Nowadays, with the advent of smart grids in smart cities, electricity consumption is being monitored more efficiently. These smart grids utilize sensors that are connected to the internet of things (IoT) to transmit electricity consumption information to a centralized server or base station. This enables the centralized server to efficiently allocate the required energy. However, due to the internet connection, these grids are vulnerable to attacks that can alter or steal data. Such attacks can lead to the transmission of incorrect information to the base station, resulting in potential grid infrastructure corruption and even blackouts.

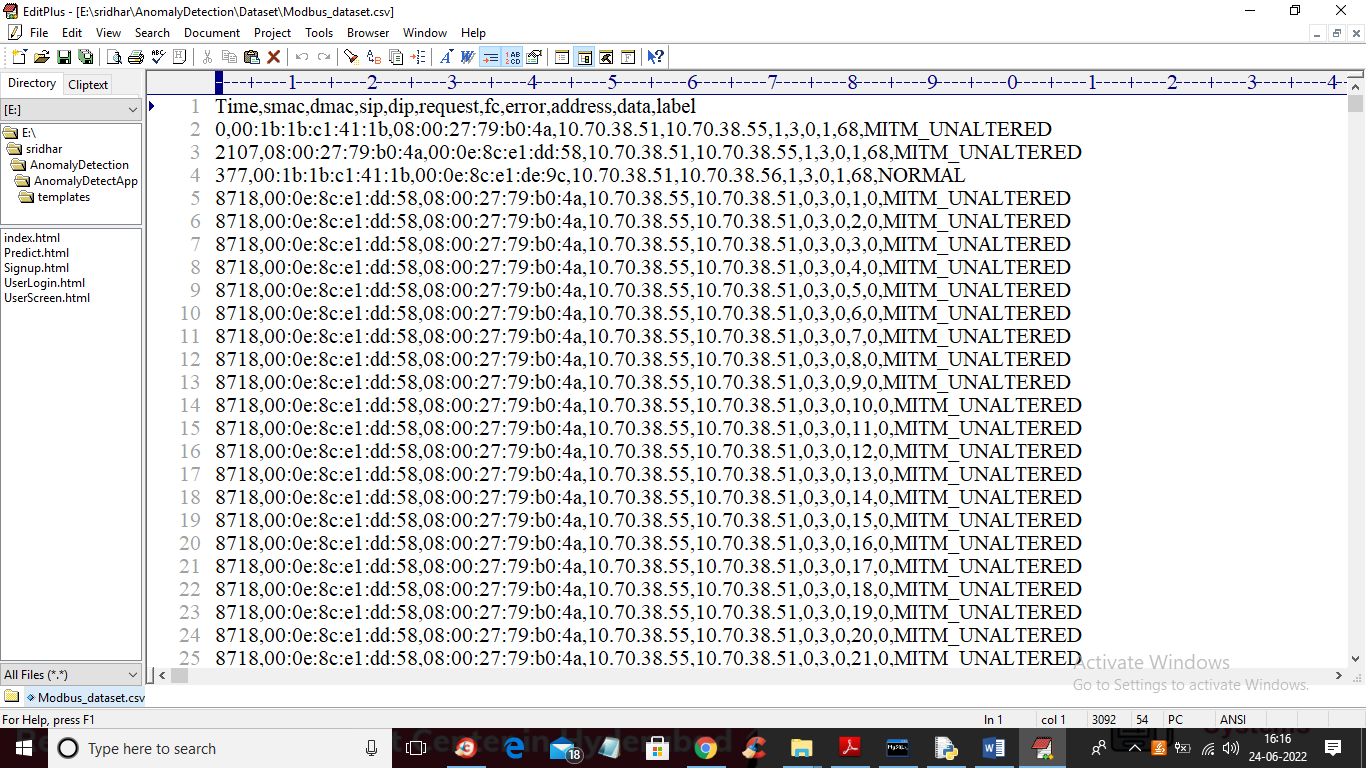
To transmit data, smart grids and supervisory control and data acquisition (SCADA) systems employ the MODBUS/TCP and DNP3 protocols. However, these protocols are susceptible to data alteration. Traditional security measures, such as statistical and signature-based detection techniques, have been introduced to mitigate these risks. Statistical techniques analyze static features of the protocol data to detect alterations, while signature-based techniques employ predefined signatures to identify attacks. However, these techniques fail to detect new or previously unseen attacks.

To address this limitation, machine learning (ML) algorithms have been introduced. However, conventional ML algorithms are not well-suited for detecting smart grid attacks. In this paper, the author proposes a novel approach using an AutoEncoder-based Generative Adversarial Network (GAN). The AutoEncoder encodes the dataset's features, which are then used to train both the encoder and decoder. The decoder receives training labels, and the resulting trained model can be utilized to predict attacks in smart grids.

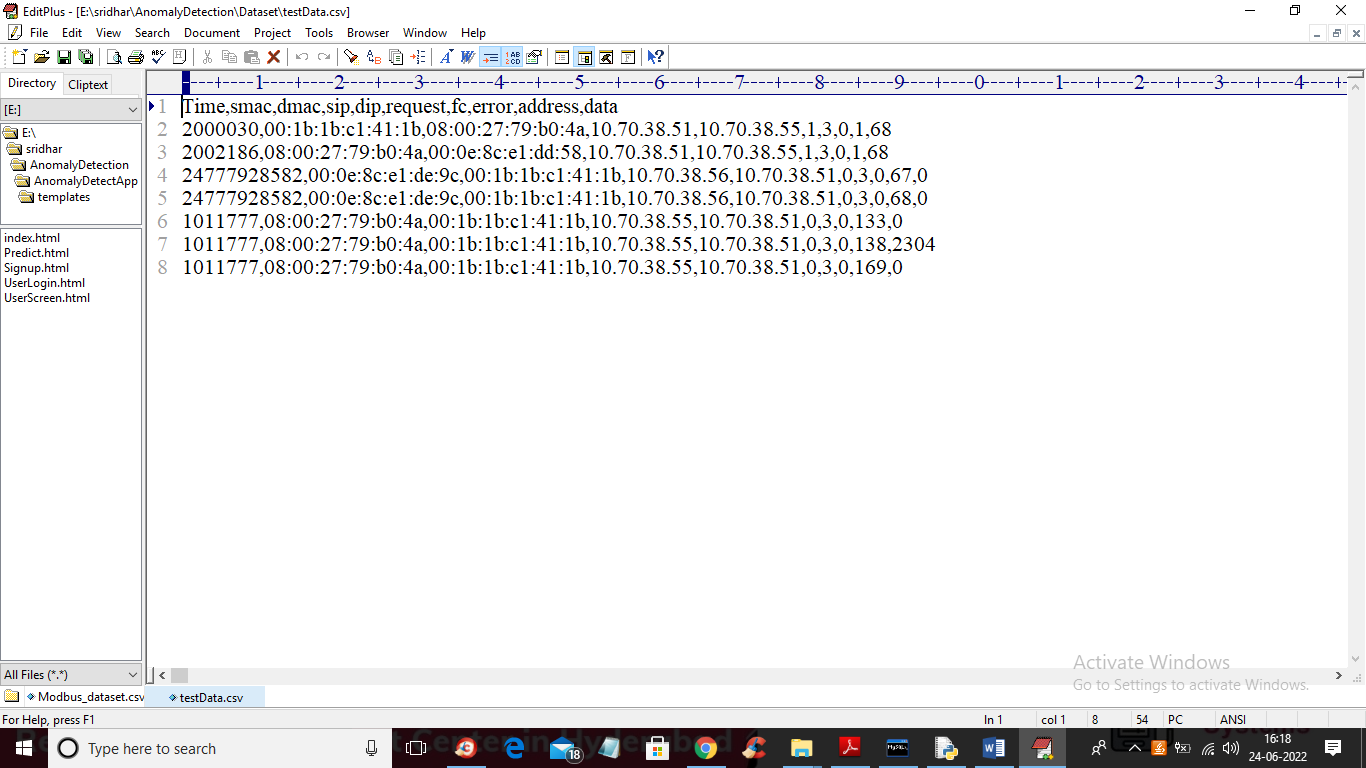
The GAN architecture consists of a Generator, which utilizes the GAN layer to generate both real and fake data, and a Discriminator, which is trained on this data to differentiate between real and fake samples. By utilizing the GAN model, the proposed approach can generate new data from a given noise input, potentially capturing various attack techniques that may be devised by an attacker. The Discriminator is then trained on this synthesized data, enabling it to effectively prevent attacks.

The main objective of this paper is to detect and classify attack types in smart grids. The detection phase involves determining whether the requested data is normal or anomalous, while the classification phase aims to identify the specific type of attack.

In our project, we have implemented the proposed AutoEncoder-GAN model, along with CNN and LSTM architectures. The MODBUS/TCP dataset was utilized to train these algorithms. The following section provides more details about the dataset.

