

# **MACHINE LEARNING**

**DAY – 18**

# CREDIT CARD FRAUD DETECTION






# INTRO

As we are moving towards the digital world — cybersecurity is becoming a crucial part of our life

When we make any transaction while purchasing any product online — a good amount of people prefer credit cards that time some these feature will misused by cyber attacker

we have many machine learning algorithms that can help us classify abnormal transactions. The only requirement is the past data and the suitable algorithm that can fit our data in a better form.





# OBJECTIVE



In this project we will build the model to that can classify the transaction into normal and abnormal

# ACTION

credit card fraud detection

- data collection
- data preprocessing and analysing
- train test split
- model creation and model training
- Evaluation
- Optimization



# ABOUT THE DATASET

The dataset contains transactions made by credit cards in September 2013 by European cardholders.

This dataset presents transactions that occurred in two days, where 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.

It contains only numerical input variables which are the result of a PCA transformation. Unfortunately, due to confidentiality issues, we cannot provide the original features and more background information about the data. Features V1, V2, ... V28 are the principal components obtained with PCA, the only features which have not been transformed with PCA are 'Time' and 'Amount'. Feature 'Time' contains the seconds elapsed between each transaction and the first transaction in the dataset. The feature 'Amount' is the transaction Amount, this feature can be used for example-dependant cost-sensitive learning. Feature 'Class' is the response variable and it takes value 1 in case of fraud and 0 otherwise.

# THANK YOU

