Cyber Attack Prediction: From Traditional Machine Learning to Generative Artificial Intelligence

Cyber-attacks are intended to perform malicious activities such as corrupting user files, stealing data, hacking and many more on victim system. Traditional algorithms unable to detect all types of attacks developed by attackers at different times. To enhance detection accuracy author of this paper giving huge survey on different ML, DL, NLP, Explainable AI and Generative AI algorithms and to main purpose is to identify algorithm who can detect all types of cyber-attack with highest accuracy.

In propose paper author has experimented with many algorithms such as SVM, Random Forest, KNN, XGBOOST, CNN, DNN and many more and each algorithm got trained on many cyber-attack datasets such as NSL-KDD, KDDCUP, UNSW15, CICIDS 2017, CICDDOS 2019, XIOTT and many more. Each algorithm performance is evaluated in terms of accuracy. All algorithms able to detect attacks between an accuracy of 90 to 99% and this experimentation will help researchers in choosing algorithms with highest accuracy.

Propose paper presents state-of-the-art benchmark cyber-attack datasets, ML and DL, and techniques for various cyber-attack predictions. In the domain of cyber-security, transparency, and explainability are essential for combating cyber threats and effectively analysing security decisions. Hence, this study provides a thorough overview of cutting-edge research on XAI for Cybersecurity applications. Propose paper describe the fundamental principles and taxonomies of state-of-the-art XAI models, along with indispensable tools, such as a comprehensive framework and accessible datasets. Propose work will be a valuable resource for researchers, developers, and security professionals seeking to leverage ML, DL, XAI, and GenAI models to address complex challenges within Cybersecurity domains.

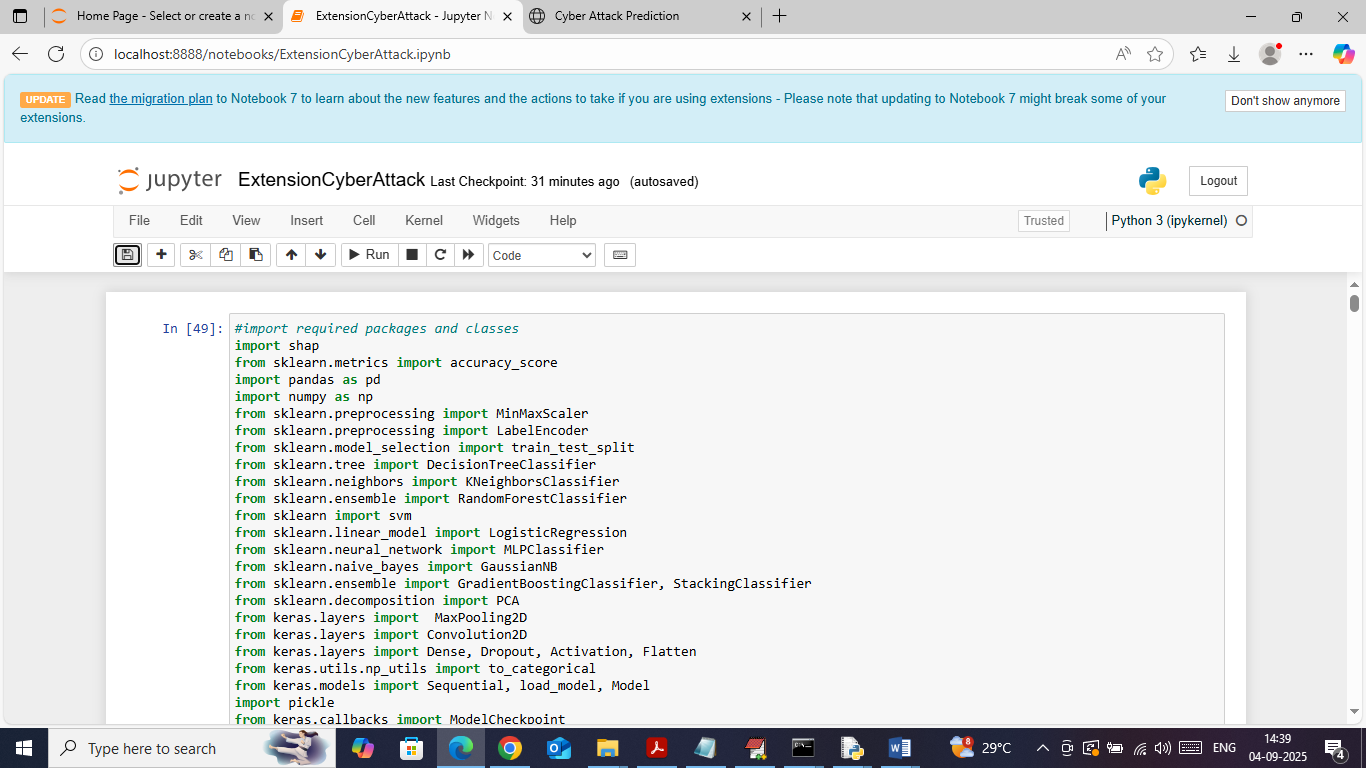
Note: for explanation we have used SHAP tool and as Generated AI author has used CHATGPT tool which is not free of cost so we have not implemented this algorithm. Training all datasets with all algorithms may take hours of time so we have implemented important algorithms with different datasets such as NSL KDD, CIC2017, CIC2019 and XIIOT dataset. All 4 datasets trained with different ML and DL algorithms such as DNN, MLP, KNN, SVM, Naïve Bayes, Logistic Regression, and Random Forest.

