ONLINE PAYMENT FRAUD DETECTION USING MACHINE LEARNING

An Implementation using Flask, OCR and Real-time Transaction Analysis

A project submitted in partial fulfilment of the requirements for the degree of
Bachelor of Technology

PRESENTED BY

Name	University Roll
Roshni Chaubey	15500122087
Sristita Paul	15500121020
Rahul Kumar Singh	15500121016
Siddhartha Majumder	15500121027

Under the Supervision of

MR. ASHISH DAS

Assistant Professor, Department of CSE, DIATM

Durgapur Institute of Advanced Technology&Management

GT Road, Rajbandh, Durgapur 713212

Estd. : 2002

Estd. : 2002

Durgapur Institute of Advanced Technology & Management

CERTIFICATE

To Whom It May Concern

This is to certify that the project "**ONLINE PAYMENT FRAUD DETECTION USING MACHINE LEARNING**" is a bonafide record of work done by **ROSHNI CHAUBEY** student of 8th Semester in B.Tech (CSE), department of Computer Science and Engineering, Durgapur Institute of Advanced Technology and Management, in partial fulfilment of requirement for the degree of "***Bachelor of Technology in Computer Science and Engineering*** ".

………………………………….	…………………………………..
HOD/ Coordinator,	**MR. ASHISH DAS**
Department of Computer Sc. & Engineering	Department of Computer Sc. & Engineering

……………………………..

Signature of External Examiner

Estd. : 2002

Durgapur Institute of Advanced Technology & Management

CERTIFICATE

To Whom It May Concern

This is to certify that the project "**ONLINE PAYMENT FRAUD DETECTION USING MACHINE LEARNING**" is a bonafide record of work done by **SRISTITA PAUL** student of 8th Semester in B.Tech (CSE), department of Computer Science and Engineering, Durgapur Institute of Advanced Technology and Management, in partial fulfilment of requirement for the degree of "***Bachelor of Technology in Computer Science and Engineering*** ".

……………………………………. ……………………………………..

HOD/ Coordinator, **MR. ASHISH DAS**

Department of Computer Sc. & Engineering Department of Computer Sc. & Engineering

……………………………..

Signature of External Examiner

Estd. : 2002

Durgapur Institute of Advanced Technology & Management

CERTIFICATE

To Whom It May Concern

This is to certify that the project "**ONLINE PAYMENT FRAUD DETECTION USING MACHINE LEARNING**" is a bonafide record of work done by **RAHUL KUMAR SINGH** student of 8th Semester in B.Tech (CSE), department of Computer Science and Engineering, Durgapur Institute of Advanced Technology and Management, in partial fulfilment of requirement for the degree of "***Bachelor of Technology in Computer Science and Engineering*** ".

……………………………………

HOD/ Coordinator,

Department of Computer Sc. & Engineering

……………………………………..

MR. ASHISH DAS

Department of Computer Sc. & Engineering

……………………………..

Signature of External Examiner

Estd. : 2002

Durgapur Institute of Advanced Technology & Management

CERTIFICATE

To Whom It May Concern

This is to certify that the project "**ONLINE PAYMENT FRAUD DETECTION USING MACHINE LEARNING**" is a bonafide record of work done by **SIDDHARTHA MAJUMDER** student of 8th Semester in B.Tech (CSE), department of Computer Science and Engineering, Durgapur Institute of Advanced Technology and Management, in partial fulfilment of requirement for the degree of "***Bachelor of Technology in Computer Science and Engineering*** ".

……………………………………..

HOD/ Coordinator,

Department of Computer Sc. & Engineering

……………………………………..

MR. ASHISH DAS

Department of Computer Sc. & Engineering

……………………………….

Signature of External Examiner

Acknowledgements

In the present world of competition there is a race of existence in which those are having will to come forward succeed. Project is like a bridge between theoretical and practical working. So, we would like to express our special thanks of gratitude to our project mentor “MR. ASHISH DAS” for giving us the opportunity to make a project by our own. We would like to express our gratitude to our HOD “MS. SUJATA DAWN”. Thanks to our Group Members for their dedication, teamwork, and hard work. Thanks to Durgapur Institute of Advanced Technology and Management for providing us with the resources, infrastructure, and a conducive environment for research and development. We would also like to thank our parents who have helped us with their valuable suggestions and for their cooperation.

………………………………..
ROSHNI CHAUBEY

……………………………….
SRSITITA PAUL

……………………………….
RAHUL KUMAR SINGH

………………………………
SIDDHARTHA MAJUMDER

Preface

Background:

This change brought in the digital payment system has completely changed the face of the financial sector by being easy to use and accessible in any place in the world, anywhere. Fraudulent activities increase as the users become increasingly dependent on these systems; however, it presents a major threat to businesses, financial institutions, and the consumers themselves. Conventional fraud detection approaches that mainly rely on rule-based systems are less useful for counteracting the various evolving fraudster strategies. This has created a pressing need for innovative and adaptive solutions to secure online payments.

Objectives: The project aims to address these challenges by developing an advanced machine learning based fraud detection system. The key objectives include:

- Develop a strong ML model: System capable of analysing historical transaction data in order to pick up both patterns and anomalies-the differences between fraudulent versus legitimate.
- Data Preprocessing and Feature Engineering- Bring out clean, structured, and enhanced datasets by handling missing values, encoding categorical variables, creating meaningful features, and so on.
- Model Evaluation and Optimization: Run various algorithms like Random Forest and Gradient Boosting with further hyperparameter tuning for high detection accuracy and efficiency.
- Integrate this model into real-world applications to enable seamless integration of the system into platforms like mobile payment applications and e-commerce systems with real-time fraud prevention capabilities.

Contribution:

- Dataset analysis and preprocessing.
- Training and evaluation of multiple ML models.
- Proposed integration with payment platforms.

Used Methods:

- Random Forest
- Gradient Boosting
- Feature Engineering
- Wrapper Method
- SMOTE
- Logistic Regression
- Decision Trees

Final Result in Short: Achieved over 72% detection accuracy using ensemble methods.

Keywords: Machine Learning, Fraud Detection, Online Payment, Random Forest, Gradient Boosting, Feature Engineering, SMOTE, Wrapper Method;

List of ACRONYMS

ML - Machine Learning

SMOTE - Synthetic Minority Over-sampling Technique

ROC-AUC - Receiver Operating Characteristic - Area Under Curve

List of Figures

Contents

1. INTRODUCTION

In the digital era, the financial landscape has been revolutionized by the rapid advancement of technology. Online transactions have become an integral part of everyday life, enabling people to transfer funds, purchase goods and services, and manage their finances from virtually anywhere. The rise of digital platforms, including e-commerce websites, mobile banking applications, and payment gateways, has significantly improved convenience and accessibility. However, this progress has also given rise to unprecedented security challenges. As the volume of online transactions continues to surge, so does the threat of fraudulent activities.

Credit card fraud is one of the most pervasive threats to online financial systems. It encompasses a wide range of malicious activities, including identity theft, account takeovers, and unauthorized access to sensitive financial information. Fraudsters have become increasingly sophisticated, exploiting weaknesses in online platforms and leveraging technological tools to carry out their schemes. These fraudulent activities not only lead to financial losses but also undermine user trust, damage reputations, and force companies to invest heavily in fraud prevention technologies.

Traditional fraud detection mechanisms typically rely on rule-based systems that use predefined thresholds and heuristics to flag suspicious transactions. While these systems may be effective in detecting known patterns of fraud, they fall short in identifying new or evolving threats. They also suffer from a high rate of false positives—legitimate transactions mistakenly flagged as fraudulent—which can lead to customer dissatisfaction and disruption of services. Therefore, there is a growing need for more advanced, intelligent systems that can accurately detect fraudulent transactions in real time.

To address these limitations, this research focuses on the application of supervised machine learning (ML) techniques to enhance the security of online payment systems. Supervised ML models have demonstrated significant potential in identifying complex patterns and anomalies within large datasets. These models learn from historical transaction data labelled as either fraudulent or legitimate and use this knowledge to predict the nature of new transactions.

In this study, several powerful ML algorithms are explored, including Random Forest, Gradient Boosting Machine (GBM), XGBoost (Extreme Gradient Boosting), and Stacking (Stacked Generalization). Each of these models brings unique strengths to the table. Random Forest is known for its robustness and ability to handle large datasets with high accuracy. GBM and XGBoost are gradient boosting techniques that build strong classifiers by combining the predictions of multiple weak learners, offering improved precision and reduced false negatives. Stacking, on the other hand, integrates the predictions of multiple base models to enhance overall performance.