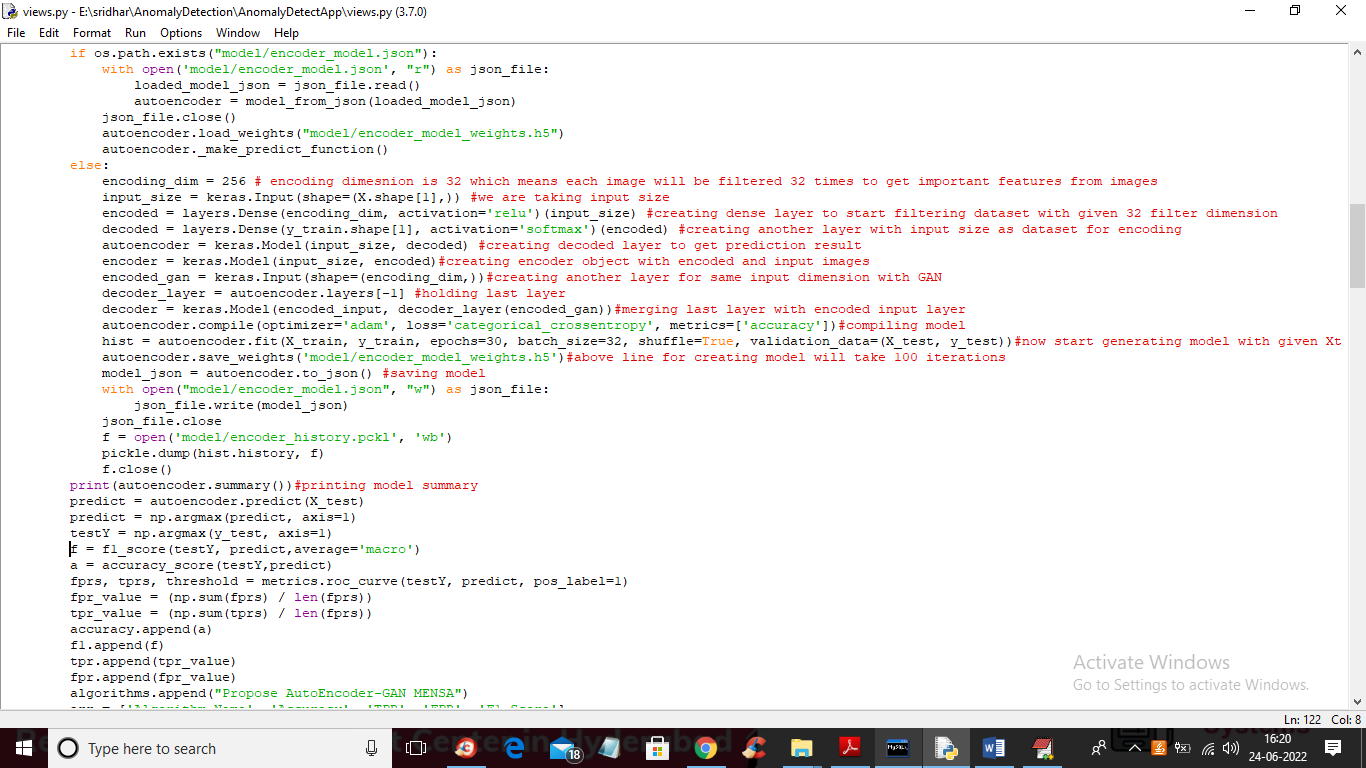


In above dataset screen first row contains dataset column names and remaining rows contains dataset values and in last column we have class label as ‘MITM’ which means ‘Man in the middle attack’ and we have different attacks in dataset and we will used above dataset to train all algorithms. After training model we will apply below test data to detect and classify attacks

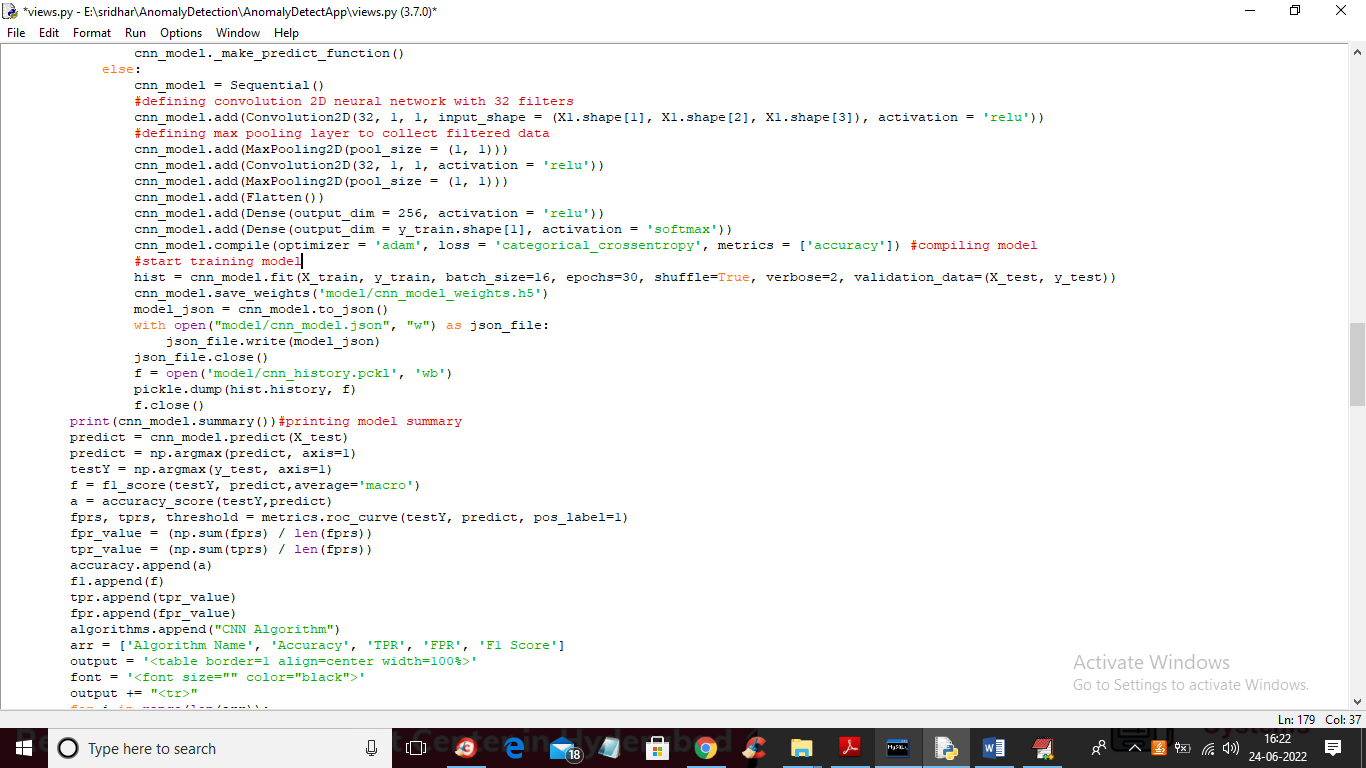


In above test data we have smart grid values but no information on attack label and when we apply above dataset on trained model then algorithm will detect and classify attack type.

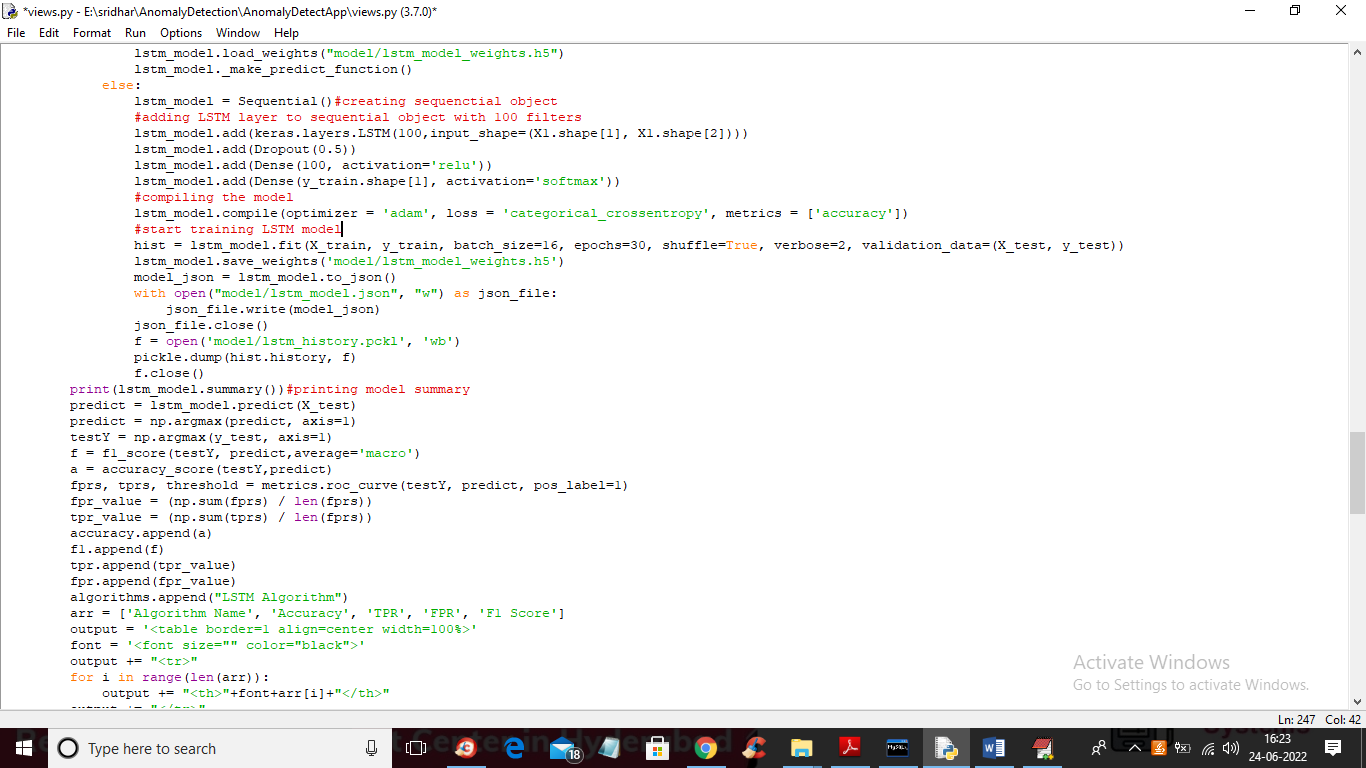
In below screen we are showing code for all 3 algorithms models



In above screen we are showing code for AutoEncoder GAN model and you can read red colour comments to know about algorithm and in last line we are calculating accuracy, FSCORE, FPR and TPR. In below screen showing code for CNN



In above screen we are using CNN to train Anomaly detection model and in below screen we can see LSTM coding.