Extension Concept

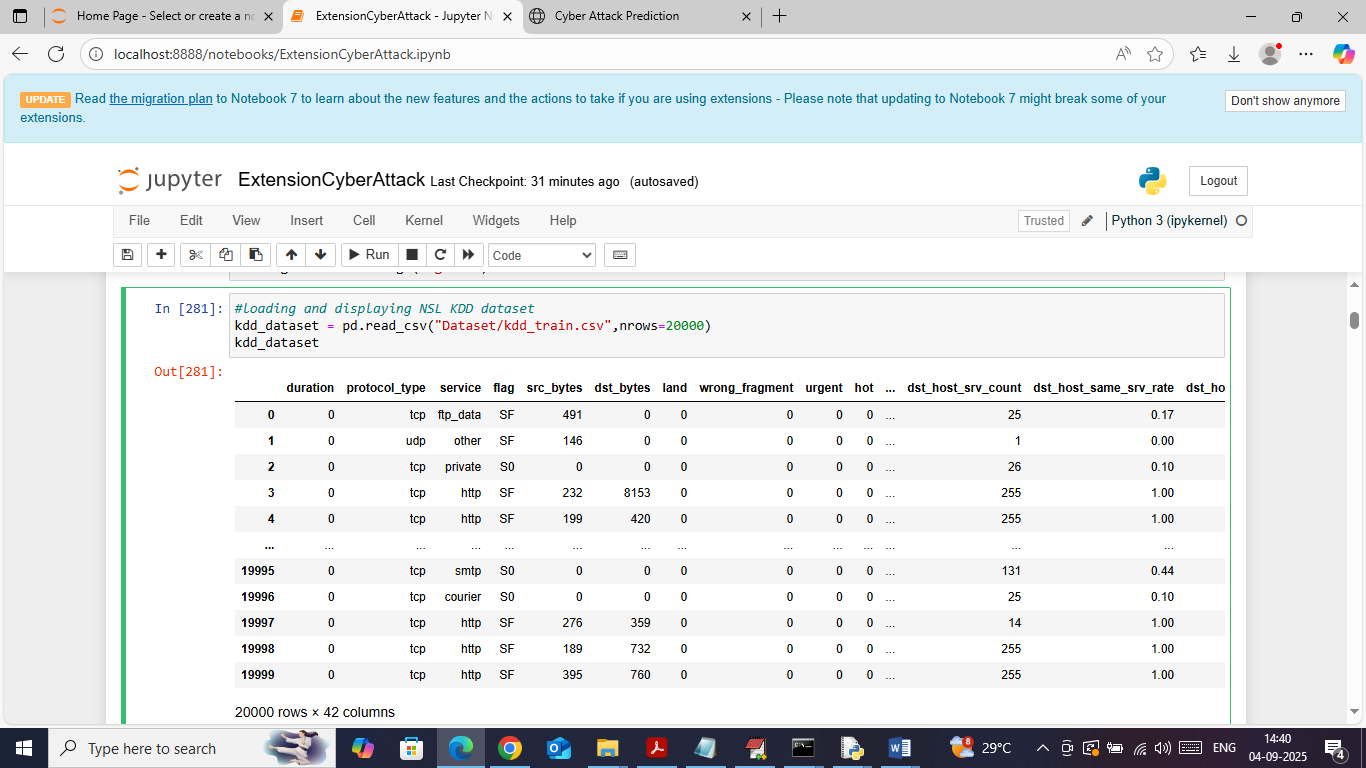
In paper author has mentioned in future work he will be implemented advance algorithms like Hybrid Model, Adversarial Learning and Multimodal Learning to further enhance cyber-attack prediction accuracy. So we have experimented with all the above models and found Hybrid model able to predict attacks from all four dataset with an accuracy between 99 to 100%. As hybrid model we have combined multiple base models like MLP, KNN and Random Forest using Stacked Classifier. Stacked classifier will trained all base models and then choose model with highest accuracy.

