ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14987486

Machine Learning-Based Online Fraud Detection and Prevention

Aravapalli Sri Chaitanya[1] (Ph.D); Mohammad Tasneem Kowsar[2]; Dari Udayasri[3]; Kanaparthi Ravikumar[4]; Borra Sai Ganesh[5]; Basa Datta Manikanta[6]

(ORCID : 0009-0008-5127-0250)[1]

[1](Assistant Professor) Artificial Intelligence & Machine Learning(CSE)
Dhanekula Institute of Engineering and Technology (JNTUK) Vijayawada, India
[2]Artificial Intelligence & Machine Learning (CSE) Dhanekula Institute of Engineering and Technology (JNTUK) Vijayawada, India
[3]Artificial Intelligence & Machine Learning (CSE) Dhanekula Institute of Engineering and Technology (JNTUK) Vijayawada, India
[4]Artificial Intelligence & Machine Learning (CSE) Dhanekula Institute of Engineering and Technology (JNTUK) Vijayawada, India
[5]Artificial Intelligence & Machine Learning (CSE) Dhanekula Institute of Engineering and Technology (JNTUK) Vijayawada, India
[6]Artificial Intelligence & Machine Learning (CSE) Dhanekula Institute of Engineering and Technology (JNTUK) Vijayawada, India

Publication Date: 2025/03/11

Abstract: As the rise of digital financial transactions exponentially increases, so does the need for efficient detection methods for online fraud, a serious threat in the form of an online cybersecurity oker. In this paper, we proposed an AI-assisted fraud detection framework involving supervised ML models (Logistic Regression, Random Forest, XGBoost) and unsupervised anomaly detection (Isolation Forest, Autoencoders) for real-time fraud detection. Additional feature engineering techniques, such as geolocation tracking, user profiling, and SMOTE for addressing class imbalance serve to improve performance. For real-time monitoring, we use a Streamlit-based interface and deploy with Flask/FastAPI a RESTful API of the trained model to easily integrate within the fintech. Precision, recall, F1-score and ROC-AUC metrics for fraud risk assessment optimize fraud detection while placing a constraint on false positives, making a balanced fraud risk assessment. The experimental results demonstrate their high accuracy and efficiency, which will guarantee this framework a large scale for use in financial institutions, e-commerce and cyber security systems. The study introduces data-driven solutions to beat evolving fraud; it helps enhance adaptive fraud detection for large systems.

Keywords: *Fraud Detection, Machine Learning, Anomaly Detection, Online Transactions, Supervised Learning, Unsupervised Learning, Financial Security, Cyber Threats.*

How to Cite: Aravapalli Sri Chaitanya; Mohammad Tasneem Kowsar; Dari Udayasri; Kanaparthi Ravikumar; Borra Sai Ganesh; Basa Datta Manikanta (2025). Machine Learning-Based Online Fraud Detection and Prevention. *International Journal of Innovative Science and Research Technology*, 10(2), 1962-1968. https://doi.org/10.5281/zenodo.14987486

I. INTRODUCTION

The rapid increase in digital financial transactions has led to a surge in fraudulent activities, posing significant risks to financial institutions, e-commerce platforms, and online payment systems. With the widespread adoption of online banking, digital wallets, and cashless transactions, cybercriminals exploit vulnerabilities in traditional fraud detection systems through techniques such as identity theft, account takeovers, phishing, and unauthorized transactions. Conventional rule-based fraud detection systems generate excessive false positives and fail to adapt to evolving fraud patterns, highlighting the need for intelligent, data-driven fraud detection frameworks.

Machine Learning (ML) and Anomaly Detection techniques have emerged as powerful tools to combat online fraud by leveraging historical transaction data to identify

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14987486

suspicious patterns. Unlike traditional systems, ML algorithms continuously learn from data, improving fraud detection capabilities. Supervised learning algorithms such as Logistic Regression, Random Forest, and XGBoost classify transactions based on labeled fraud data, while unsupervised anomaly detection techniques like Isolation Forest and Autoencoders detect novel fraud patterns by identifying deviations from normal behavior. These approaches minimize false positives and enhance fraud detection accuracy.

