Securing Smart Sensing Production System using ML & DL Algorithms

Internet of Things enabled cyber physical systems such as Industrial equipment’s and operational IT to send and receive data over internet. This equipment’s will have sensors to sense equipment condition and report to centralized server using internet connection. Sometime some malicious users may attack or hack such sensors and then alter their data and this false data will be report to centralized server and false action will be taken. Due to false data many countries equipment and production system got failed and many algorithms was developed to detect attack but all this algorithms suffers from data imbalance (one class my contains huge records (for example NORMAL records and other class like attack may contains few records which lead to imbalance problem and detection algorithms may failed to predict accurately). To deal with data imbalance existing algorithms were using OVER and UNDER sampling which will generate new records for FEWER class but this technique improve accuracy but not up to the mark.

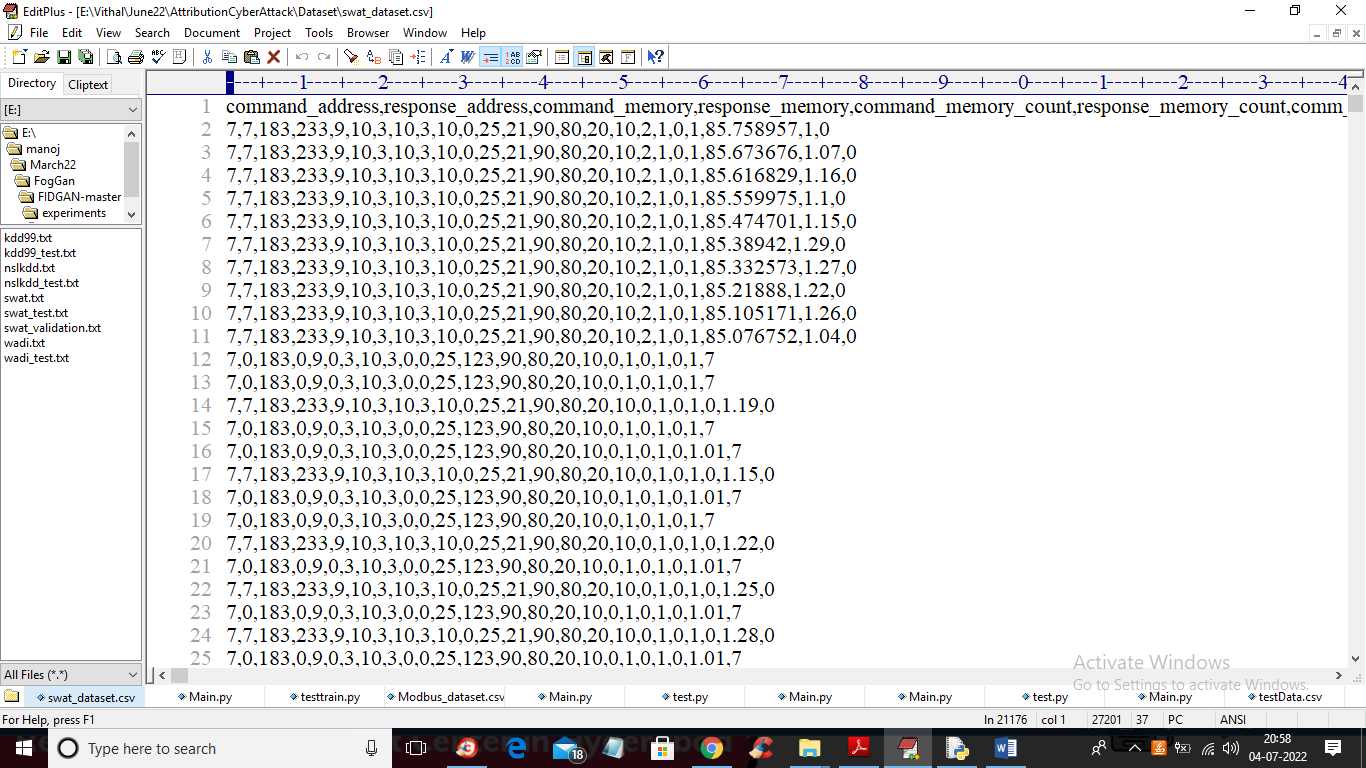
To overcome from this issue we are introducing novel technique without using any under or oversampling algorithms and this technique consists of two parts

1. Auto Encoder: auto encoder deep learning will get trained on imbalanced dataset and then extract features from it and this extracted featured will get trained with DECISION TREE algorithm to predict label for known or unknown attacks. Decision tree get trained on reduced number of features obtained from PCA (principal component analysis) algorithm.
2. Deep Neural Network (DNN): in this level DNN algorithm get trained on known and unknown attacks. If any records contains attack signature then DNN will identify attack label or class and attribute them.

To implement this project we have used SWAT (secure water production treatment) and this dataset contains IOT request and response signature and associate each dataset with unique attack label and dataset contains below cyber-attack labels

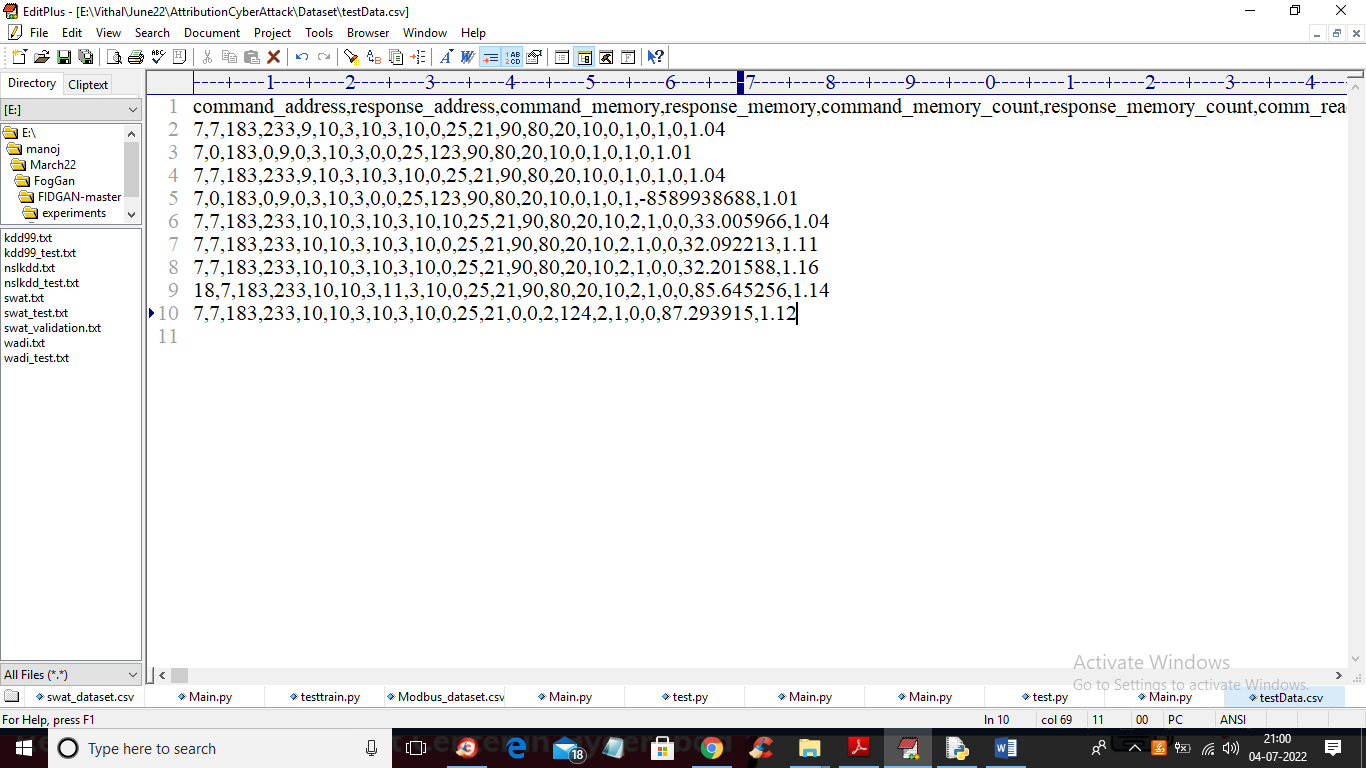
**'Normal', 'Naive Malicious Response Injection (NMRI)', 'Complex Malicious', 'Response Injection (CMRI)', 'Malicious State Command Injection (MSCI)', 'Malicious Parameter Command Injection (MPCI)', 'Malicious Function Code Injection (MFCI)', 'Denial of Service (DoS)'**

Above are the attacks found in dataset and dataset contains above labels as integer value of its index for example NORMAL label index will be 0 and continues up to 8 class labels. Below screen showing dataset details



In above dataset screen first row contains dataset column names and remaining rows contains dataset values and in last column we have attack type from label 0 to 7. We will used above dataset to train propose Auto Encoder, decision tree and DNN algorithms.

