Detection and Isolation of Sensor Attacks for Autonomous Vehicles: Framework, Algorithms, and Validation

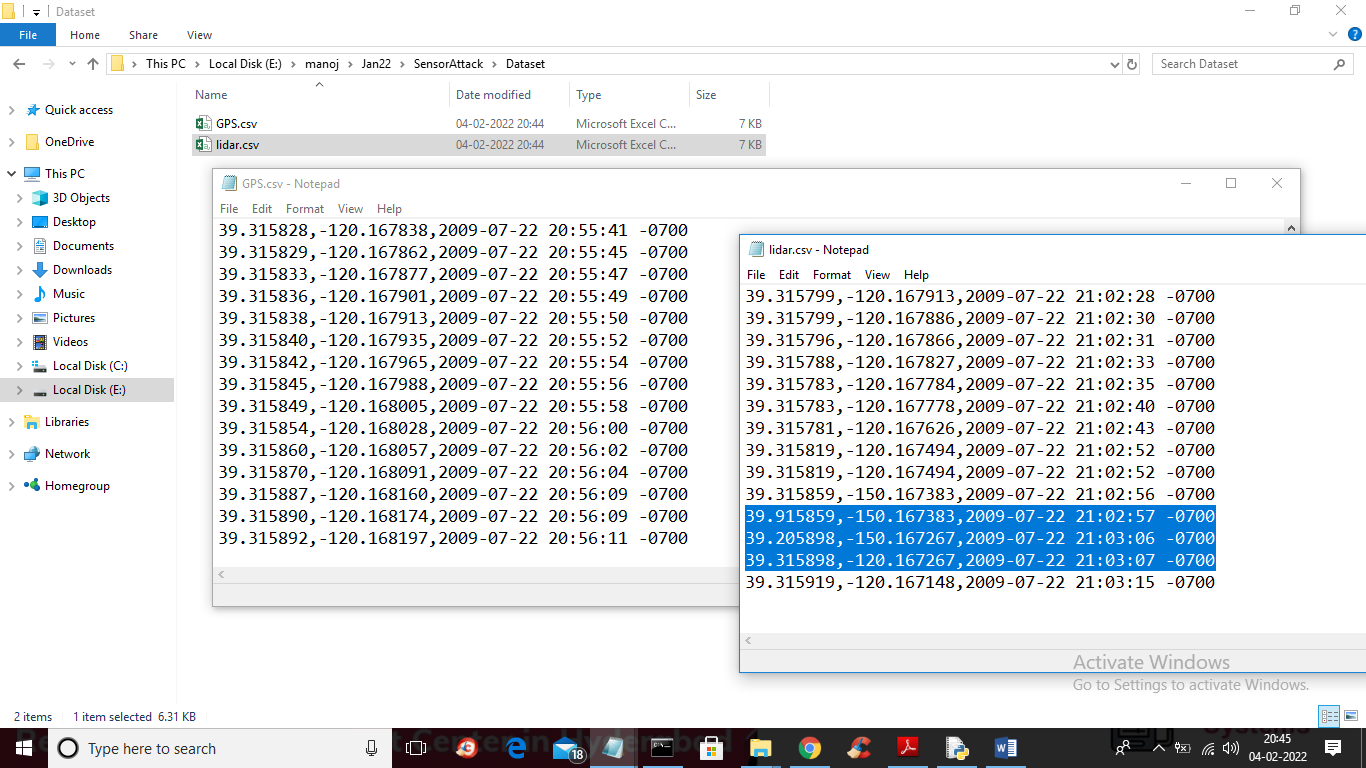
In this paper author introduced new model (based on mathematical formula) to detect cyber sensor attack from autonomous vehicles. Now-a-days self-driving vehicles are gaining lots of popularity as it can drive by itself by using sensor data and sometime this sensor data can be hacked or attack to report false information (report obstacle on road when there is no obstacle or report no obstacle when obstacle available on road (False Injection Attack) or DDOS attack where sensor not allowed to send data to destination or STEALTHY attack where attacker modifies the data or REPLAY attack where attacker replace new values with old values.

To prevent above attacks many technologies were introduced such as DATA ENCRYPTION or Machine Learning Algorithms but this techniques are not efficient as encryption required KEYS management and machine learning algorithms require training of data.

To overcome from above problem author introduced MODEL BASED Mathematical algorithms such Extended KALMAN Filter (EKF) and CUSUM algorithms. EKF algorithm can be used to predict new location of vehicles by monitoring previous location and CUSUM will be used to find variation between original vehicle location and EKF prediction and if there is huge variation observed then ATTACK ALARM will be raised.

In propose paper author using multiple sensors data such as GPS and LIDAR and both this sensor data will be monitored by EFK and CUSUM. CUSUM will apply 8 RULES/CASES on variation data to detect type of attack such as BOTH LIDAR & GPS ATTACK or only GPS Attack or only LIDAR attack.

To implement this project author has used vehicles GPS and LIDAR dataset and we are also using same dataset to detect attack and this dataset contains vehicle latitude and longitude with time details and below is the screen shots of both datasets

