

# MACHINE LEARNING PROJECT CS6301

TOPIC:

CREDIT CARD FRAUD DETECTION  
USING NEURAL NETWORKS

NAME :

- 1) AKASH MURUGESH K – 2018103510
- 2) ADHITHYA K – 2018103504
- 3) SHARON TINCY B S – 2018103064

# **ABSTRACT**

## **CREDIT CARD FRAUD DETECTION**

### **NEED:**

For years, fraud has been a major issue in sectors like banking, medical, insurance, and many others. Due to the increase in online transactions through different payment options, such as credit/debit cards, PhonePe, Gpay, Paytm, etc., fraudulent activities have also increased. Moreover, fraudsters or criminals have become very skilled in finding escapes so that they can loot more.

Since no system is perfect and there is always a loophole in them, it has become a challenging task to make a secure system for authentication and preventing customers from fraud. So, Fraud detection algorithms are very useful for preventing frauds.

### **ROLE OF MACHINE LEARNING:**

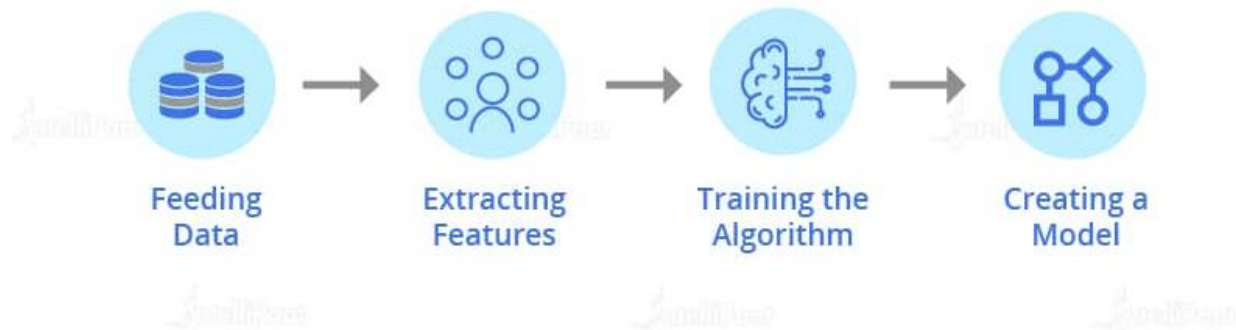
#### **RULE-BASED APPROACH OR TRADITIONAL APPROACH IN FRAUD DETECTION ALGORITHMS:**

In the rule-based approach, the algorithms are written by fraud analysts. They are based on strict rules. If any changes have to be made for detecting a new fraud, then they are done manually either by making those changes in the already existing algorithms or by creating new algorithms. In this approach, with the increase in the number of customers and the data, human effort also increases. So, the rule-based approach is time-consuming and costly.

#### **ML-BASED FRAUD DETECTION ALGORITHMS**

In the rule-based approach, the algorithms cannot recognize the hidden patterns. Since they are based on strict rules, they cannot predict fraud by going beyond these rules. But in real world, fraudsters are very skilled and can adopt new techniques every time to commit a crime. Therefore, there is a need for a system that can analyze patterns in data and predict and respond to new situations for which it is not trained or explicitly programmed.

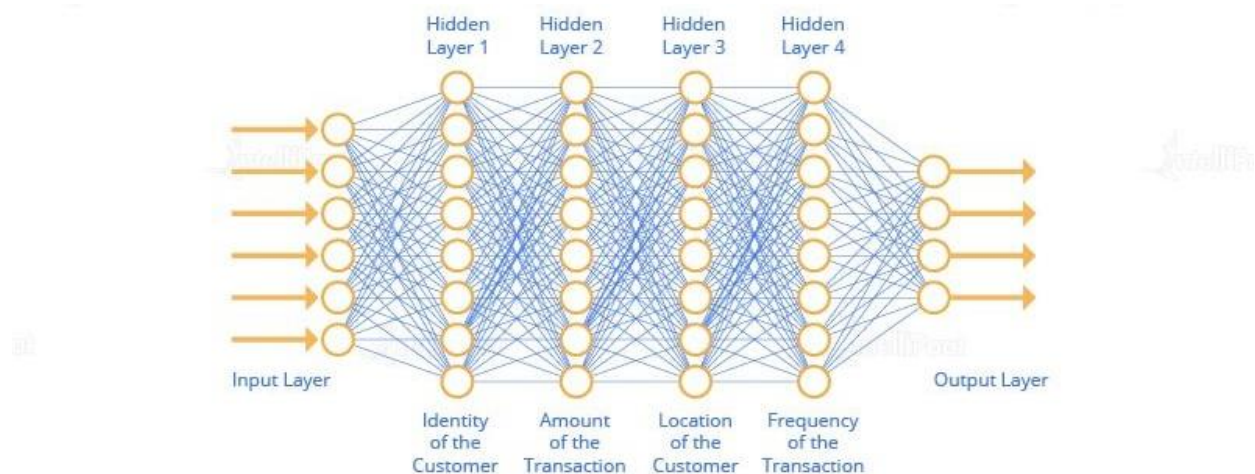
Hence, we use Machine Learning for detecting fraud. Here, a machine tries to learn by itself and becomes better by experience. It tries to identify hidden patterns that help in detecting a fraud which is not been previously recognized. Also, it is an efficient way of detecting fraud because of its fast computing. It does not even require the guidance of a fraud analyst.



### Using Neural Networks:

Neural Networks is a concept inspired by the working of a human brain. Neural networks in Deep Learning uses different layers for computation. It uses cognitive computing that helps in building machines capable of using self-learning algorithms that involve the use of data mining, pattern recognition, and natural language processing. It is trained on a dataset passing it through different layers several times.

It gives more accurate results than other models as it uses cognitive computing and it learns from the patterns of authorized behavior and thus distinguishes between '**fraud**' and '**genuine**' transactions.



There are different layers in a neural network that focus on different parameters to make a decision whether a transaction is 'fraud' or 'non-fraud.' In the diagram it is shown how the layers of neural networks represent and work on different parameters.

First, the data is fed into the neural network. After that, the Hidden Layer 1 checks the amount of transaction, and similarly other layers check for the location, identity, IP address of the location, the frequency of transaction, and the mode of payment. There can be more business-specific parameters. These individual layers work on these parameters, and computation is done based on the models' self-learning and past experience to calculate the probabilities for detecting frauds.

Thus, neural networks work on data and learn from it, and it improves the model's performance over every iteration. This is how neural networks are used for implementing fraud detection algorithms.

### **TRAINING:**

A neural network based fraud detection system will be trained on a large sample of labelled credit card account transactions and tested on a holdout data set that consisted of all account activity over a subsequent two-month period of time. The neural network will be trained on examples of fraud due to lost cards, stolen cards, application fraud, counterfeit fraud, mail-order fraud and NRI (non-received issue) fraud. The performance of the network is evaluated in terms of "**detection accuracy**" and "**earliness of fraud detection**".

### **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.

## **HOW TO TACKLE THESE CHALLENGES?**

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