In below screen we are using NEW test data which contains only signature and there is no class label and propose algorithm will detect and attribute class labels.

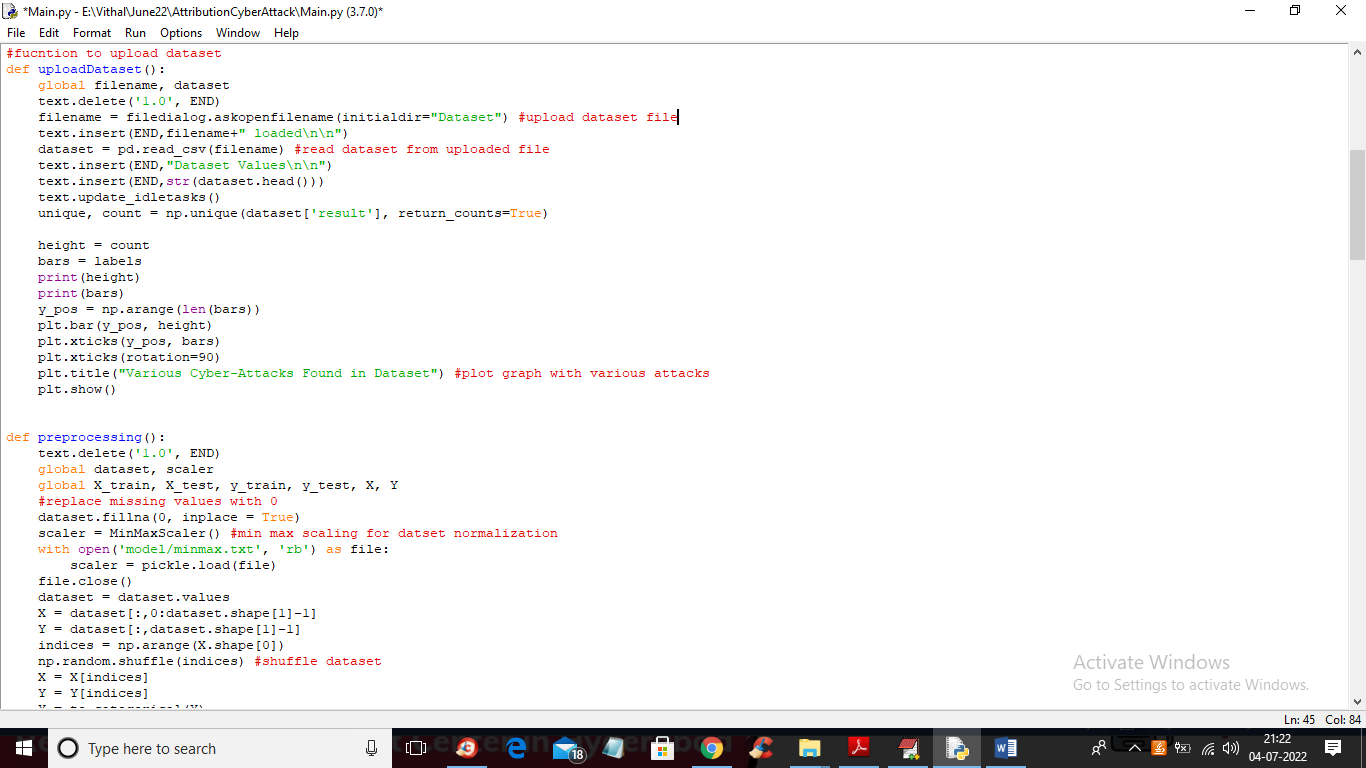


In above test data we have IOT request signature without class labels.

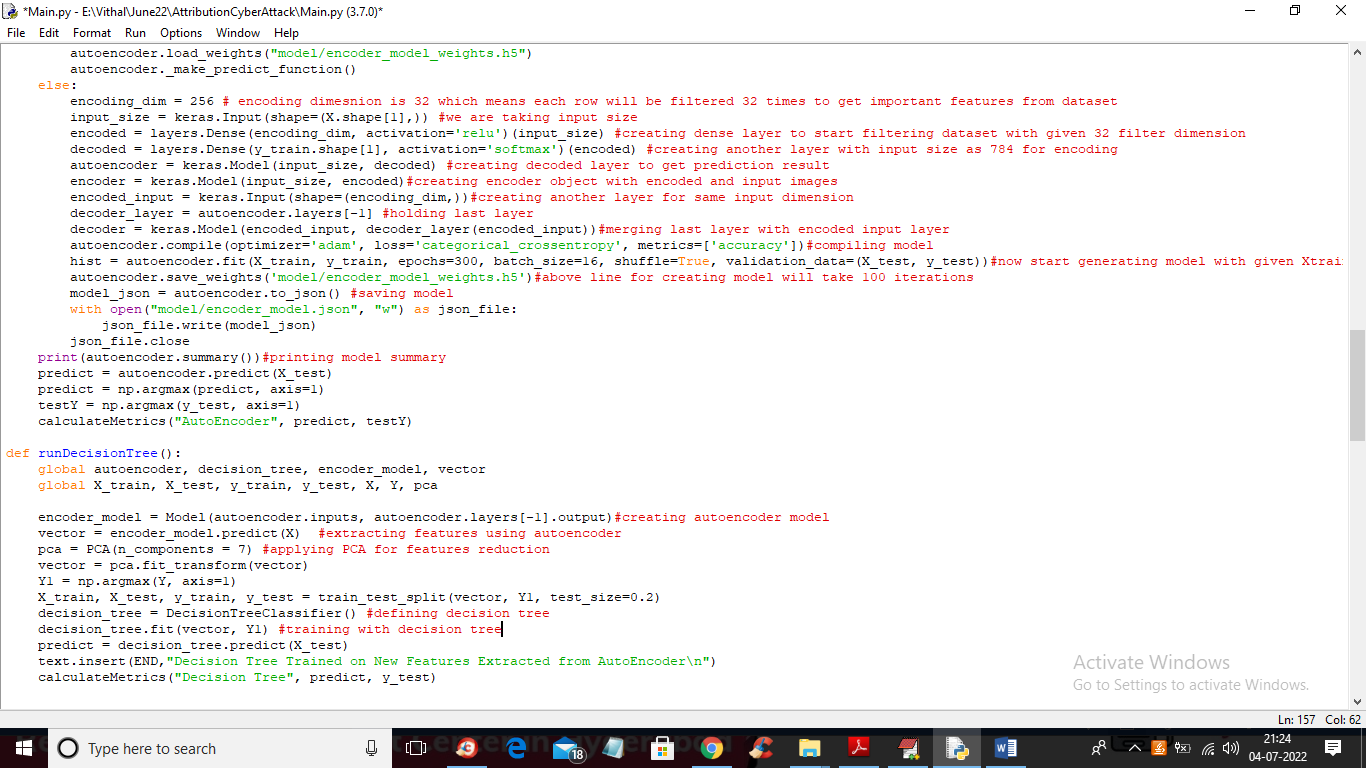
To implement this project we have designed following modules

1. Upload SWAT Water Dataset: using this module we will upload dataset to application and then read dataset and then find different attacks found in dataset
2. Preprocess Dataset: using this module we will replace all missing values with 0 and then apply MIN-MAX scaling algorithm to normalized features values and then split dataset into train and test where application used 80% dataset for training and 20% for testing
3. Run AutoEncoder Algorithm: using this module we will trained AutoEncoder deep learning algorithm and then extract features from that model.
4. Run Decision Tree with PCA: extracted features from AutoEncoder will get transform using PCA to reduce features size and then retrain with Decision tree. Decision tree will predict label for each record based on dataset signatures
5. Run DNN Algorithm: predicted decision tree label will further train with DNN (deep neural network) algorithm to detect and attribute attacks
6. Detection & Attribute Attack Type: using this module we will upload unknown or un-label TEST DATA and then DNN will predict attack type
7. Comparison Graph: using this module we will plot comparison graph between all algorithms
8. Comparison Table: using this module we will display comparison table of all algorithms which contains metrics like accuracy, precision, recall and FSCORE.