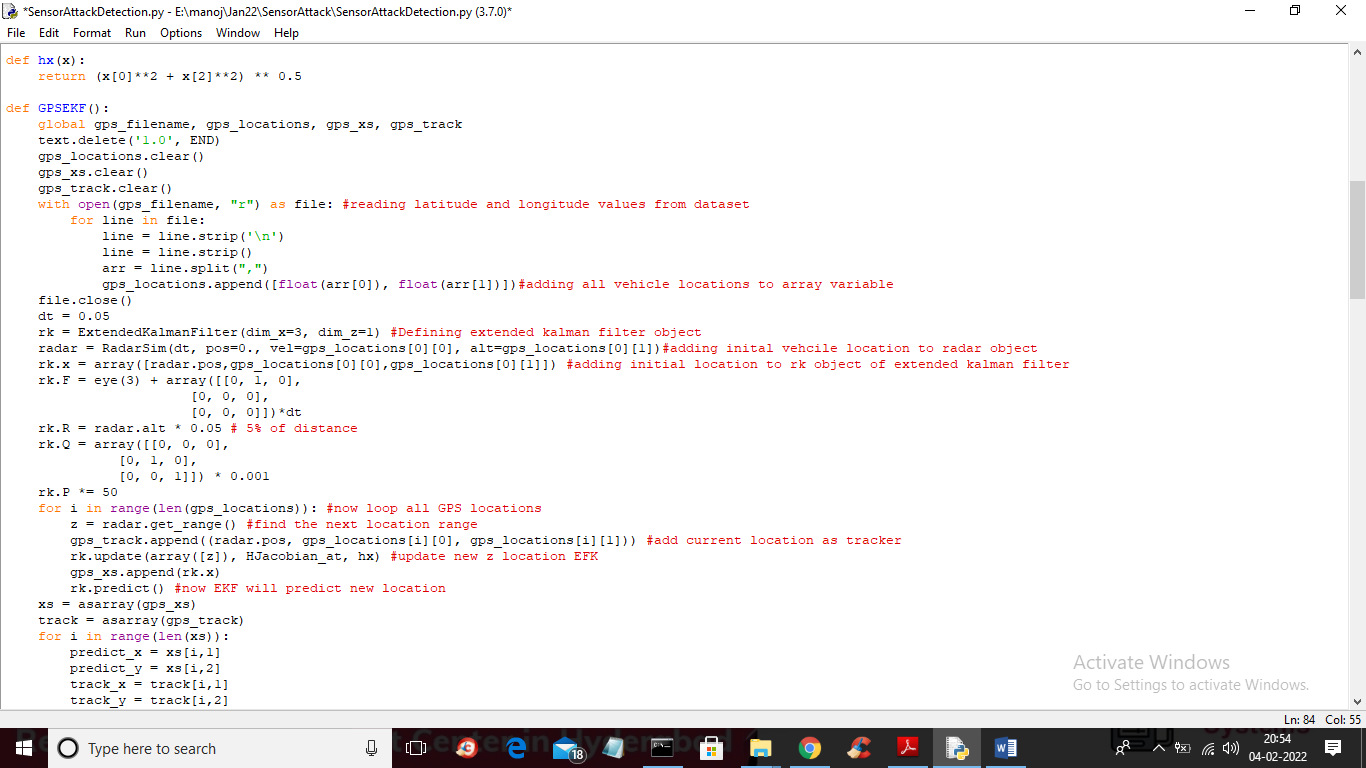


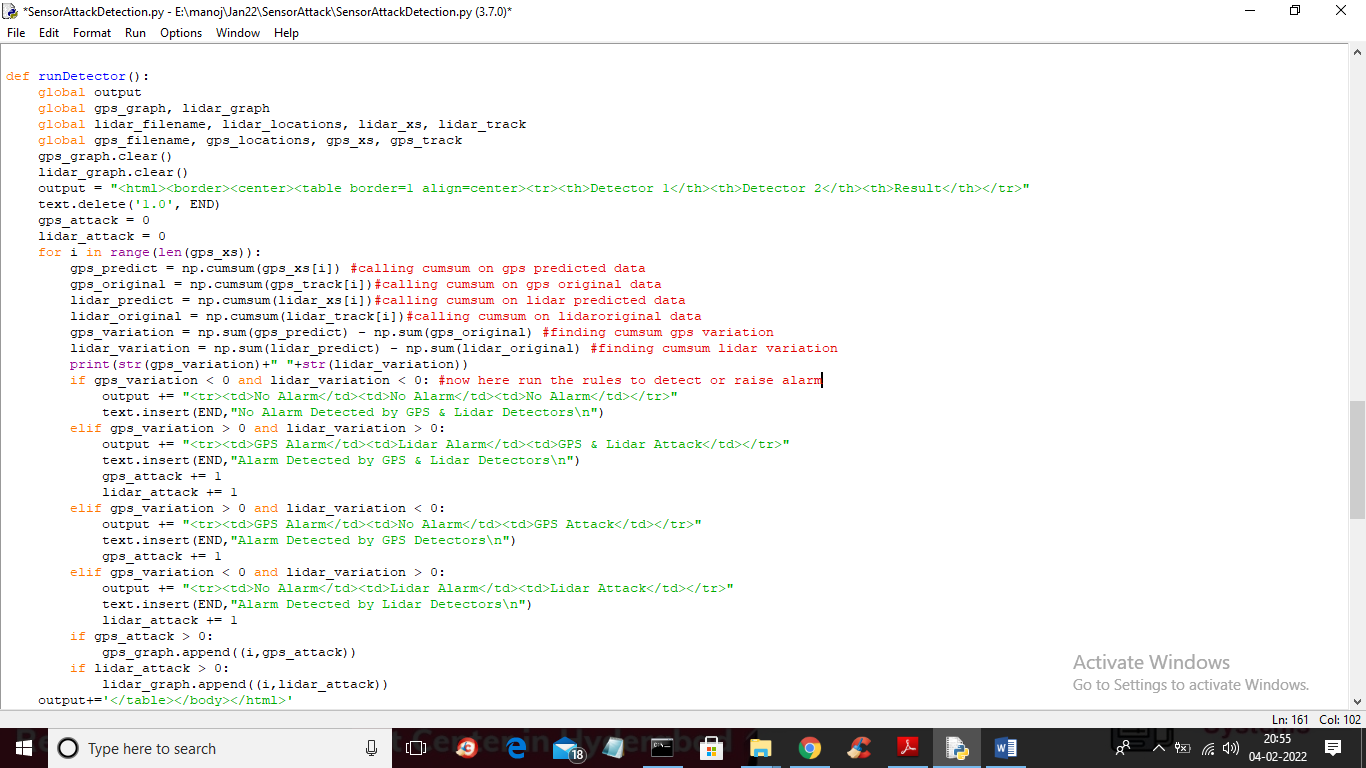
In above screen we have GPS and LIDAR dataset and in lidar.csv file in selected blue colour text we can see it has received longitude value as -150 where most of records received -120 and this sudden jumped in values will be detected by EKF and CUSUM and report it as attack.

To implement this project we have designed following modules

1. Upload GPS Dataset: using this module we will upload GPS dataset to application
2. Upload LiDAR Dataset: using this module we will upload LiDAR dataset to application
3. Run GPS Extended Kalman Filter: using this module we will apply Kalman filter algorithm to predict vehicle locations by monitoring original vehicle locations of GPS data
4. Run LIDAR Extended Kalman Filter: using this module we will apply Kalman filter algorithm to predict vehicle locations by monitoring original vehicle locations of LIDAR data
5. Run Rule Based CUSUM Detector: this module will apply CUSUM on both EKF data to find variations and if huge variations detected then attack alarm will be raised
6. Attack Detection Graph: using this module we will plot total attacks detected by LIDAR and GPS

