AI in Finance: Enhancing Credit Card Fraud Detection Using Machine Learning for Improving Accuracy, Real-Time Prevention and Increasing Financial Security

Shaik Fiaza Tazeen[1], D.Murali[2]

[1]*PG Student, QUBA College of engineering and technology*

[2]*Associate Professor, QUBA College of engineering and technology*

Abstract: In the realm of digital finance, credit card fraud has become a growing concern due to the surge in online transactions. This project offers a machine learning-based solution to detect fraudulent transactions, leveraging Random Forests to differentiate between legitimate and fraudulent activities in real time. The web application provides users with an intuitive interface for loading datasets, training models, making predictions, visualizing fraud patterns, and generating performance reports. The methodology includes preprocessing steps like encoding transaction types, scaling numeric features, and splitting the data into training and testing sets. A Random Forest classifier is optimized using GridSearchCV to maximize accuracy. The project also features a fraud detection simulation, allowing users to input transaction details and receive predictions on potential fraud via an interactive interface. While traditional methods like logistic regression and decision trees have been widely used, this project focuses on Random Forests for enhanced accuracy and efficiency. The model excels in handling high-dimensional data and minimizing overfitting. Comprehensive visualizations, such as histograms and pie charts, provide deep insights into transaction patterns, offering a clear understanding of fraud trends and system performance.

Index Terms— **credit card fraud, online transactions, machine learning, Random Forest, data preprocessing, fraud detection, GridSearchCV, real- time prediction, transaction behavior, model performance, hyperparameter tuning, interactive interface, financial losses, fraud trends, visualizations, accuracy, computational efficiency.**

1. INTRODUCTION

1.1 MOTIVATION

In today's digital era, the banking industry has experienced a profound transformation, marked by a major shift toward online transactions. While this has brought exceptional convenience and efficiency, it has also led to a rise in fraudulent activities. These fraudulent transactions pose significant risks to financial institutions and their customers, resulting in considerable financial losses and eroding trust in digital banking systems. Consequently, developing robust and efficient fraud detection systems has become a critical priority for the banking sector.

Traditional fraud detection methods typically rely on rule-based systems and manual reviews, which are not only time-intensive but also susceptible to errors and inefficiencies. These approaches struggle to keep up with fraudsters' constantly evolving tactics, as they adapt to evade conventional security measures. This has created an urgent need for more advanced, intelligent solutions that can detect fraudulent activities with greater accuracy and in real-time.

This project explores the application of artificial intelligence (AI) and machine learning (ML) techniques to enhance credit card fraud detection in banking transactions. By leveraging the power of predictive analytics, this study aims to identify and mitigate fraudulent transactions more effectively than traditional methods. The focus is on analyzing transaction data to uncover patterns and anomalies indicative of fraud, thereby providing a proactive approach to fraud prevention.The dataset used in this project includes detailed information about transactions, such as the amount, initial and post-transaction balances of both the customer and the recipient, and the type of transaction.

Rigorous data preprocessing is performed to ensure high-quality inputs for the machine learning models. This includes steps like data normalization, feature selection, and the use of correlation heatmaps to refine the dataset. Various machine learning models are employed, including Logistic Regression, Random Forest, and Gradient Boosting. These models are chosen for their ability to handle large volumes of data and their robustness in making predictions.

They are trained and evaluated using key performance metrics such as accuracy, precision, recall, and F1-score, which provide a comprehensive assessment of their effectiveness in detecting fraud.In comparison to existing models like Decision Trees and Naive Bayes, the approaches used in this study show significant improvements. Ensemble methods, in particular, demonstrate superior performance by combining the strengths of multiple models, resulting in higher detection rates and lower false positive rates. This highlights the potential of AI and machine learning techniques in revolutionizing fraud detection systems.

1.2 DEFINITION

Fraud detection in digital banking involves the systematic identification and prevention of fraudulent activities within financial transactions. As online banking and digital payment systems gain widespread use, the risk of fraud has increased, prompting the need for more advanced detection methods. The primary goal of fraud detection is to safeguard financial institutions and their customers from monetary losses while ensuring the security and trustworthiness of digital banking platforms. This process requires analyzing large volumes of transactional data to identify patterns and anomalies that signal potential fraudulent behavior. Fraud detection systems employ various techniques to identify suspicious activity. Traditional methods typically rely on rule- based systems, which use predefined rules and patterns to flag transactions as potential fraud risks.