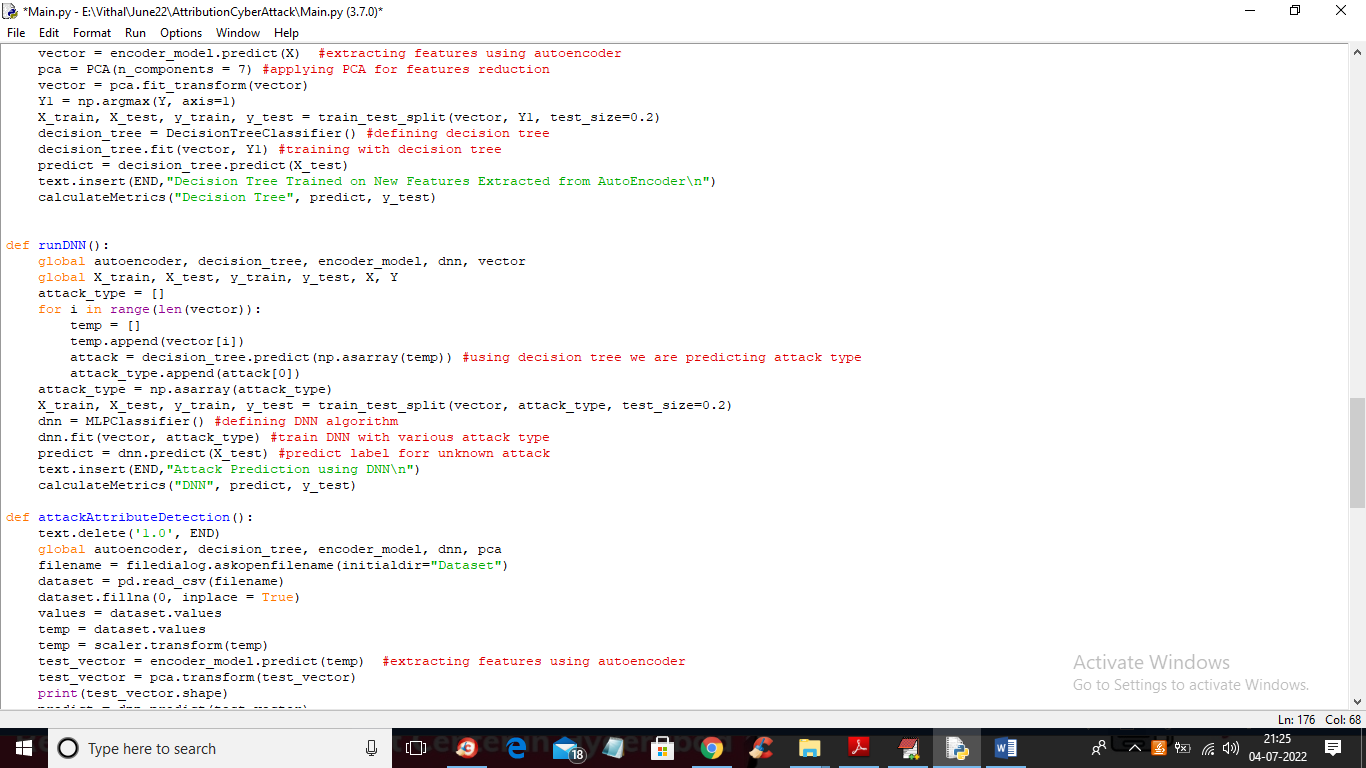
In below screen you can read red colour comments to know about algorithms implementation



In above screen read red colour comments to know about dataset loading and min-max normalization



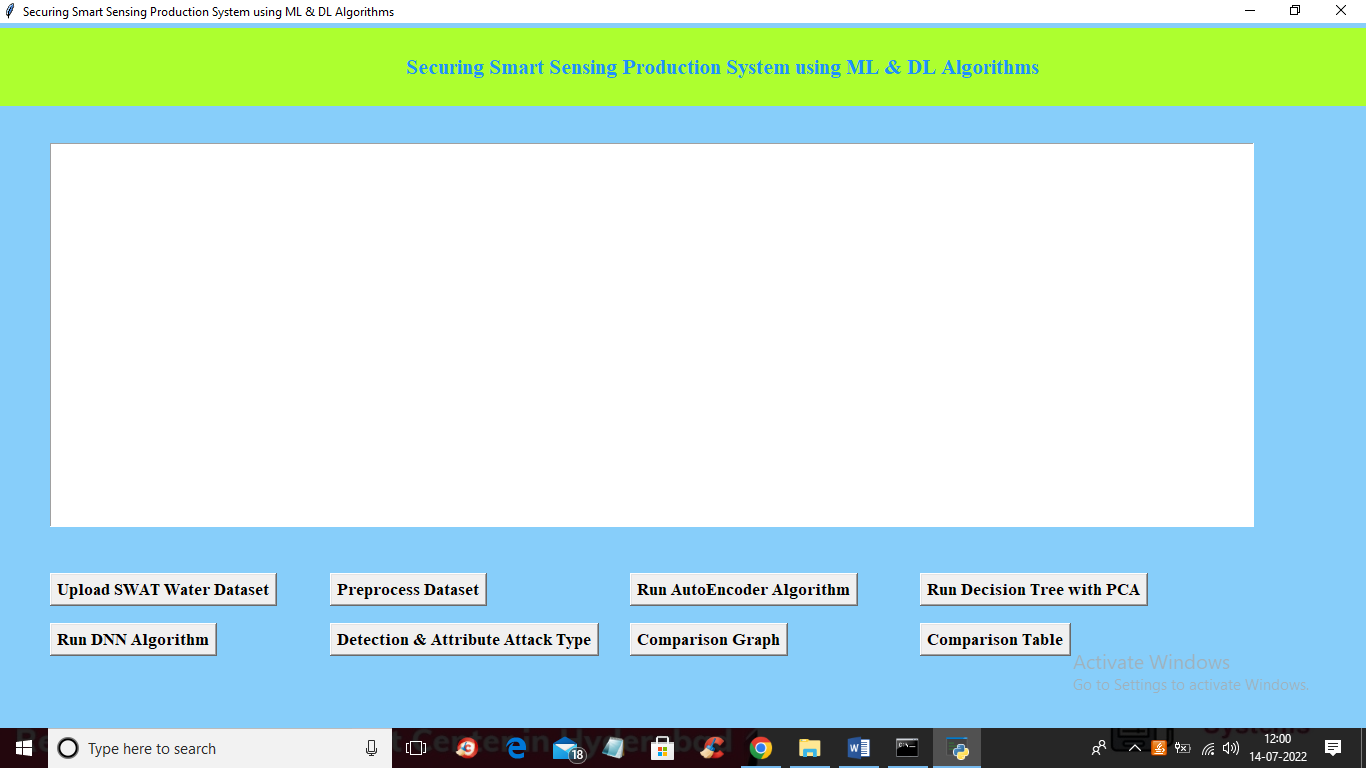
In above screen you can see we are using AutoEncoder, PCA and decision tree to train dataset and in below screen we are using DNN algorithms to train dataset with predicted labels from Decision Tree.