In below screen you can see code for Kalman filter and CUSUM

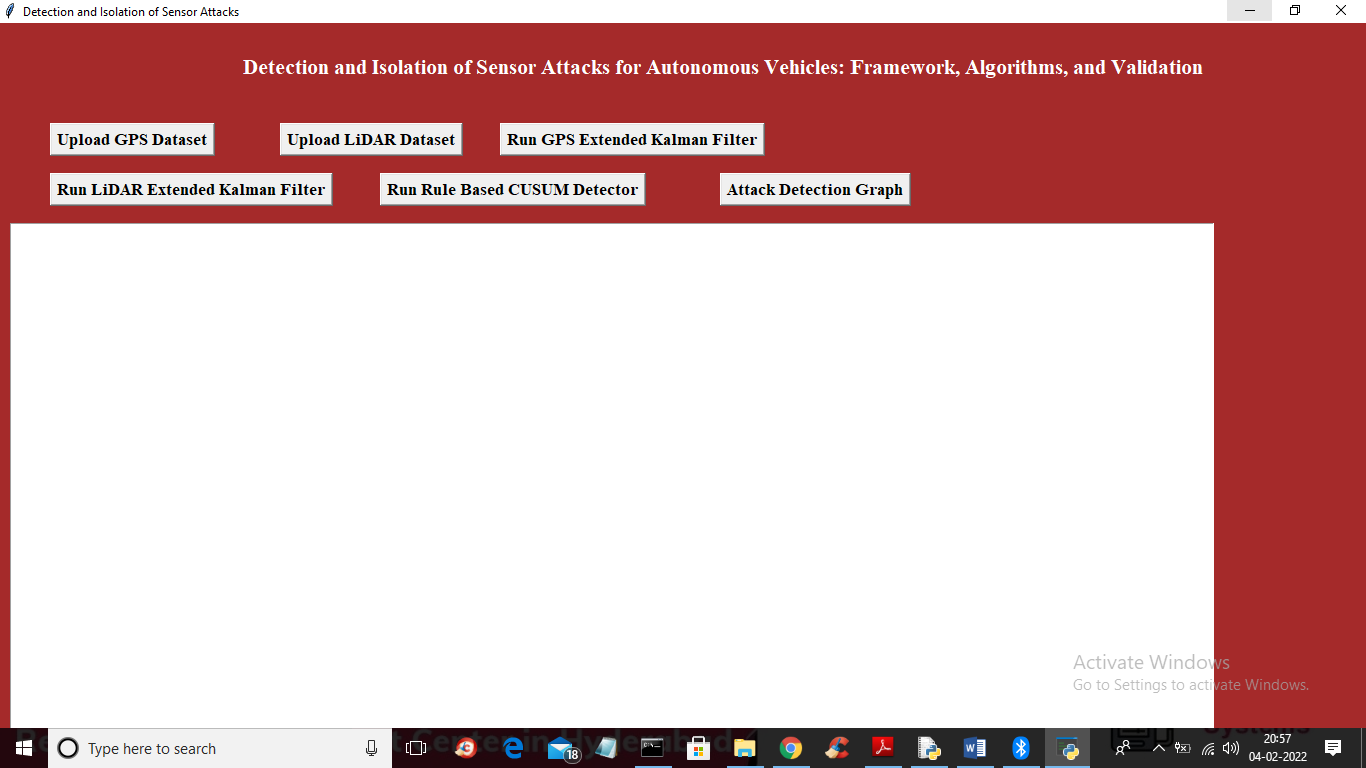




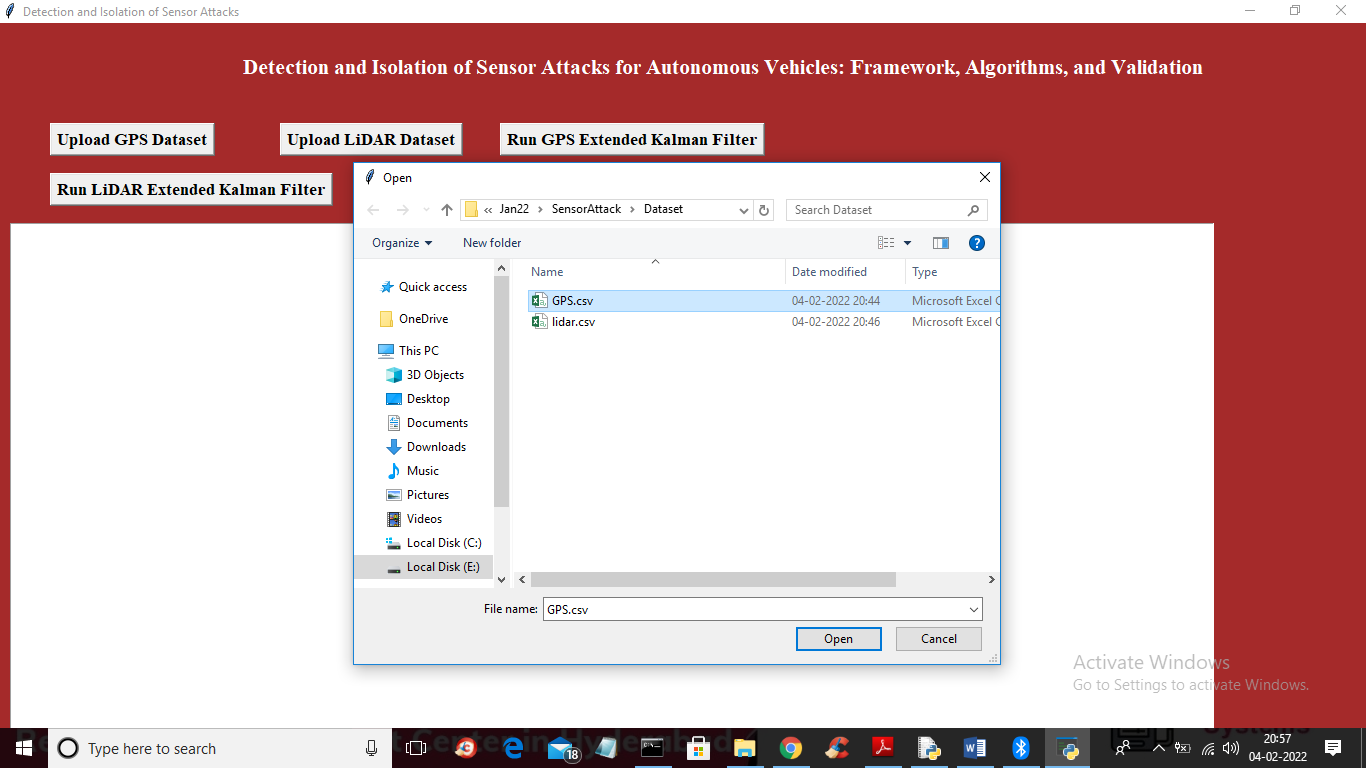
In above 2 screen read red colour comments to know about algorithms