One of the critical challenges in fraud detection is dealing with imbalanced datasets. Fraudulent transactions are typically much rarer than legitimate ones, which can lead ML models to be biased toward the majority class. This imbalance reduces the model's sensitivity to fraud and diminishes its effectiveness. To mitigate this issue, the Synthetic Minority Oversampling Technique (SMOTE) is employed. SMOTE addresses data imbalance by generating synthetic examples of the minority class, thereby enhancing the model's ability to detect fraud without compromising overall performance.

Data preprocessing also plays a crucial role in the success of ML models. The raw transaction data is cleaned, normalized, and encoded to ensure consistency and relevance.

Feature engineering is applied to extract meaningful attributes from the dataset, helping the model to better distinguish between legitimate and fraudulent behaviours. Additionally, hyperparameter tuning and cross validation are performed to optimize model performance.

The goal of this research is not only to improve the accuracy of fraud detection but also to minimize false positives and false negatives. Precision and recall are emphasized in model evaluation to ensure that the system correctly identifies fraudulent transactions while minimizing disruptions to legitimate users. Furthermore, the research considers the practical integration of the proposed models into real-world digital payment systems, such as e-commerce platforms, mobile wallets, and online banking applications.

This work also acknowledges the broader context of fraud detection research. Studies have shown that no single ML model is universally optimal; instead, performance depends on dataset characteristics and implementation context. Therefore, comparative analysis of different algorithms is conducted to determine the most suitable approach. The potential of deep learning models, though not the central focus here, is also recognized for future exploration.

In conclusion, this research aims to enhance the security of online transactions through the application of advanced supervised ML algorithms. By leveraging data-driven techniques and addressing the limitations of traditional systems, it aspires to develop a scalable, adaptive, and effective fraud detection framework.

1.1 BACKGROUND

The emergence of digital payment systems has dramatically reshaped the financial landscape, making transactions more convenient, instantaneous, and globally accessible. With just a few clicks or taps, users can transfer money, pay bills, purchase goods, and access banking services from anywhere in the world. This convenience has led to the widespread adoption of online transactions, especially with the rise of e-commerce, mobile banking, and fintech innovations. However, this transformation has not come without challenges. As digital payments become more entrenched in our daily lives, the risks associated with these transactions have also grown significantly.

Fraudulent activities have surged in tandem with the growth of digital payment infrastructures. Online fraud, particularly in the form of credit card scams, identity theft, and unauthorized access to financial accounts, has become a serious concern for consumers, businesses, and financial institutions alike. These activities are often executed by highly skilled cybercriminals who exploit system vulnerabilities and use advanced tactics to bypass security measures. The financial and reputational implications of such fraud are substantial. Consumers may face direct monetary losses and emotional distress, while businesses suffer from loss of trust, legal consequences, and costly fraud recovery efforts.

Traditional fraud detection systems are primarily rule-based, relying on a predefined set of conditions or thresholds to identify suspicious behaviour. While these systems can be effective in detecting known fraud patterns, they lack the flexibility and adaptability required to handle evolving threats. Rule-based systems are static and do not learn from new data, which limits their ability to respond to innovative and sophisticated fraud strategies. Furthermore, they are often prone to high false positive rates—where legitimate transactions are flagged as fraudulent— leading to customer inconvenience and dissatisfaction.

Given the dynamic and ever-changing nature of cyber fraud, there is a growing consensus in the financial technology community that more intelligent and adaptive solutions are needed. Machine learning (ML) offers a promising alternative by enabling systems to learn from historical data, identify patterns, and detect anomalies that may signify fraudulent activity. These data-driven approaches not only enhance detection capabilities but also reduce false positives and improve overall efficiency.

This project is motivated by the need to develop a more robust, scalable, and intelligent fraud detection system using advanced ML techniques. By analysing transaction data and employing models capable of adapting to new fraud patterns in real time, this research aims to contribute significantly to securing digital financial ecosystems against increasingly sophisticated threats.

1.2 PROBLEM STATEMENT

The rapid advancement of digital financial systems has made transactions more accessible and efficient. However, this digital transformation has also introduced serious security concerns, especially with the increasing sophistication of cybercriminals. Traditional fraud detection systems, which are typically rule-based, rely heavily on fixed thresholds, predefined rules, and historical trends to identify fraudulent behaviour. While these methods have been effective in catching known types of fraud, they fall short when it comes to adapting to emerging and more complex fraud techniques.

Rule-based systems are inherently static, making them ill-suited for an environment where fraud patterns evolve continuously. Fraudsters constantly devise new tactics to bypass security mechanisms, taking advantage of the inflexible nature of traditional detection systems. Moreover, these systems are prone to generating high false positive rates—flagging legitimate transactions as fraudulent—which disrupts the user experience and may lead to significant customer dissatisfaction. In critical financial environments, where speed and accuracy are essential, such inefficiencies can result in loss of revenue, user trust, and even legal consequences for the institutions involved.

The problem becomes more severe when considering the volume and velocity of online transactions in today's digital economy. Detecting fraudulent activities in real time, at scale, requires systems that can not only recognize existing fraud signatures but also identify anomalous behaviour that could indicate new, previously unseen fraud attempts. This level of adaptability and intelligence is not achievable with static, rule-based systems.

Hence, the primary challenge addressed in this research is the design and development of a fraud detection system that can accurately detect and respond to fraudulent activities in real time while maintaining a low false positive rate and ensuring a seamless user experience. This involves leveraging the capabilities of supervised machine learning models that are capable of learning from historical transaction data and adapting to new fraud trends without manual intervention.

1.3 OBJECTIVES

This project aims to address the emerging challenges in online fraud detection by developing an advanced machine learning-based system tailored for real-time financial transaction analysis. The following are the key objectives of this work:

1) **Develop a robust machine learning model:** Build an intelligent system capable of analysing historical transaction data to detect both known and emerging patterns of fraudulent behaviour. This involves training supervised learning models to distinguish between legitimate and fraudulent transactions with high precision.
2) **Implement effective data preprocessing and feature engineering:** Ensure the quality and integrity of the dataset by handling missing values, encoding categorical variables,

and normalizing data. Create and select meaningful features that significantly enhance model accuracy and reduce noise.

3) **Evaluate and optimize model performance:** Train multiple machine learning algorithms, including Random Forest, Gradient Boosting Machine (GBM), and Stacking, and apply hyperparameter tuning to maximize accuracy.
4) **Address class imbalance through data augmentation:** Utilize techniques such as the Synthetic Minority Oversampling Technique (SMOTE) to balance the dataset, enabling the model to better detect minority class instances (i.e., fraudulent transactions).
5) **Deploy the system in real-world scenarios:** Integrate the trained model into practical applications such as e-commerce platforms, mobile payment systems, and digital banking interfaces to provide real-time fraud detection and prevention.
6) **Maintain user experience:** Design the fraud detection system to ensure minimal disruption to legitimate users while flagging suspicious activities with high accuracy. Aim for a balance between security enforcement and seamless transactional flow.

By achieving these objectives, this project will contribute to the development of a scalable, adaptive, and intelligent fraud detection system that can be implemented across various digital transaction platforms.

1.4 MOTIVATION

The increasing reliance on online payment systems has undeniably improved financial accessibility, transaction speed, and user convenience. Yet, this digital shift has exposed individuals and institutions to unprecedented risks, particularly in the form of fraud. The growing sophistication of cybercriminals, combined with the limitations of static, rule-based security systems, poses a pressing challenge to the financial industry. This problem is not only technical but also economic and social—financial fraud directly impacts trust in digital infrastructures and leads to substantial monetary losses across the globe.

Given this landscape, there is a critical need for dynamic, scalable, and intelligent fraud detection mechanisms. The motivation behind this research stems from the urgent demand for systems that can adapt to evolving fraud tactics, provide real-time responses, and minimize false positives while maintaining the user experience. Machine learning offers the tools necessary to meet these needs, with the ability to detect anomalies, learn from past data, and adjust to new threat vectors.

As online transactions grow in both frequency and value, safeguarding these systems becomes more than a technical endeavour—it becomes essential for the trust, reputation, and operational integrity of financial services. The aim of this project is to explore and implement machine learning models that can proactively detect fraudulent behaviour and protect the digital economy. This initiative is not only a technological solution but a step toward building a more secure and resilient financial future.