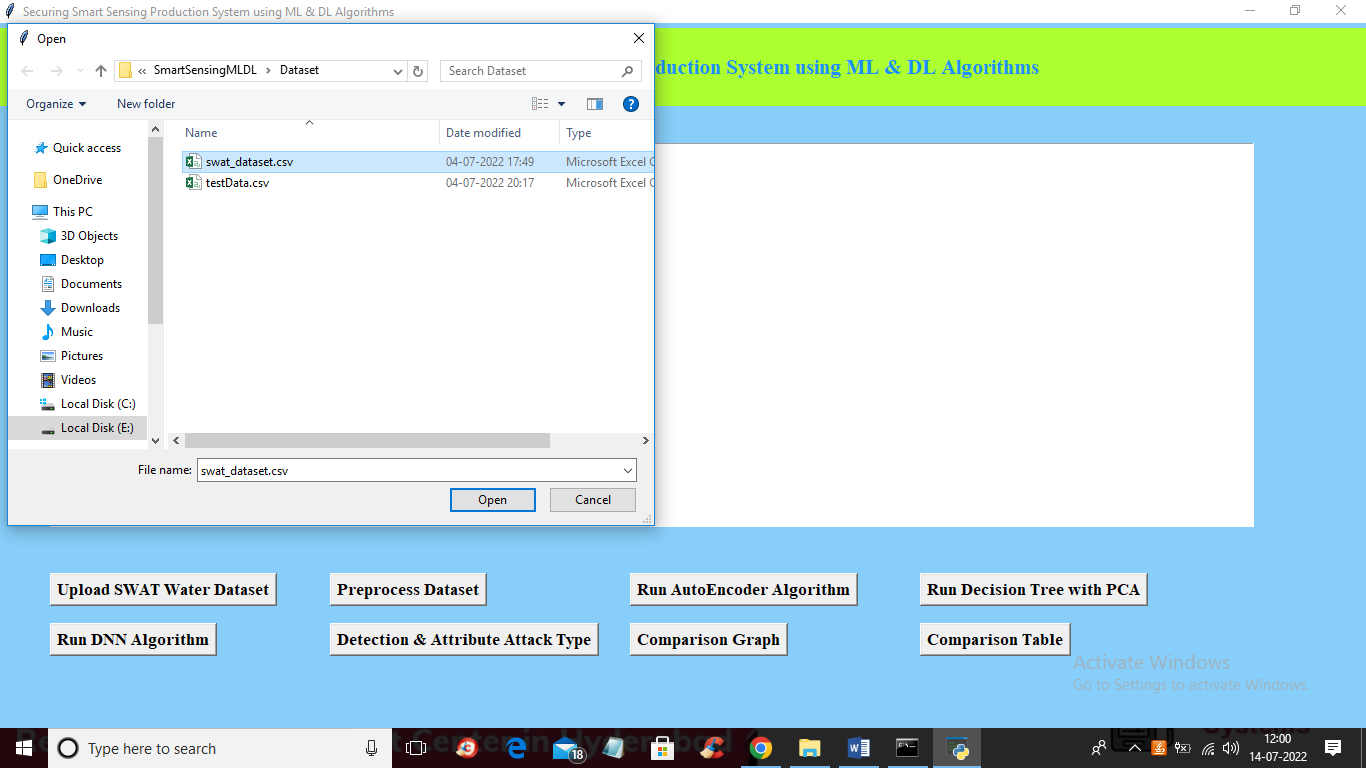
In above screen we are training dataset with DNN algorithms

SCREEN SHOTS

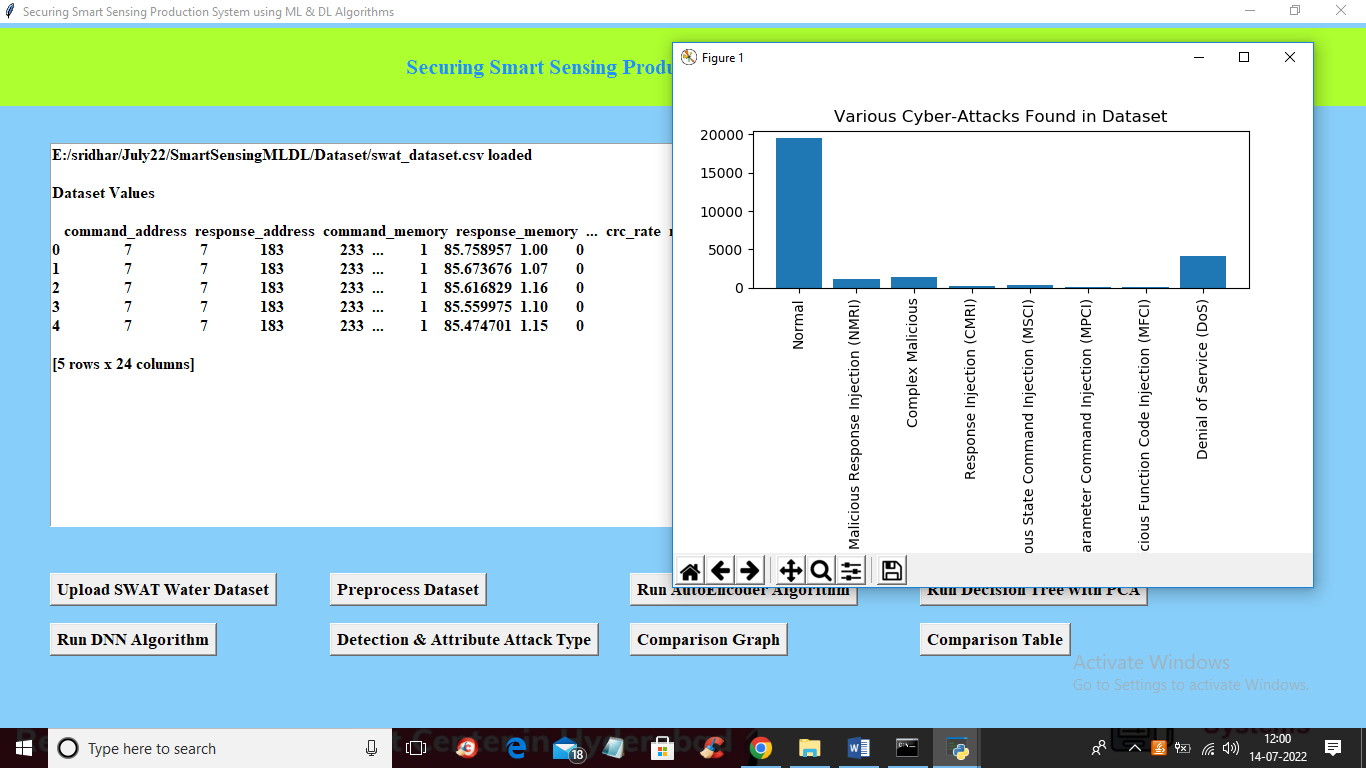
To run project double click on ‘run.bat’ file to get below screen