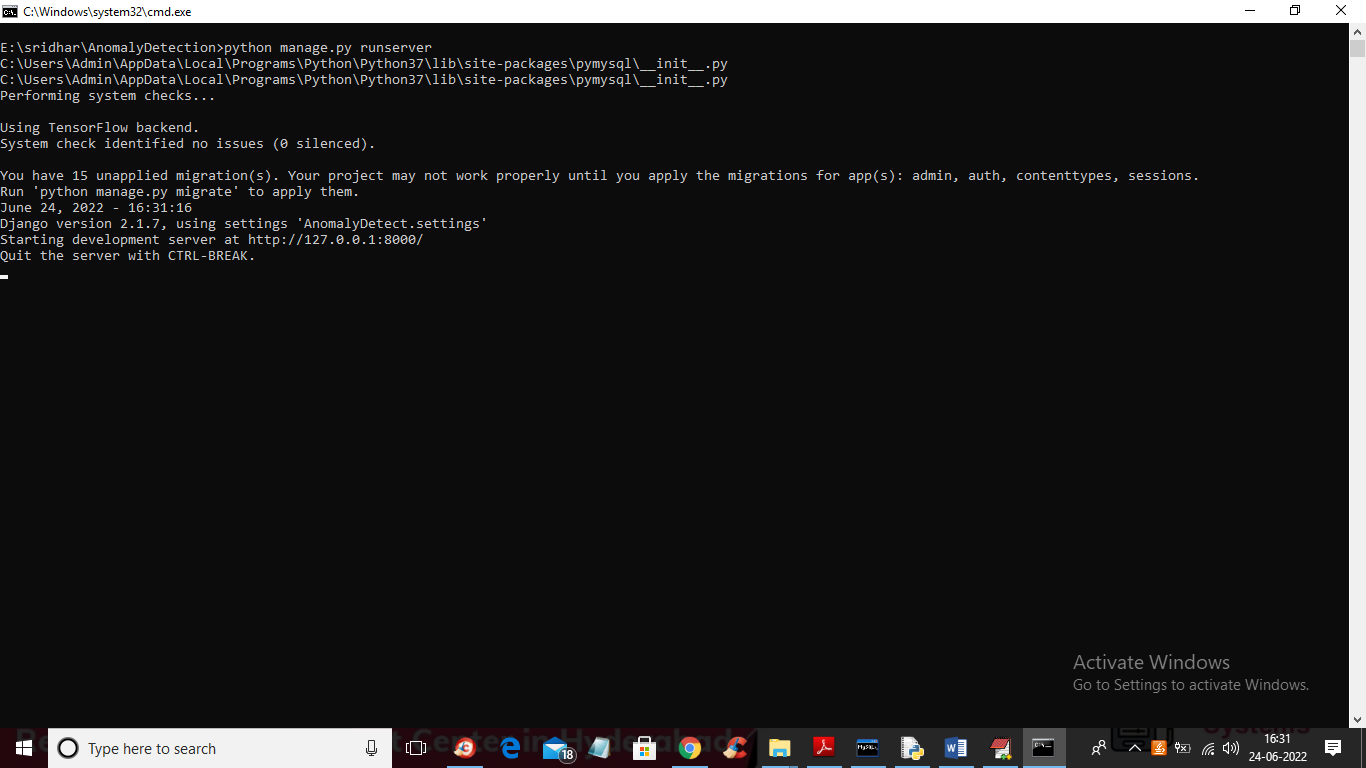
In above screen you can read red colour comments to know about LSTM and to implement this project we have designed following modules

1. New User Signup Here: using this module we will allow user to signup with the application
2. User Login: using this module user can login to application
3. Load & Preprocess Dataset: using this module we will read MODBUS/TCP dataset and then convert or encode all non-numeric data to numeric and then replace missing values with 0 and then find different attacks in dataset and then split processed dataset into train and test part where application used 80% dataset for training and 20% for testing
4. Run Encoder-GAN MENSA Model: 80% processed dataset will be input to AutoEncoder GAN algorithm to trained a model and this model can be applied on 20% test data to calculate prediction accuracy and FSCORE
5. Run CNN: 80% processed dataset will be input to CNN algorithm to trained a model and this model can be applied on 20% test data to calculate prediction accuracy and FSCORE
6. Run LSTM: 80% processed dataset will be input to LSTM algorithm to trained a model and this model can be applied on 20% test data to calculate prediction accuracy and FSCORE
7. Detection & Classification: using this module we will upload test data and then trained model will detect and classify attack from test data.

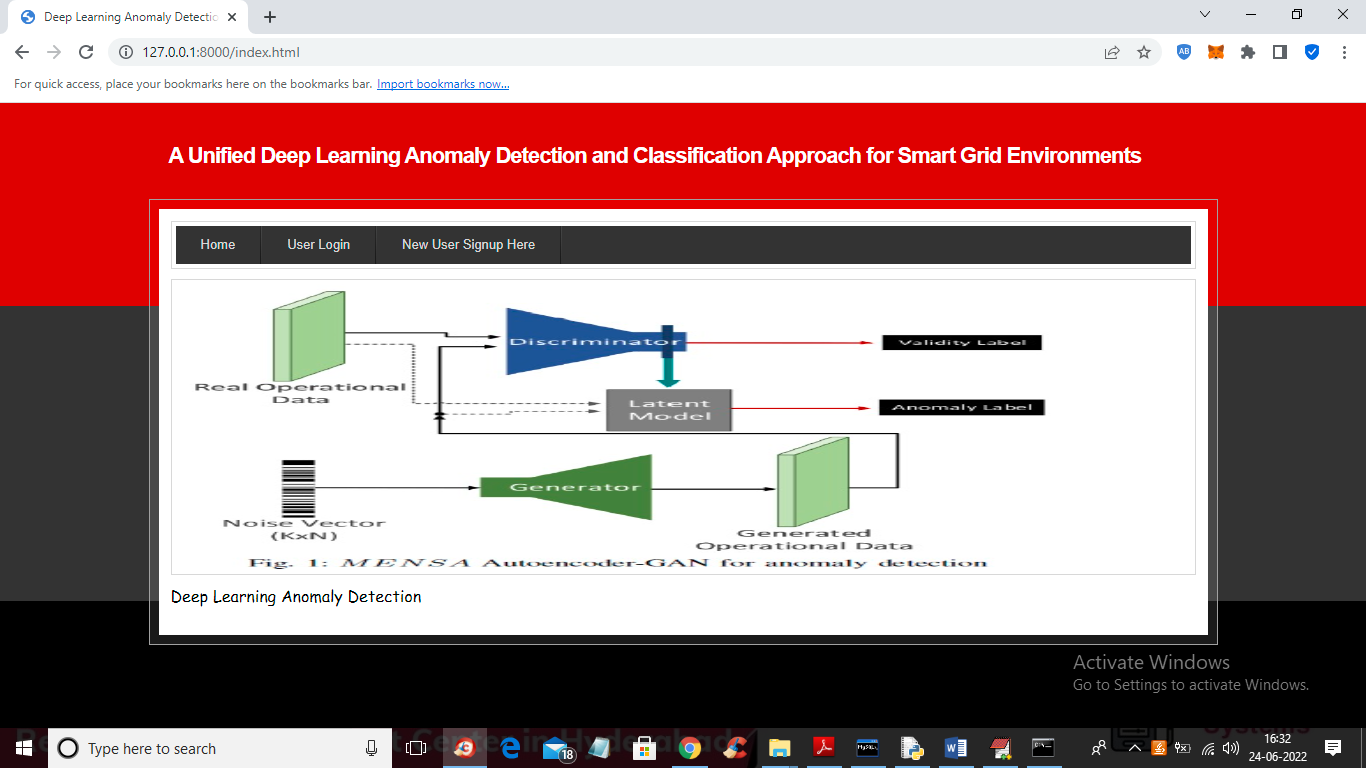
SCREEN SHOTS

To run project install python 3.7 and then install MYSQL database and then copy content from ‘DB.txt’ file and then paste in MYSQL.

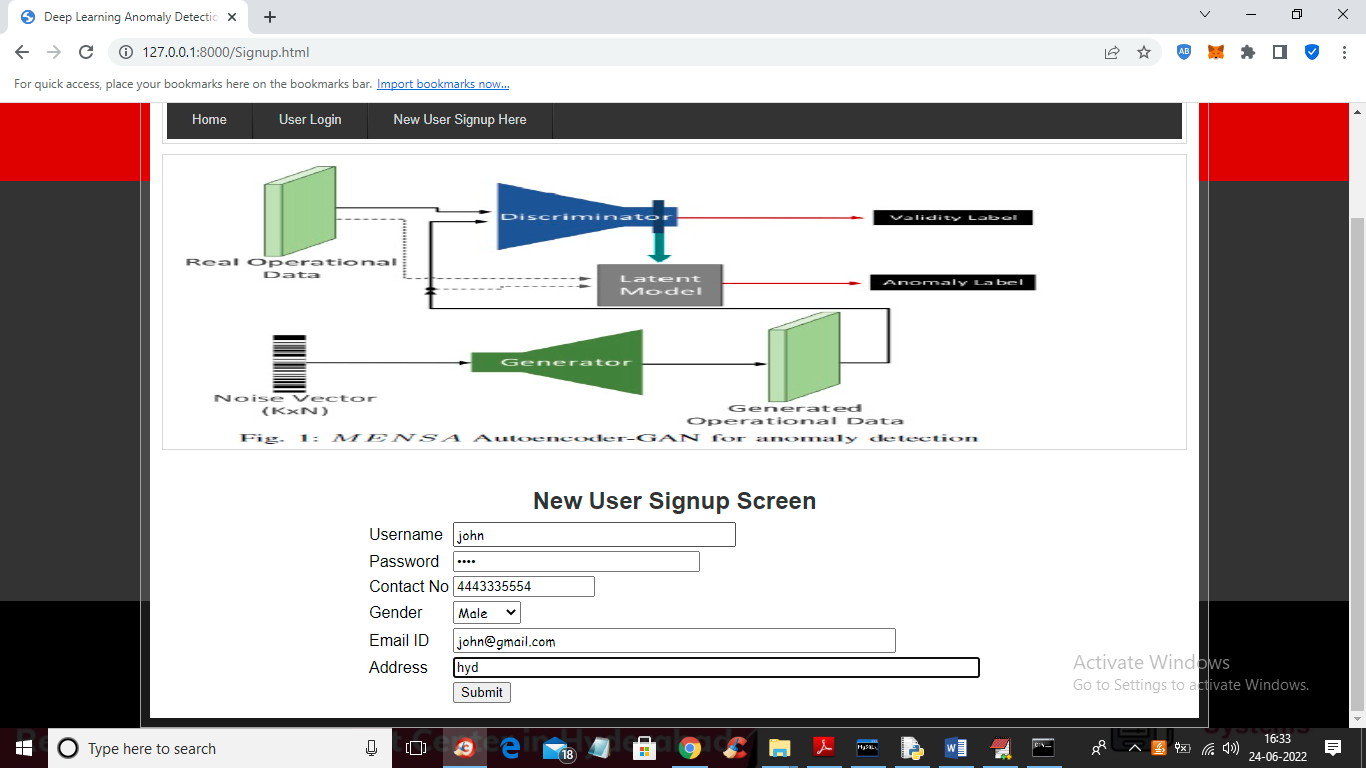
Now double click on ‘run.bat’ file to start python DJANGO server and get below screen