SCREEN SHOTS

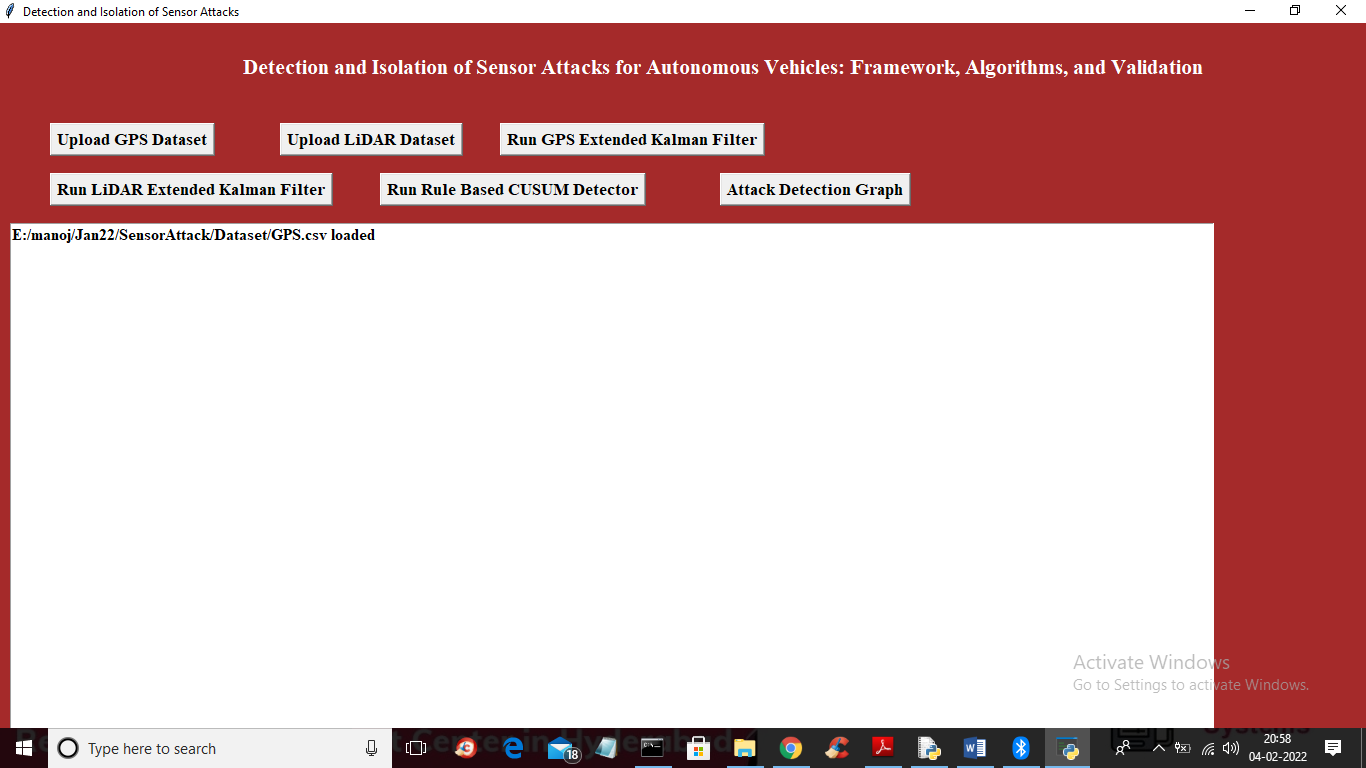
To run project double click on ‘run.bat’ file to get below screen



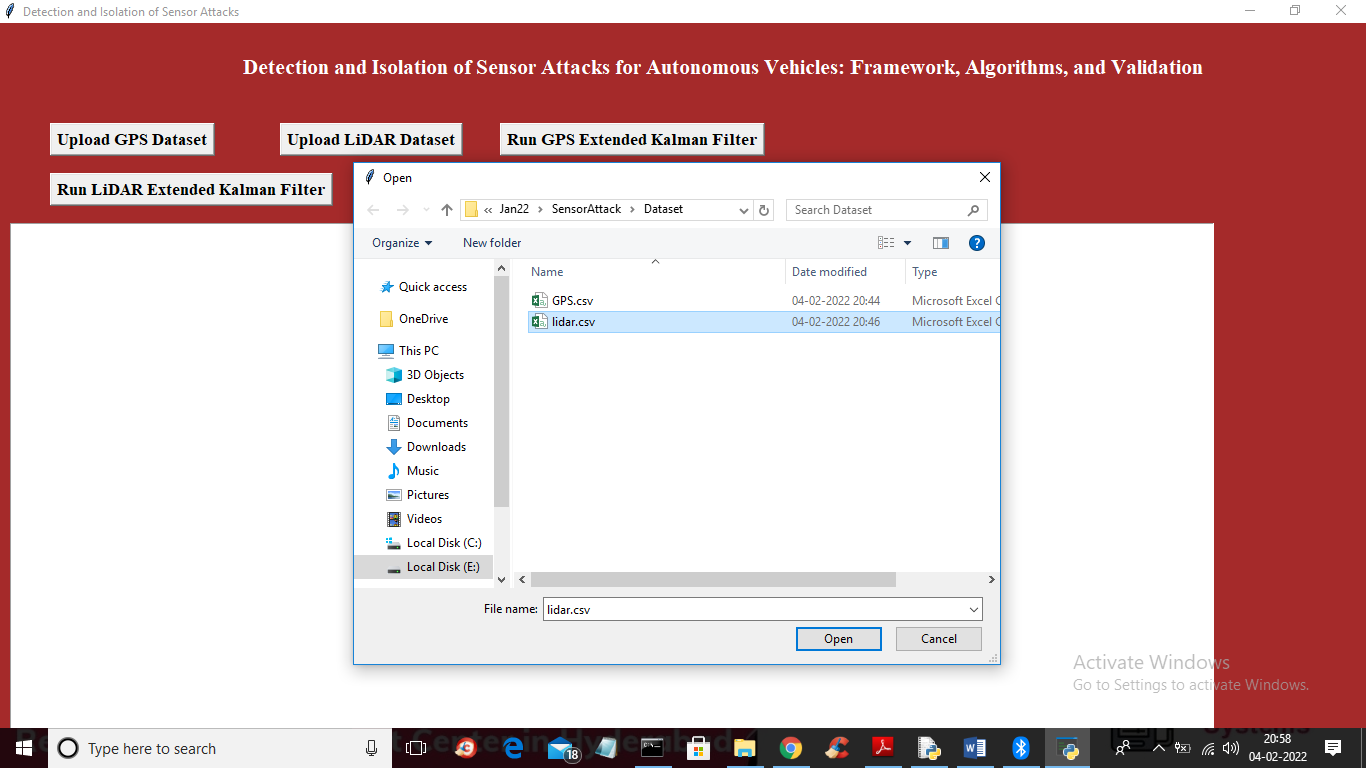
In above screen click on ‘Upload GPS Dataset’ button to upload GPS dataset and to get below screen