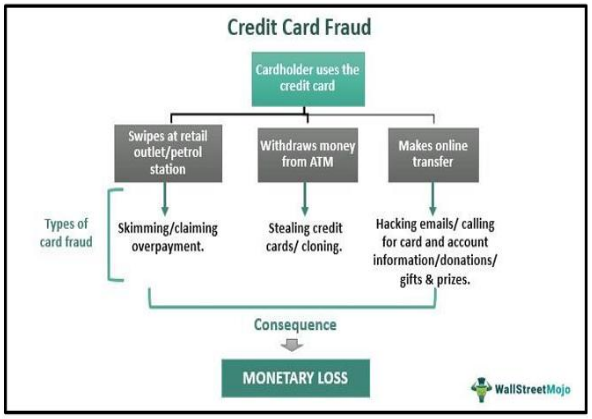

Credit Card Fraud
Cardholder uses the credit card
Swipes at retail outlet/petrol station
Withdraws money from ATM
Makes online transfer
Types of card fraud
Skimming/claiming overpayment.
Stealing credit cards/ cloning.
Hacking emails/ calling for card and account information/donations/ gifts & prizes.
Consequence
MONETARY LOSS
WallStreetMojo

Fig-1.2 : Types of Credit Card Fraud in Banking System

II SYSTEM ANALYSIS

2.1 LITERATURE SURVEY

1. Zheng, Y.-J., Zhou, X.-H., Sheng, W.-G., Xue, Y., & Chen, S.-Y. (2018). Generative adversarial network based Telecom Fraud Detection at the Receiving Bank. Neural Networks, 102, 78–86.

Zheng et al. (2018) introduced a Generative Adversarial Network (GAN) approach for detecting telecom fraud at the receiving bank. GANs are used to generate synthetic data that mimic legitimate transactions, helping the model learn to distinguish between genuine and fraudulent activities. This technique improves the system's ability to detect and prevent fraud in telecom banking services.

2. Liu, J.-M., et al. (2017). A hybrid semi-supervised approach for Financial Fraud Detection. 2017 International Conference on Machine Learning and Cybernetics (ICMLC).

Liu et al. (2017) proposed a hybrid semi-supervised learning approach for financial fraud detection. This method combines labeled and unlabeled data to improve the model's learning process and detection accuracy. By leveraging semi-supervised techniques, the model can effectively identify fraudulent transactions even with limited labeled data, enhancing its practical applicability.

III SYSTEM ANALYSIS

An in-depth examination of project data using a variety of phases, methods, functions, and entities constitutes the analysis of computer data, project data, algorithm data, and other inner and outer data relevant to the proposed study. System analysis is a collection of scientific methods for figuring out the specifications for project task design. For the design of the suggested system, system analysis examined a variety of functional and non-functional requirements. In order to create a logical model of the system, the current system analysis has examined numerous publications pertinent to the project's work and planned the design using a variety of tools, including class diagrams, sequence diagrams, data flow diagrams, and data dictionaries.

3.1 EXISTING SYSTEM:

Existing systems for Credit Card fraud detection in banking transactions have evolved significantly, incorporating various technological advancements to tackle the complex issue of financial fraud. Traditional methods often relied on rule-based systems and statistical techniques, which used predefined rules and historical data to identify suspicious activities. These systems were designed to flag transactions that deviated from established patterns, but they struggled with the ever- evolving nature of fraudulent techniques. While effective to some extent, these methods were limited in their ability to adapt to new and sophisticated fraud strategies, leading to a higher rate of false positives and missed detections.

3.1.1 DISADVANTAGES:

Existing Credit Card fraud detection systems, while advanced, have several notable disadvantages. Traditional rule-based systems, which were once the cornerstone of fraud detection, often struggle to keep up with the constantly evolving tactics used by fraudsters. These systems rely on predefined rules and patterns, which can quickly become outdated as fraud strategies become more sophisticated. Consequently, they tend to generate a high number of false positives—flagging legitimate transactions as fraudulent—which can overwhelm the review process and lead to the on unnecessary customer inconvenience.

3.2 PROPOSED SYSTEM:

The proposed system for online credit card fraud detection is built using a machine learning framework, with Random Forest as the primary model. The system utilizes various transaction- related features such as transaction amount, balances before and after the transaction, time step, and more, to predict whether a transaction is fraudulent or not. The data preprocessing steps ensure that the input data is clean and ready for model training, which significantly enhances the model's performance. The system is designed to provide real-time predictions for credit card transactions, flagging those that are suspected to be fraudulent.

