GUARDING TRANSACTION WITH AI-POWERED CREDIT CARD FRAUD DETECTION AND PREVENTION

INTRODUCTION

OBJECTIVES

DATASET OVERVIEW

DATA PREPROCESSING

REGRESSION TECHNIQUES USED

MODEL EVALUATION METRCIS

INSIGHTS AND ANALYSIS

CONCLUSION

INTRODUCTION

In today’s digital economy , credit card transaction have become an integral part of daily financial activities , enabling seamless payments across the globe. However , with the surge in online transaction, the risk of fraudulent activities has escalated, posing significant threats to consumers and financial institutions alike. Traditional fraud detection systems, reliant on rule-based mechanisms, often fall short in identifying sophisticated fraud patterns. This gap has led to the emergence of Artificial Intelligence(AI) as a powerful tool for enhancing credit card fraud detection and prevention. AI leverages advanced algorithms, machine learning, and real-time data analysis to identify anomalies, predict fraudulent behaviours, and mitigate risks more effectively than conventional methods. This paper explores the transformative role of AI in securing transactions, highlighting key technologies, implementation strategies, and potential challenges in combating credit card fraud.

OBJECTIVE

* + - 1. Analyse the limitations of traditional fraud detection methods and the need for AI integration.
      2. Explore the key AI technologies utilized in fraud detection, such as machine learning, neural networks, and data mining.
      3. Assess the effectiveness of AI algorithms in identifying fraudulent transaction in real time.
      4. Highlight case studies of successful AI implementation in fraud prevention across financial institutions.
      5. Identify potential challenges, including data privacy concerns and algorithmic bias, and propose strategies to address them.

DATASET OVERVIEW

Kaggle Dataset:

Real card transaction with fraud labels. Link

Paysim Dataset:

Fake mobile money transaction with fraud tags.

IEES-CIS Dataset:

Online transaction with user info and fraud labels. Link

DATA PREPROCESSING

DATA CLEANING :

Handling missing values and removing duplicates to ensure accurate data for analysis.

DATA TRANFORMATION:

Scaling and transforming data to make it ready for machine learning models.

DATA BALANCING:

Addressing class imbalance in fraud detection by using techniques like SMOTE or undersampling.

FEATURE ENGINEERING:

Creating new features from existing data to improve model performance and insights.

REGRESSION TECHNIQUES USED

LINEAR REGRESSION:

Used to find trends in data, but not often for fraud detection.

LOGISTIC REGRESSION:

Predicts if a transaction is fraudulent (yes or no).

RIDGE AND LASSO REGRESSION:

Improves models by preventing overfitting and identifying key features.

POLYNOMIAL REGRESSION:

Used for complex relationships in data, helping to detect hidden fraud patterns.

MODEL EVALUATION MATRICS

ACCURACY:

Shows how many predictions were correct overall.

PRECISION:

Measures how many of the predicted fraud cases were actually fraud.

RECALL:

Shows how many actual fraud cases were caught by the model.

F1 -SCORE:

A balance between precision and recall, useful when both matter.

ROC-AUC:

Measures how well the model can tell the difference between fraud and non-fraud.

INSIGHT AND ANALYSIS:

FINDING PATTERNS:

Analysing data helps identify common signs of fraud, like specific times, amounts, or locations.

CLASS IMBALANCE:

Fraud detection often has more legitimate transactions that fraud cases. This imbalance can affect model accuracy, so balancing techniques are used to improve results.

COMPARING MODELS:

By checking metrics like precision and recall, we can see which models catch more fraud while avoiding mistakes.

FALSE POSITIVES/NEGATIVES:

False positives (legit transaction flagged as fraud) annoy customers, while false negatives (fraud missed) cause financial loss. Balancing these errors is important.

FEATURE IMPORTANCE:

Analysing which factors (e.g., amount, time, location) matter most helps improve the fraud detection model.

CONCLUSION

Fraud detection is important to prevent financial losses and protect both businesses and customers. By using machine learning models and evaluating them with metrics like precision and recall, we can improve fraud detection accuracy. Data preparation, such as balancing the dataset and creating useful features, helps make the model better. Managing false positives and negatives is a challenges , but balancing them is key to a system. Overall regular model checks and feature analysis help keep the systems effective as fraud patterns change.