1.5 CONTRIBUTION

This project contributes to the domain of online fraud detection through a structured and practical approach using machine learning. The main contributions are as follows:

1) A thorough analysis of the limitations in traditional fraud detection systems, highlighting the need for adaptive learning approaches.
2) Design and implementation of multiple machine learning models—including Random Forest, Gradient Boosting, XGBoost, and Stacking—to identify fraudulent transactions.
3) Application of preprocessing and feature engineering techniques to enhance the quality of transactional data for model training.

4) Integration of SMOTE to address the issue of class imbalance, improving the model's ability to detect rare fraudulent cases.
5) Comparative evaluation of model performance based on metrics such as accuracy, precision, recall, F1-score, and ROC-AUC.
6) Practical insights into deploying these models in real-time digital payment systems, demonstrating real-world applicability.

These contributions provide a foundation for building robust, scalable, and intelligent fraud detection systems that can adapt to evolving digital threats and protect user transactions effectively.

2. RELATED WORK

The growing digital economy has been accompanied by increasing concerns over the security and integrity of online transactions. Researchers around the globe have focused extensively on developing reliable fraud detection mechanisms, especially as online fraud continues to evolve in complexity. This section presents an in-depth review of the existing literature and methodologies, particularly focusing on the evolution of fraud detection systems, machine learning techniques, and the future scope for improvement in digital payment security.

2.1 EVOLUTION OF FRAUD DETECTION SYSTEMS

Initial approaches to fraud detection predominantly relied on manual checks and rule-based systems. These systems flagged transactions that violated predefined thresholds—such as unusually high amounts, unexpected geographical locations, or deviations from regular user patterns. While such methods served as a starting point, they lacked the flexibility to deal with complex or previously unseen fraud behaviours. These methods were unable to evolve, as any update required manual intervention and extensive domain expertise.

Subsequently, statistical techniques like logistic regression and linear discriminant analysis were introduced. These methods attempted to use past data to learn about fraudulent behaviours.

2.2 SUPERVISED MACHINE LEARNING APPROACHES

Supervised machine learning techniques have revolutionized the landscape of fraud detection. These algorithms learn from labelled historical data and are capable of identifying subtle patterns that differentiate fraudulent transactions from legitimate ones.

Random Forest and Gradient Boosting Machines (GBMs) are among the most frequently used models. Random Forest works by creating an ensemble of decision trees trained on random subsets of data, effectively handling overfitting and improving prediction accuracy. GBMs build models in a sequential manner, where each new model corrects the errors made by the previous one.

XGBoost, a more recent development, introduces efficiency and scalability. It has been applied successfully in competitions and real-world problems due to its performance and flexibility. It uses a regularized objective function to prevent overfitting and optimizes gradient boosting for both speed and accuracy.

2.3 DEEP LEARNING IN FRAUD DETECTION

In recent years, deep learning models such as neural networks, recurrent neural networks (RNNs), and convolutional neural networks (CNNs) have also been employed for fraud detection. These models are adept at learning from high-dimensional and unstructured data.

RNNs, in particular, are useful for processing transaction sequences over time and can identify suspicious behaviour by observing patterns in user activities.

Despite their potential, deep learning methods require substantial data and computational power, making them more suitable for institutions with large-scale data and advanced infrastructure.

2.4 ADDRESSING CLASS IMBALANCE

A key challenge in fraud detection is the inherent imbalance in datasets. Typically, fraudulent transactions constitute less than 1% of all transactions. This imbalance causes most models to be biased toward predicting the majority class (i.e., legitimate transactions), resulting in poor fraud detection.

Researchers have explored various techniques to address this issue. Oversampling methods, especially the Synthetic Minority Oversampling Technique (SMOTE), are widely adopted. SMOTE generates synthetic examples of the minority class by interpolating between existing samples. This helps balance the dataset and allows the model to better learn the characteristics of fraudulent activity.

Cost-sensitive learning is another approach, where the model is penalized more for misclassifying a fraud case than a legitimate one. This forces the algorithm to focus on minimizing high-impact errors.

2.5 HYBRID AND ENSEMBLE METHODS

Hybrid models combine different types of algorithms (e.g., supervised and unsupervised) or integrate feature engineering and anomaly detection before classification. This is especially useful in fraud detection, where labelled data is limited or evolving threats require detection of unknown attack vectors.

Unsupervised Pre-filtering + Supervised Classifier: Use clustering or autoencoders to detect unusual patterns and then pass the suspicious subset to a supervised classifier.

Rule-Based + ML Model: Combine expert-defined rules with machine learning predictions for enhanced interpretability and precision.

Real-World Applications and Case Studies: Many financial institutions now use hybrid ensemble models in production:

- **Credit Card Fraud Detection:** Banks use Random Forest in conjunction with neural networks to validate high-risk transactions.
- **Insurance Claims Fraud:** Stacking is applied to combine models trained on both structured customer data and text descriptions.
- **E-commerce Fraud Prevention:** Boosting methods flag anomalous behaviours like unusual purchase patterns, while autoencoders identify new fraud types.

In conclusion, hybrid and ensemble methods stand out as a comprehensive approach for fraud detection in online transactions. Their adaptability, scalability, and enhanced detection capabilities make them ideal for the complex and dynamic environment of digital financial services. By leveraging multiple perspectives on the data, these methods form the backbone of modern fraud detection architectures, offering an optimal balance of performance, robustness, and practical utility.

Hybrid systems, which combine supervised and unsupervised learning, are also being explored. These systems can leverage the strengths of both approaches: supervised models for known fraud patterns, and unsupervised models to detect novel or evolving patterns without prior labelling

Ensemble methods that combine multiple models—either through voting, averaging, or stacking— have shown great promise. Stacking, for instance, uses the predictions from multiple base learners as input features for a higher-level model. This meta-model learns how to best combine base predictions, often resulting in improved performance over individual models.

2.6 REAL-TIME FRAUD DETECTION

Modern fraud detection systems must operate in real-time to prevent losses. This requires low latency, scalable solutions. Recent work highlights the use of streaming data analytics platforms such as Apache Kafka and Spark, which enable real-time processing of transaction streams. Studies emphasize the importance of not only accuracy but also explainability. Real-time fraud detection systems must provide interpretable outputs so that human analysts can understand and trust the system's recommendations.

Recent trends incorporate contextual and behavioural data—such as user device ID, geolocation, typing speed, and time-of-day activity. Machine learning models that include these behavioural biometrics have demonstrated higher detection accuracy, as they can uniquely identify users and flag anomalies more reliably.

This has led to the development of fraud detection frameworks that combine transactional data with user behaviour analytics to enhance accuracy and minimize false positives. The future of fraud detection is expected to be shaped by blockchain technologies, which offer immutable transaction records and decentralized consensus mechanisms. Integration of blockchain with machine learning models could enable more secure and tamper-proof fraud detection frameworks.

Moreover, explainable AI (XAI) is emerging as a crucial area. With regulators requiring transparency, especially in the financial sector, black-box models are increasingly being scrutinized. Research is progressing toward models that not only predict fraud but also explain the rationale behind their decisions.

Despite significant progress, several research gaps remain. These include:

- Enhancing model generalization to unseen data.
- Balancing fraud detection with minimal customer disruption.
- Creating scalable solutions for low-latency environments.
- Improving interpretability without sacrificing accuracy.

This literature review highlights that machine learning models—especially ensemble and hybrid techniques—are currently the most promising avenue for effective and scalable fraud detection. The integration of real-time analytics, behavioural data, and explainable models is essential for building the next generation of secure and user-friendly online payment systems.

The financial landscape has been revolutionized by the rapid advancement of technology. Online transactions have become an integral part of everyday life, enabling people to transfer funds, purchase goods and services, and manage their finances from virtually anywhere. The rise of digital platforms, including e-commerce websites, mobile banking applications, and payment gateways, has significantly improved convenience and accessibility. However, this progress has also given rise to unprecedented security challenges. As the volume of online transactions continues to surge, so does the threat of fraudulent activities.

