**API For Credit Card Fraud Detection**

POST /signup HTTP/1.

API (Signup)

Input Data JSON{username, email, password, location, dob, phone}

GET /signup?verify={JWT\_TOKEN}

JWT\_TOKEN is Stored in Redis Database and have expiration time

API (Login)

POST /login HTTP/1.1

INPUT JSON{email, password}

­­­­

Validate email and password field

Server

If exists return’s {JWT} along with status: true

If user Not exists send’s a status false along with error

POST /apikey HTTP/1.1 (POST/GET/DELETE)

POST APIKEY

Input JSON {“apiname”: “name”}

Server/Database

Response JSON

{"apiname": "ccfd\_2",

"publickey": "ccfd\_+F-\_2#!WRfQoeQva!uAoIc/PquvVUTW^wzY$w2m3.fraud\_detention",

"privatekey": "d4e4$4eeFNk4cKN&T6AIYq6fXVfXID"}

POST FileUpload

POST /fileupload HTTP/1.1

Multipart/form-data

Server/Database

ByteData to AWS S3 Returns Location to File and Orignal File name

And Bucket details

S3 Bucket

Server

User have Options to call a certain

DataBase

Algorithm In API and API send the JavaScript Env Update Database

Data to python Env

Python recives

Parameters

Python Env

JavaScript Env

Python env writes a JSON file and

Javascript Env will read it and Update

Ex :- python index.py -id {mongodb ObjectID} -f {Unique file name} -rf{random forest} MongoDb Object for a user

It Gives random forest accuracy, F1 Score and confusion matrix