SCREEN SHOTS

We have coded this project using JUPYTER notebook and then used separate notebook for propose and extension work. In below screen showing model training, evaluation, dataset processing and visualization code and output with blue colour comments.



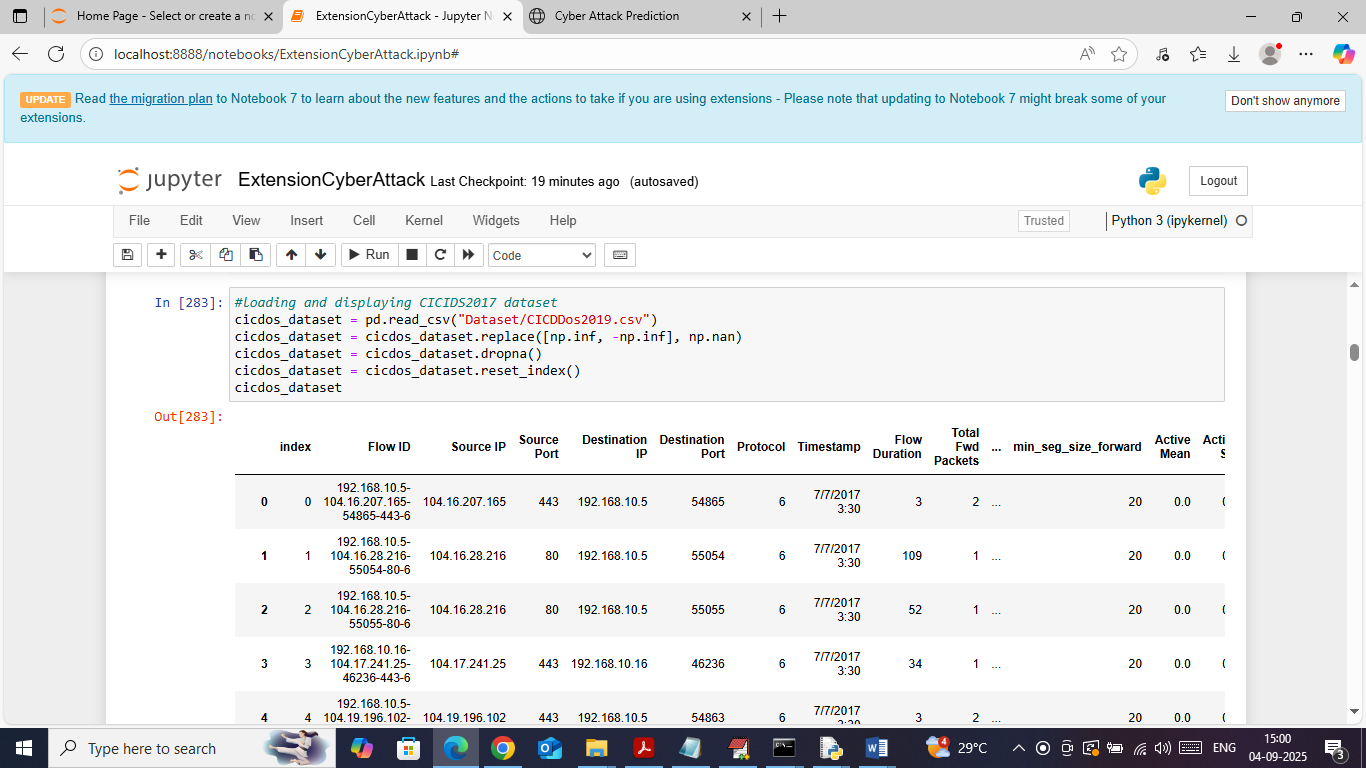
In above screen importing required python classes and packages