Feature engineering plays a crucial role in fraud detection by transforming raw transaction data into meaningful features such as transactional behavior, geospatial tracking, user profiling, and device fingerprinting.However, the class imbalance in fraud detection datasets poses a significant challenge, as fraudulent transactions constitute only a small fraction of overall data.Techniques such as Synthetic Minority Oversampling Technique (SMOTE) address this imbalance by generating synthetic samples of the minority class, improving model generalization and reducing bias.

For real-time fraud detection, a web-based monitoring system using Streamlit provides an intuitive interface for visualizing fraudulent activities and monitoring transaction risks dynamically.The trained ML models are deployed as RESTful APIs via Flask or FastAPI, enabling seamless integration with financial institutions and e-commerce platforms.This deployment ensures scalability and efficient fraud detection in high-volume transactional environments. Real-time alert mechanisms notify financial institutions and customers of suspicious transactions, enhancing security and enabling prompt intervention.

Model performance is evaluated using precision, recall, F1-score, and ROC-AUC to balance fraud detection sensitivity and false positive reduction. Precision measures the proportion of correctly identified fraudulent transactions, recall assesses the model's ability to detect fraud cases, the F1-score balances precision and recall, and ROC-AUC evaluates the model's overall discriminatory power.

Fraud takes various forms, including financial fraud (credit card fraud, mortgage fraud), identity theft, payment fraud (account takeovers, chargeback fraud), cyber fraud (phishing, malware attacks), and corporate fraud (insider trading, asset misappropriation).To counter fraud, organizations employ rule-based systems, ML models, behavioural analytics, anomaly detection, real-time monitoring, multi-factor authentication (MFA), and graph analytics.

Despite advancements, fraud detection faces challenges such as high false positives and false negatives, evolving fraud tactics, data privacy concerns, scalability issues, and integration with legacy systems. Future fraud detection will rely on AI-driven models, blockchain technology for transparency, advanced biometric authentication, and federated learning for privacy-preserving fraud detection. Explainable AI (XAI) will also enhance interpretability and trust in fraud detection decisions.

This research aims to develop a scalable, AI-powered fraud detection system that continuously adapts to evolving fraud tactics, providing a robust security solution for financial institutions and digital payment services. With the ongoing evolution of cyber threats, AI-driven fraud detection is essential for safeguarding financial ecosystems and ensuring the security of online transactions.

II. LITERATURE SURVEY

Machine learning methods have played a pivotal role in fraud detection in multiple fields, with recent research examining diverse models for increased accuracy and efficiency. U. Siddaiah [1] points to the efficiency of XGBoost in fraud detection, with particular emphasis on the importance of Synthetic Minority Over-sampling Technique (SMOTE) in class imbalance. He recommends further research on the application of autoencoders in anomaly detection, which would enhance fraud detection by learning representations of data in an unsupervised way. M. Naga Raju [2] also emphasizes the effectiveness of Long Short-Term Memory (LSTM) networks to extract sequential patterns, specifically in Unified Payments Interface (UPI) fraud cases. He recommends the creation of hybrid real-time models to enhance fraud detection systems by combining various approaches.

Pinku Ranjan [3] assesses the Random Forest performance, with a significant accuracy of 96.64%. His work emphasizes the need for data preprocessing to maintain balanced datasets, which is essential for reducing bias and enhancing detection rates. Deepanshu Thapa [4] contends that the XGB Classifier provides the highest precision at 99.95%, emphasizing the critical role of feature engineering and ensemble learning. He highlights the use of strong features and good optimized machine learning pipelines for real-time fraud detection. Reem A. Alzahrani [5] emphasizes click fraud detection using both machine learning and deep learning methodologies. Her paper mentions a 97.34% accuracy via Recurrent Neural Networks (RNN), exhibiting deep learning capability against fraud prevention. She also points to the need for adaptive learning and real-time analysis in order to offset the fast-developing fraudulent actions.

When it comes to fraud detection in e-commerce, Abed Mutemi [6] discusses deep models, specifically for their support of LSTM because it is efficient with sequential data. His work recognizes the limitations of small real-world datasets and changing nature of fraud schemes, necessitating enhanced data gathering and responsive measures. Rayene Bounab [7]'s work in the area of detecting healthcare fraud uses SMOTE-ENN, an oversampling and noise elimination strategy, to address class imbalance. Employing Decision Trees, her model attains an accuracy level of 99%, which proves the efficiency of tackling data imbalance problems. She also recommends future research to investigate deep learning methods, which can potentially enhance detection rates in the healthcare industry.