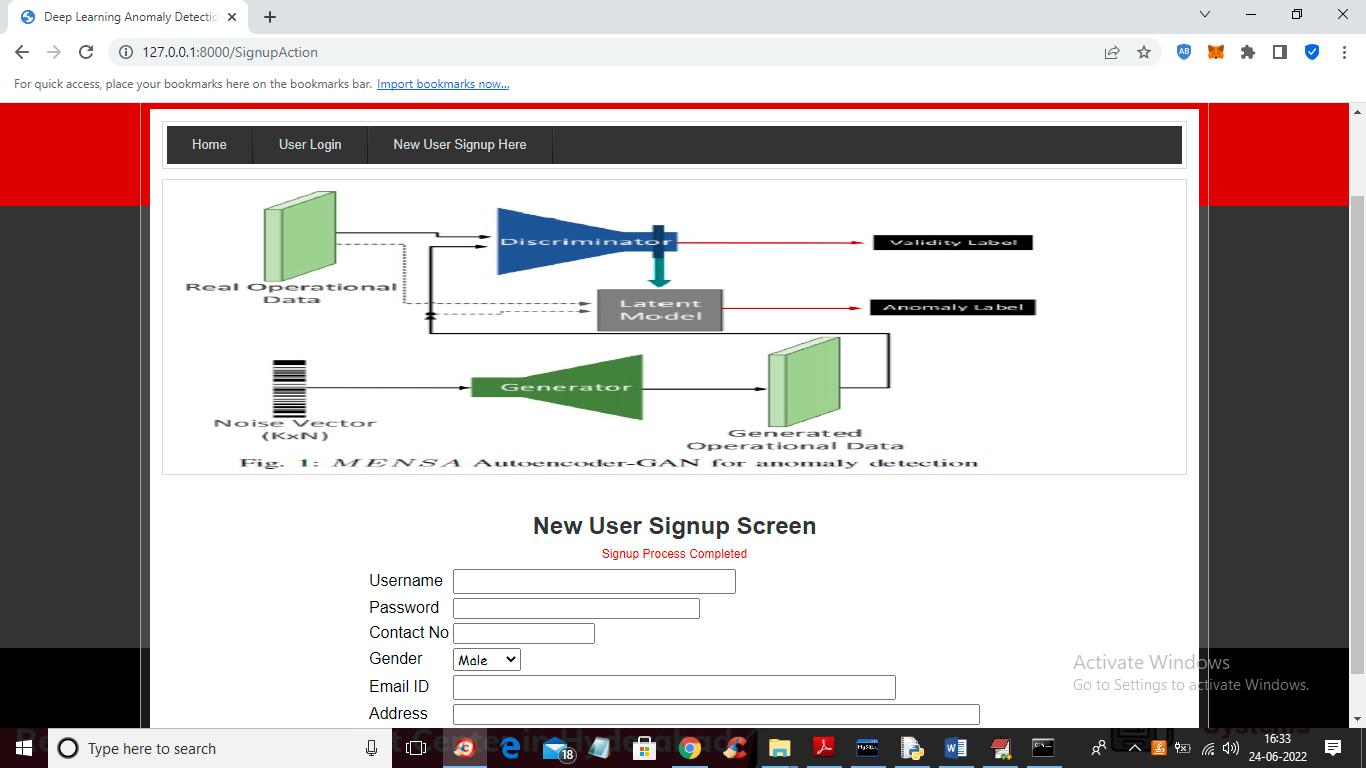
In above screen python DJANGO server started and now open browser and enter URL as <http://127.0.0.1:8000/inde\x.html> and press enter key to get below screen



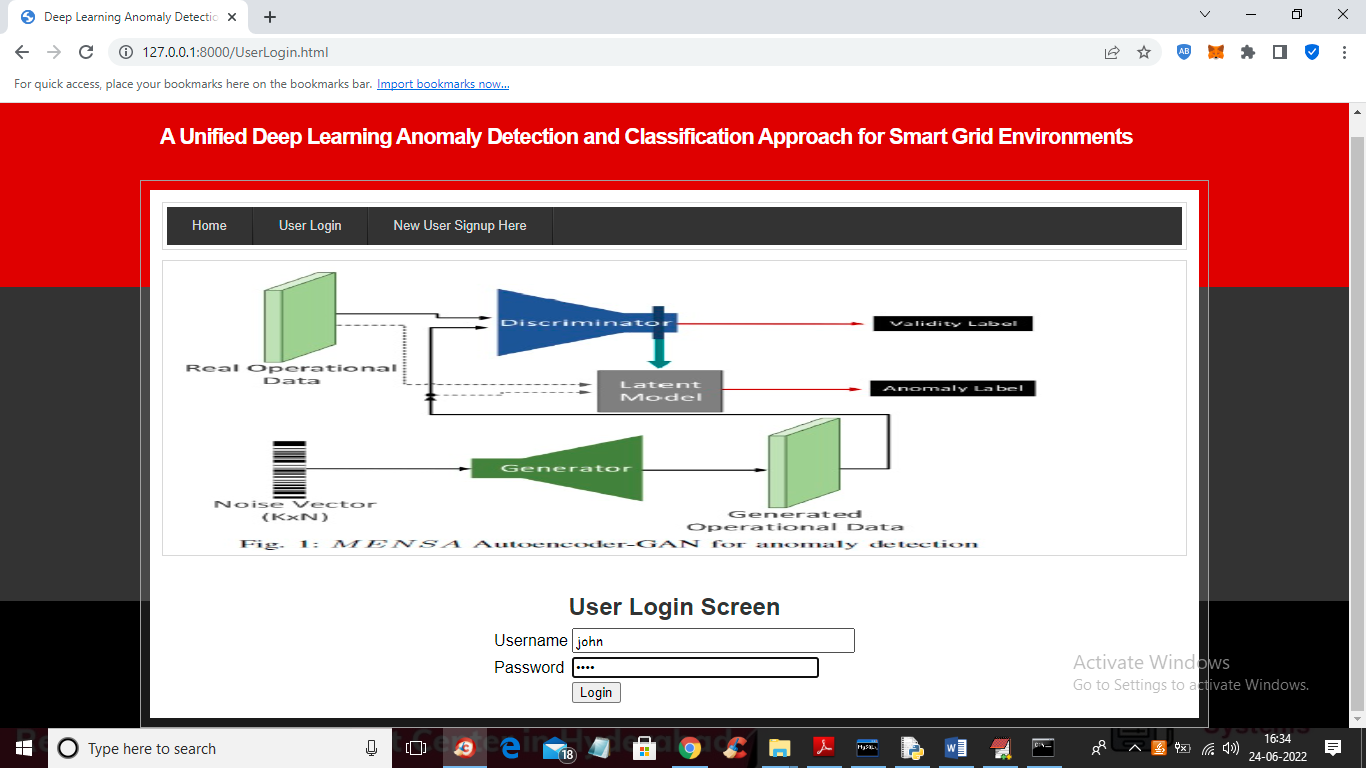
In above screen click on ‘New User Signup Here’ link to get below signup screen



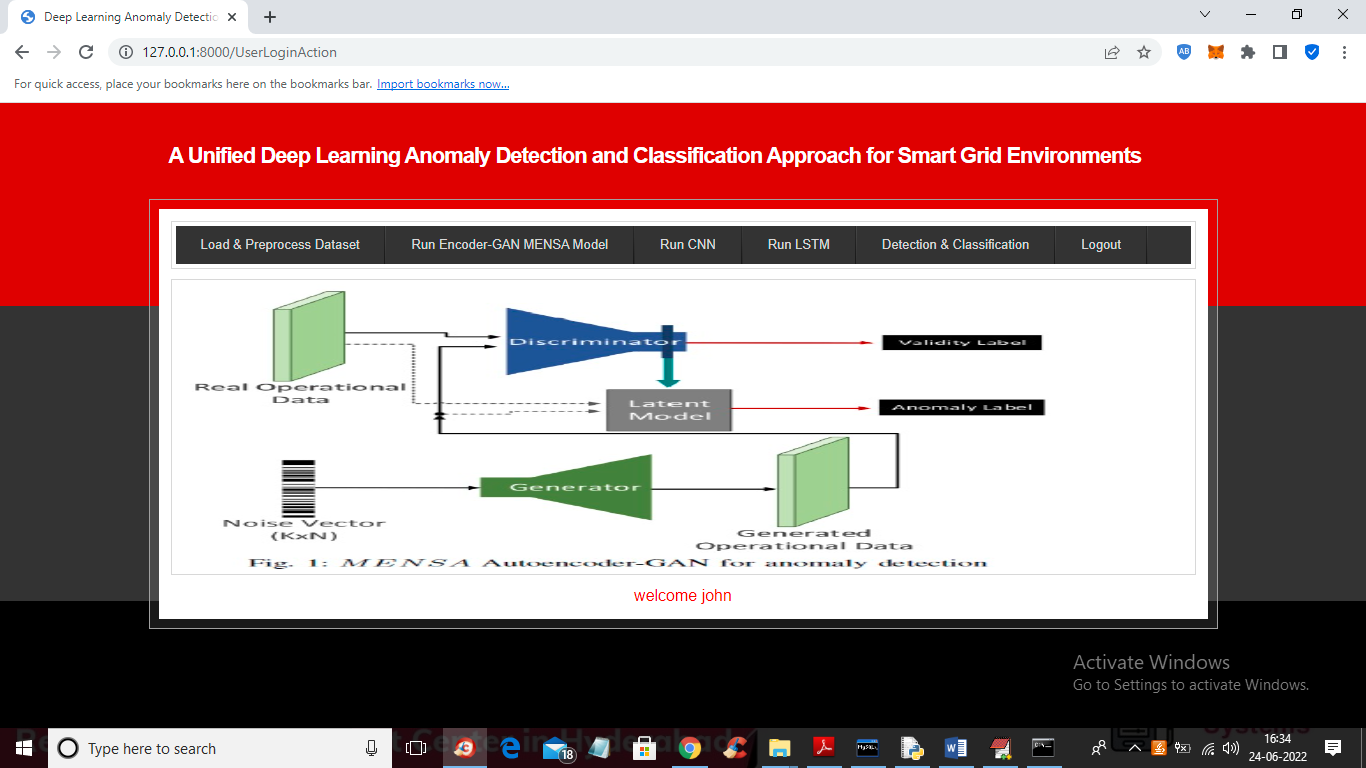
In above screen user is signing up and then press button to get below screen