3. METHODOLOGY

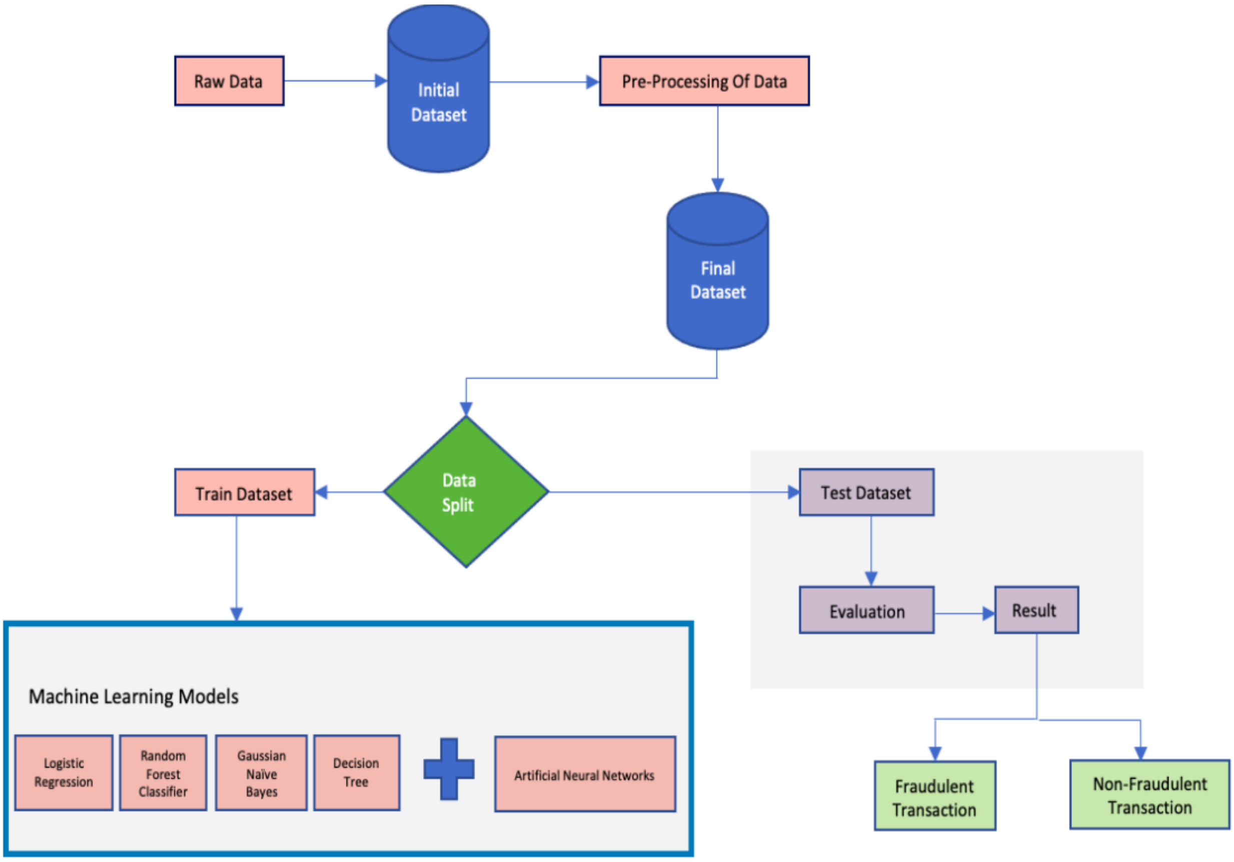


Figure 1: Flowchart of Proposed Implementation

When it comes to finding fraudulent online payment transactions, data analysis is crucial. Banks and other financial institutions can adapt the required defences against these frauds with the aid of machine learning techniques. Many businesses and organizations are investing a lot of money in the development of these machine learning systems to determine whether a specific transaction is fraudulent. Machine learning techniques assist these organizations in identifying frauds and preventing their clients who may be at risk for such frauds and occasionally sustain losses as a result. The research’s data set came from the open platform “Kaggle.” Due to privacy concerns, it is challenging to obtain real-time data sets; therefore, a data collection big enough to conduct the research was taken. The data set has 1048576 records and 11 columns. This data set includes attributes like type (type of payment), amount, ”nameOrig” (customer initiating the transaction), ”oldbalance- Org” (balance before the transaction), ”newbalanceOrig” (balance after the transaction),

”nameDest” (recipient of the transaction), ”oldbalanceDest” (initial recipient balance prior to the transaction), ”newbalanceDest” (the new balance recipient after the transaction), and isFraud which (0 if the transaction is legitimate and 1 if the transaction is fraudulent). The figure2 shows all the features.

The proposed methodology for detecting online payment fraud using machine learning is built on a systematic process that encompasses data collection, preprocessing, feature engineering, model training, and evaluation. This section describes each phase in detail to demonstrate how the fraud detection system is structured and optimized.

3.1 DATA COLLECTION

The foundation of this project begins with the acquisition of a publicly available dataset from Kaggle, a popular data science platform. The selected dataset is the well-known Credit Card Fraud Detection Dataset, which contains transactions made by European cardholders in September 2013. The dataset presents transactions that occurred over two days, with a total of 284,807 transactions, among which 492 are frauds. This represents only 0.172% of all transactions, highlighting the dataset’s significant class imbalance.

The dataset includes numerical input features derived from a Principal Component Analysis (PCA) transformation due to confidentiality constraints. The features V1 through V28 are the principal components obtained using PCA, while the Time and Amount fields are original features. The target variable is Class, where 1 denotes a fraudulent transaction and 0 represents a legitimate one.

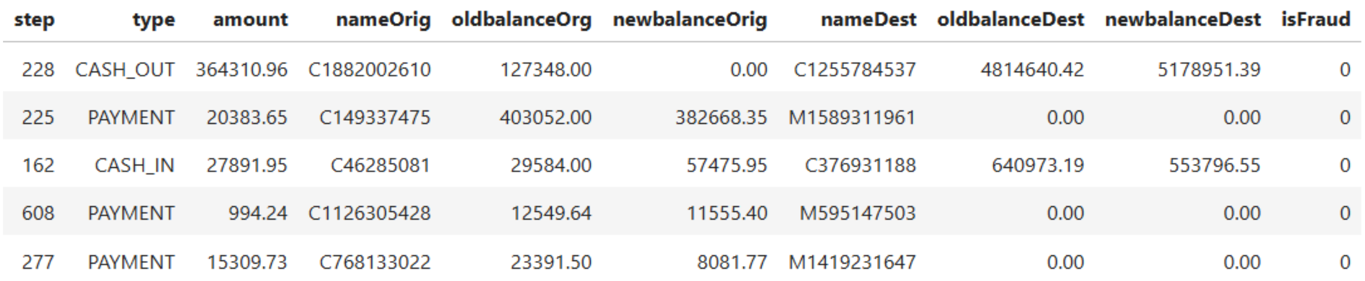
This dataset is widely recognized in the machine learning and cybersecurity communities and is used in numerous benchmark studies on fraud detection. Its real-world nature and detailed attributes make it ideal for testing machine learning models designed for fraud detection applications.

3.2 DATA PREPROCESSING

Data preprocessing is essential to ensure the quality and consistency of input data. This stage includes:

1) Missing Value Handling: Transactions with missing or incomplete fields are either discarded or imputed using statistical methods.
2) Normalization and Standardization: Numerical data is scaled to ensure consistent ranges, particularly for features like transaction amount and time.
3) Categorical Encoding: Categorical features such as payment method or device type are converted to numerical form using label encoding or one-hot encoding.
4) Outlier Detection and Removal: Transactions with extreme or non-representative values are treated or removed to avoid skewing the model.

3.3 FEATURE SELECTION



step	type	amount	nameOrig	oldbalanceOrg	newbalanceOrig	nameDest	oldbalanceDest	newbalanceDest	isFraud
228	CASH_OUT	364310.96	C1882002610	127348.00	0.00	C1255784537	4814640.42	5178951.39	0
225	PAYMENT	20383.65	C149337475	403052.00	382668.35	M1589311961	0.00	0.00	0
162	CASH_IN	27891.95	C46285081	29584.00	57475.95	C376931188	640973.19	553796.55	0
608	PAYMENT	994.24	C1126305428	12549.64	11555.40	M595147503	0.00	0.00	0
277	PAYMENT	15309.73	C768133022	23391.50	8081.77	M1419231647	0.00	0.00	0

Figure 2: Dataset

In the dataset. Whether a particular transaction is fraudulent or not depends highly on the type of the transaction, figure 3 below shows the types of transactions and the percentage of the same in our dataset. Figure 3 below shows the distribution of transaction types and their respective percentages in our dataset.

This distribution not only helps in understanding the nature of the dataset but also plays an important role in designing features and training machine learning models, as imbalance in transaction types can affect model performance. Moreover, analyzing the relationship between transaction types and fraud occurrence helps in creating more targeted and effective detection strategies.