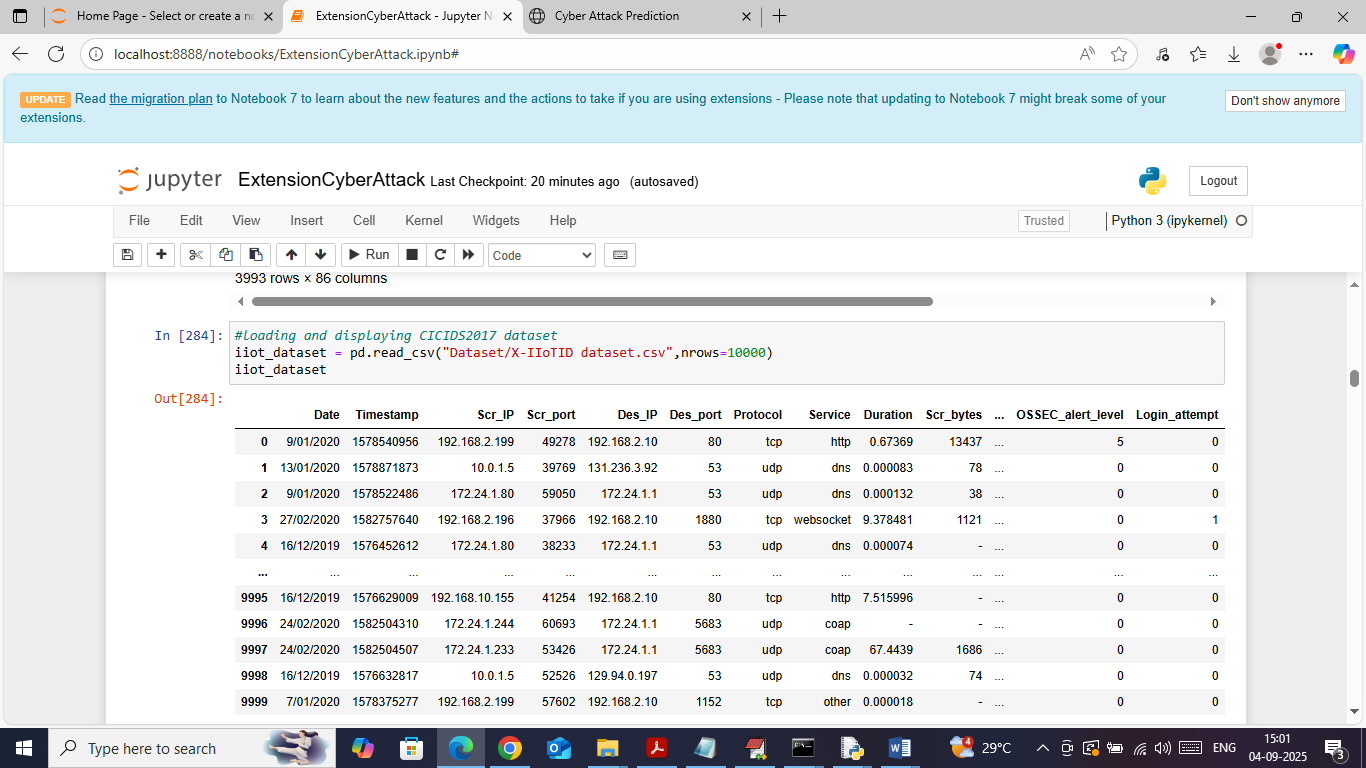
In above screen loading and displaying values of NSL KDD dataset



