# Acropolis Institute of Technology & Research, Indore

## Department of IT (Information Technology)

A

Synopsis Report

On

Minor Project

# Credit Card Fraud Detection


**Guided By**

Prof. Manish Vyas

**Submitted By**

Khushi Agrawal (0827IT221076)

Amay Saxena (0827IT221014)

Akshat Soni (0827IT221011)

Ameer Saif Khan (0827IT221015)



Department of IT (Information Technology)

Acropolis Institute of Technology & Research, Indore

Session Sep-Jan (2024-25)

# Acropolis Institute of Technology & Research, Indore

**Department of IT (Information Technology)**

A

Synopsis Report

On

Minor Project

## Credit Card Fraud Detection

# 1. Introduction:

## 1.1. Overview:

- **What Is Credit Card Fraud Detection?**

Credit card fraud detection is a set of methods and techniques designed to block fraudulent purchases, both online and in-store. This is done by ensuring that you are dealing with the right cardholder and that the purchase is legitimate. Overall, credit card fraud detection is a critical area of research in the financial industry, with significant potential for improving fraud detection rates and reducing financial losses.

## 1.2. Purpose of the project/Innovativeness and usefulness:

The purpose of this project is to detect the fraudulent transactions made by credit cards. The primary purposes of this project are as follows:

- **Prevent Fraud:** By identifying fraudulent transactions early on, organisations can protect their clientele and minimise financial losses.
- **Reduce costs:** Reduce manual intervention and chargebacks to save time and resources.
- **Ensure Scalability:** Offer a system that complies with financial standards and can expand across sectors.

# 2. Literature Survey:

## 2.1. Existing Problem:

The existing systems designed to address sign language recognition have several limitations:

- **Limitations of Rule-Based Systems:** These systems are only effective based on predefined rules and may fail to detect new or evolving types of fraud.
- **Inability to Adapt:** Rule-based systems struggle to adapt to new fraud patterns as they rely on static, predefined rules.
- **Challenges with Traditional Methods:** While machine learning algorithms and statistical techniques offer improvements, they still face challenges in fully capturing complex and dynamic fraud patterns.

## 2.2 Proposed Solution:

- **Suggested Solution**
    - The model used must be simple and fast enough to detect the anomaly and classify it as a fraudulent transaction as quickly as possible.
    - Imbalance can be dealt with by properly using some methods which we will talk about in the next paragraph.
    - For protecting the privacy of the user the dimensionality of the data can be reduced.
    - A more trustworthy source must be taken which double-check the data, at least for training the model.

# 3. Theoretical Analysis:

## 3.1. Block Diagram:

## 3.2. Required Resources:

- **Hardware Requirements:**

    1. **Computer/Server:** To develop and train machine learning models, you'll need a computer with sufficient processing power (CPU/GPU) and memory (RAM), especially if you're working with large datasets.

    2. **Storage Devices:** A high-capacity SSD or external storage for large datasets.

- **Software Requirements:**

    1. Python (Scikit-learn, TensorFlow, PyTorch).

    2. R: For statistical analysis.

    3. Libraries: Scikit-learn, Pandas, NumPy (data manipulation and machine learning).

    4. TensorFlow/PyTorch: for advanced models.

    5. Data Storage: MySQL/PostgreSQL (relational databases).

    6. MongoDB (non-relational databases).

## 4. Methodology to be adopted/ Planning of work:

The project methodology and work plan involve the following key phases:

1. **Data Collection:**

Gather data using past transaction records from financial institutions. Public datasets such as those from Kaggle can complement real data.

2. **Data Preprocessing:**

Clean and preprocess the collected data. This includes data augmentation, normalization, and labeling.

3. **Model Development:**

Create a credit card fraud detection model using deep learning techniques like convolutional neural networks (CNNs) or recurrent neural networks (RNNs).

4. **Real-Time Recognition:**

Implement the model to provide real-time credit card fraud recognition.
This phase involves integrating the trained model into a functional system.

5. **Testing and Evaluation:**

Rigorously test the system's accuracy, performance, and reliability.
Identify and address any issues or discrepancies in the recognition process.

6. **User Interface:**

Develop an intuitive and user-friendly interface for the system.
Ensure that it is accessible and easy to use for the end users.

7. **Documentation:**

Create comprehensive project documentation, including user manuals, installation guides, and technical documentation for system maintenance.

## 5. Applications:

Credit card fraud detection is used in various applications:

- **Online Retailers:** To prevent unauthorized transactions and protect against fraud in e-commerce.
- **Banking and Financial Institutions:** For securing online and in-store transactions and monitoring account activities.
- **Mobile Payments:** To ensure secure transactions through apps and mobile wallets.
- **Insurance Companies:** To identify fraudulent claims and ensure legitimate transactions.

## 6. Impact of the Work on Real Life / End User:

- **Financial Protection**: Effective fraud detection systems can help prevent unauthorized transactions, protecting users from financial losses.
- **Increased Trust**: When users know that their financial institutions have robust fraud detection measures in place, they are more likely to trust and use their services.
- **Impact on Credit Scores:** Rapid detection can limit the duration and impact of fraud on a user's credit score, helping them maintain a healthier financial profile.
- **User Experience:** Effective fraud detection can balance security and convenience, ensuring that legitimate transactions are not unnecessarily flagged, enhancing the overall user experience.

## 7. Expected outcomes/Benefits:

The expected outcomes and benefits of credit card fraud detection for end users include:

### 1. Financial Security

- **Prevention of Unauthorized Transactions**: Users are protected from fraudulent transactions, reducing or eliminating potential financial losses.

### 2. Quick Issue Resolution

- **Faster Dispute Settlements**: Fraud detection systems typically notify users of suspicious activity in real-time, allowing for rapid resolution of disputes.

### 3. Better Transaction Experience

- **Seamless Usage with Security**: With effective fraud detection in place, legitimate transactions are processed smoothly without unnecessary declines, while fraud attempts are flagged instantly.

### 4. Enhanced Fraud Awareness

- **Increased Vigilance Among Users**: Regular alerts and notifications raise awareness about potential threats, encouraging users to adopt better security practices like monitoring account activity.

## 8. References:


1. **Bence Jendruszak (2024).** Credit Card Fraud Detection: What is It, How It Works and Its Importance**:** https://seon.io/resources/credit-card-fraud-detection/

2. **Ravindra Saini (2023).** A Survey on Detection of Fraudulent Credit Card Transactions Using Machine Learning Algorithms**:** https://ieeexplore.ieee.org/document/10076122

3. **Malam Alamri (2022).** Survey of Credit Card Anomaly and Fraud Detection Using Sampling Techniques: https://safetyculture.com/topics/data-collection/