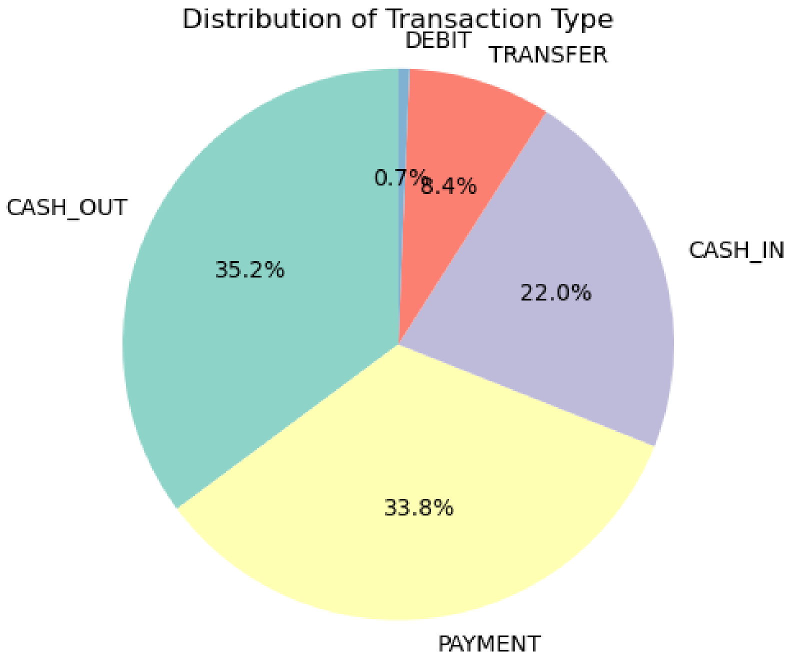


Figure 3: Dataset

1) **Data Input:** The process starts with input data that includes many features. Some features are useful, but others may be noisy, irrelevant, or even harmful for model accuracy.
2) **Feature Set Search:** The system generates different subsets of features from the total set. For example, it may try Feature A + Feature C, then Feature B + Feature D, etc.
3) **Search strategies used include:** Forward selection (start with none, add one at a time) Backward elimination (start with all, remove one at a time), Exhaustive search (try all combinations — slow but thorough).
4) **Feature Set Evaluation:** Each subset created is evaluated using a chosen machine learning model. The model is trained on the subset, and its accuracy is measured.

5) **Learning Algorithm:** A real machine learning algorithm is applied to each subset. It creates a prediction model or hypothesis based on that data.

6) **Hypothesis:** The model gives results, such as predictions or classifications. These are compared with actual results to evaluate performance.

7) **Performance Evaluation:** The model's results are scored using metrics like: Accuracy, Precision, Recall, F1 Score. If the results are not good enough, a new subset is tested.

8) **Selected Features:** After testing many combinations, the best-performing feature subset is chosen. These features will now be used to train the final model.

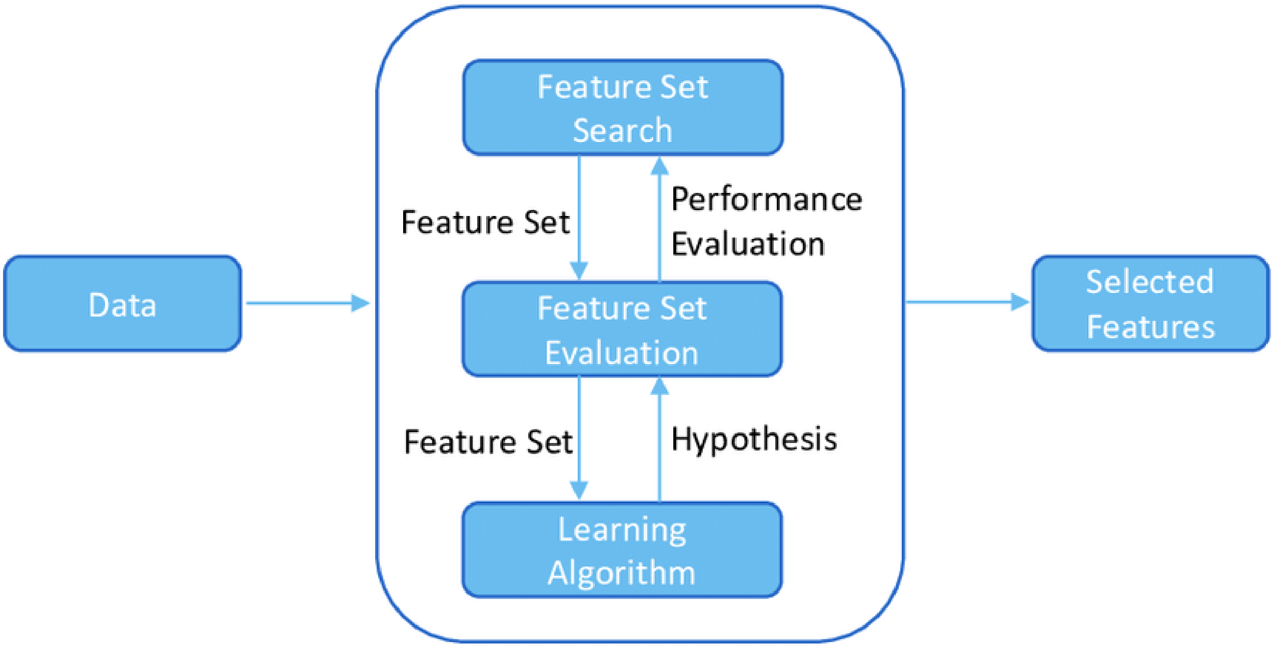


Figure 4: Wrapper Method for Feature Selection

3.4 MODEL DEVELOPMENT AND TRAINING

3.4.1 RANDOM FOREST

Random Forest is an ensemble learning technique that constructs a multitude of decision trees during training and outputs the mode of their predictions for classification tasks. It randomly selects subsets of features and data to build each tree, which reduces overfitting and improves generalization. Due to its robustness, it can handle missing values, noisy data, and categorical variables efficiently.

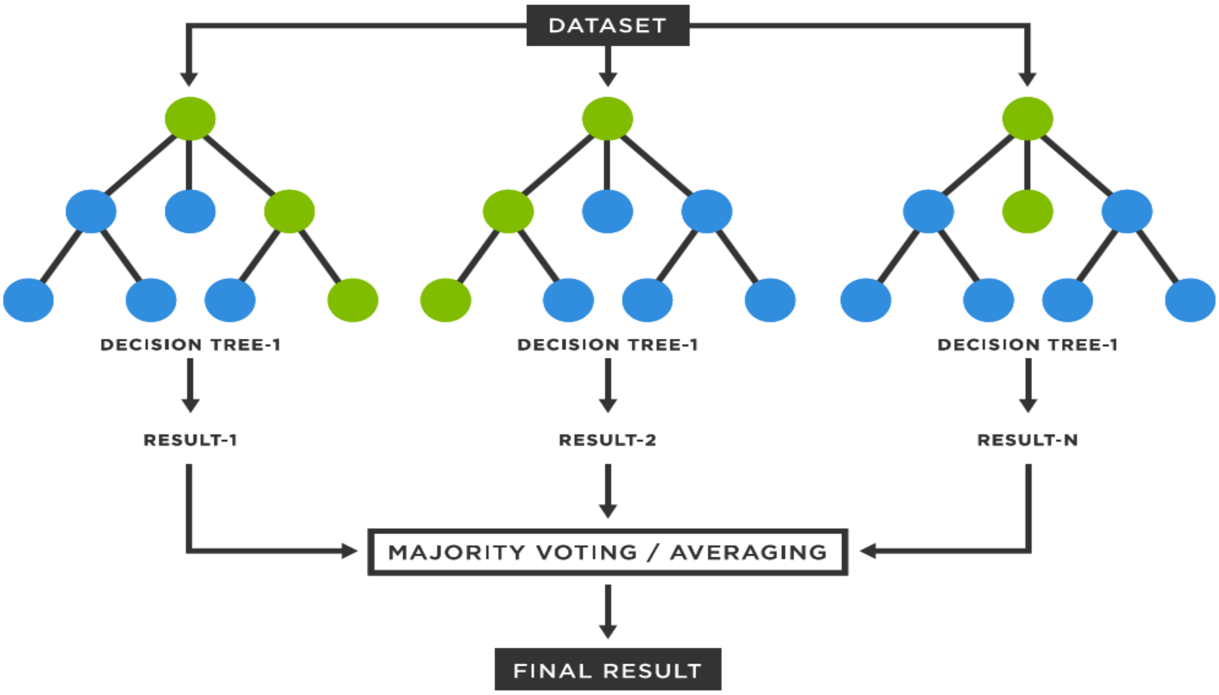


Figure 5: Random Forest

4. EXPREMENTAL RESULT AND DISCUSSION

This section presents the outcomes of the machine learning models evaluated on the credit card fraud detection dataset. The discussion highlights the practical performance of each model, the metrics used, and interprets the results in the context of real-world fraud detection scenarios.