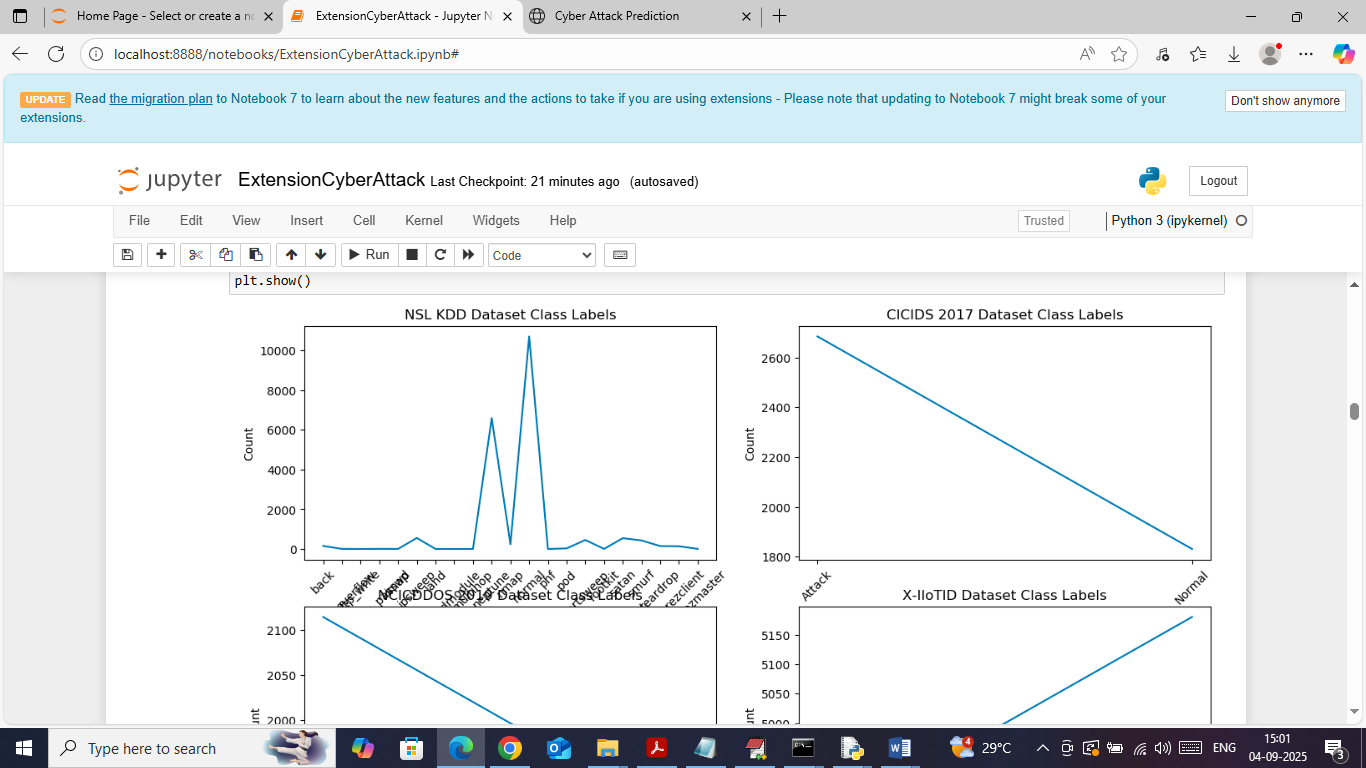
In above screen loading and displaying CICIDS2017 dataset values



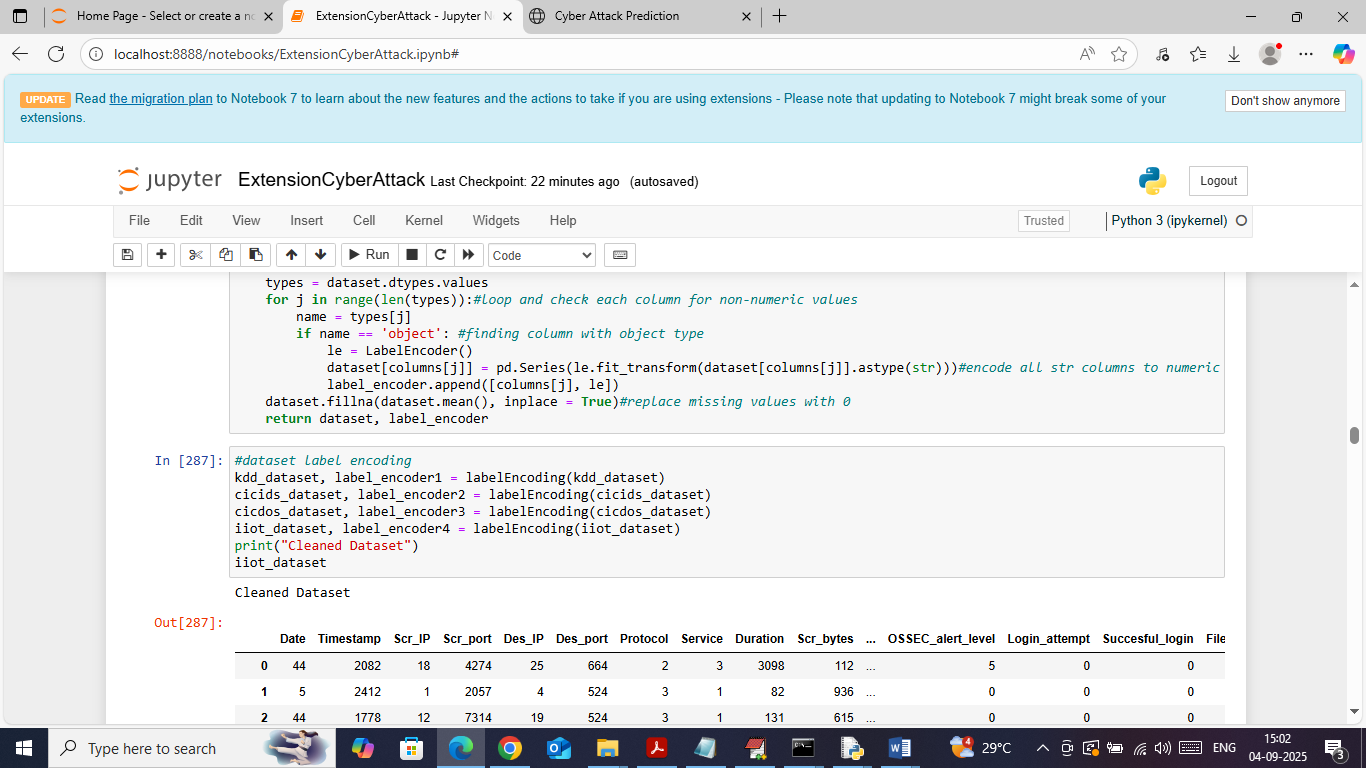
In above screen loading and displaying CICDDOS2019 dataset values