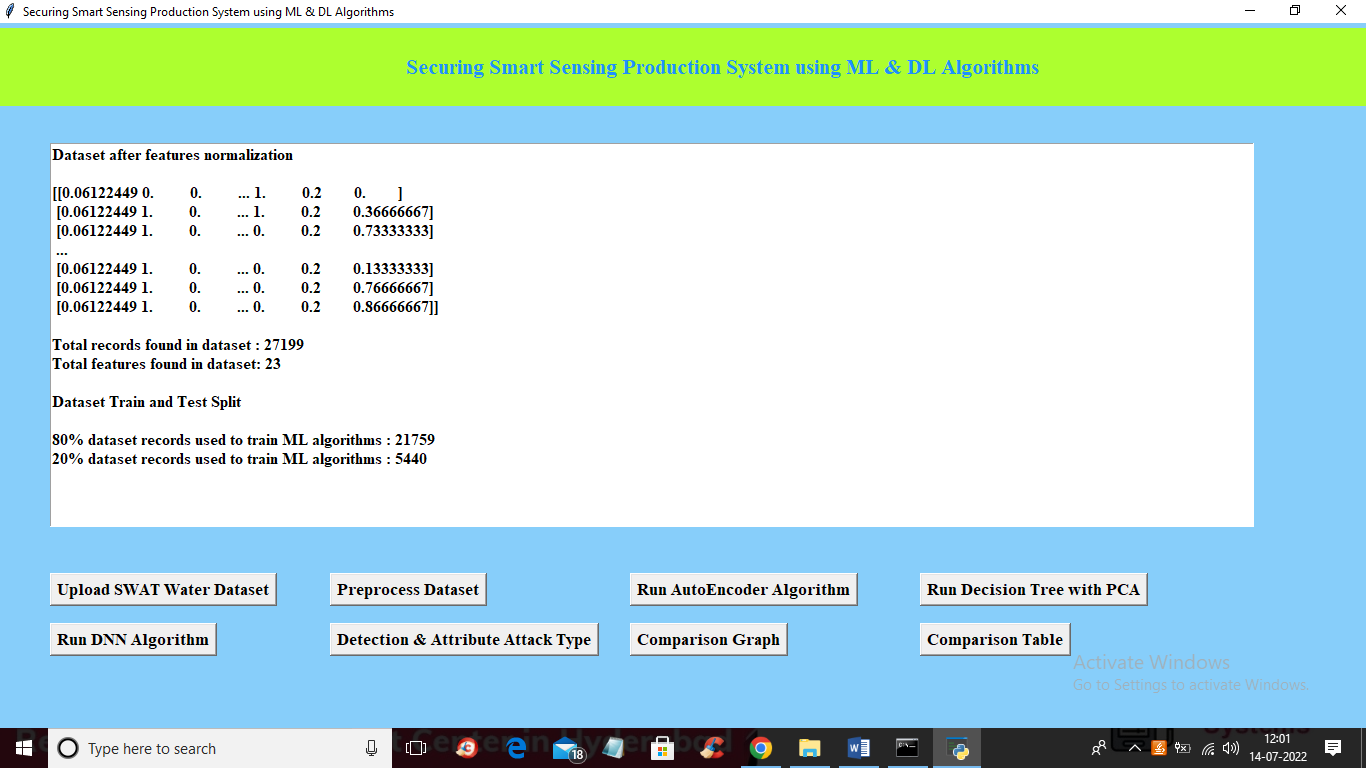
In above screen click on ‘Upload SWAT Water Dataset’ button to upload dataset to application and get below output



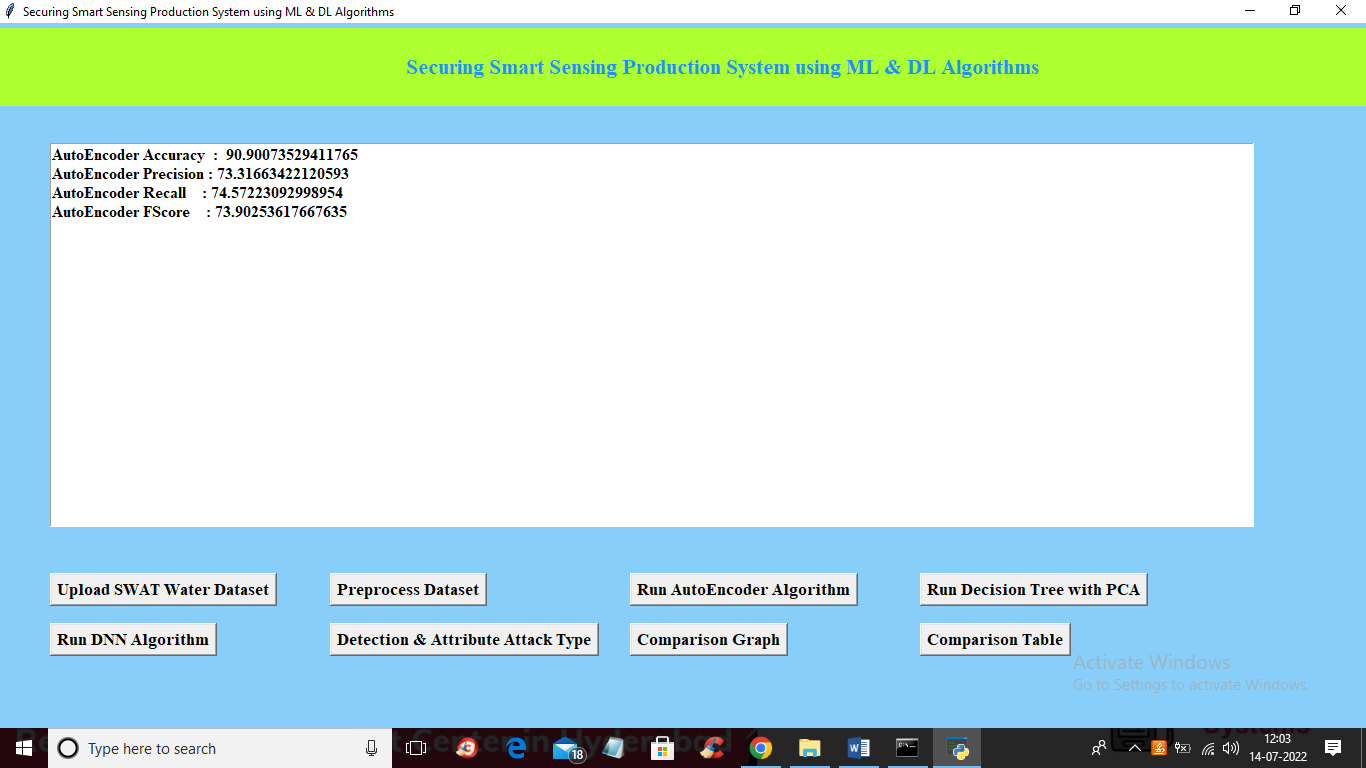
In above screen selecting and uploading SWAT dataset file and then click on ‘Open’ button to load dataset and get below output