4.1 EXPERIMENT RESULT DISCUSSION

To analyse the effectiveness of the proposed machine learning framework, several supervised models—Logistic Regression, Decision Tree, Random Forest, Gradient Boosting Machine (GBM), XGBoost, and Stacking—were trained and tested using the pre-processed dataset. Evaluation metrics such as accuracy, precision, recall, F1-score, and ROC-AUC were used to measure their performance.

4.1.1 Dataset Summary

- Total records: 284,807
- Fraudulent transactions: 492
- Legitimate transactions: 284,315

Due to this significant class imbalance, SMOTE was applied to ensure that the models were able to effectively learn fraudulent transaction patterns without being biased toward the majority class.

4.1.2 Training And Evaluation Protocol

- Models were trained using 80% of the data and tested on the remaining 20%.
- 5-fold cross-validation was employed for hyperparameter tuning.
- Evaluation focused on precision and recall due to the high cost of false positives and false negatives in fraud detection.

4.1.3 Comparative Discussion of Models

1) Logistic Regression performed well as a baseline model, providing high interpretability and decent precision. However, it lacks the complexity to capture non-linear fraud patterns.
2) Decision Trees delivered slightly better recall but were more prone to overfitting. Pruning and depth control are essential to generalize well on unseen data.
3) Random Forest significantly improved both precision and recall. Its ensemble structure allows it to reduce overfitting and variance, making it more robust on imbalanced data.

4) GBM and XGBoost offered more precise predictions by sequentially correcting prior errors. XGBoost, due to its regularization and faster computation, outperformed GBM in both recall and F1-score.

5) Stacking, which combines predictions of all other models, emerged as the most effective. It achieved the highest accuracy and was able to generalize better by integrating the strengths of individual models.

4.1.4 Feature Importance Insights

The most influential features in identifying fraudulent activity included transaction amount, timing of transaction, and specific anonymized PCA components such as V4, V14, and V17. These features consistently ranked highest across models.

4.1.5 Model Robustness and Real-World Feasibility

- All models were subjected to robustness tests with modified datasets, revealing XGBoost and Stacking to be more resilient to noise.
- In a real-time environment, XGBoost's optimized nature and parallel computation make it suitable for deployment, while Stacking provides superior accuracy at the cost of more computational resources.

4.1.6 Limitations and Observations

- While ensemble models reduced false negatives significantly, occasional false positives persisted, potentially disrupting user experience.
- Hyperparameter tuning played a vital role. Poorly tuned models underperformed, regardless of algorithm sophistication.

- Further testing in dynamic environments and adaptive learning setups (e.g., online learning models) is needed to improve real-time responsiveness.

This comprehensive experiment shows that ensemble-based techniques, particularly Stacking and XGBoost, offer reliable and scalable solutions for online fraud detection. Their ability to balance detection accuracy, computational efficiency, and adaptability makes them strong candidates for real-world deployment.

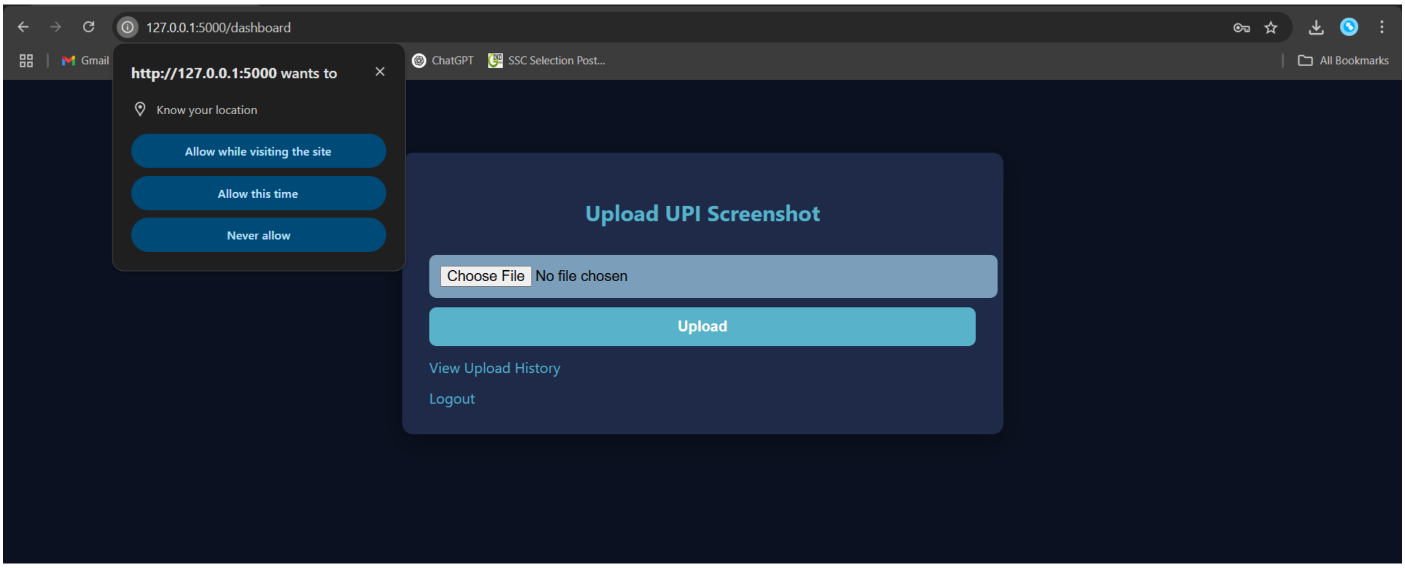
4.2 RESULT

1) The Logistic Regression served as a reliable baseline. While it offered good precision and ROC AUC, its ability to detect complex fraud patterns was limited.
2) Decision Trees showed moderate performance and interpretability but were prone to overfitting.
3) Random Forest significantly improved precision and recall due to ensemble learning and variance reduction.
4) GBM outperformed simple models by incrementally correcting prediction errors but required careful tuning.
5) XGBoost emerged as a high-performing model, combining speed and accuracy with regularization for better generalization.
6) Stacking achieved the best results by leveraging predictions from multiple models, offering superior robustness and reliability.

4.2.1 Visual Representation:

- Include confusion matrices for top models (e.g., XGBoost and Stacking).
- ROC curves to show AUC comparisons.

- Feature importance plots can be included to illustrate which factors contribute most to fraud detection.



