VIEHGROUP

Low Level Document (LLD)
Credit Card Fraud Detection System

Version number: 1.0
Last date of revision: 30 January 2022

Akshay Ashu
Chirag Sharma

VIEHGROUP

DECLARATION

We declare that this written submission represents us ideas is our own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources.

We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.

We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Revision History

Version	Date	Author	Reviewer	Approver	Comments
0.1	26-01-2022	Akshay Ashu	Chirag Sharma		Draft version
0.2	27-01-2022	Akshay Ashu	Chirag Sharma		Suggested some selections like key notes, screen validations and attributes to be added
0.3	28-01-2022	Chirag Sharma	Akshay Ashu		Suggested document format related comments like correction of version, adding one sections for open issues etc
0.4	29-01-2022	Akshay Ashu	Chirag Sharma		Suggested some changes like correct sequence diagram, changes in data design sections etc
1.0	30-01-2022	Chirag Sharma	Akshay Ashu		Baseline version

Table of Contents

1. Introduction:

1.1 Scope of the Document

- This section will cover details regarding scope of the document
- Low level design document will be at component level i.e., for website portal there will be one LLD

1.2 Intended Audience

- This section will cover categories of audiences who will be referring/reviewing this document

1.3 System Overview

- This section will capture overview of system application i.e for what system is being developed
- Who are the stake holders of system?
- What are other external Systems through which this will be interacting

2. Project Briefing:

In proposed system, I present a behavior and Location Analysis (BLA).Which does not require fraud signatures and yet is able to detect frauds by considering a cardholder’s spending habit. Card transaction processing sequence by the stochastic process of an BLA. The details of items purchased in Individual transactions are usually not known to any Fraud Detection System (FDS) running at the bank that issues credit cards to the cardholders. Hence, I feel that BLA is an ideal choice for addressing this problem. Another important advantage of the BLA -based approach is a drastic reduction in the number of False Positives transactions identified as malicious by an FDS although they are actually genuine. An FDS runs at a credit card issuing bank. Each incoming transaction is submitted to the FDS for verification. FDS receives the card details and the value of purchase to verify, whether the transaction is genuine or not. The types of goods that are bought in that transaction are not known to the FDS. It tries to find any anomaly in the transaction based on the spending profile of the cardholder, shipping address, and billing address, etc. If the FDS confirms the transaction to be of fraud, it raises an alarm, and the issuing bank declines the transaction.

The credit card fraud detection features uses user behavior and location scanning to check for unusual patterns. These patterns include user characteristics such as user spending patterns as well as usual user geographic locations to verify his identity. If any unusual pattern is detected, the system requires reverification. The system analyses user credit card data for various characteristics. These characteristics include user country, usual spending procedures. Based upon previous data of that user the system recognizes unusual patterns in the payment procedure. So now the system may require the user to login again or even block the user for more than 3 invalid attempts.

3. Problem Statement:

Now a days there’s a lot of Credit Card Fraud happening around the world, which is a major concern for the entire Banking system and also for the Law Enforcement Agencies.

4. Problem Solution:

In the proposed system, We present a behaviour and location analysis (BLA). Which does not require fraud signatures and yet is able to detect fraud by considering a cardholder’s spending habit.
Card translation processing sequence by the stochastic process of an BLA. The details of items purchased in individual transactions are usually not know to any fraud detection system running at the bank that issues credit cards to the cardholders.
Hence , we feel that BLA is an ideal choice for addressing this problem.

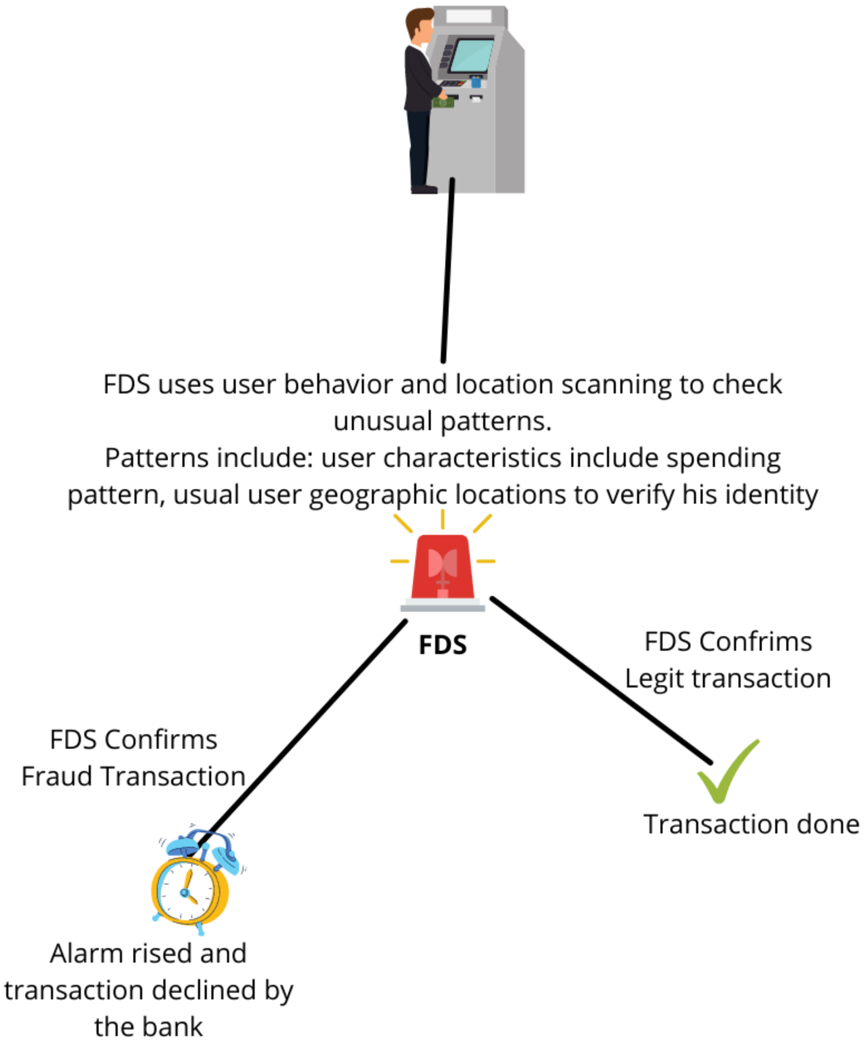
5. Objective of the Project:

Objective of this project is to create a behaviour and location based Credit card fraud detection system.

6. Scope of Project:

It will be very helpful for the banks because at the time of credit card fraud, the FDS confirms the translation to be of fraud, it raises an alarm, and the issuing bank declines the transaction.

7. Block Diagram:



FDS uses user behavior and location scanning to check unusual patterns.

Patterns include: user characteristics include spending pattern, usual user geographic locations to verify his identity

FDS Confirms Legit transaction

Transaction done

FDS Confirms Fraud Transaction

Alarm rised and transaction declined by the bank

8. Requirements Gathering:

- Window 10 Operating system
- Visual studio software
- 2 Team members for the research part
- Project integration idea from IEEE website
- Few Github Non copyrighted source codes

9. Analysis:

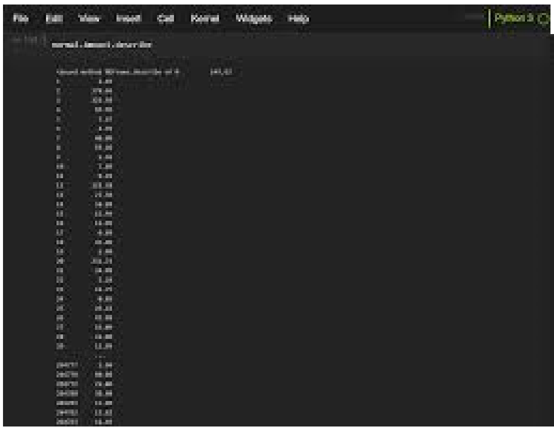
In this project we are using BLAST-SSAHA HYBRIDIZATION. In bioinformatics, SSAHA is one of the fastest tools for sequence alignment. It is approximately four times faster than BLAST and FASTA. If there is no memory constraint, then SSAHA would be the ideal choice for sequence alignment. In this section, we first discuss basics of BLAST and SSAHA algorithms, and then, propose a hybridized algorithm named as BLAH that can be efficiently used for credit card fraud detection. BLAST comprises three steps. In the first step, it compiles a list of high-scoring words (neighbouring words) from a given query sequence. In the second step, each neighbouring word is compared with the database sequences. If the neighbouring word is identical to a word (sequence fragment) in database, a hit is recorded. Usually, a neighbouring word is shorter compared to database sequences, and hence, it matches only with a fragment of a sequence in database. In this step, only one neighbouring word may hit a database sequence. In the third step, every hit sequence is extended in both directions and the extension is stopped as soon as the similarity score becomes less than a threshold value. All the extended segment pairs whose scores are equal to or greater than the threshold is retained. These segment pairs are called High-scoring Segment Pairs (HSPs) and the best one is called the Maximal Segment Pair (MSP).

In credit card application, the cardholder’s past transactions form profile sequences. Last few transactions including the incoming one are taken as a query sequence which is aligned with the profile sequences. There may be some fraudulent transactions in the query sequence that would not match with the cardholder’s profile form a fraud sequence.

10. Final Screenshot of Project Output

```
******** End of Initial Population
****************

[illegible]
```



Credit Card Fraud Detection System

```
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
import sklearn
import scipy
import seaborn as sns
from sklearn.metrics import classification_report,accuracy_score
from sklearn.ensemble import IsolationForest
from pylab import rcParams
rcParams['figure.figsize'] = 14,8
RANDOM_SEED = 42
LABELS = ["Normal", "Fraud"]
```

```
data = pd.read_csv('creditcard.csv', sep=',')
data.head()
```