

Creditcard Fraud Prediction

1. Introduction

1.1. Overview

Detecting fraud transactions is of great importance for any credit card company. Predicting a fraud transaction can prevent huge money loss and can increase the security of the transactions. Machine Learning algorithms can be used to classify a normal transaction and a fraud transaction.

1.2. Purpose

When a fraud creditcard transaction is detected, actions can be taken to avoid malicious activity and inturn increasing the security of the transactions.

2. Literature Survey

2.1. Existing Problem

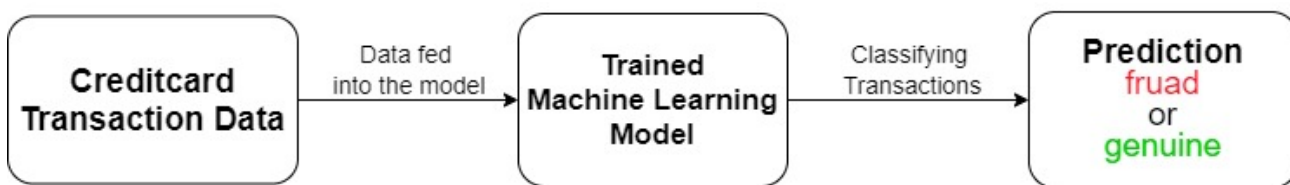
A Cyber attack on a bank or an individual can lead to huge money loss and the amount of loss can sometimes be unimaginable. These losses cannot be recovered which make this a huge problem.

2.2. Proposed Solution

Attributes or parameters of a transaction can be used in a Machine Learning Approach, Supervised Learning in this case to detect any kind of malicious activities and these transactions can be ceased at the first place.

3. Theoretical Analysis

3.1. Block Diagram of the Solution



3.2. Hardware and Software Requirements

Hardware Requirements:

1. 4GB RAM or more.
2. 500 GB Hard Disk or SSD.

Software Requirements:

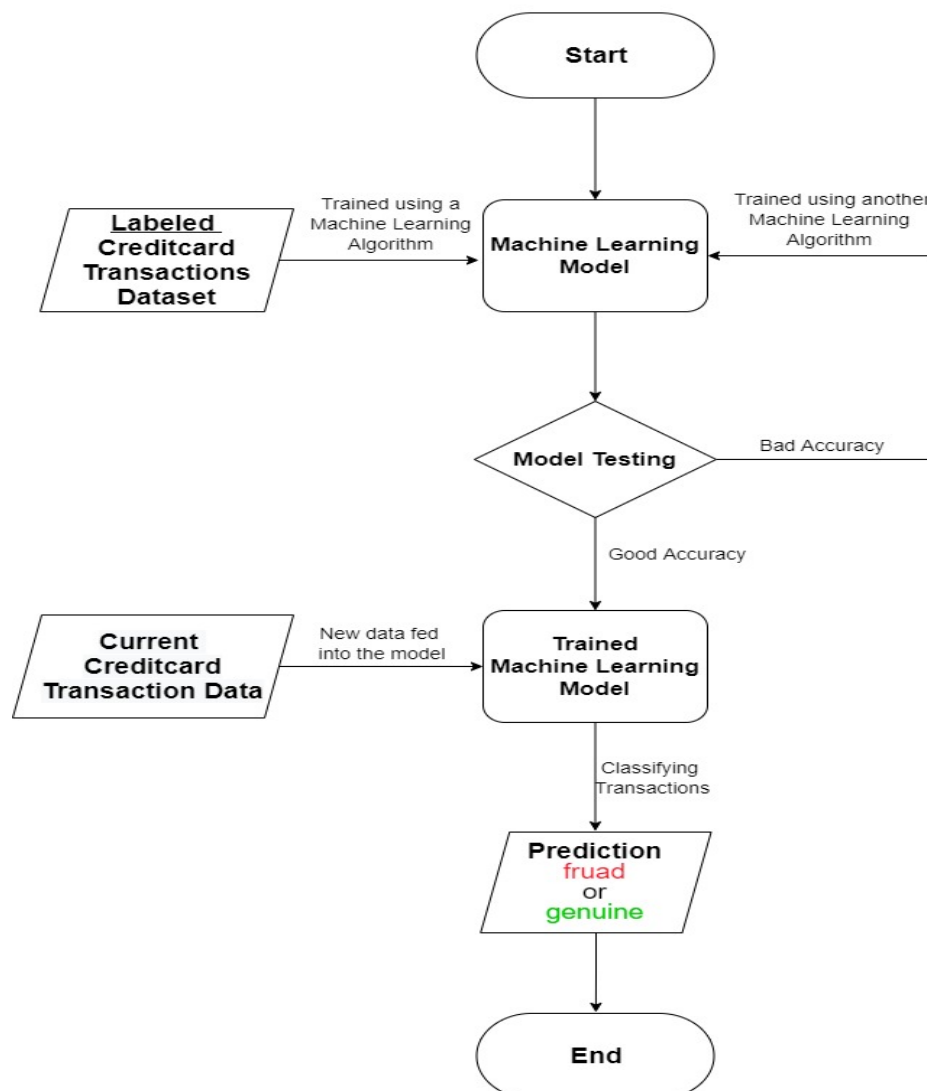
1. Java Runtime Environment(JRE) version 1.7 or more.
2. WEKA Machine Learning tool.
3. Apache Eclipse IDE.