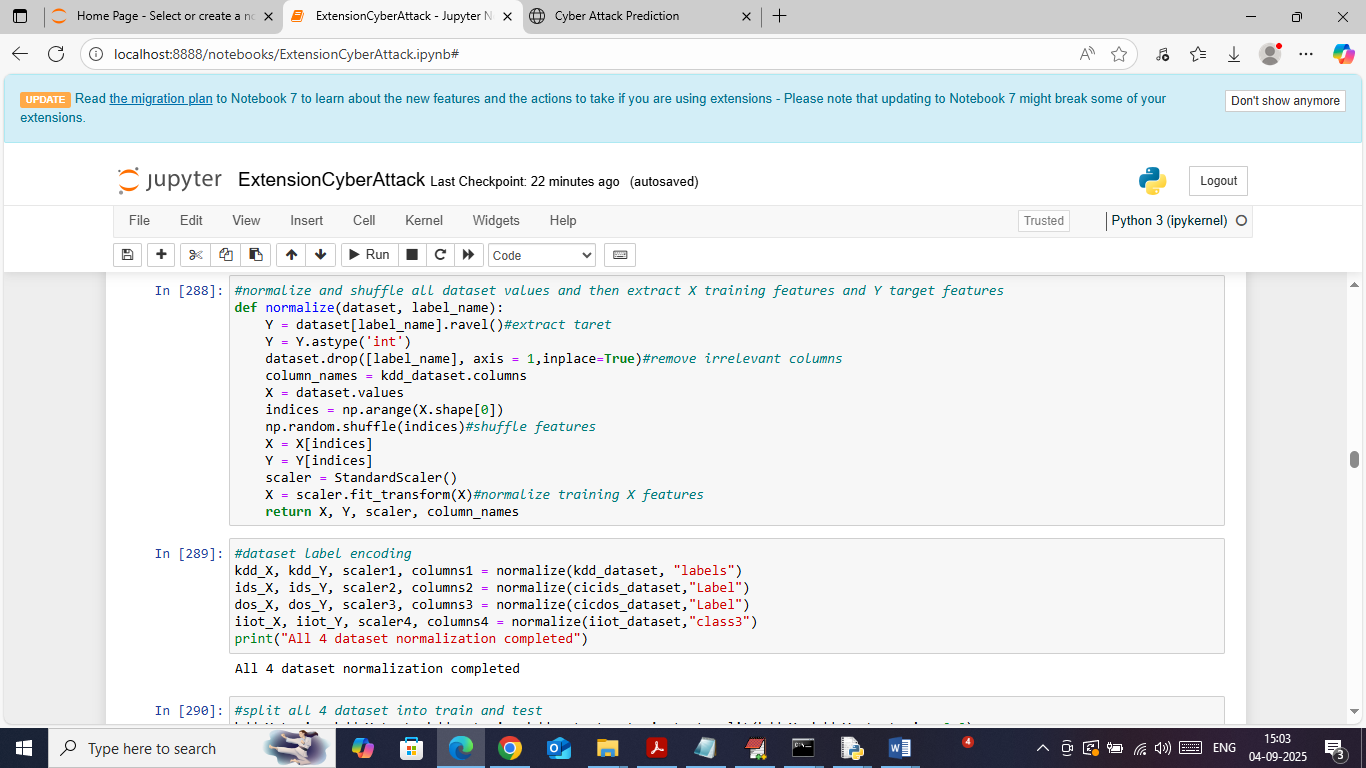
In above screen loading and displaying XIOTIOT dataset values