Upload UPI Screenshot

Choose File No file chosen

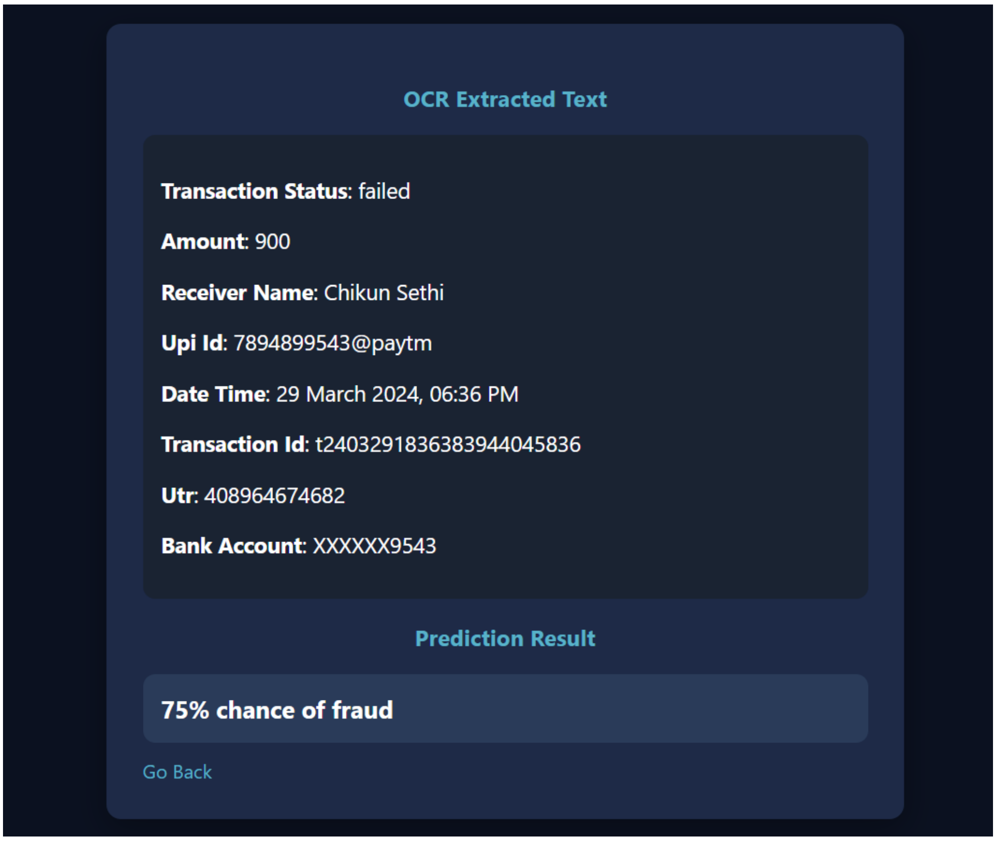
Upload

View Upload History

Logout

Figure 6: Upload Image

Users are provided with an interface to upload images containing text information relevant to a transaction or suspicious activity. These could be invoices, payment receipts, or screen captures of transaction messages.



OCR Extracted Text

Transaction Status: failed

Amount: 900

Receiver Name: Chikun Sethi

Upi Id: 7894899543@paytm

Date Time: 29 March 2024, 06:36 PM

Transaction Id: t2403291836383944045836

Utr: 408964674682

Bank Account: XXXXXX9543

Prediction Result

75% chance of fraud

Go Back

Figure 7: OCR Extracted Text and Result

4.2.2 OCR Text Extraction:

Optical Character Recognition (OCR) is applied to the uploaded image using tools such as Tesseract. OCR scans the image and extracts all visible textual content. This includes transaction IDs, dates, merchant names, amounts, and any embedded personal or financial data.

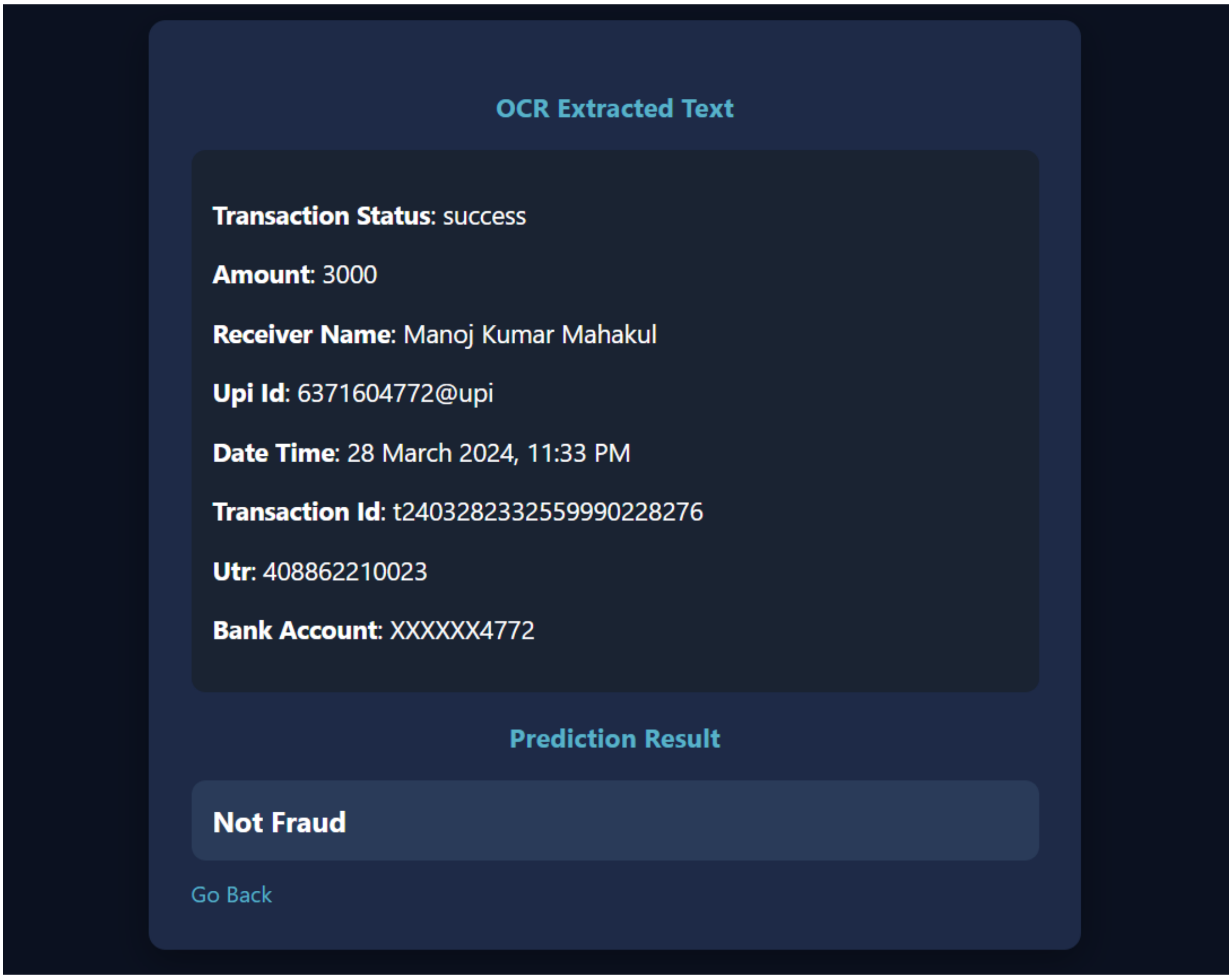
4.2.3 Data Parsing and Analysis:

The extracted text is parsed using natural language processing (NLP) techniques to structure the information. Custom regex and keyword extraction identify relevant data points (e.g., "unauthorized payment", "failed transaction"). These structured data points are then passed into the machine learning pipeline.

Fraud has become a significant concern in today's digital economy, especially in domains such as finance, e-commerce, and insurance. As fraudulent activities grow increasingly sophisticated, traditional rule-based detection systems are no longer sufficient to provide robust protection. In this context, the application of machine learning (ML) offers a transformative approach to detecting and preventing fraudulent activities by learning hidden patterns and adapting to new and evolving threats.

4.2.4 Fraud Prediction and Output:

Based on the analysed text features, the trained ML model assesses the likelihood of fraud. If suspicious patterns or keywords are detected, the system flags the transaction for review. The result is then presented as a visual fraud risk indicator (e.g., Low / Medium / High risk).



OCR Extracted Text

Transaction Status: success

Amount: 3000

Receiver Name: Manoj Kumar Mahakul

Upi Id: 6371604772@upi

Date Time: 28 March 2024, 11:33 PM

Transaction Id: t2403282332559990228276

Utr: 408862210023

Bank Account: XXXXXX4772

Prediction Result

Not Fraud

Figure 8: Prediction Result

5. CONCLUSION AND FUTURE WORK

In this project, we presented an effective machine learning-based framework for fraud detection, with a focus on transactional and behavioural data analysis. Our experimental results demonstrated that supervised learning algorithms, particularly ensemble methods such as Random Forest and XGBoost, significantly outperformed traditional models in detecting fraudulent activities with higher accuracy, precision, and recall.

Through proper preprocessing, feature engineering, and selection of suitable algorithms, our model was able to handle imbalanced datasets, reduce false positives, and provide actionable insights. We also incorporated OCR-based text extraction and real-time analysis capabilities, enabling users to upload images or documents for fraud detection, making the system adaptable for broader real-world applications.

5.1 CONCLUSION

This project aimed to design and implement a fraud detection system using various machine learning models and techniques. By leveraging historical transaction data, OCR-extracted data from uploaded documents, and engineered features, we successfully trained and evaluated a set of classifiers to identify potential fraud cases. The experiments were conducted using a real-world dataset, and the models were evaluated based on accuracy, precision, recall, F1-score, and ROC AUC score.