4. EXPERIMENTAL INVESTIGATIONS

A traditional programming can also be used to classify the transactions instead of Machine Learning approach but traditional programming may not be able to discover more number of patterns or patterns that are complex. Since, in the current scenario there is a high chances of existence of complex patterns, Machine Learning Approach which is more capable of discovering patterns is more suitable. Supervised learning algorithm called Random Forest can be best fit for this type of dataset.

5. Flow Chart of the solution

Control Flow (Supervised Learning Model)

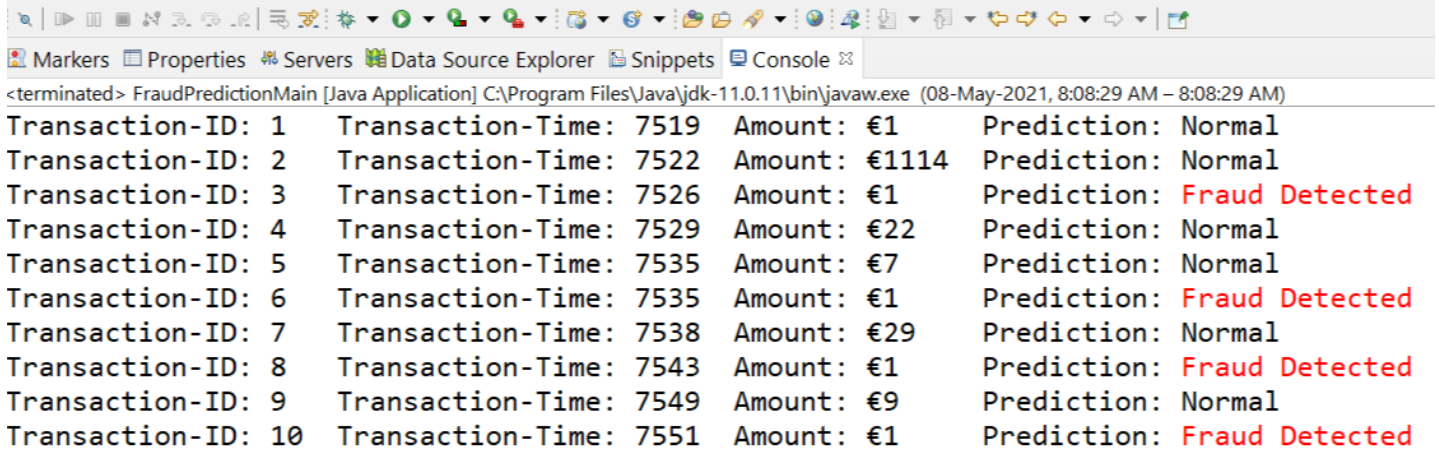


6. Result

When the transaction data in the form of .arff is fed into the trained model (Random Forest Model), using src/FraudPredictionMain.java, the following is the output:

iud_detection/src/main/java/my_pack/FraudPredictionMain.java - Eclipse IDE

te Search Project Run Window Help



```
<terminated> FraudPredictionMain [Java Application] C:\Program Files\Java\jdk-11.0.11\bin\javaw.exe (08-May-2021, 8:08:29 AM - 8:08:29 AM)
Transaction-ID: 1    Transaction-Time: 7519    Amount: €1    Prediction: Normal
Transaction-ID: 2    Transaction-Time: 7522    Amount: €1114    Prediction: Normal
Transaction-ID: 3    Transaction-Time: 7526    Amount: €1    Prediction: Fraud Detected
Transaction-ID: 4    Transaction-Time: 7529    Amount: €22    Prediction: Normal
Transaction-ID: 5    Transaction-Time: 7535    Amount: €7    Prediction: Normal
Transaction-ID: 6    Transaction-Time: 7535    Amount: €1    Prediction: Fraud Detected
Transaction-ID: 7    Transaction-Time: 7538    Amount: €29    Prediction: Normal
Transaction-ID: 8    Transaction-Time: 7543    Amount: €1    Prediction: Fraud Detected
Transaction-ID: 9    Transaction-Time: 7549    Amount: €9    Prediction: Normal
Transaction-ID: 10   Transaction-Time: 7551    Amount: €1    Prediction: Fraud Detected
```

7. Advantages and Disadvantages

Advantages: The trained model has an accuracy for 99.9561% which means the model can exactly predict the transactions in almost all the cases.

Disadvantages: The chances of detecting a genuine transaction as fraud is more than the chances of detecting a fraud transaction as a genuine one. Which implies that there is a considerable probability of misclassifying a fraud transaction.

8. Applications

The model can be used to detect all kinds of suspicious transactions which can later be examined and proceeded. Any kind of new patterns or techniques of attack once recorded in the past or by the other company can be used to re-train the model and the model becomes secured to the new techniques as well.

9. Conclusion

In this way, the model can be trained many times according to the new patterns and can be made resistant to any kind of malicious transactions.

10. Future Scope

The accuracy and precision of the current Random Forest model is quite high. But with the help of Nueral Networks, Deep Learning approach, the model can be more accurate and precise.