**Project title:** CREDIT CARD FRAUD DETECTION

**Team name:** B

**Team size:** 3

**Team members:**

1. Faroque Ahmed
2. Alamgir hossain
3. Tareq hasan

**Introduction:**

Credit card fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. Credit card fraud is also an adjunct to identity theft. Banks, merchants and credit card processors companies lose billions of dollars every year to credit card fraud. Credit card data can be stolen by criminals using a variety of methods. Bluetooth-enabled data skimming devices can be placed on the card reader on the pump that dispenses your petrol. The data might be stolen in a mass breach by hackers of a large retailer, as was the case with Target and Home Depot in recent years. Sometimes the criminal is simply the clerk at the checkout line at the grocery or in a restaurant, where the victim’s card is swiped through a small device or surreptitiously jotted down.

**Scope or objectives of the project:**

There are two objectives of credit card fraud detection. **It helps merchants and banks reduce the number of payment fraud cases and helps merchants grow their revenues**. Credit card companies detect fraud by flagging several different kinds of transactions. Among them are large purchases made just after small ones, online purchases and purchases that don’t fit a cardholder’s profile. Credit card companies also monitor cardholder transaction habits to establish individual customer profiles. These help issuers determine which purchases are standard operating procedure for the cardholder, and which ones deserve closer scrutiny. 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 revivification. 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.

**Core features:**

* The system stores previous transaction patterns for each user.
* Based upon the user spending ability and even country, it calculates user’s characteristics.
* More than 20 -30 %deviation of user’s transaction (spending history and operating country) is considered as an invalid attempt and system takes action.

**Advantages:**

* Due to Behavior and location analysis approach, there is a drastic reduction in the number of False Positives transactions identified as malicious by an FDS although they are actually genuine.
* The system stores previous transaction patterns for each user.
* Based upon previous data of that user the system recognizes unusual patterns in the payment procedure.
* The System will block the user for more than 3 invalid attempts.

***Finally it can be said that the objectives of credit card fraud detection are to reduce losses due to payment fraud for both merchants and issuing banks and increase revenue opportunities for merchants.***

**Attribute Study**

|  |  |
| --- | --- |
| **Attributes name** | **Explanation** |
| * 1. **Time** | The feature 'Time' contains the seconds elapsed between each transaction and the first transaction in the dataset. This dataset presents transactions that occurred in two days |
| * 1. **PCA Variables (V1,V2,…….,V28)** | The data set contains only numerical input variables which are the result of a PCA (Principal Component Analysis) transformation. Unfortunately, due to confidentiality issues, the original features and more background information about the data are not provided. Features V1, V2, ... V28 are the principal components obtained with PCA |
| * 1. **Amount** | The feature 'Amount' is the transaction Amount, this feature can be used for example-dependent cost-sensitive learning. The amount of money withdrawn by someone in a transaction is simply called here ‘Amount’. |
| * 1. **Class** | The feature 'Class' is the response variable and it takes value 1 in case of fraud and 0 otherwise. We have 492 frauds out of 284,807 transactions. The dataset is highly unbalanced, the positive class (frauds) account for 0.172% of all transactions. |