Dr. Yogesh W. Bhowte [8] focuses on detecting financial fraud, and he talks about the importance of feature engineering

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14987486

and big data analytics in detecting fraudulent transactions. His work highlights the importance of scalable fraud detection systems that can handle enormous amounts of financial data in real time. Dr. Shaik Rehana Banu [9] proposes a hybrid Convolutional Neural Network (CNN)-RNN financial fraud detection model with an accuracy of 99.2%. She emphasizes data preprocessing as being important in sharpening model performance and eliminating false positives. Finally, Ibomoiye Domor Mienye [10] explores deep learning models including LSTM and Gated Recurrent Units (GRU) to detect credit card fraud. His results show hybrid models improve detection performance, and future work lies in developing methodologies to effectively mitigate class imbalance. These studies overall highlight the paradigm-shifting effect of machine learning on fraud detection, with new developments in deep learning, feature engineering, and real-time analysis leading the way towards more robust fraud prevention solutions.

III. PROPOSED SOLUTION

The proposed fraud detection system is a strong machine learning-based system that is capable of detecting fraudulent financial transactions with great accuracy and efficiency.As fraudulent activities are becoming more sophisticated, the system incorporates sophisticated ensemble learning algorithms and efficient data preprocessing schemes to handle huge amounts of financial data with ease.One of the most important elements of the system is the Random Forest Classifier (Pinku Ranjan [3]), a type of ensemble model composed of many decision trees used to increase predictive power and reduce overfitting. The model is well-generalizing across all the types of financial transactions and provides consistent fraud detection.

The major difficulty in fraud detection is class imbalance—fraudulent transactions tend to be considerably less than authentic ones.To address this, the Synthetic Minority Over-sampling Technique (SMOTE) is utilized (Rayene Bounab [7]).SMOTE provides balancing to the dataset by creating synthetic examples of fraudulent transactions so that the model can better learn patterns of fraud.The dataset is preprocessed carefully, and categorical features such as transaction type and account numbers are encoded as numerical values using Label Encoding (Deepanshu Thapa [4]).This conversion renders the dataset suitable for machine learning models.In addition, feature engineering targets high-impact financial features with irrelevant attributes and IDs removed that might bring in bias (Dr. Yogesh W.Bhowte [8]).The strategy guarantees the model learns about transaction behaviors and not memorizing particular instances.

In real-time fraud detection, the trained model is implemented as a Flask-based RESTful API (Dr. Shaik Rehana Banu [9]).This API harmoniously integrates into financial systems and enables transactions to be assessed in real-time.The /predict endpoint accepts formatted JSON payloads of transaction information.When a request is made, the system dynamically encodes categorical features, prepares the data, and classifies the transaction as fraudulent or genuine based on the trained Random Forest model.The API is equipped with robust error-handling mechanisms (Reem A.Alzahrani [5]) to validate incoming data, ensuring smooth operation even when faced with missing or malformed inputs.Additionally, the system is designed with a high-throughput, low-latency architecture (Abed Mutemi [6]), making it highly scalable for financial environments where transactions occur at an extremely high frequency.

To evaluate the performance of the model, various metrics of evaluation are utilized, such as confusion matrix, classification reports, and AUC-ROC curves (U.Siddaiah [1]).These metrics allow analyzing precision, recall, and F1-score to ensure that the model has a robust balance between fraud detection and avoiding false positives.Feature importance analysis is conducted to determine how various variables play a role in fraud detection (M.Naga Raju [2]).In addition, hyperparameter optimization through grid search and random search maximizes model performance by identifying the optimal parameters with the optimal balance of computational efficiency and prediction power (Ibomoiye Domor Mienye [10]).

IV. METHODOLOGY

The fraud detection system adopts a systematic four-phase process: data preprocessing, model building, deployment, and testing, to have a thorough and technically sound process. During the data preprocessing phase, raw financial transaction data is converted into structured form optimized for machine learning. This involves dealing with missing values, encoding categorical variables with Label Encoding, and feature selection. Categorical features like transaction type and account numbers are numerically converted to make them compatible with the Random Forest model. SMOTE creates synthetic minority class instances to overcome class imbalance, enhancing the model's capability to identify fraudulent patterns.