The model's accuracy of 98.6% demonstrates its reliability in correctly identifying both fraudulent and legitimate transactions. By using a confusion matrix and correlation heatmap, the system also provides visual insights into the relationships between features and how well the model distinguishes fraud. At the core of the system is the Random Forest classifier, known for its robustness and ability to handle large and complex datasets. This algorithm works by constructing multiple decision trees during training, each analyzing a subset of features, and then combining the results of these trees to make a final prediction. Its ability to reduce overfitting by averaging multiple predictions makes it particularly suitable for detecting fraud in highly imbalanced datasets, where fraudulent transactions are rare compared to legitimate ones. The high accuracy and low error rates are supported by the system's confusion matrix, which shows minimal misclassification of legitimate transactions as fraudulent and vice versa.

3.3 MODELS:

The code implements several machine learning models, including Logistic Regression, Random Forest, and K-Nearest Neighbors (KNN), to detect fraudulent credit card transactions. Each model has its strengths and limitations, providing a diverse set of techniques for comparison. Logistic Regression is a simple yet effective model for binary classification tasks like fraud detection. It works by estimating the probability that a given transaction is fraudulent based on the provided features. Although Logistic Regression is fast and interpretable, it may struggle with complex relationships in the data, especially in high-dimensional spaces like credit card fraud detection, where interactions between features might be intricate.

3.4 MODULES USED IN PROPOSED SYSTEM

3.4.1 USER

- View Home page: Here user view the home page of the Classifications web application.
- View Upload page: In the about page, users can learn more about the prediction.
- Input Model: The user must provide input values for the certain fields in order to get results.
- View Results: User view's the generated results from the model.
- View score: Here user have ability to view the score in %

3.4.2 SYSTEM

- Working on dataset: System checks for data whether it is available or not and image files. load the
- Pre-processing: Data need to be pre-processed according the models it helps to increase the accuracy of the model and better information about the data.
- Training the data: After pre-processing the data will split into two parts as train and test data before training with the given algorithms.
- Model Building: To create a model that predicts the personality with better accuracy, this module will help user.
- Generated Score: Here user view the score in %
- Generate Results: We train the machine learning algorithm and predict the hate speech

IV. SYSTEM REQUIREMENTS SPECIFICATION

4.1 SYSTEM REQUIREMENTS SPECIFICATION

Software requirements specifications (SRS), also known as software system requirements specifications, offer a comprehensive description of the duties that a system must do. The use cases in this section describe how the software interacts with its users. The SRS also contains non functional specifications in addition to the usage case. Non-functional specifications are criteria that limit design or execution (such as requirements for performance engineering, quality standards or design constraints).

4.1 SOFTWARE REQUIREMENTS

• Operating System	:	Windows 11
• Server-side Script	:	Python
• IDE	:	Visual Studio Code
• Framework	:	Streamlit
• Dataset	:	Credit Card Data Collection

4.2 HARDWARE REQUIREMENTS

• Processor	:	I3/Intel Processor
• RAM	:	4GB
• Hard Disk	:	160GB
• Key Board	:	Standard Windows Keyboard
• Monitor	:	SVGA

4.1.1 MACHINE LEARNING CLASSIFICATIONS

Although supervised and unsupervised learning are two of the most widely accepted machine learning methods by businesses today, there are various other machine learning techniques. Following is an overview of some of the most accepted ML methods.

4.3 FEASIBILITY STUDY

Finding the optimum solution to meet performance requirements is the goal of a feasibility study. They include a description of identification, an assessment of potential system candidates, and the choice of the best candidate.

- Economic Feasibility
- Technical Feasibility
- Behavioral Feasibility

V SYSTEM DESIGN

5.1 ARCHITECTURE DESIGN

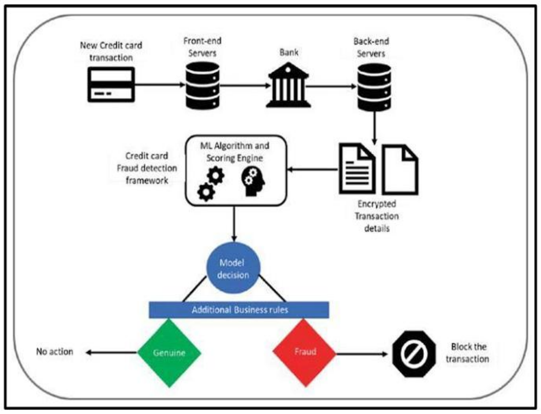

New Credit card transaction
Front-end Servers
Bank
Back-end Servers
Credit card Fraud detection framework
ML Algorithm and Scoring Engine
Encrypted Transaction details
Model decision
Additional Business rules
No action
Genuine
Fraud
Block the transaction

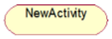
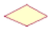
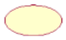
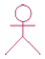
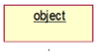
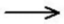
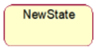
Fig-5.1: System Architecture Diagram

The system architecture for the proposed credit card fraud detection model is designed to efficiently handle the data flow from input to prediction while ensuring scalability and reliability. At its core, the architecture consists of three main layers: the data ingestion layer, the processing layer, and the presentation layer. The data ingestion layer collects and preprocesses transaction data, including features like transaction amount, sender and recipient balances, and transaction type. This data is then fed into the processing layer, where various machine learning models, such as Logistic Regression, Random Forest, and K-Nearest Neighbors, are applied for fraud detection.

