ACROPOLIS INSTITUTE OF TECHNOLOGY AND RESEARCH

Department of Information Technology

Synopsis

On

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 youare 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 bycredit cards. The primary purposes of this project are as follows:

- **Prevent Fraud:** By identifying fraudulent transactions early on, organizations can protect their clientele and minimize financial losses.
- **Reduce costs:** Reduce manual intervention and chargebacks to save time and resources.
- **Ensure Scalability:** Offer a system that complies with financial standardsand 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 fraudpatterns as they rely on static, predefined rules.
- **Challenges with Traditional Methods:** While machine learningalgorithms and statistical techniques offer improvements, they still facechallenges in fully capturing complex and dynamic fraud patterns.

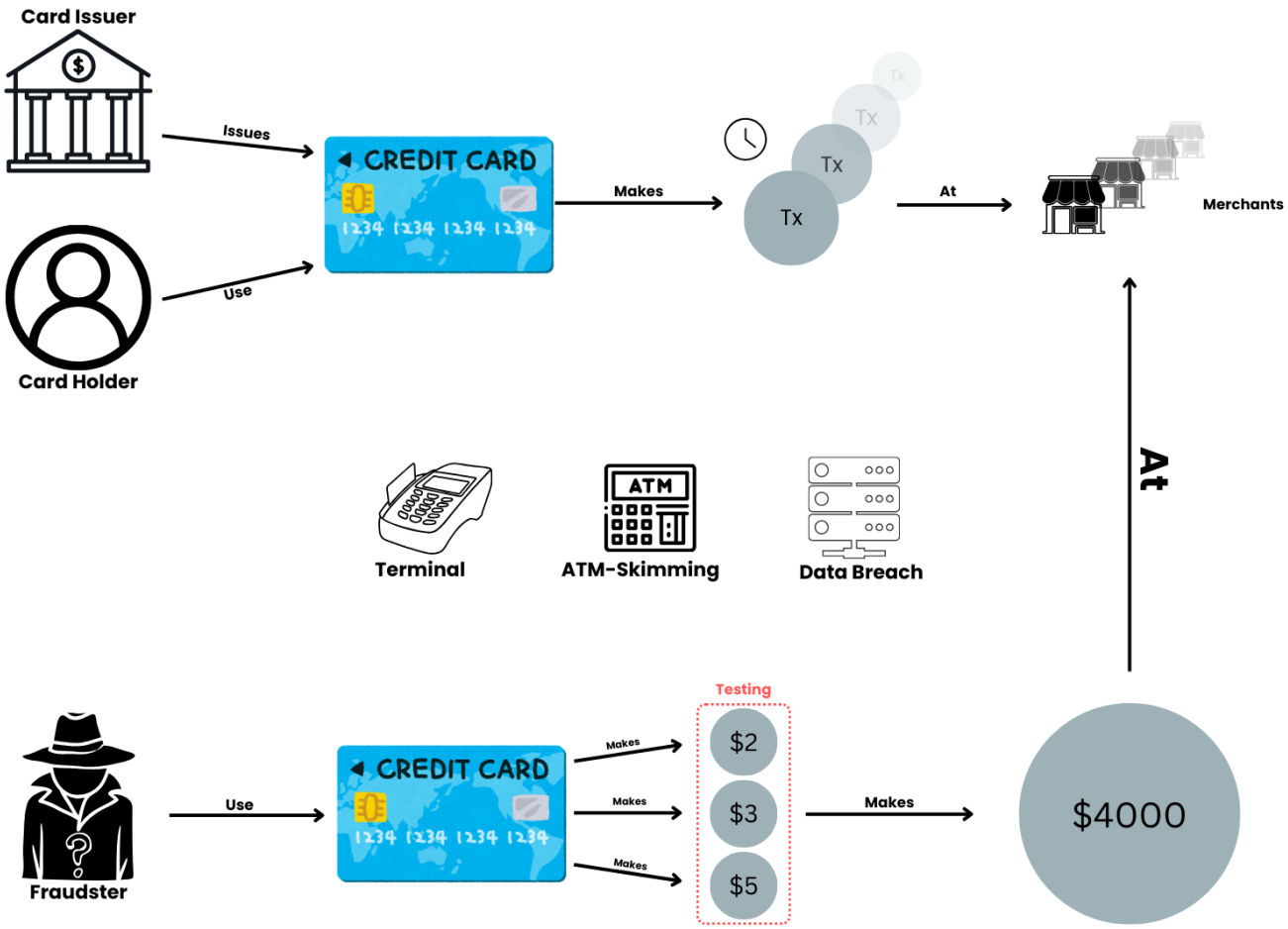
2.2 . Proposed Solution:

Suggested Solution

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

3. THEORETICAL ANALYSIS:

3.1. Block Diagram:



- **Acquiring Card Information:** Fraudsters obtain credit card details through skimming or data breaches.
- **Initial Testing:** They start with small transactions, around $2-$3, at common merchants like Starbucks.
- **Gradual Increase:** Transaction amounts are increased to test the card's usability.
- **Final Large Purchase:** Once confirmed, they make a big purchase using the card.
- **Switching to New Cards:** After validation, they move on to the next stolen card.
- **Role of Graph Databases:** These databases help detect such testing patterns, preventing large fraudulent transactions.

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 forlarge datasets.

- **Software Requirements:**

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

2. R: For statistical analysis.

3. Libraries: Scikit-learn, Pandas, NumPy (data manipulation andmachine 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. Publicdatasets 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 protectagainst fraud in e-commerce.
- **Banking and Financial Institutions:** For securing online and in-storetransactions and monitoring account activities.
- **Enhanced Security for Online Payments:** Provides an extra layer of security for online transactions, helping to prevent fraud in e-commerce and online banking scenarios.
- **Insurance Companies:** To identify fraudulent claims and ensurelegitimate transactions.
- **Legal and Regulatory Compliance:** Helps financial institutions meet regulatory requirements for monitoring transactions and preventing fraud in line with anti-money laundering (AML) and Know Your Customer (KYC) laws.

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 haverobust 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 andimpact of fraud on a user's credit score, helping them maintain a healthierfinancial profile.
- **User Experience:** Effective fraud detection can balance security and convenience, ensuring that legitimate transactions are not unnecessarilyflagged, enhancing the overall user experience.

7. EXPECTED OUTCOMES/BENEFITS:

The expected outcomes and benefits of credit card fraud detection for endusers 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 CardTransactions Using Machine Learning Algorithms**:** https://ieeexplore.ieee.org/document/10076122

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

4. Westerlund, Fredrik (2017). "CREDIT CARD FRAUD DETECTION (Machine learning algorithms)." Thesis, Umeå universitet, Statistik, 2017: http://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-136031

5. Grafiati (2021). Journal articles on the topic 'Credit card fraud detection'. https://www.grafiati.com/en/literature-selections/credit-card-fraud-detection/journal/

Guided By:

Prof. (Dr.) Manish Vyas

Group Members:

Khushi Agrawal (0827IT221076)

Amay Saxena (0827IT221014)

Akshat Soni (0827IT221011)

Ameer Saif Khan (0827IT221015)