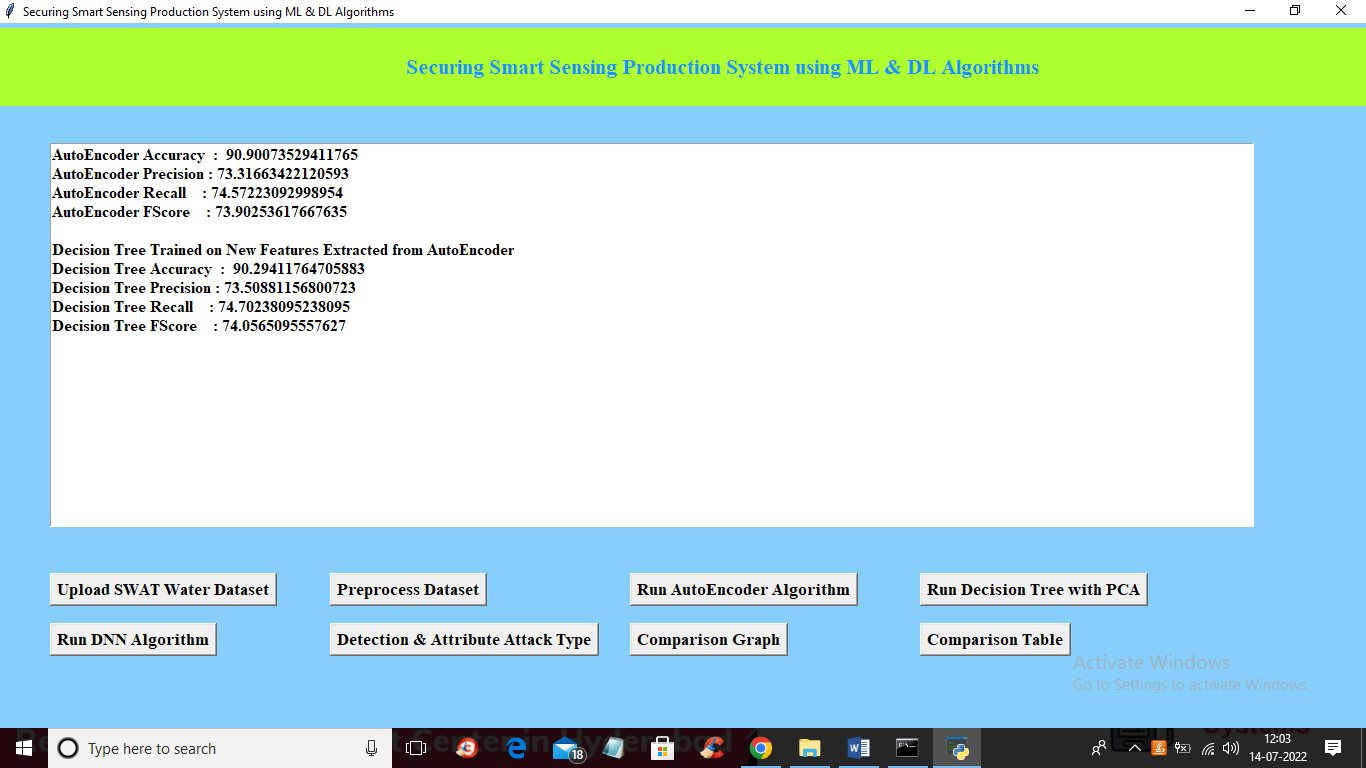
In above screen dataset loaded and in graph x-axis contains ATTACK NAME and y-axis contains count of those attacks found in dataset and we can see ‘NORMAL’ class contains so many records and other attacks contains very few records so it will raise data imbalance problem which can be solved using AutoEncoder, Decision Tree and DNN. Now close above graph and then click on ‘Preprocess Dataset’ button to remove missing values and then normalized values with MIN-MAX algorithm



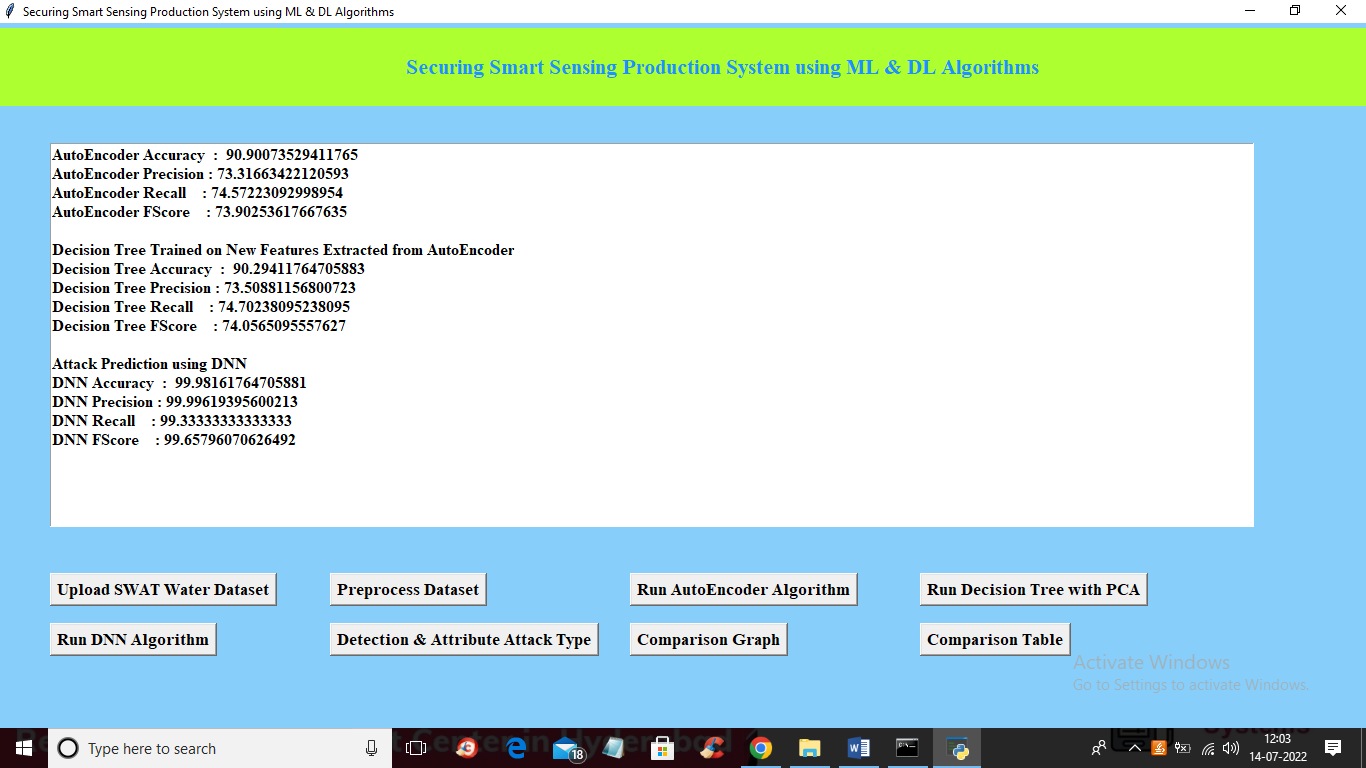
In above screen all values are normalized ( converting data between 0 and 1 called as normalization) and then we can see total records in dataset and then dataset train and test split records count also displaying. Now dataset is ready and now click on ‘Run AutoEncoder Algorithm’ button to train dataset with AutoEncoder and get below accuracy



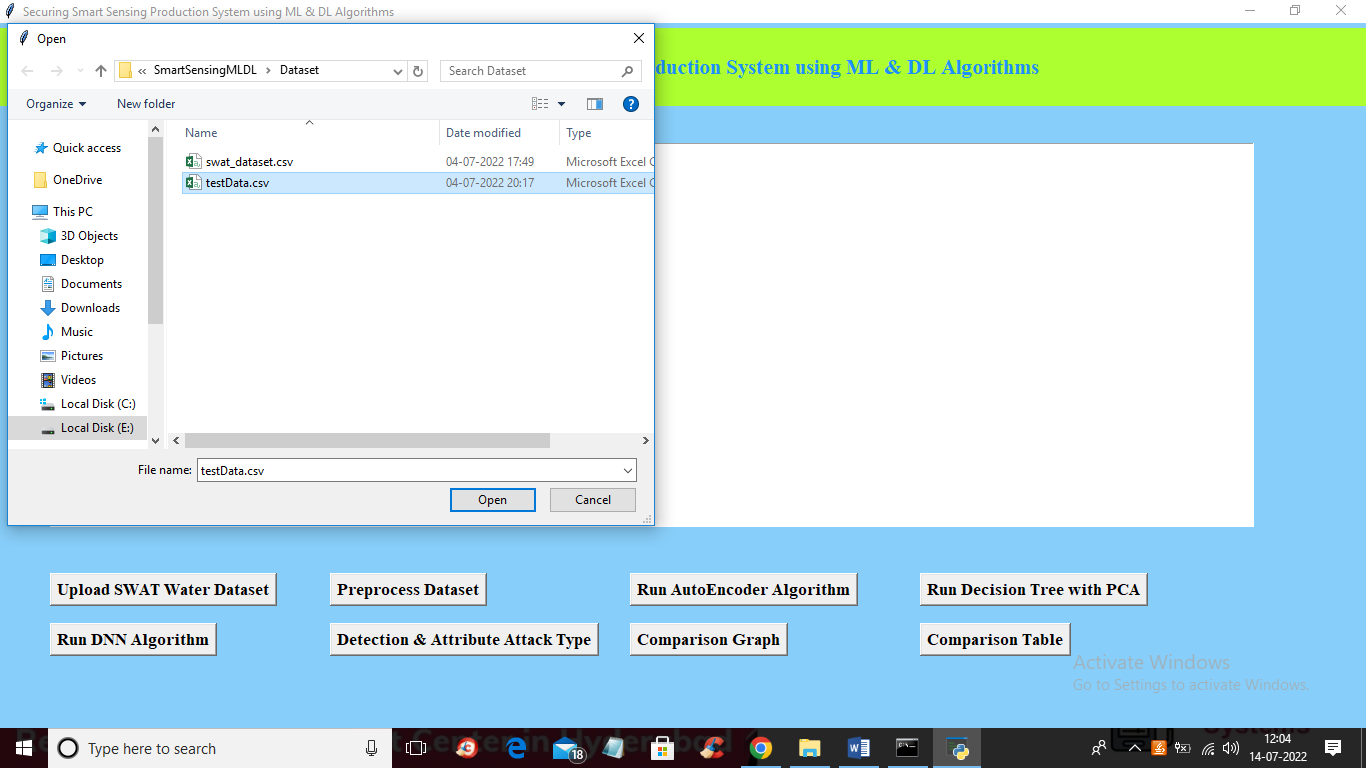
In above screen with AutoEncoder we got 90% accuracy and this accuracy can be enhance by implementing Decision Tree with PCA algorithm and now click on ‘Run Decision Tree with PCA’ button to get below output