The model development stage emphasizes machine learning algorithm selection and optimization. Random Forest Classifier is used based on its ensemble learning nature to avoid overfitting and increase predictive stability. The training procedure includes domain-guided feature selection and hyperparameter optimization with grid search and k-fold cross-validation to fine-tune the number of estimators, maximum depth of trees, and splitting values.This optimization ensures high precision, recall, and F1-score for high fraud detection.

To ensure real-time deployment, the system is wrapped around a Flask-based RESTful API and seamlessly interacts with financial systems. The API includes a /predict endpoint accepting JSON payloads, encoding categorical features, normalizing numerical features, and passing the data to the trained model. The API outputs a probabilistic class label for transaction legitimacy, and it comes equipped with extensive error-handling functions to confirm received data.To ensure scalability, the system effectively handles high transaction volumes without compromising on latency.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14987486

Table 1Model Metrics

Algorithm	Accuracy	Precision	Recall	F1 Score
Logistic Regression	91.5	88.7	83.4	85.9
Decision Tree	93.2	90.1	86.8	88.4
Random Forest	97.6	96.2	94.1	95.1
XGBoost	98.3	97.5	95.8	96.6
SVM	95.1	94.3	89.7	91.9
K-Means	78.4	78.5	81.2	79.8

Model performance is assessed with a confusion matrix, precision-recall, and SHAP values to facilitate interpretability. Stress testing and load balancing ensure performance under stress, and retraining on the fly adjusts the model to changing fraud patterns.This adaptive, scalable, and highly efficient platform offers financial institutions a robust fraud prevention tool, minimizing risks and guaranteeing transaction integrity in online finance.

V. ALGORITHMS

➢ *Logistic Regression*

Logistic Regression is a supervised algorithm that is highly applied in binary classification, thereby being suitable for fraud detection. It labels financial transactions as fraud or genuine by considering important attributes such as the amount of a transaction, geolocation, time stamp, and user activity. The model applies the logistic (sigmoid) function to transform input variables into a probability between 0 and 1, supporting threshold-based prediction. Transactions beyond a specified value are labeled fraudulent, while the rest are tagged as genuine.

$$P(Y=1|X)=1/1+e^{-(\beta 0+\beta 1X1+\beta 2X2+...+\beta nXn)}$$

One of the main benefits of Logistic Regression is that it is interpretable, with its coefficients reflecting the impact of each feature on predictions. This adds transparency to fraud detection, which helps financial institutions in risk assessment. Logistic Regression is also computationally efficient, which makes it suitable for structured data and real-time fraud detection, where decisions need to be made quickly. Although more sophisticated models such as decision trees and deep learning are available, Logistic Regression is a good baseline because of its simplicity and performance.

➢ *XGBOOST*

XGBoost or Extreme Gradient Boosting is an ensemble learning algorithm with high performance using gradient boosting, targeted at regression and classification problems. XGBoost refines basic gradient boosting with new features such as regularization, parallelism, and improved tree construction to make it efficient and fast. XGBoost builds decision trees sequentially, with each tree trying to fit the mistakes of the last trees through optimization of a loss function using second-order Taylor approximation for accurate updates.

$$F_m(x)=F_{m-1}(x)+\gamma h_m(x)$$

One of the biggest strengths of XGBoost is that it can efficiently process large-scale, high-dimensional data. It uses L1 (Lasso) and L2 (Ridge) regularization to avoid overfitting and enhance generalization. It also uses tree-pruning methods like depth-wise and loss-guided growth, which minimize unnecessary splits and improve interpretability. The algorithm also has missing value handling, in-built cross-validation, and parallel processing, making it extremely scalable and ideal for complex machine learning applications where speed and accuracy are needed.

➢ *Random Forest*

Random Forest is a strong ensemble learning method that builds many decision trees and makes predictions by aggregating their predictions to improve accuracy and stability. It employs bagging (Bootstrap Aggregating), training each tree on a randomly sampled subset of the data with replacement. It also chooses a random subset of features at every split, which decreases correlation between trees and enhances generalization. Predictions are made by majority voting for classification or averaging for regression.

$$y\hat{}=mode\{T1(x),T2(x),...,Tn(x)\}$$

One of the primary benefits of Random Forest is that it can manage high-dimensional data, noisy features, and missing values and reduce overfitting. It also assigns feature importance scores, facilitating interpretability and feature selection. The method is insensitive to outliers and performs well with structured and unstructured data. It can be computationally costly, particularly with big datasets or large numbers of trees. Optimized hyperparameter tuning (e.g., n_estimators, max_depth) is important. In spite of its complexity, Random Forest has a very good predictive performance and is commonly applied to fraud detection, medical diagnosis, and recommender systems.