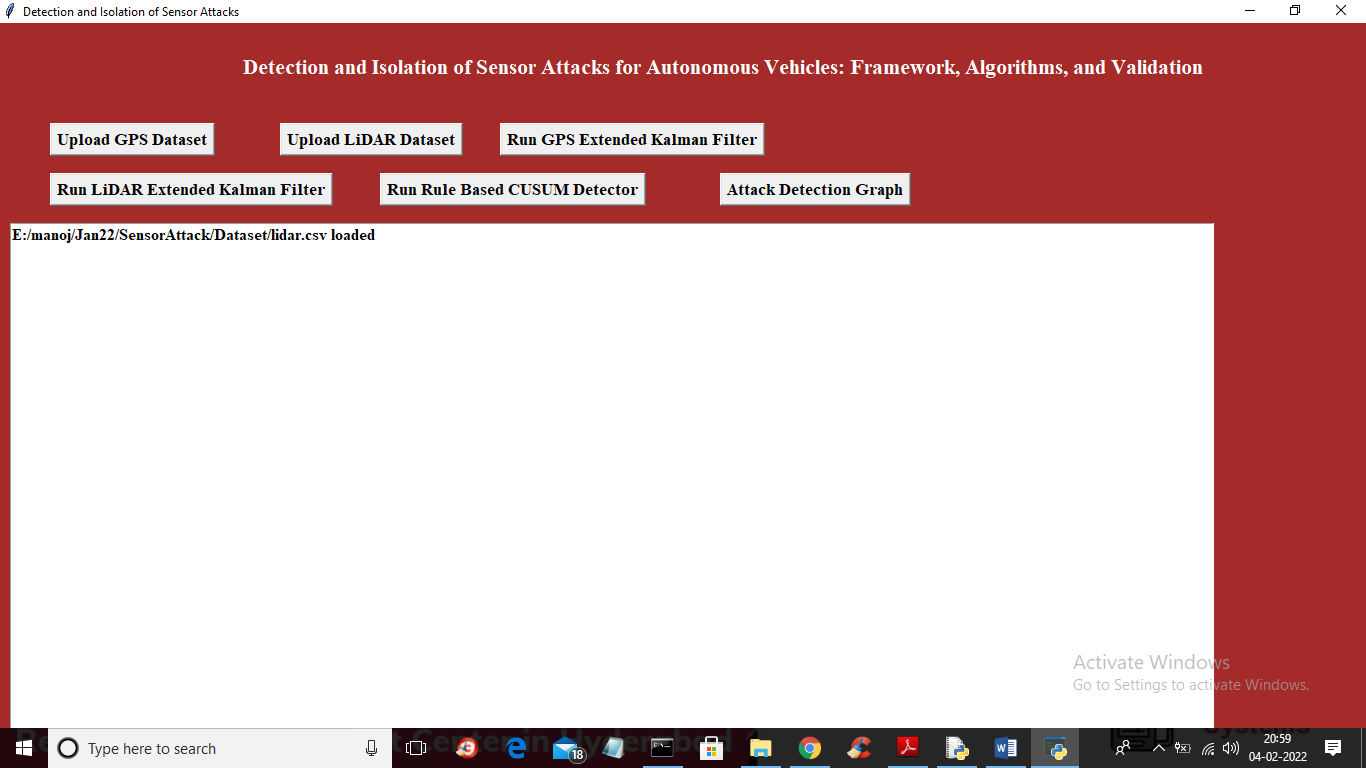
In above screen selecting and uploading GPS dataset and then click on ‘Open’ button to load dataset and to get below screen



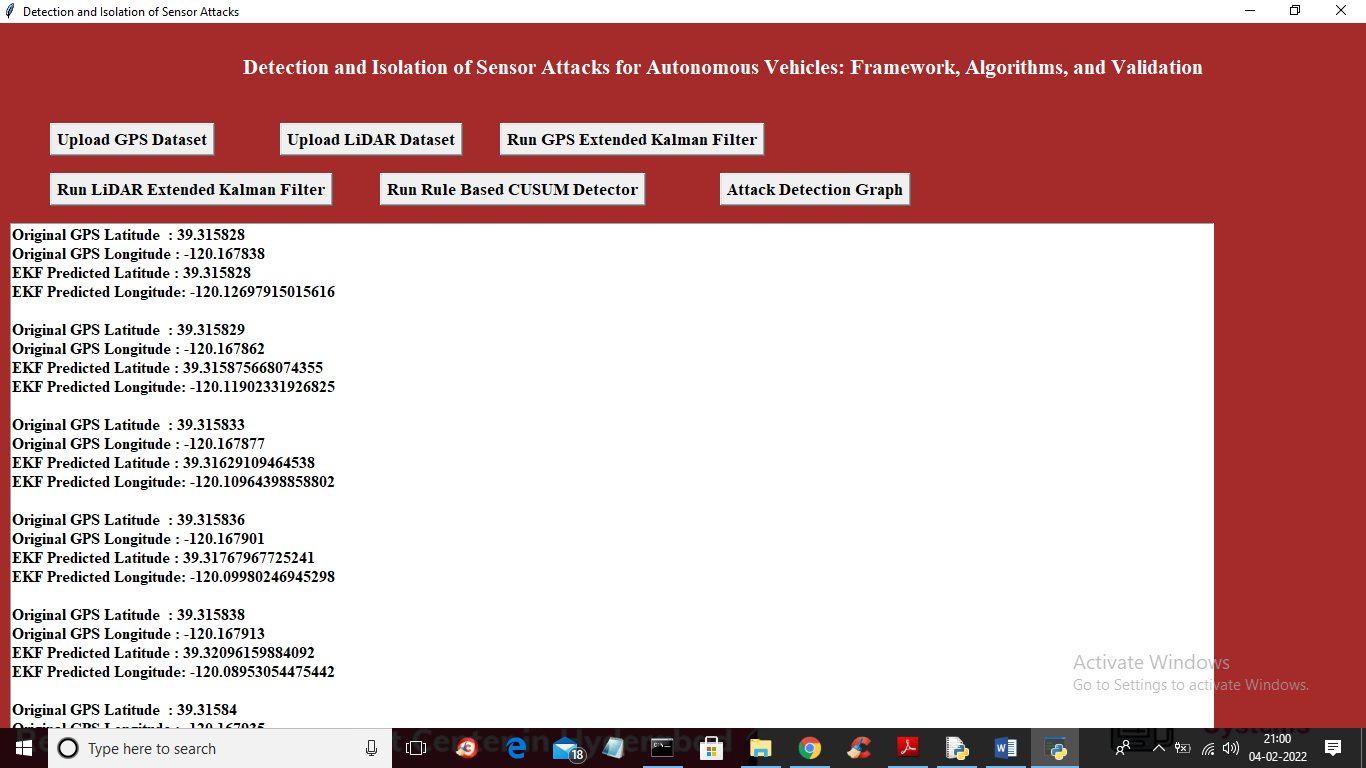
In above screen GPS dataset loaded and now click on ‘Upload LIDAR Dataset’ button to upload LIDAR dataset and to get below screen



