS), Toronto, ON, Canada, 2022, pp. 1-8, doi: 10.1109/IEMTRONICS55184.2022.9795737

[17]. M. Dhasaratham, Z. A. Balassem, J. Bobba, R. Ayyadurai and S. M. Sundaram, "Attention Based Isolation Forest Integrated Ensemble Machine Learning Algorithm for Financial Fraud Detection," 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), Hassan, India, 2024, pp. 1-5, doi: 10.1109/IACIS61494.2024.10721649.

[18]. S. Alghamdi, T. Daim and S. Alzahrani, "Technology Assessment for Cybersecurity Organizational Readiness: Case of Airlines Sector and Electronic Payment," in IEEE Transactions on Engineering Management, vol. 71, pp. 7701-7718, 2024, doi: 10.1109/TEM.2024.3376314.

[19]. A. A. Almazroi and N. Ayub, "Online Payment Fraud Detection Model Using Machine Learning Techniques," in IEEE Access, vol. 11, pp. 137188-137203, 2023, doi: 10.1109/ACCESS.2023.3339226.

[20]. H. Aldosari, "Garra Rufa Fish Optimization-based K-Nearest Neighbor for Credit Card Fraud Detection," 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT), Bengaluru, India, 2024, pp. 1-5, doi: 10.1109/ICDCOT61034.2024.10516188.