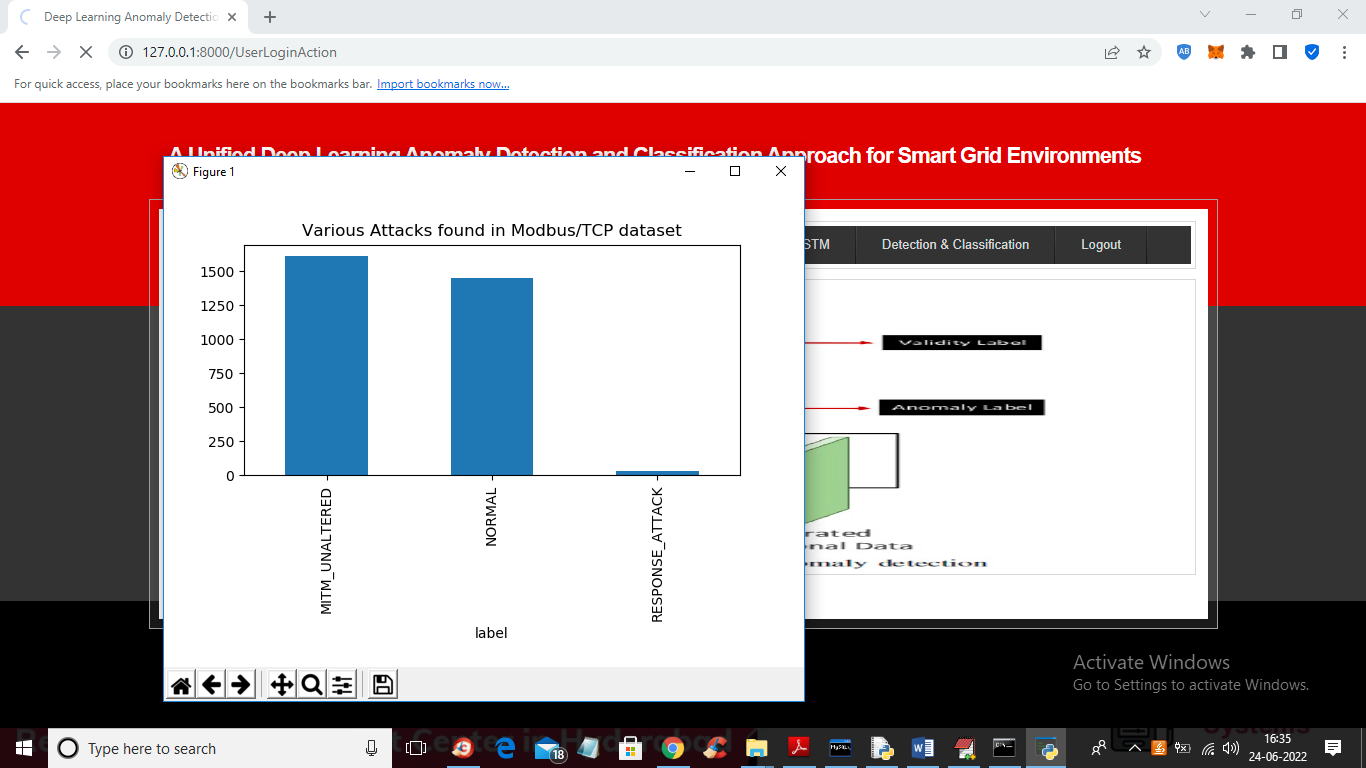
In above screen user signup task completed and now click on ‘User Login’ link to get below login screen



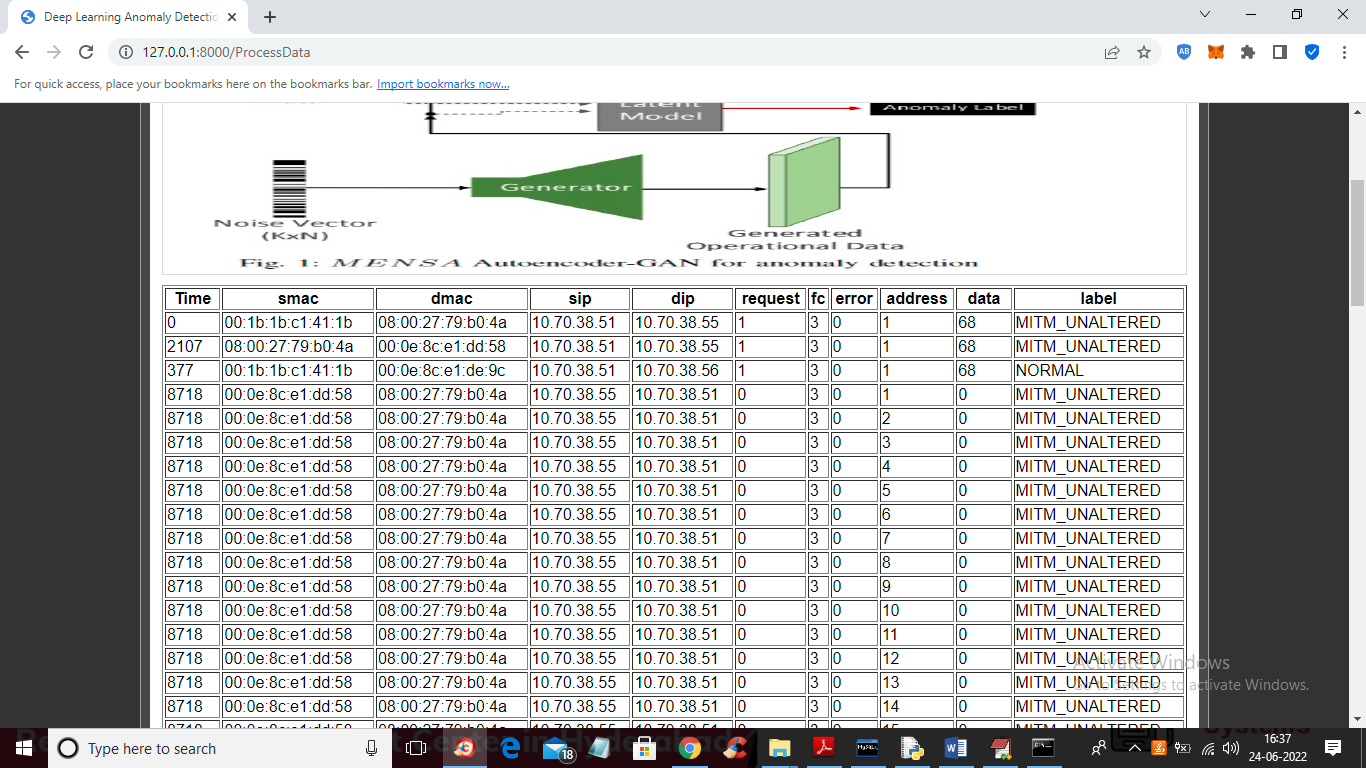
In above screen user is login and after login will get below screen



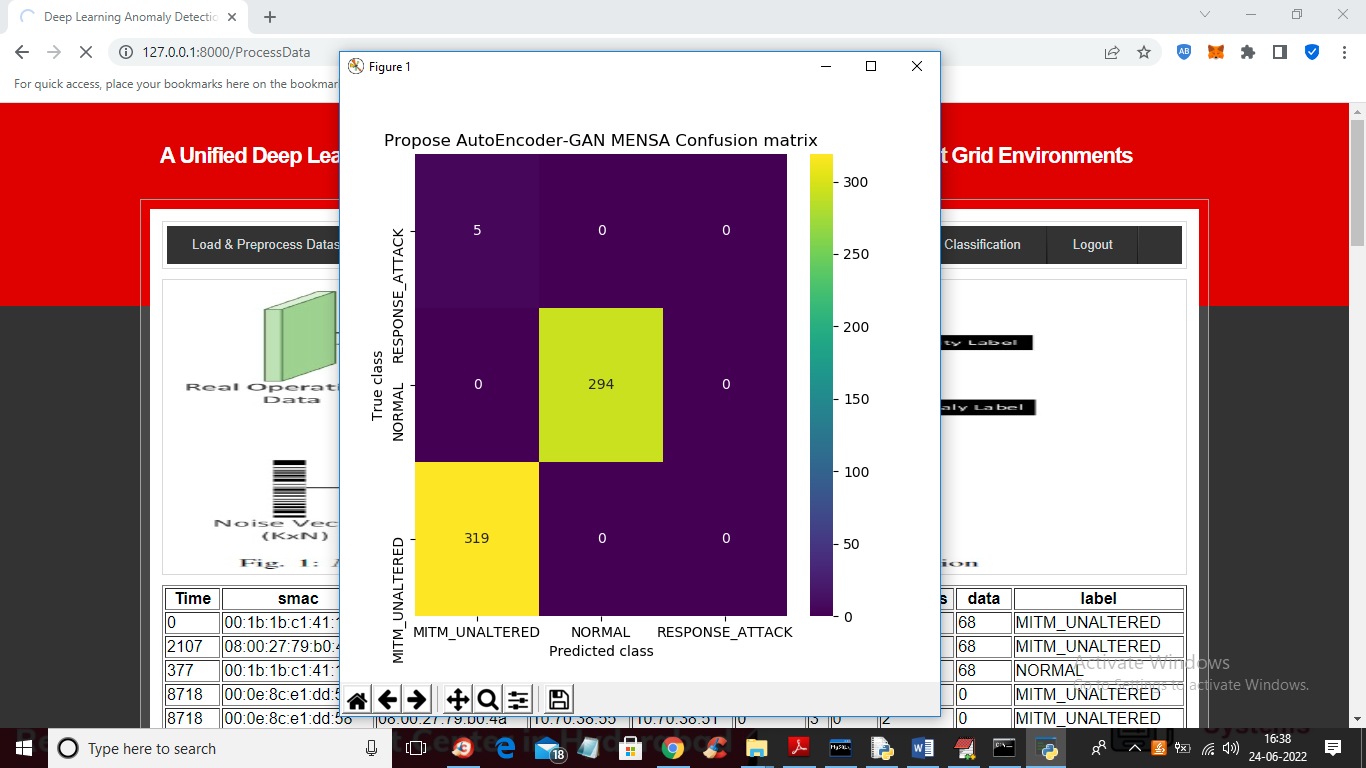
In above screen user can click on ‘Load & Preprocess Dataset’ link to read process dataset and then get below output



