Expanding Horizon
ICEEM
Engineering the world
with Holistic Development

ICEEM
INTERNATIONAL CENTER OF EXCELLENCE IN ENGINEERING AND MANAGEMENT

Department of Computer Science & Engineering

A.Y.: 2024 - 2025

Presentation on
"Credit Card Fraud Detection"

1.Ritesh Paithankar

Table of Contents

- Problem Statement
- Motivation
- Objectives
- Introduction
- Literature Survey
- Methodology

Implementation with Screenshots

Result Analysis

Conclusion

Future Scope

References

Problem Statement

Identify fraud of credit card transactions

- Define the specific issue: the rise of credit card fraud and its impact on individuals and businesses.
- Include data/statistics to emphasize the problem's scale.

Challenges:

- Addressing imbalanced datasets and evolving fraud patterns
- Balancing accuracy and real time fraud detection

Goal:

- Build an accurate and efficient system to detect credit card Fraud

Motivation

Expanding Horizon
CEEM
Engineering the world
with Holistic Development

- The rising prevalence of credit card fraud leads to significant financial losses for individuals, banks, and businesses.
- Fraud detection is crucial to maintain trust in digital payment systems and protect sensitive customer information.
- Traditional rule-based methods are insufficient against evolving fraud patterns, necessitating advanced, AI-powered solutions.

Objectives

Expanding Horizon
CEEM
Engineering the world
with Holistic Development

- Develop an effective system to identify fraudulent transactions in real-time.
- Minimize false positives to avoid inconveniencing legitimate users.
- Utilize machine learning techniques to adapt and improve detection accuracy.
- Propose a scalable, efficient, and cost-effective fraud detection model.

Introduction

- Credit card fraud involves unauthorized transactions or misuse of card information, costing billions annually.

- Common types include card-not-present (CNP) fraud, lost/stolen card use, and synthetic identity fraud.
- With increasing transaction volumes, automated systems powered by machine learning are essential for effective fraud detection.

Literature Survey

Expanding Horizon
CEEM
Engineering the world with Holistic Development

Sr. No.	Paper Title	Author Name	Methodology	Contribution	Drawback
1	Credit Card Fraud Detection Using Neural Network	Raghavendra Patidar, Lokesh Sharma	Decision Tree Algorithm, Random Forest Classifier	Combines neural networks (for pattern recognition) with genetic algorithms (for parameter optimization) to enhance fraud detection capabilities.	Requires large datasets for initial training, challenging to implement in early stages due to lack of patterns.