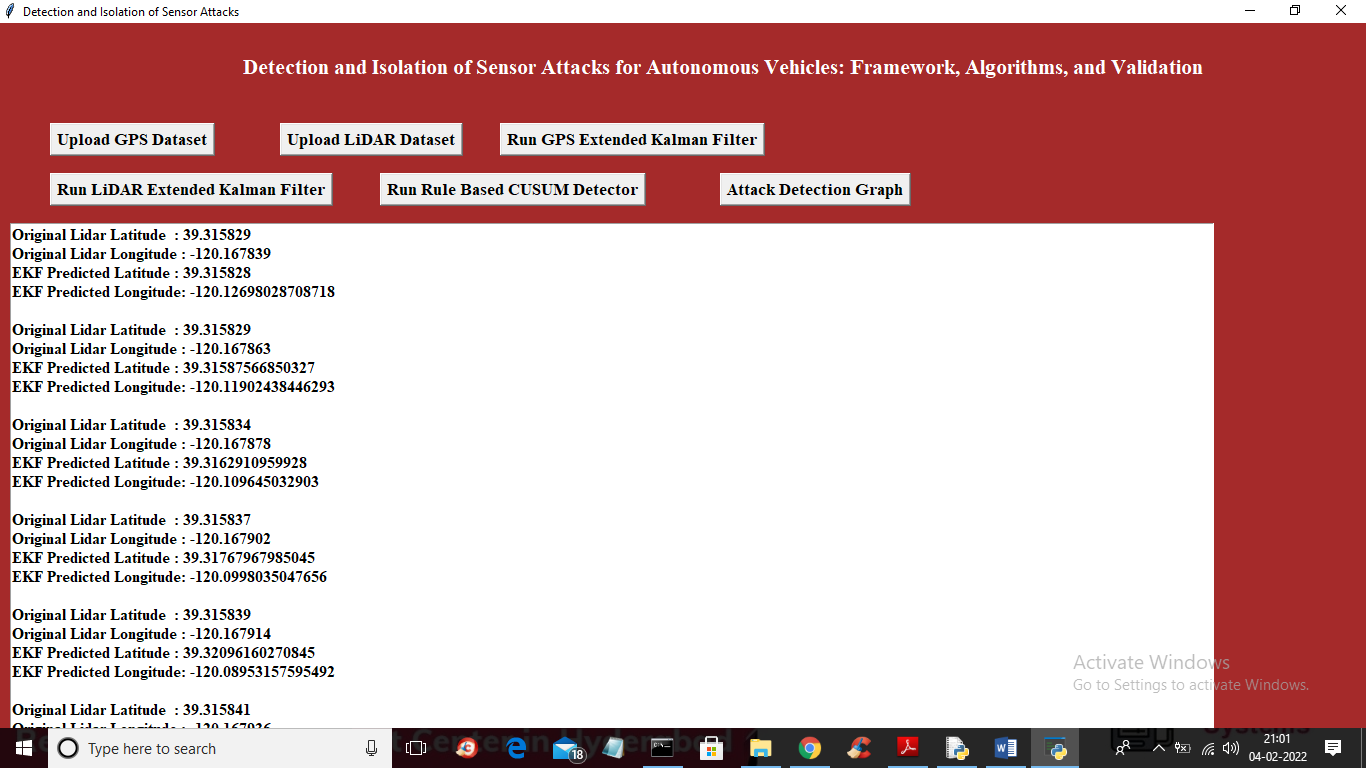
In above screen selecting and uploading ‘lidar.csv’ file and then click on ‘Open’ button to load dataset and to get below screen



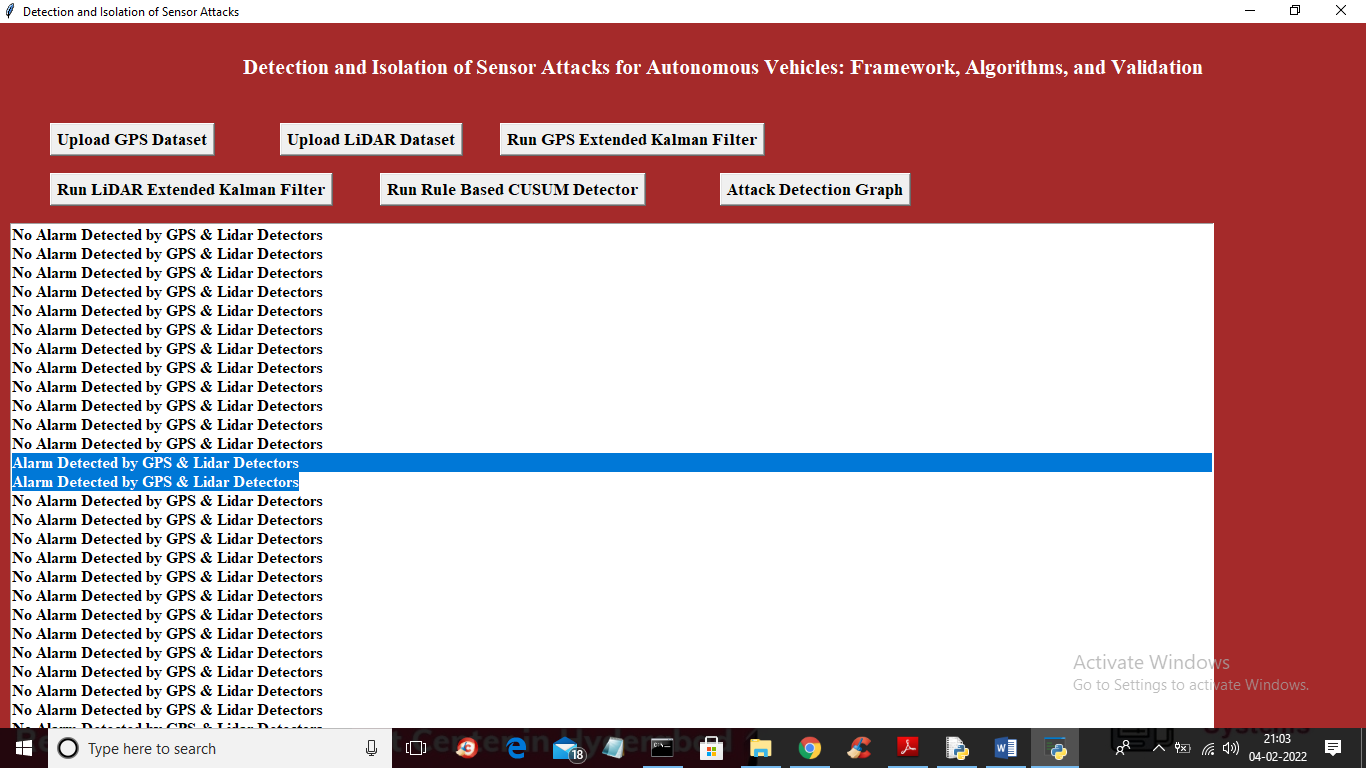
In above screen lidar dataset loaded and now click on ‘Run GPS Extended Kalman Filter’ button to run EKF on GPS data and to get below output