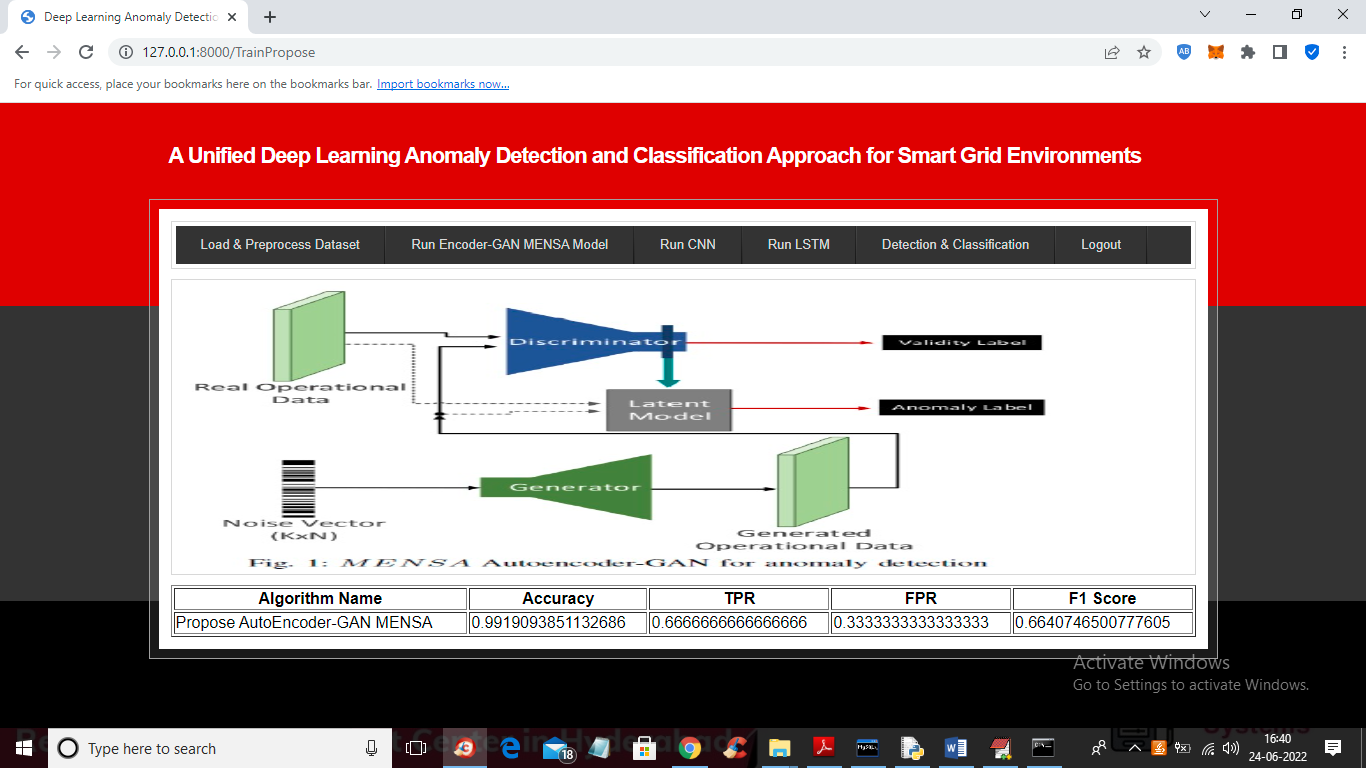
In above screen dataset is loaded and processed and then in graph we are plotting different records found in dataset like ‘Normal packet, MITM (man in the middle attack) and Response attack. In above graph x-axis represents attack type and y-axis represents number of records in that attack and now close above graph to get below screen



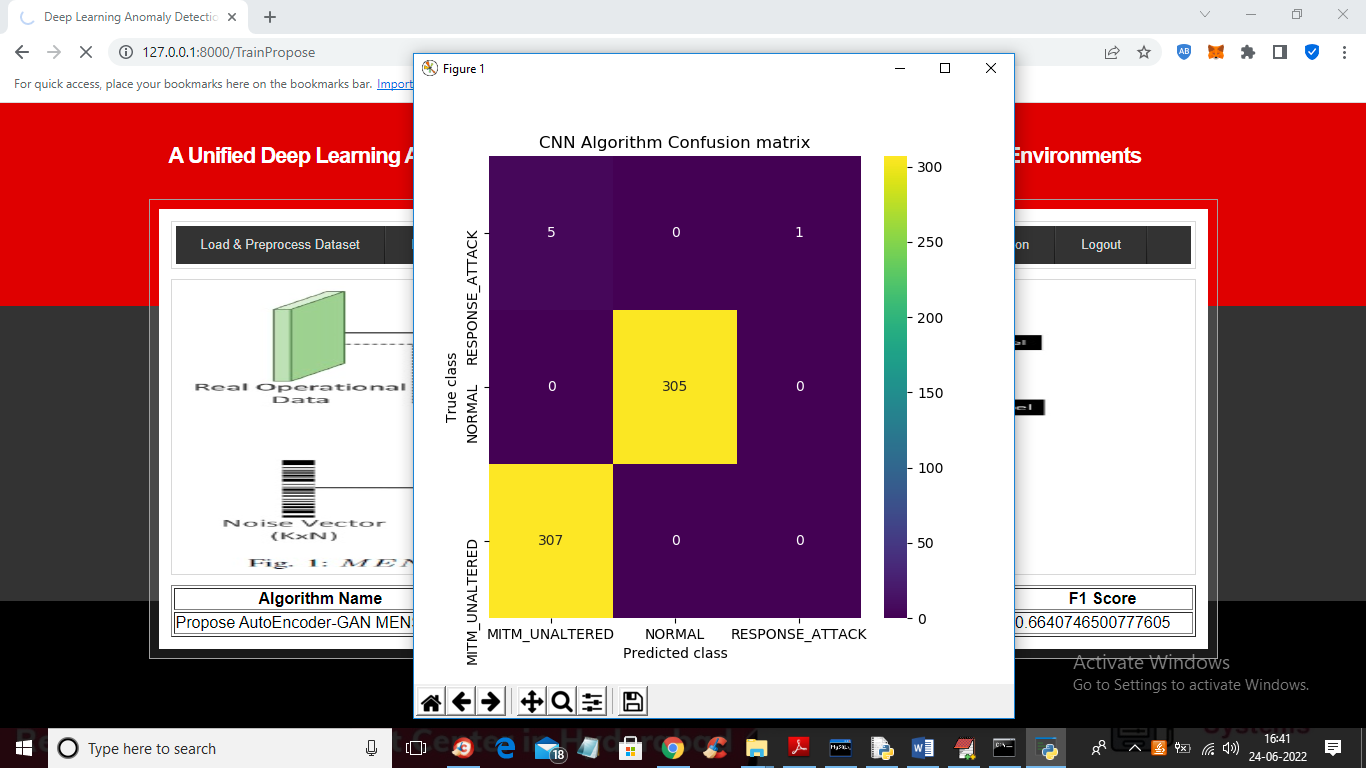
In above screen we can see dataset loaded and now click on ‘Run Encoder-GAN MENSA Model’ link to train AutoEncoder algorithm and get below output