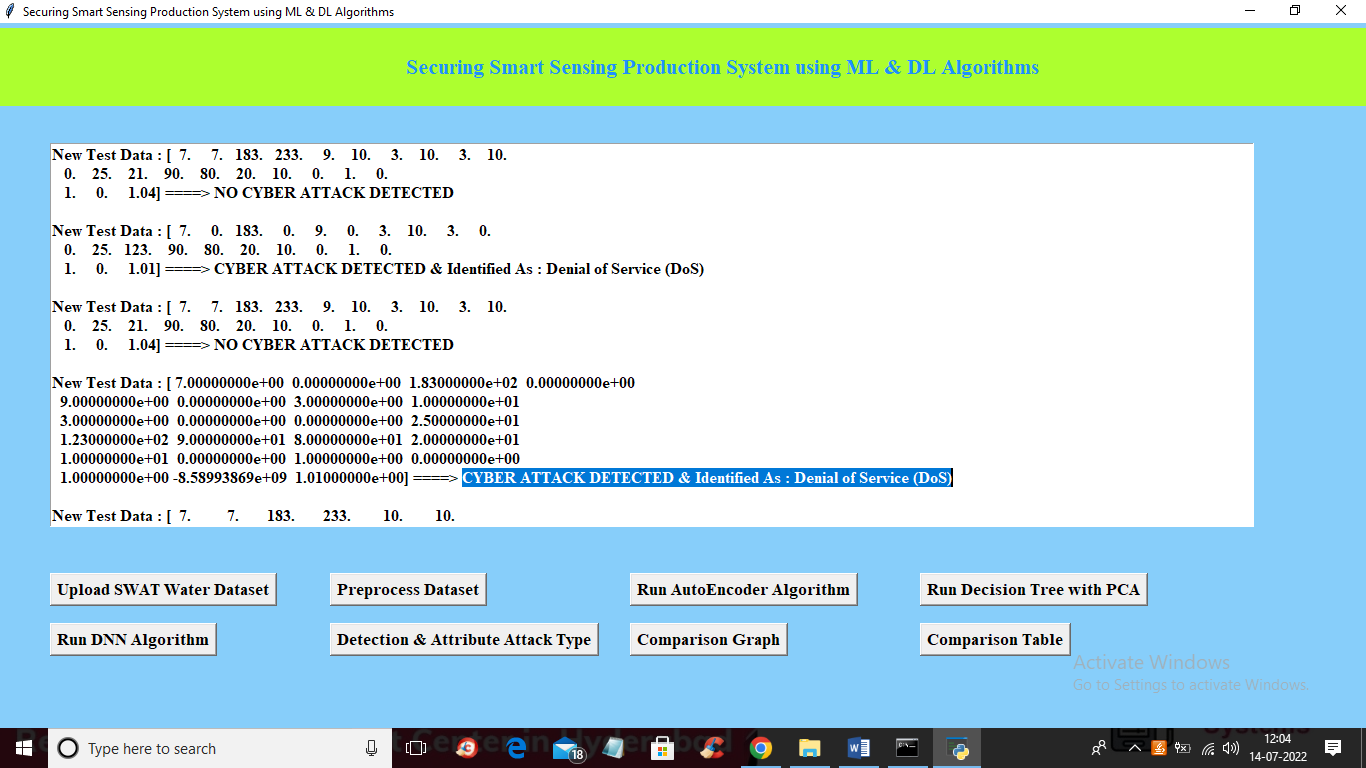
In above screen we can see with decision tree accuracy and precision value is enhanced and now click on ‘Run DNN Algorithm’ button to further enhance accuracy and get below output



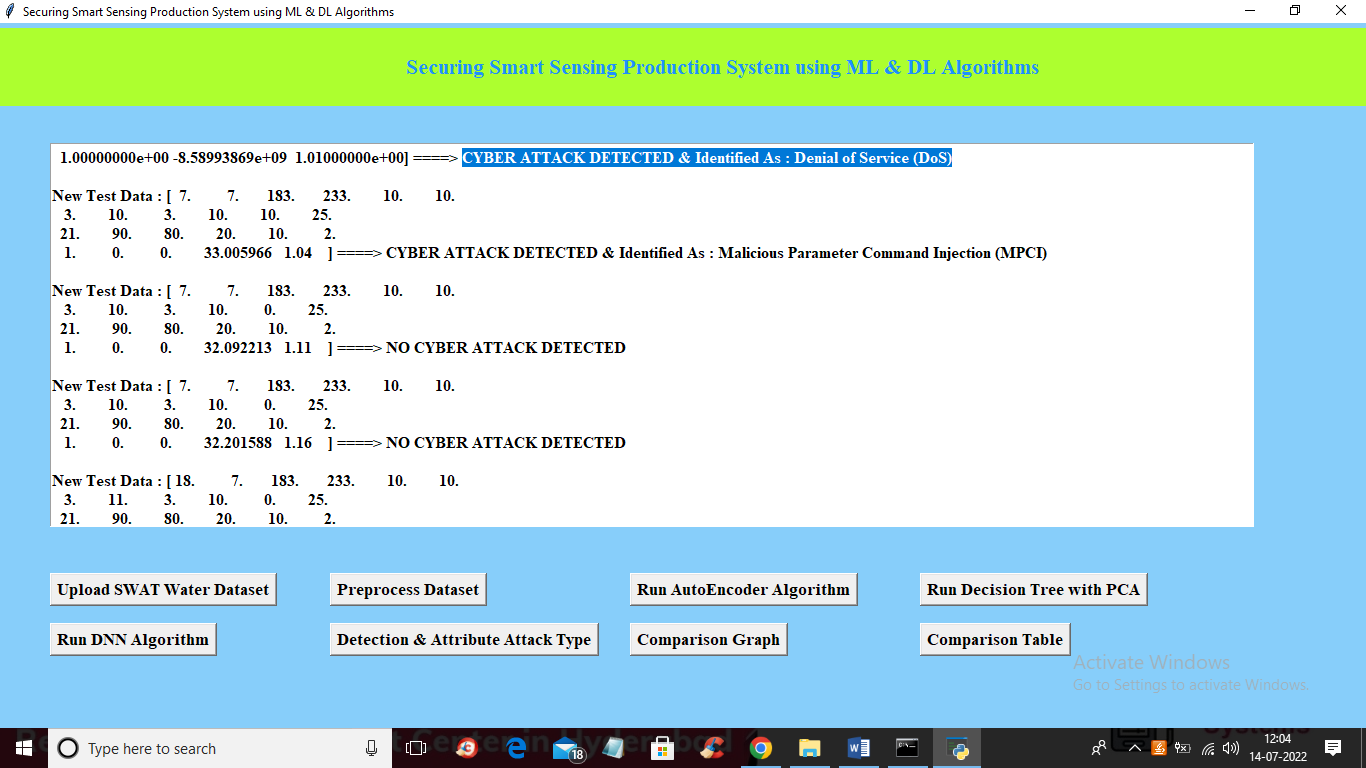
In above screen with DNN we got 99% accuracy and this accuracy may vary from 95 to 100% as we are splitting dataset into random train and test. Now click on ‘Detection & Attribute Attack Type’ button to upload test DATA and detect attack attributes