➢ *Decision Tree*

Decision Trees are interpretable and general-purpose supervised learning algorithms for classification and regression. They partition the feature space recursively into homogeneous subsets based on decision rules derived from criteria such as Gini impurity, entropy, or mean squared error. Splitting is continued until a stopping criterion is reached, e.g., maximum tree depth or minimum samples per leaf node.

$$Entropy: -\sum p_i \log_2 p_i$$

A significant strength of Decision Trees is their interpretability, as they can easily visualize the decision-making process. They can easily work with both numerical and categorical data without the need for heavy preprocessing. They are, however, susceptible to overfitting, particularly if grown excessively deep, picking up noise from the data. The

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14987486

danger can be avoided by pruning, applying constraints on splits and leaf nodes, or ensembling with the help of techniques such as Random Forests and Gradient Boosted Trees. In spite of these difficulties, Decision Trees are still a valuable tool for representing intricate decision boundaries in fraud detection, medical diagnosis, and recommendation systems, among other applications.

VI. RESULTS

In the fielded environment, the fraud detection system is designed to provide effective real-time analysis and timely decision-making. The front-end of the system is a simple web-based interface named "Check Your Data Secure," which gathers critical transaction parameters via a formatted input form. Once submitted, the information is passed to a back-end API where a strong machine learning model analyzes the data. This model relies on real-time feature transformation for fraudulent/legitimate transaction classification purposes, returning the decision as quick feedback to the user. Deployment strategy promotes clean segregation of presentation layer from processing engine for optimum scalability as well as reliability during heavy load times. This combined approach not only boosts the overall effectiveness of the system but also optimizes data collection and fraud analysis, enhancing the security of financial transactions across the entire deployment structure.

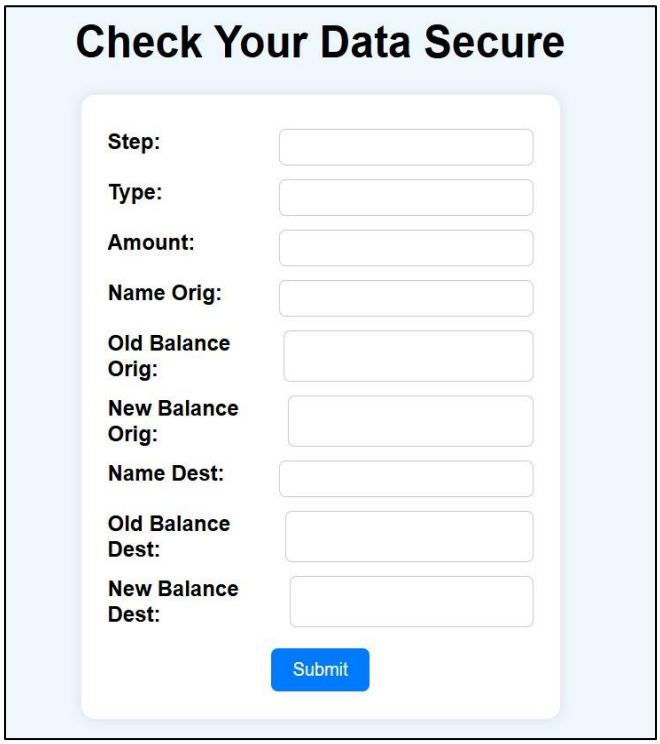

Fig 1 Deployment View

Once the user inputs the transaction information in the corresponding fields and submits it, the fraud detection system processes the data in real time. The system scans the input through an advanced fraud detection model that is capable of detecting suspicious patterns and anomalies. Through the analysis of different factors like transaction value, location, user history, and other important parameters, the model decides whether the transaction is genuine or fraudulent. The analysis process is quick, using machine learning algorithms to identify possible fraud effectively. After the analysis, the system quickly returns a result, indicating to the user whether the transaction is safe to continue or has been marked as fraudulent. This feedback in real-time prevents unauthorized transactions and adds security. The smooth integration of the fraud model guarantees fast and precise decision-making, enabling enterprises and consumers to reduce risks and have faith in financial transactions.