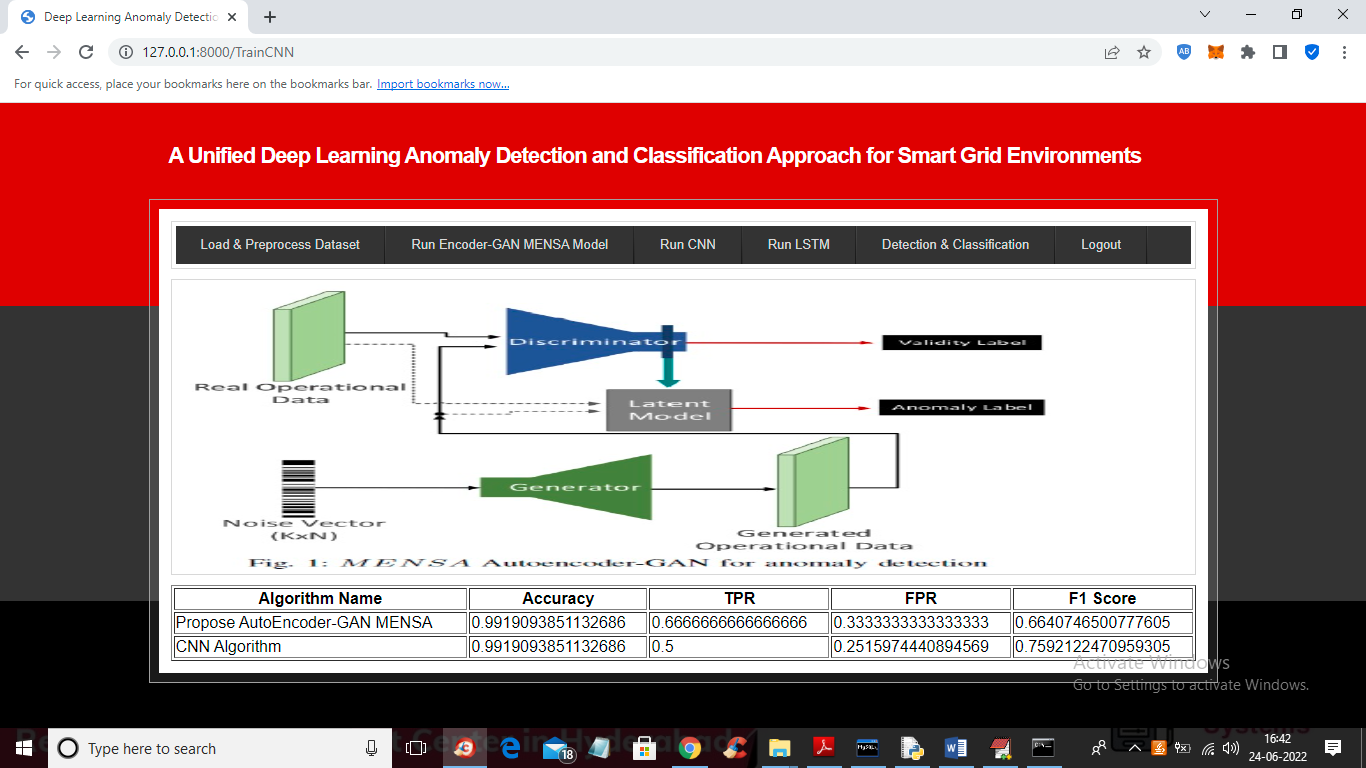
In above AutoEncoder confusion matrix graph x-axis represents Predicted classes and y-axis represents TRUE classes and in yellow boxes in above graph predicted correctly and only 5 records are incorrectly predicted using AutoEncoder algorithm and now close above graph to get below output



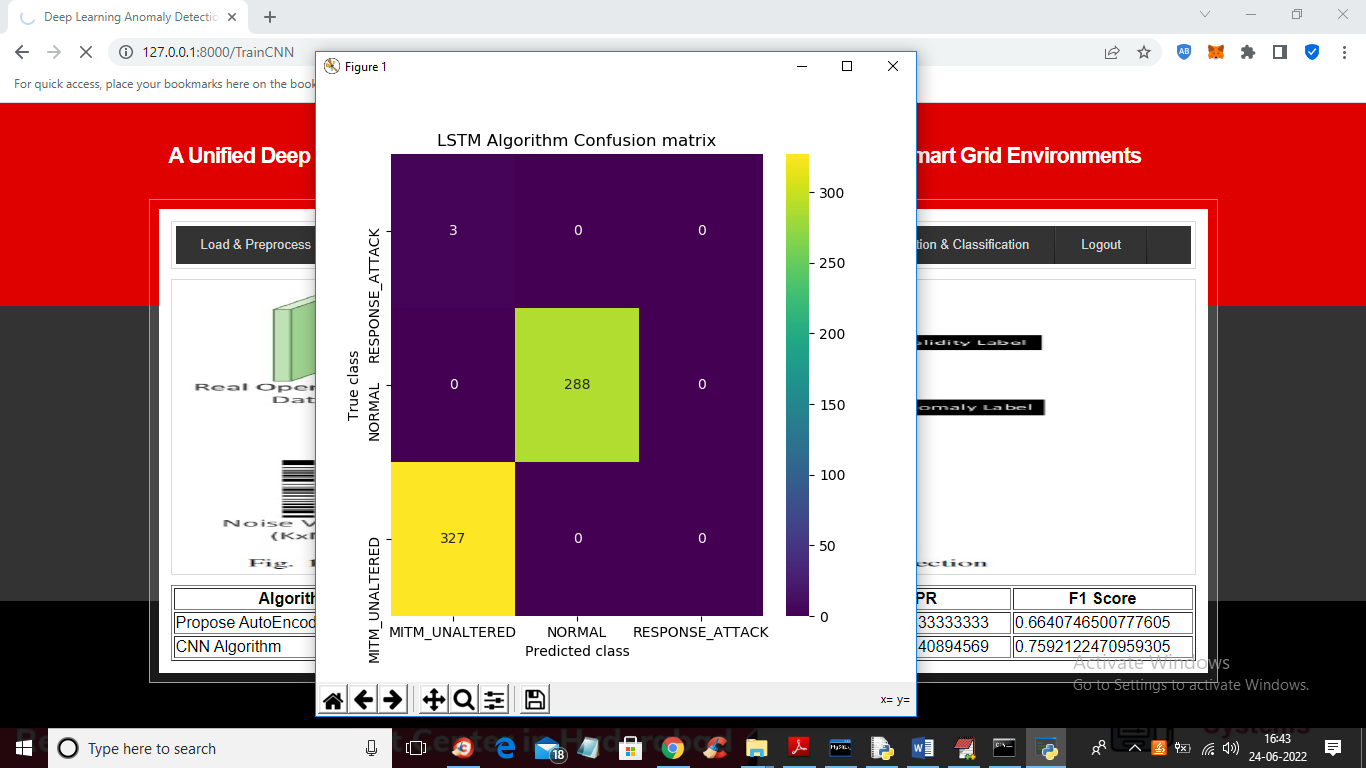
In above screen with AutoEncoder we got 0.99% accuracy and now click on ‘Run CNN’ link to get below output



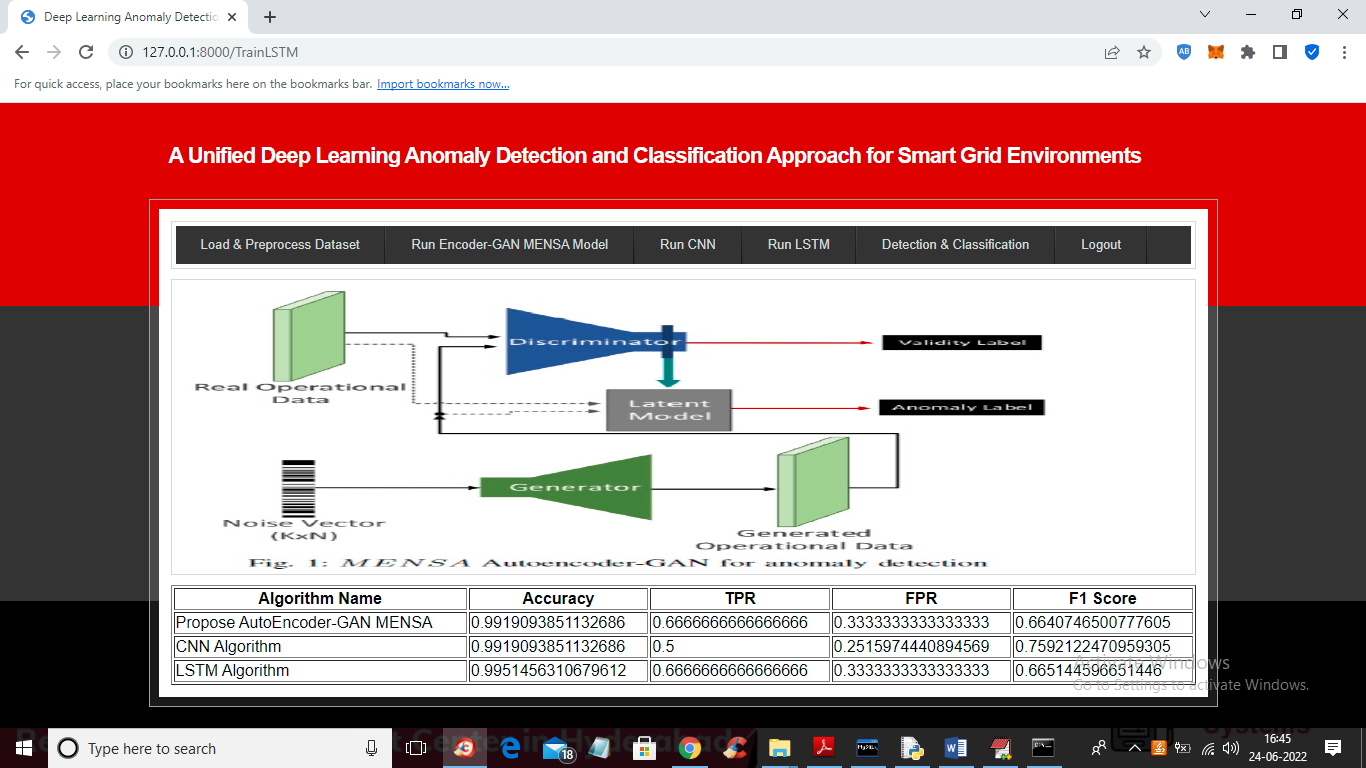
In above CNN confusion matrix graph we can see CNN able to predict ‘Response Attack’ also which is not detected by AutoEncoder and in above graph in first row last column we can see CNN predicted 1 record as Response Attack which was missed by AutoEncoder and now close above graph to get below output