The processing layer includes model training and evaluation components to continuously improve the system's accuracy. Finally, the presentation layer serves as the user interface, enabling users to input transaction details and receive real-time predictions on potential fraud. Additionally, the architecture supports data visualization tools that showcase performance metrics and insights, enhancing user experience and decision-making capabilities. Overall, this structured architecture ensures an effective and responsive fraud detection system capable of adapting to evolving transaction patterns.

5.2 INTRODUCTION TO UML DIAGRAMS

As the strategic importance of software grows, the industry searches for ways to automate software development, enhance quality, cut costs, and accelerate time-to-market. Component technology, visual programming, patterns, and frameworks are a few examples of these techniques. When a company grows, it searches for ways to control the scope and size of its systems. reduce their complexity.

S.NO	SYMBOL NAME	NOTATION	DESCRIPTION
1.	Initial Activity		This diagram depicts the flows initial point or activity.
2.	Final Activity		A bull's eye icon marks the conclusion of the activity graphic.
3.	Activity		Represented by a rectangle with a rounded edge.
4.	Decision		One that requires decision-making.
5.	Use Case		Explain how a user and a system communicate.
6.	Actor		A function a user has in relation to the system.
7.	Object		A Real-Time entity.
8.	Message		To communicate between the lives of object.
9.	State		It depicts events that occur during an objects lifetime.

VI. SYSTEM TESTING

6.1 SOFTWARE TESTING TECHNIQUES

Software testing is a method for evaluating the quality of software products and identifying defects so that they can be rectified. Software testing makes an effort to accomplish its goals, but there are significant constraints. On the other side, for testing to be effective, dedication to the set objectives is required.

6.1.1 Testing Objectives

- The user stories, designs, specifications, and code that make up the work products
- To ensure that all conditions are satisfied.
- Ensuring that the test object is complete and meets the expectations of users and stakeholders

6.1.2 Test Case

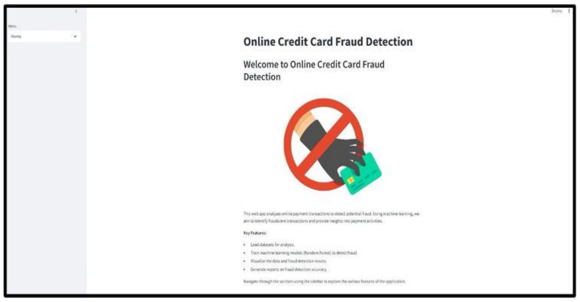
Design Every engineering product can be tested in one of these.

6.2 TESTING OF A WHITE BOX

Black box testing and white box testing are two types of software testing methodologies. White Box testing, also known as structural testing, clear box testing, open box testing, and transparent box testing, is covered in this article. It focuses on evaluating the infrastructure and software's fundamental code against current inputs and anticipated and desired outcomes. It emphasises internal structure analysis and is focused on a program's internal activities. To construct test cases for this type of testing, programming knowledge is needed. Focusing on the inputs and outputs of the software while also ensuring its security is the core aim of white box testing. The phrases "clear box," "white box," and "transparent box" all allude to being able to see through the exterior covering of the software. White testing a box is used by designers. This stage involves testing every line of the program's code. Prior to handing off the programme or software to the testing team, the developers run white-box testing on it to ensure that it conforms with the requirements and to identify any mistakes.

VII RESULTS

7. OUTPUT SCREENSHOTS WITH DESCRIPTION



Online Credit Card Fraud Detection

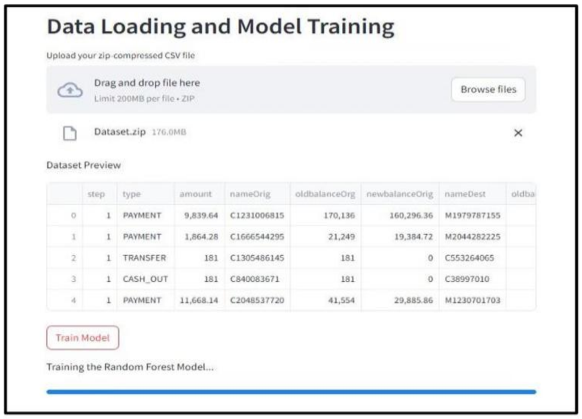
Welcome to Online Credit Card Fraud Detection

This web app analyzes online payment transactions to detect potential fraud. Using machine learning, we aim to identify fraudulent transactions and provide insights into payment activities.