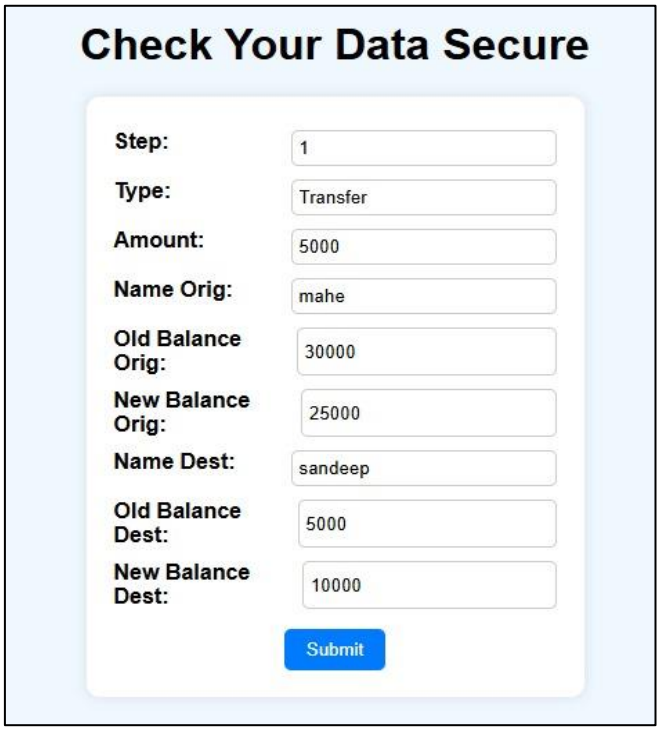

Fig 2 Checking Fraud

After the user enters the transaction details and clicks the Submit button, the fraud detection system analyzes the input using advanced machine learning algorithms. It evaluates key factors such as transaction amount, location, and user history to determine if the transaction is legitimate or fraudulent. If fraud is detected, the system immediately displays a warning message, alerting the user that the transaction is suspicious. This real-time detection helps prevent unauthorized activities, ensuring security and trust in financial transactions. By identifying fraudulent transactions instantly, the system minimizes risks and enhances protection for both businesses and users.

Fig 3 Fraud Detection

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14987486

On receipt of transaction information, the fraud detection system undertakes real-time processing and anomaly identification. Through sophisticated machine learning algorithms, the system examines crucial transactional parameters like amount, geolocation, device fingerprinting, user behavioral patterns, and historical transactions. The model utilizes statistical and AI-based fraud detection methods like supervised learning and anomaly detection to identify the legitimacy of the transaction. If no fraud is detected, the system provides a validation response, validating the authenticity of the transaction and authorizing further processing. This real-time feedback mechanism increases security, providing smooth and risk-free financial transactions. The fraud detection system combines real-time monitoring, feature engineering, and predictive analytics to constantly enhance detection accuracy. Through AI-based decision-making, the system successfully reduces false positives while keeping strong fraud prevention in place. This methodology allows for commercial and financial institutions to handle legitimate transactions effectively, with high security, operational dependability, and customer confidence.

Fig 4 Not Fraud View

VII. CONCLUSION

The fraud detection mechanism in this project is a machine learning-driven solution that effectively identifies fraudulent financial transactions with minimal false positives. It uses supervised and unsupervised learning algorithms such as Logistic Regression, Decision Trees, Random Forest, XGBoost, Support Vector Machines (SVM), and K-Means Clustering. Supervised algorithms such as XGBoost and Random Forest make decisions based on labeled historical data, whereas unsupervised algorithms such as K-Means Clustering identify anomalies by recognizing patterns that deviate from the normal pattern of transactions.

The data, derived from actual financial transactions, was subjected to deep preprocessing, such as dealing with missing values, detection of outliers, normalization of numerical features, and categorical feature encoding via Label Encoding and One-Hot Encoding. Feature engineering was utilized to improve model performance. Class imbalance was dealt with using the Synthetic Minority Over-sampling Technique (SMOTE). Feature selection techniques like Recursive Feature Elimination (RFE) and Principal Component Analysis (PCA) were used to reduce dimensionality while retaining informative features. Hyperparameter tuning with Grid Search and Random Search also enhanced model performance.