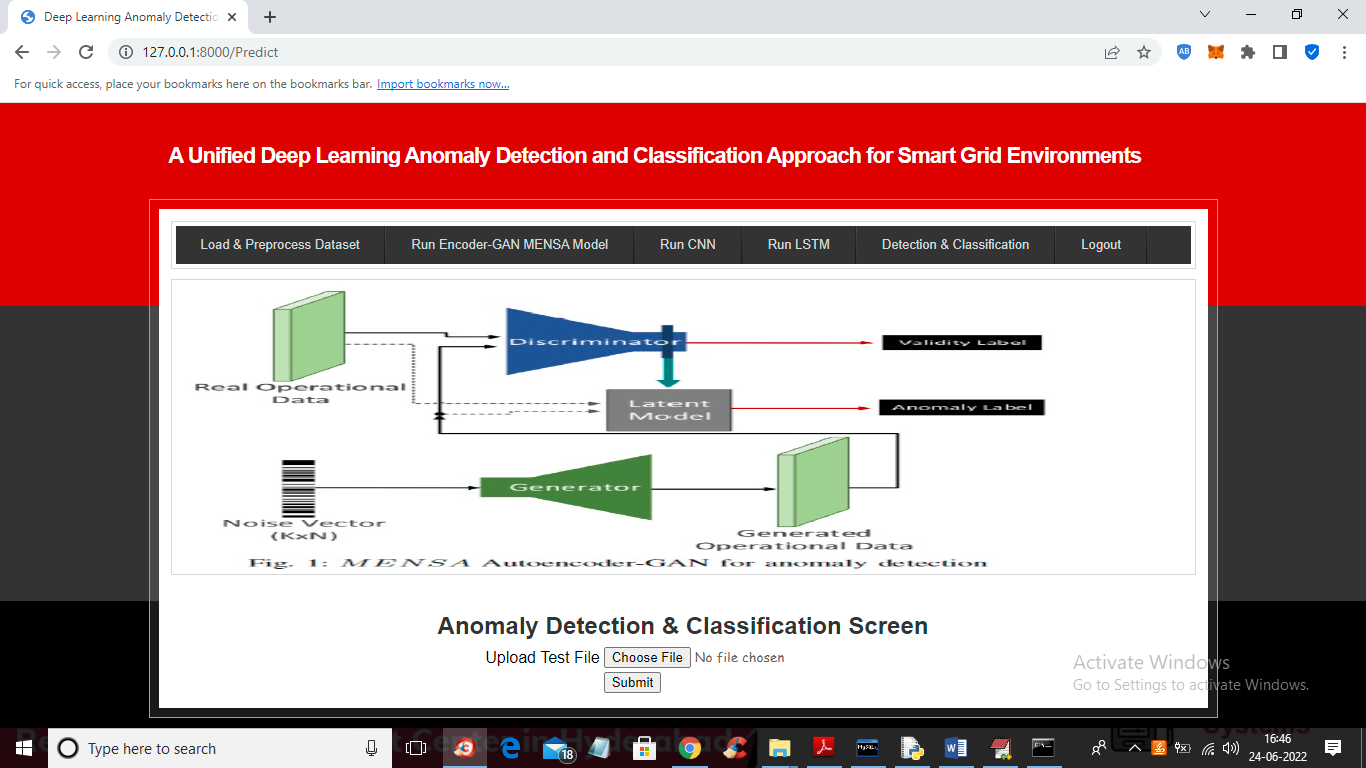
In above screen with CNN also we got accuracy as 0.99 but its FSCORE value is high compare to AutoEncoder and now click on ‘Run LSTM’ to get below output



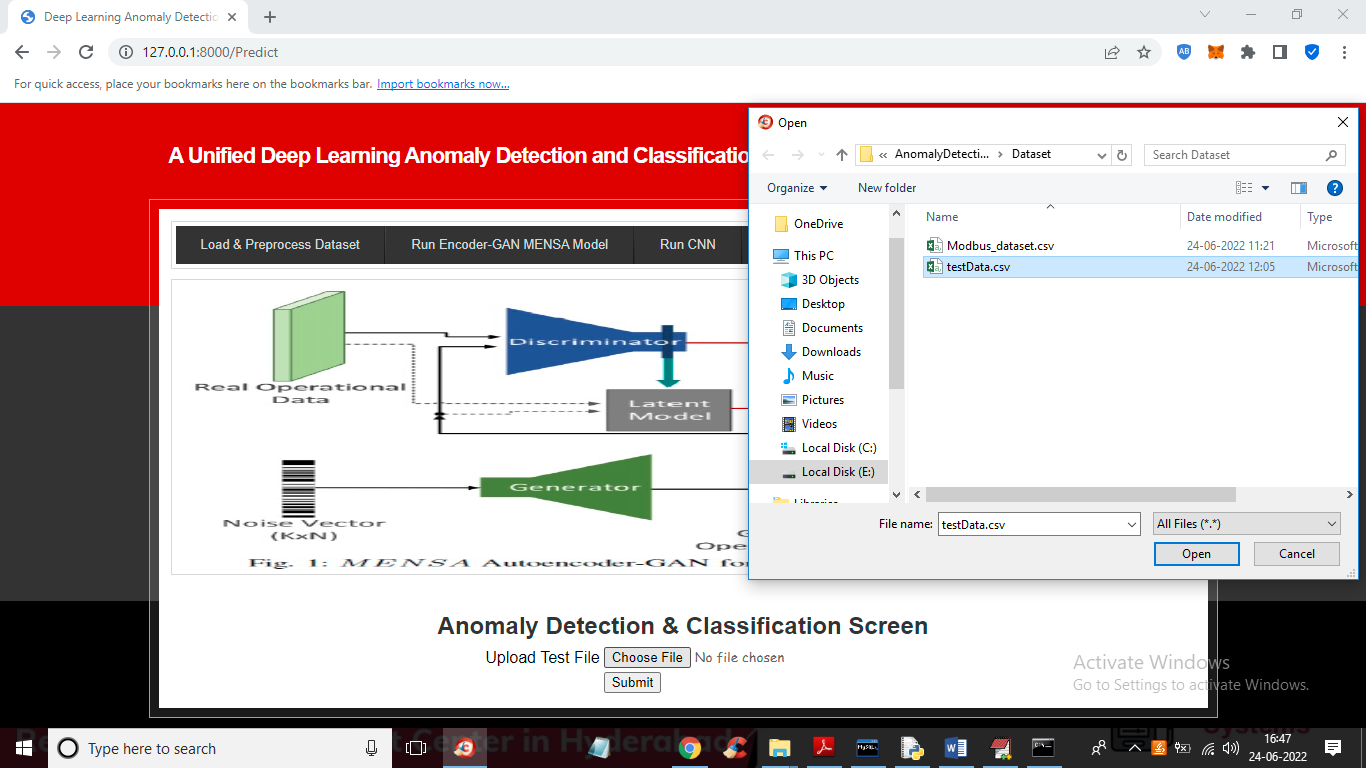
In above LSTM confusion matrix graph we can see LSTM predicted only 3 classes as incorrect but this also unable to detect ‘Response Attack’ class as in last column we can see all values as 0 which means it’s not predicting ‘Response Attack’ but its performance is good as only 3 classes are incorrectly predicted and now close above graph to get below output



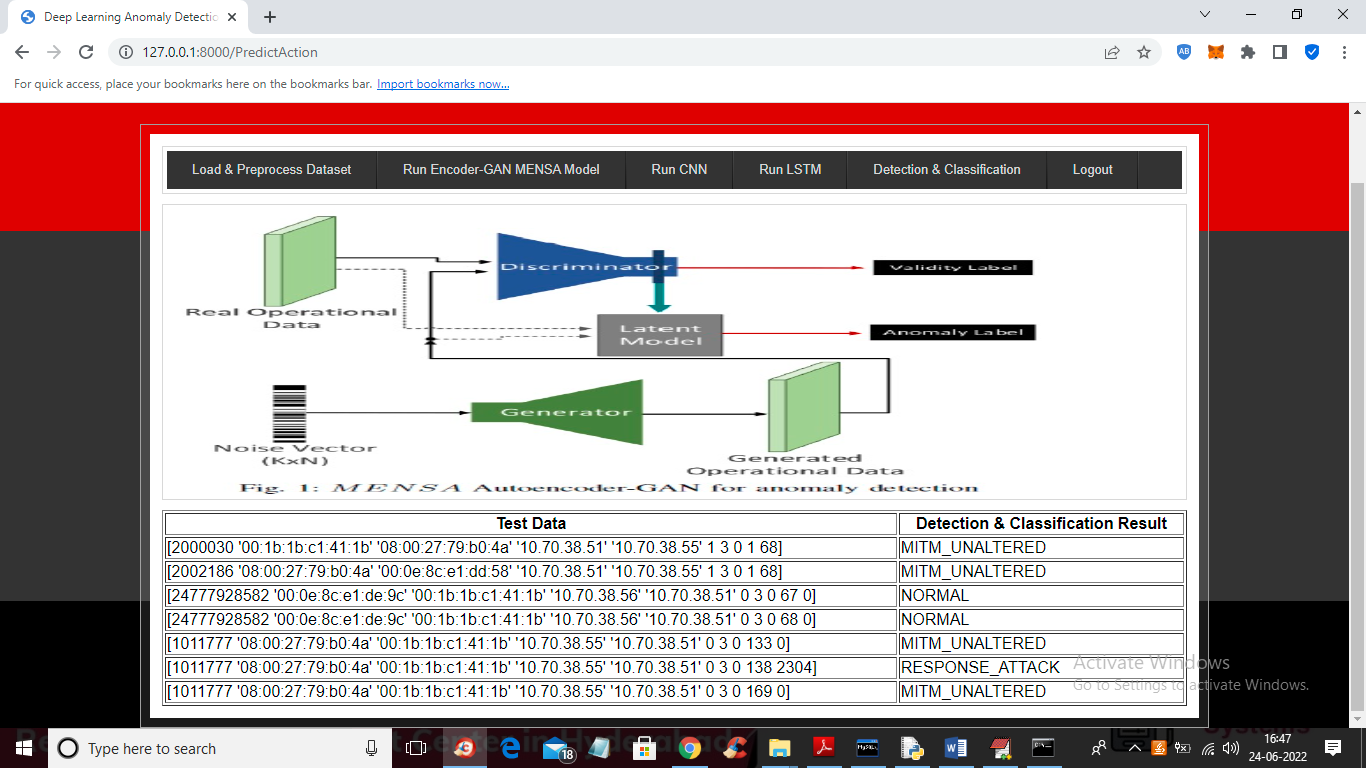
In above screen we can see accuracy, FPR, TPR and FSCORE for all 3 algorithms and from ALL LSTM has got high accuracy as 0.9951 and now click on ‘Detection & Classification’ link to get below screen



In above screen click on ‘Choose File’ and upload test file and this file you can find inside ‘dataset’ folder



In above screen selecting and uploading ‘testData.csv’ file and then click on ‘Open’ and ‘Submit’ button to get below output



In above screen first column contains dataset TEST values and second column contains detection and classification of attack type. In above screen first two records classified as attack type ‘MITM (man in the middle attack) and next 2 records classified as normal.

So by using this algorithms we are detecting and classifying attack from SMART GRID MODBUS dataset.