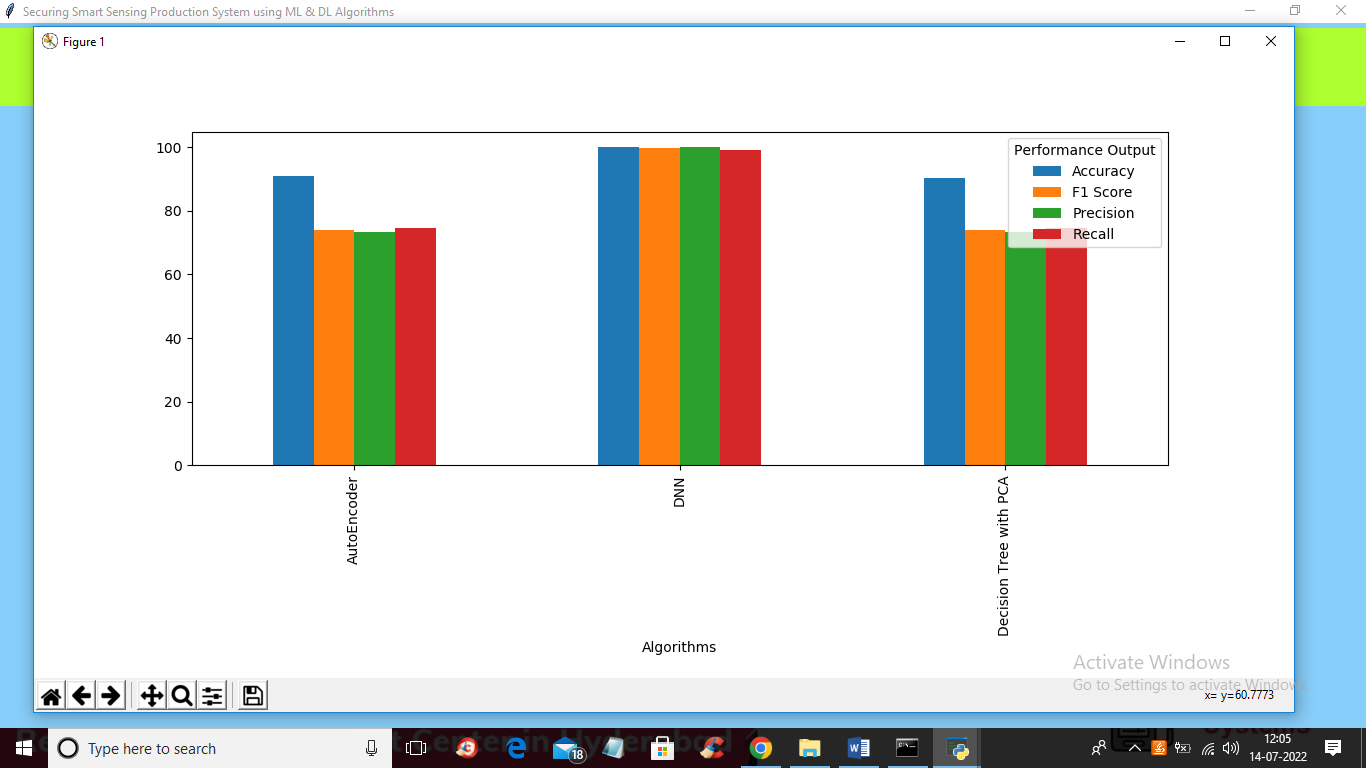
In above screen selecting and uploading ‘TEST DATA’ file and then click on ‘Open’ button to get below output



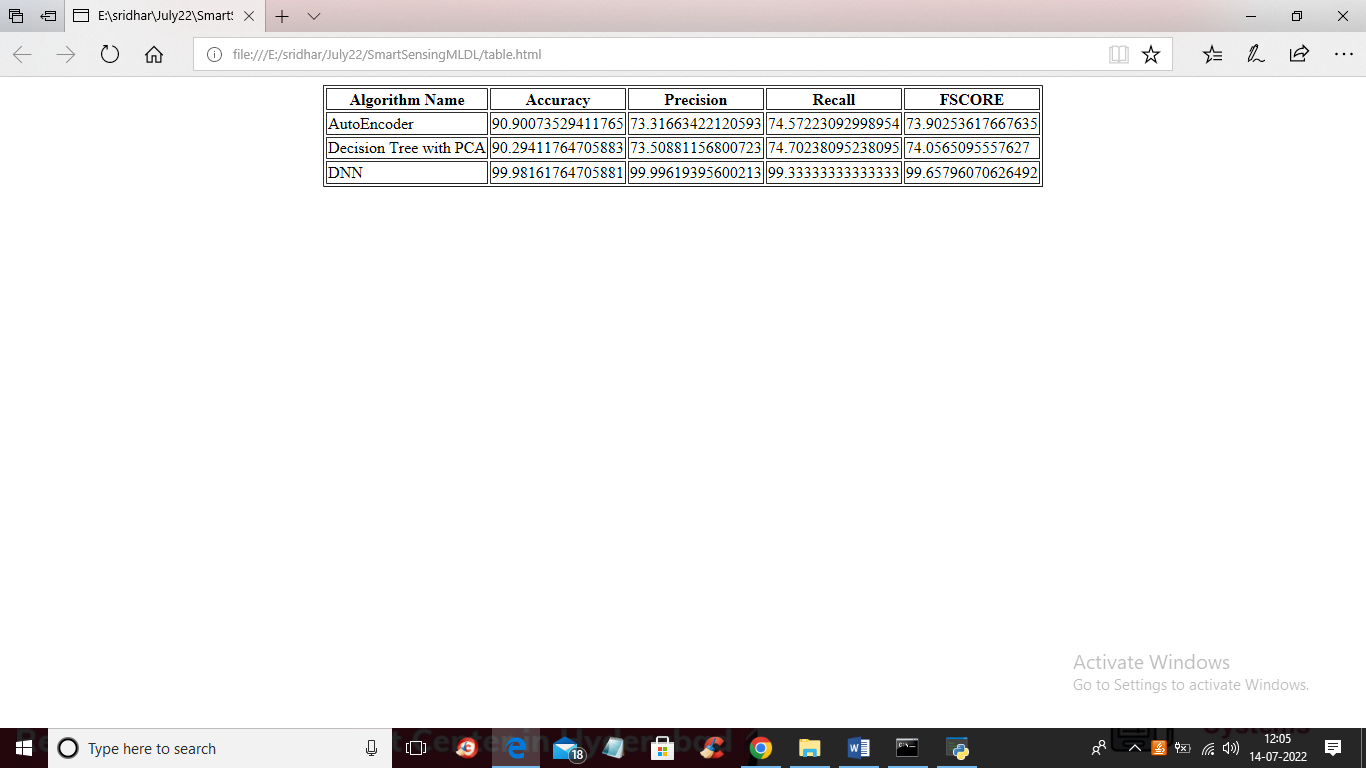
In above screen in square bracket we can see TEST data values and after arrow =🡺 symbol we can see detected ATTACK TYPE and scroll down above text area to view all detection



In above screen we can see detected various attacks and now click on ‘Comparison Graph’ button to get below graph



In above graph x-axis represents algorithms names and y-axis represents different metric values such as precision, recall, accuracy and FSCORE with different colour bars and in all algorithms DNN got high accuracy and now close above graph and then click on ‘Comparison Table’ to get below comparison table of all algorithms



In above table we can see algorithm names and its metrics values such as accuracy and precision and other.