Key Features:

- Load datasets for analysis.
- Train machine learning models (Random Forest) to detect fraud.
- Visualize the data and fraud detection results.
- Generate reports on fraud detection accuracy.

Navigate through the sections using the sidebar to explore the various features of the application.



Data Loading and Model Training

Upload your zip-compressed CSV file

Dataset Preview

	step	type	amount	nameOrig	oldbalanceOrg	newbalanceOrig	nameDest	oldba
0	1	PAYMENT	9,839.64	C1231006815	170,136	160,296.36	M1979787155	
1	1	PAYMENT	1,864.28	C1666544295	21,249	19,384.72	M2044282225	
2	1	TRANSFER	181	C1305486145	181	0	C553264065	
3	1	CASH_OUT	181	C840083671	181	0	C38997010	
4	1	PAYMENT	11,668.14	C2048537720	41,554	29,885.86	M1230701703	

Training the Random Forest Model...

VIII CONCLUSION AND FUTURE ENHANCEMENTS

8. CONCLUSION

The proposed credit card fraud detection system presents an effective approach to addressing the growing challenge of fraudulent transactions in the financial sector. By leveraging machine learning algorithms such as Random Forest, Logistic Regression, and K-Nearest Neighbors, the system achieves a high level of accuracy in identifying suspicious activities. Notably, the Random Forest model stands out with an impressive 98% accuracy rate, owing to its ability to handle large datasets and complex feature interactions. Timely fraud detection is essential for financial institutions, and this system's real-time processing capability enables the swift analysis of incoming transaction data, providing immediate feedback on the likelihood of fraud.

This responsiveness helps minimize risk, enhances customer trust, and safeguards institutional reputation. The inclusion of data visualization tools adds further value by offering clear insights into transaction trends, model performance, and fraud patterns. These visualizations support better decision-making and allow stakeholders to monitor system effectiveness over time. Looking ahead, the system can be improved by integrating advanced techniques such as deep learning, which may further boost detection capabilities. Implementing feedback loops for continuous model retraining using new transaction data will help the system adapt to evolving fraud tactics. Additionally, features like multi-factor authentication and user behavior analytics could enhance overall system security.

FUTURE ENHANCEMENTS

Future enhancements to the proposed credit card fraud detection system can significantly boost its accuracy, adaptability, and user experience. Incorporating advanced machine learning techniques—such as deep learning and ensemble methods—can improve the detection of complex fraud patterns. Models like Long Short-Term Memory (LSTM) networks can capture temporal dependencies in transaction sequences, enhancing detection of sophisticated tactics. Integrating real-time feedback mechanisms and online learning will enable continuous model retraining, keeping the system responsive to emerging threats. User-reported false positives and negatives can further refine model accuracy.

Enhancing the user interface with customizable alerts and actionable insights can increase user engagement and trust. Features like setting transaction thresholds, receiving alerts for unusual activity, and integrating multi-factor authentication (MFA) or biometric verification can further strengthen security. Additionally, incorporating user behavior analytics—tracking spending habits, transaction frequency, and location patterns—can reduce false positives and support more nuanced fraud detection.

REFERENCE

[1] Y.-J. Zheng, X.-H. Zhou, W.-G. Sheng, Y. Xue, and S.-Y. Chen, "Generative adversarial network based Telecom Fraud Detection at the Receiving Bank," Neural Networks, vol. 102, pp. 78–86, 2018.

[2] J.-M. Liu et al., "A hybrid semi-supervised approach for Financial Fraud Detection," 2017

International Conference on Machine Learning and Cybernetics (ICMLC), 2017.

[3] D. Sarma et al., “Bank fraud detection using community detection algorithm,” 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), 2020.

[4] Z. Sangi, “A data mining based fraud detection hybrid algorithm in E- bank,” 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), 2020.

[5] Al-Shehari, T. and Alsowail, R.A., 2021. An insider data leakage detection using one-hot encoding, synthetic minority oversampling and machine learning techniques. Entropy, 23(10), p.1258.

[6] Fanai, H., & Abbasimehr, H. (2023). A novel combined approach based on Deep Autoencoder and deep classifiers for credit card fraud detection. Expert Systems with Applications, 217, 119562.

[7] N. K. Gyamfi and J.-D. Abdulai, “Bank fraud detection using support vector machine,” 2018 IEEE 9th Annual Information Technology.