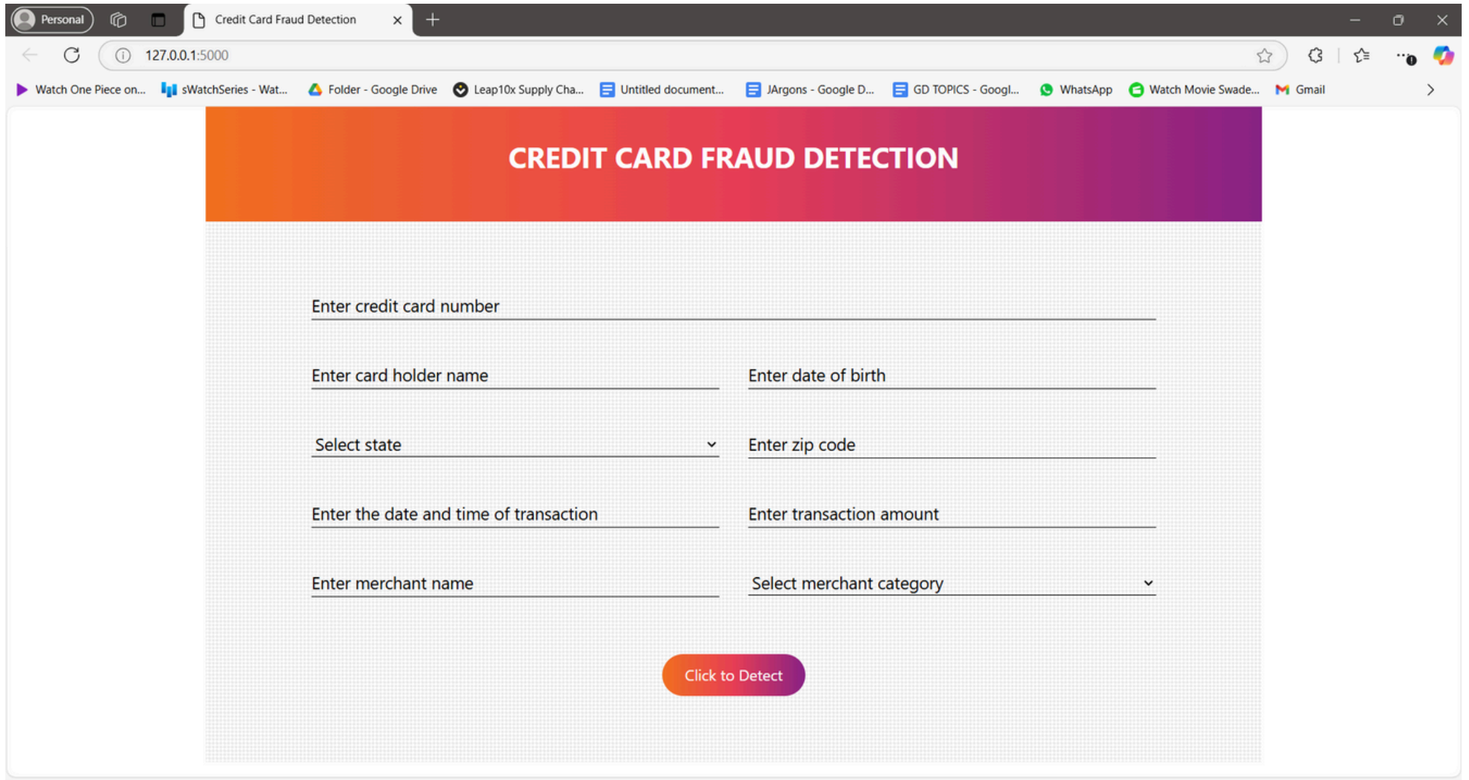
Methodology

Expanding Horizon
CEEM
Engineering the world
with Holistic Development

- **Data Collection:**
- Use transaction datasets containing labeled data (fraudulent and non-fraudulent transactions).
- **Data Preprocessing:**
- Handle missing values, normalize numerical features, and encode categorical variables.
- Address data imbalance using techniques like oversampling (SMOTE) or undersampling.
- **Feature Selection:**
- Identify key attributes like transaction amount, time, location, and user behavior.
- **Model used:**
- **Model Training:**
- Train supervised models (e.g., logistic regression, random forests, neural networks) using labeled data.
- Test unsupervised models for anomaly detection in unlabeled datasets.

Expanding Horizon
CEEM
Engineering the world
with Holistic Development

Implementation with Screenshots



RESULT

VALID TRANSACTION

Back to Home

Result Analysis

Expanding Horizon
CEEM
Engineering the world
with Holistic Development

- **Performance Metrics:**
  Discuss the performance of your fraud detection model using:
- **Accuracy:** The percentage of correctly identified transactions (fraud vs. non-fraud).
- **Precision and Recall:** How well the model identifies true fraud cases.
- **F1-Score:** A balance between precision and recall.
- **Visual Representations:**
- Confusion Matrix: Show how well the model classifies fraud and non-fraud transactions.
- ROC Curve: Demonstrate the trade-off between true positive rate and false positive rate.
- Bar charts or pie charts comparing fraud detection rates with other models.
- **Insights:**
  Highlight any observations, such as:
- Patterns in fraudulent transactions (e.g., time of day, geographic trends).
- Model strengths (e.g., high recall for fraud cases) and weaknesses (e.g., false positives).

Conclusion

Expanding Horizon
CEEM
Engineering the world
with Holistic Development

- Summarize the key findings:
- Explain how the solution effectively addresses credit card fraud detection.
- Emphasize its real-world implications, such as reducing fraud-related losses for businesses and protecting customers.

- Reflect on the significance of AI/ML in fraud detection and its potential to outpace traditional methods.

Future Scope

Expanding Horizon
CEEM
Engineering the world
with Holistic Development

- **Improvements to the Model:**
- Explore more sophisticated techniques like deep learning (e.g., LSTM for time-series data).
- Consider hybrid models that combine supervised learning with anomaly detection.

- **Scalability:**
- Propose enhancing the system to handle larger datasets or work in high-frequency transaction environments.

- **Real-Time Detection:**
- Suggest improvements in real-time detection systems using advanced stream processing tools (e.g., Apache Kafka).

- **Privacy and Security:**
- Advocate for methods like federated learning to improve user data privacy while maintaining detection accuracy.
- Use blockchain technology to secure payment systems and reduce fraud risks.

References

- Jitendra Dara,Laxman Gundemoni, “Credit Card Security And E-Payment.”2006.
- The New England Debit Card Task Force “Best Practice Guide for Managing Debit Card Fraud.” IEEE July 2005.