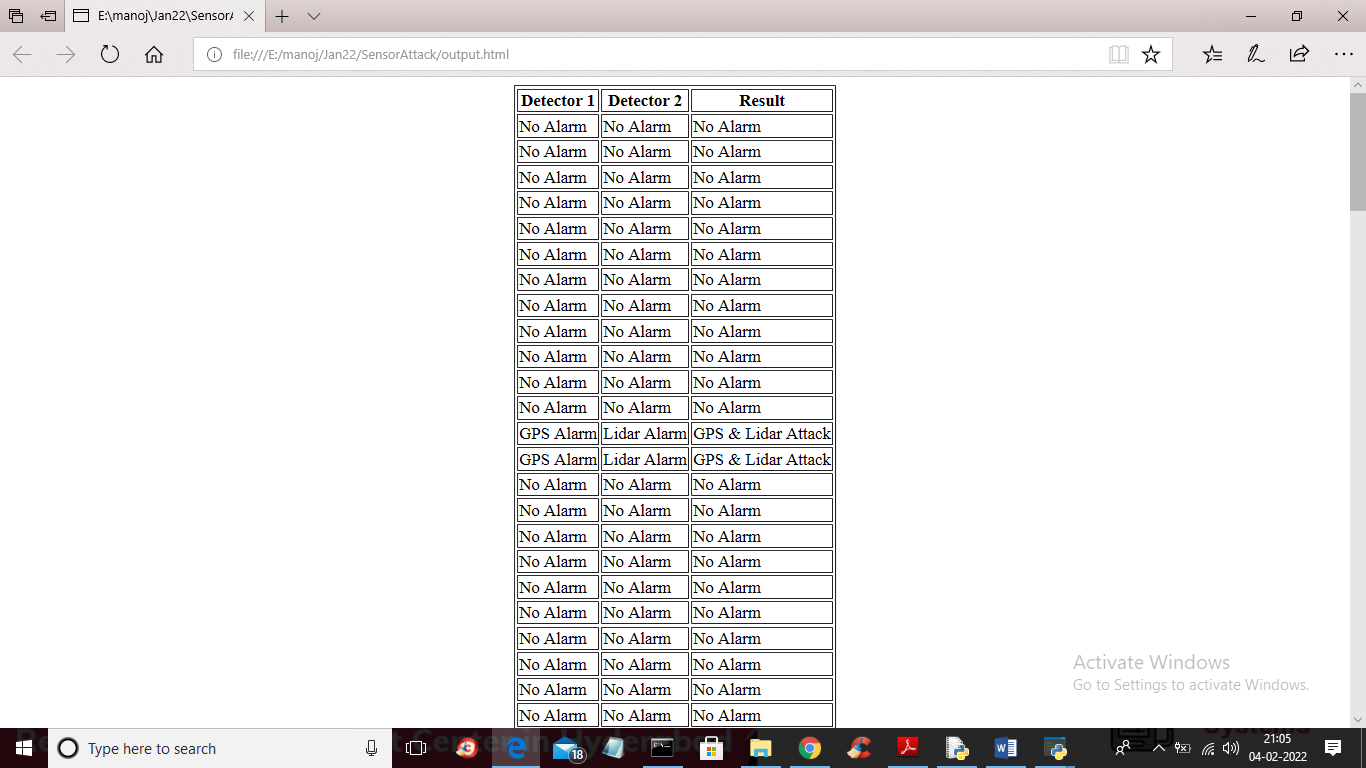
In above screen for each original GPS location EKF has predicted next location and you can scroll down above screen to view all values and now click on ‘Run LIDAR Extended Kalman Filter’ button to apply EKF on LIDAR dataset and get below output