For online fraud detection, the trained models were deployed through a Flask-based RESTful API and seamlessly interfaced with financial transaction systems. There is a specialized /predict endpoint that receives transaction data, performs feature transformations, and provides fraud predictions, which are archived in a relational database (MySQL/PostgreSQL) for post-analysis. The infrastructure is deployed on cloud resources (AWS/GCP) for scalability, high reliability, and low-latency processing of transactions at high volume. Docker containerization was utilized for uniform deployment across environments.

Security features like data encryption, role-based access control (RBAC), and API authentication protect transaction data. The project offers a scalable, high-performance fraud detection system integrating advanced machine learning, real-time API deployment, cloud infrastructure, and security best practices, providing financial institutions with a comprehensive solution for fraud prevention and digital banking security.

REFERENCES

[1]. U. Siddaiah, P. Anjaneyulu, M. Ramesh, Y. Haritha. "Fraud Detection in Online Payments using Machine Learning Techniques" .DOI:10.1109/ICICCS56967.2023.10142404.

[2]. M. Naga Raju, Yarramreddy Chandrasena Reddy, Polavarapu Nagendra Babu, Venkata Sai Pavan Ravipati, Velpula Chaitanya. "Detection of Fraudulent Activities in Unified Payments Interface using Machine Learning -LSTM Networks". DOI : 10.1109/ICCPCT61902.2024.10672890.

[3]. Pinku Ranjan, Kammari Santhosh, Somesh Kumar, Arun Kumar. "Fraud Detection on Bank Payments Using Machine Learning". DOI : 10.1109/ICONAT53423.2022.9726104.

[4]. Deepanshu Thapa, Aditya Harbola ,Aditya Joshi, Vandana Rawat, Neha Pandey. "Machine learning Models for Detecting Anomalies in Online Payment: A Comparative Analysis". DOI : 10.1109/NMITCON58196.2023.10276124.

[5]. Reem A. Alzahrani, Malak Aljabri, Rami Mustafa, A. Mohammad. "Ad Click Fraud Detection Using Machine Learning and Deep Learning Algorithms". DOI : 10.1109/ACCESS.2025.3532200.

[6]. Abed Mutemi, Fernando Bacao."E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review". DOI: 10.26599/BDMA.2023.9020023.

[7]. Rayene Bounab, Karim Zarour, Bouchra Guelib, Nawres Khlifa."Enhancing Medicare Fraud Detection Through Machine Learning: Addressing Class Imbalance With SMOTE-ENN". DOI - 10.1109/ACCESS.2024.3385781.

[8]. Dr. Yogesh W Bhowte, Dr. Arundhati Roy, Dr. K. Bhavana Raj, Dr. Megha Sharma, Dr. K. Devi, Dr.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14987486

Prem Latha Soundarraj."Advanced Fraud Detection Using Machine Learning Techniques in Accounting and Finance Sector". DOI - 10.1109/ICONSTEM60960.2024.10568756.

[9]. Dr. Shaik Rehana Banu, Dr. Taviti Naidu Gongada, Kathari Santosh, Harish Chowdhary, Sabareesh R, Dr. S. Muthuperumal."Financial Fraud Detection Using Hybrid Convolutional and Recurrent Neural Networks: An Analysis of Unstructured Data in Banking". DOI - 10.1109/ICCSP60870.2024.10543545.

[10]. Ibomoiye Domor Mienye, Nobert Jere. "Deep Learning for Credit Card Fraud Detection: A Review of Algorithms, Challenges, and Solutions". DOI - 10.1109/ACCESS.2024.3426955.

[11]. Saad Hammood Mohammed, Abdulmajeed Al-Jumaily, Mandeep S. Jit Singh, Víctor P. Gil Jiménez, Aqeel S. Jaber, Yaseein Soubhi Hussein, Mudhar Mustafa Abdul Kader Al-Najjar, Dhiya Al-Jumeily."A Review on the Evaluation of Feature Selection Using Machine Learning for Cyber-Attack Detection in Smart Grid". DOI - 10.1109/ACCESS.2024.3370911.