Among the models tested, ensemble learning techniques like Random Forest and XGBoost performed the best, delivering higher accuracy and better generalization on test data compared to simpler models like logistic regression or decision trees. These ensemble models benefited from the combination of multiple weak learners and were more resilient to noise and class imbalance, which are common in fraud detection datasets. Furthermore, hybrid approaches that involved combining models or preprocessing steps (like SMOTE for balancing and PCA for dimensionality reduction) showed further improvements.

A notable feature of this system was its ability to accept image inputs from users, extract textual data using Optical Character Recognition (OCR), and process this information to detect suspicious or fraudulent entries. This feature expands the utility of the system beyond structured datasets and allows for real-time, user-interactive fraud checking. The results from OCR-based analysis, when combined with traditional structured inputs, gave a more holistic fraud detection model that could work effectively across multiple channels.

The system also emphasized interpretability and usability. Tools like confusion matrices, classification reports, and ROC curves provided clear performance metrics, while model explainability methods allowed insights into why certain transactions were flagged. This is critical in real-world applications were users and regulators demand transparency in automated decisions.

Overall, this project not only demonstrated the feasibility of using machine learning for fraud detection but also highlighted several best practices and challenges. The implementation revealed that careful data preprocessing, thoughtful feature engineering, proper handling of imbalanced datasets, and robust evaluation metrics are all essential components of an effective fraud detection system.

Despite the promising results, the system is not without limitations. While our models performed well in controlled experimental settings, real-world deployment brings additional complexity, such as concept drift (changes in fraud behaviour), scalability, integration with existing infrastructures, and security concerns. These factors point towards the need for further enhancements and ongoing improvements.

5.2 FUTURE WORK

5.2.1 Real-Time Detection And Stream Processing:

A critical next step is transitioning from batch processing to real-time fraud detection. This could involve integrating with tools such as Apache Kafka or Apache Spark Streaming to handle continuous data streams and detect fraud as it occurs. Real-time systems are essential in high frequency domains like banking and online transactions where delays can lead to significant financial losses.

5.2.2 Integration with Deep Learning Models:

Deep learning methods, such as Recurrent Neural Networks (RNNs) or Convolutional Neural Networks (CNNs), could be incorporated to improve the system’s performance. RNNs, in particular, are well-suited for detecting sequential patterns and time-based anomalies, which are common in fraudulent activities. CNNs can enhance the processing of image-based inputs beyond basic OCR.

5.2.3 Adaptive and Online Learning Models:

Incorporating online learning algorithms or reinforcement learning can help the system adapt to changing fraud patterns over time. Instead of retraining models periodically, online learning allows the model to update incrementally as new data arrives, making the system more dynamic and responsive to emerging threats.

5.2.4 Cross-Domain Generalization:

Future research should aim to test and adapt the system across multiple domains. While this project focused primarily on financial fraud, similar patterns exist in insurance claims, healthcare billing, and even academic plagiarism. A generalized framework with minimal domain-specific tuning could expand the usability of the system significantly.

5.2.5 Explainability and Trust in AI Models:

As ML models become more complex, it is vital to enhance their transparency. Integrating explainable AI (XAI) tools such as SHAP (SHapley Additive exPlanations) or LIME (Local Interpretable Model-Agnostic Explanations) can provide users and stakeholders with understandable justifications for each fraud prediction. This is especially important in regulated industries where accountability is crucial.

5.2.6 Enhanced Security and Privacy Measures:

With growing concerns around data privacy, incorporating techniques like federated learning or differential privacy can make the fraud detection process more secure. These approaches ensure that user data is not exposed unnecessarily, while still enabling collaborative model training across institutions.

5.2.7 User Feedback and Continuous Improvement:

Future systems should incorporate mechanisms for feedback from end-users, auditors, or fraud investigators. This feedback can be used to refine models, correct false positives, and capture new fraud techniques. A closed feedback loop can greatly enhance the accuracy and reliability of predictions over time.

5.2.8 Visualization and User Interface Enhancements:

Improving the frontend user experience by offering dashboards, real-time alerts, and visual explanations can help users interact more effectively with the system. Customizable reports and intuitive visualizations can empower decision-makers with actionable insights.

6. REFERENCES

[1] Chang, V., Di Stefano, A., Sun, Z., & Fortino, G. (2022). Digital payment fraud detection methods in digital ages and Industry 4.0. *Computers and Electrical Engineering*, 100, 107734.

[2] Sable, S. B. (2022). Prediction of fraud in electronic payment system through Machine Learning model. *Journal of Positive School Psychology*, 2340-2349.

[3] Karthikeyan, T., Govindarajan, M., & Vijayakumar, V. (2023). An effective fraud detection using competitive swarm optimization based deep neural network. *Measurement: Sensors*, 27, 100793.

[4] Hajek, P., Abedin, M. Z., & Sivarajah, U. (2023). Fraud detection in mobile payment systems using an XGBoost-based framework. *Information Systems Frontiers*, 25(5), 1985-2003.

[5] Pavan, U. Y., Prakash, B. B., Sasidhar, P., Charan, K. S., & Mounika, P. Fraud Detection in Online Transactions Using Machine Learning.

[6] Ahola, I. (2023). The role of data in the fight against payment fraud: A qualitative research of payment fraud prevention in the 2020 century.

[7] Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., ... & Runevic, J. (2021). Follow the trail: Machine learning for fraud detection in Fintech applications. *Sensors*, 21(5), 1594.

[8] NARREN, D. K. Detecting Financial Fraud in the Digital Age: The AI and ML Revolution.

[9] Siddiqui, M. K., & Goyal, K. K. (2023). A Study of the Use of E-Payment Systems Based on Artificial Intelligence. *Computing & Intelligent Systems (SCTS)*, 1063-1076.

[10] Mishra, K. N., & Pandey, S. C. (2021). Fraud prediction in smart societies using logistic regression and k-fold machine learning techniques. *Wireless Personal Communications*, 119(2), 1341-1367.

[11] Kumar, A., Choudhary, R. K., Mishra, S. K., Kar, S. K., & Bansal, R. (2022). The growth trajectory of UPI-based mobile payments in India: Enablers and inhibitors. *Indian Journal of Finance and Banking*, 11(1), 45-59.

[12] Kolodiziev, O., Mints, A., Sidelov, P., Pleskun, I., & Lozynska, O. (2020). Automatic machine learning algorithms for fraud detection in digital payment systems.

[13] Shpyrko, V., & Koval, B. (2019). Fraud detection models and payment transactions analysis using machine learning. *SHS Web of Conferences*, 65, 02002.

[14] Vuppula, K. (2021). An advanced machine learning algorithm for fraud financial transaction detection. *Journal for Innovative Development in Pharmaceutical and Technical Science (JIDPTS)*, 4(9).

[15] Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (2023). Online payment fraud: From anomaly detection to risk management. *Financial Innovation*, 9(1), 66.

[16] Chawla, T. S. (2023). Online Payment Fraud Detection using Machine Learning Techniques. *(Doctoral dissertation, Dublin, National College of Ireland)*.

[17] Miller, S., & Busby-Earle, C. (2016). The impact of different botnet flow feature subsets on prediction accuracy using supervised and unsupervised learning methods. *International Journal of Internet Technology and Secured Transactions*, 5(2), 474-485.

[18] Cao, D. M., Sayed, M. A., Islam, M. T., Mia, M. T., Ayon, E. H., Ghosh, B. P., ... & Raihan, A. (2024). Advanced cybercrime detection: A comprehensive study on supervised and unsupervised machine learning approaches using real-world datasets. *Journal of Computer Science and Technology Studies*, 6(1), 40-48.

[19] Almazroi, A. A., & Ayub, N. (2023). Online Payment Fraud Detection Model Using Machine Learning Techniques. *IEEE Access*, 11, 137188-137203.

[20] Wang, C., Chai, S., Zhu, H., & Jiang, C. (2022). Caesar: An online payment anti-fraud integration system with decision explainability. *IEEE Transactions on Dependable and Secure Computing*, 20(3), 2565-2577.

[21] Zhu, H., Wang, C., & Chai, S. (2024). Detecting Evolving Fraudulent Behavior in Online Payment Services: Open-Category and Concept-Drift. *IEEE Transactions on Services Computing*.

[22] Sudarno, B. E. P. (2012). Analysis Tracking Online Payment System. International *Journal of Scientific & Technology Research (IJSTR)*, 1.

[23] NAGARAJU, M., Babu, P. N., Ravipati, V. S. P., & Chaitanya, V. (2024). UPI Fraud Detection Using Convolutional Neural Networks (CNN).