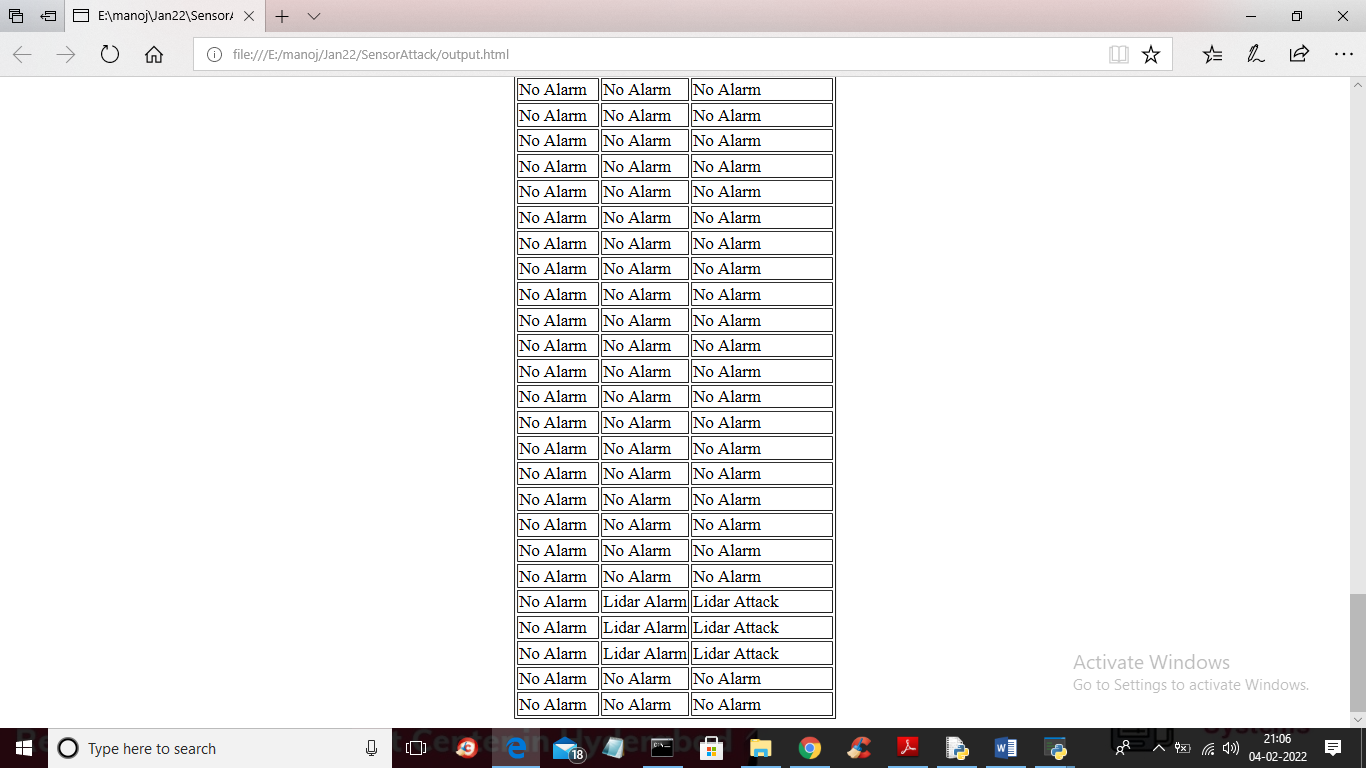
In above screen for each LIDAR original latitude and longitude EKF has predicted location and we can see there is narrow difference between original and predicted values. Now click on ‘Run Rule Based CUSUM Detector’ button to find variations between original and predicted values and then run RULES to raise attack alarm



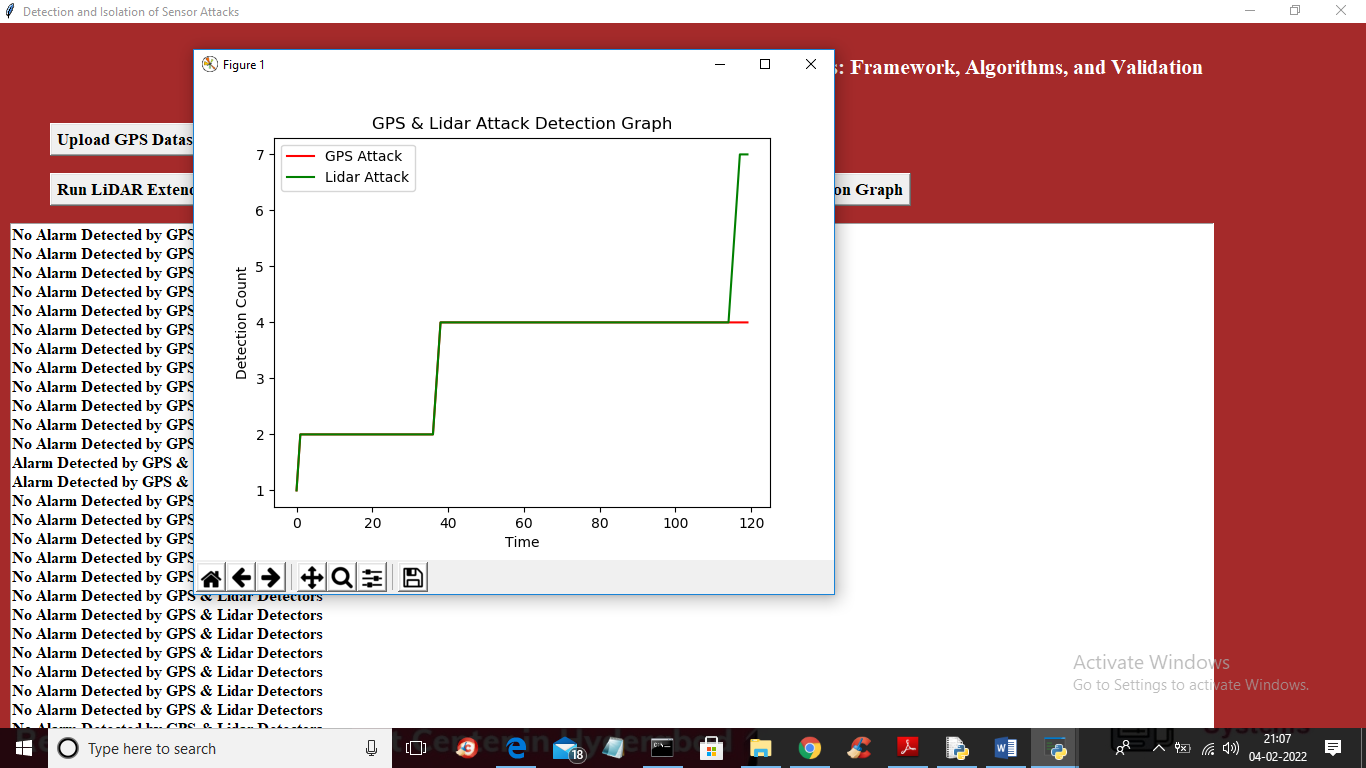
In above screen for each latitude and longitude CUSUM has applied rules to detect attack and in above screen in blue colour text we can see GPS and LIDAR attack detected and in other records NO ALARM DETECTED. You can scroll down above screen to view all detections. Now click on ‘Attack Detection Graph’ button to get below output



In above screen we developed code for 2 detectors and we can see alarm and no alarm for both detectors and below is the other records output



In above screen last lines we can see only LIDAR attack detected and below is the detection graph for both detectors



In above graph x-axis represents TIME and y-axis represents attack detection count and red line represents GPS attack and green line represents Lidar attack and in above graph we can see GPS (detector 1) detected total 4 attacks from 0 to 120 records and lidar (detector 2) detected 7 attacks