A216 Khushi Patil

Credit Card Fraud Detection

Using Machine Learning

Contents

- Introduction
- Literature Review
- Algorithm
- Libraries Used
- Limitations
- Possible Outcomes

INTRODUCTION

- Credit card fraud detection using machine learning is a critical application in the financial industry.
- The digital payments market is soaring as the world shifts towards online and card-based payment methods at a faster rate. With such a shift comes the growing issue of cybersecurity and fraud, which is more common than ever. According to a recent report, credit card fraud within the next 5 years will cause global losses of about $43 billion.
- Enhancing credit card fraud detection is a priority for all banks and financial organisations. By using Machine learning (ML), credit card fraud detection is becoming easier and more efficient. ML-based fraud detection solutions can track patterns and prevent abnormal transactions.

Importance and relevance

1.
- Credit card fraud is a significant problem, costing billions of dollars annually, and machine learning can help mitigate these losses.

2.
- credit card fraud detection is vital for safeguarding financial interests, building trust, ensuring legal compliance, and protecting the integrity of the global financial system.

3.
- Its relevance will continue to grow as technology advances and cybercriminals develop increasingly sophisticated methods for carrying out fraudulent activities.

LITERATURE REVIEW

- Machine learning models can recognise unusual credit card transactions and fraud. The first and foremost step involves collecting and sorting raw data, which is then used to train the model to predict the probability of fraud.

- The solutions offered by machine learning for credit card fraudulent detection involve:

1. Classifying whether credit card transactions are authentic or fraudulent using algorithms such as logistic regression, random forests.

2. Predicting whether it is the cardholders or the fraudsters using the credit cards through credit card profiling

3. Using outlier detection methods to identify considerably different transactions (or 'outliers') from regular credit cards transactions to detect credit card fraud.

Main Trends, debates, or gaps

1. Recent Trends in credit card fraud detection involve advanced technologies like deep learning and behavioral analytics.

2. Debates center around finding the right balance between accuracy and false positives and determining whether to use adaptive or static rules.

3. Gaps include addressing emerging threats, cross-border fraud, resource constraints for smaller entities, and improving strategies to manage false positives.
   These trends, debates, and gaps underscore the ongoing evolution and complexity of credit card fraud detection efforts.

ALGORITHM

- We will primarily focus on the Random Forest algorithm for credit card fraud detection.
- Random Forest is a powerful and versatile ensemble learning algorithm that is widely used in machine learning for its ability to improve prediction accuracy, handle noisy data, and reduce overfitting. It has applications in various domains, including finance, healthcare, and image recognition.
- Random Forest is an ensemble learning method that builds multiple decision trees and combines their predictions improve accuracy.
- Random Forest is known for its robustness, ability to handle large datasets, and resistance to overfitting.

Benefits of using machine learning

1. **Faster detection :**
A machine learning model can quickly identify any drifts from regular transactions and user behaviours in real time. By recognising anomalies, such as a sudden increase in transactional amount or location change, ML algorithms can minimise the risk of fraud and ensure more secure transactions.

2. **Higher accuracy:**
Conventional fraud detection techniques cause errors at the payment gateways that sometimes result in genuine customers being blocked. With sufficient training data and insights, ML models can achieve higher accuracy and precision, reducing these errors along with the time required to be spent on performing manual analysis.

3. **Improved efficiency with larger data:**
Once an algorithm picks up different transactional patterns and behaviours, it can efficiently work with large datasets to separate authentic payments from fraudulent ones. The models can analyse huge amounts of data in seconds while offering real-time insights for improved decision-making capabilities.

Limitations

1. Our model may not catch sophisticated fraud patterns immediately, and it may generate false positives in certain cases.

2. Challenges include imbalanced datasets, evolving fraud tactics, and computational resource requirements.

Main challenges involved in credit card fraud detection:

1. Enormous Data is processed every day and the model build must be fast enough to respond to the scam in time.
2. Imbalanced Data i.e most of the transactions *(99.8%)* are not fraudulent which makes it really hard for detecting the fraudulent ones
3. Data availability as the data is mostly private.
4. Misclassified Data can be another major issue, as not every fraudulent transaction is caught and reported.

5.Adaptive techniques used against the model by the scammers

POSSIBLE OUTCOMES

- We expect our model to significantly improve fraud detection rates compared to traditional methods.
- Enhanced fraud detection can lead to reduced financial losses for both financial institutions and cardholders.
- Our model can provide a safer and more secure financial environment.

Thank You !