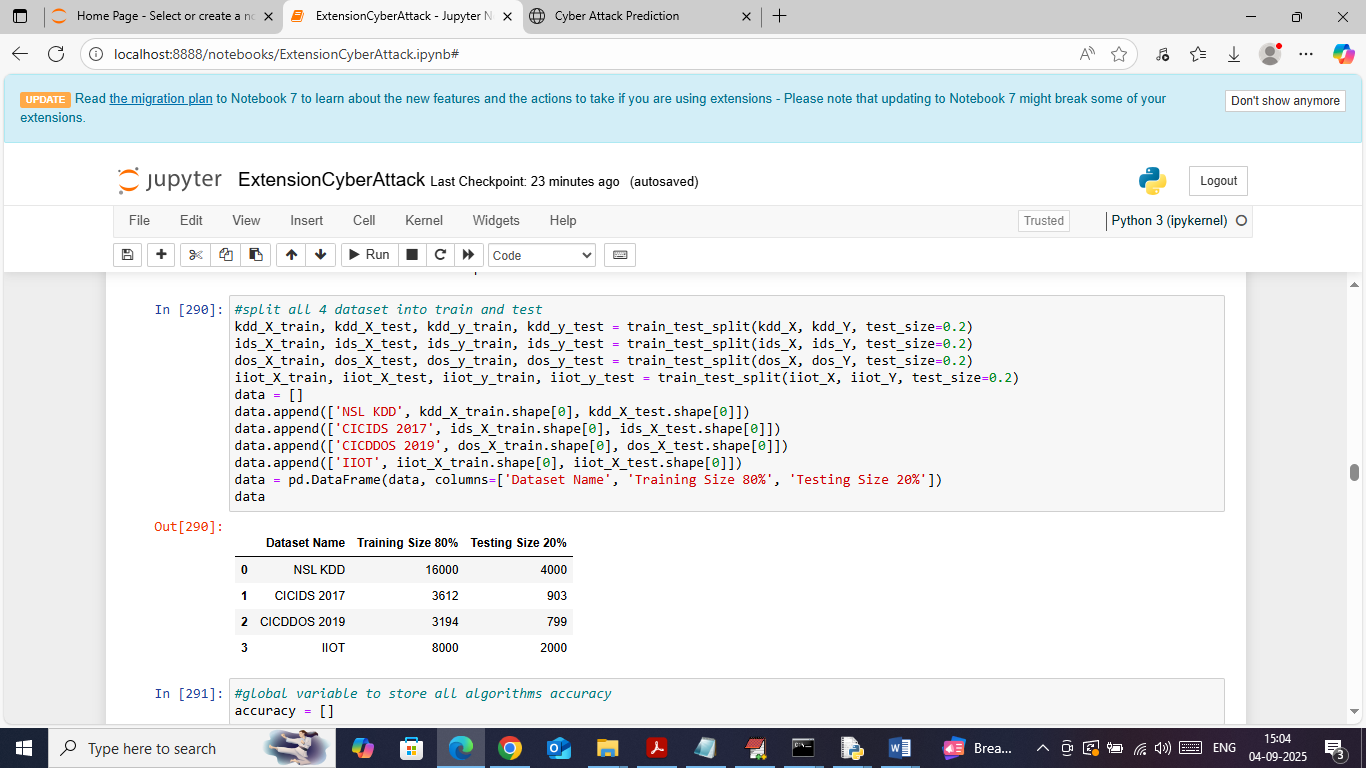
In above screen visualizing graph of different attacks found in dataset where x-axis represents attack names from each dataset and y-axis represents counts



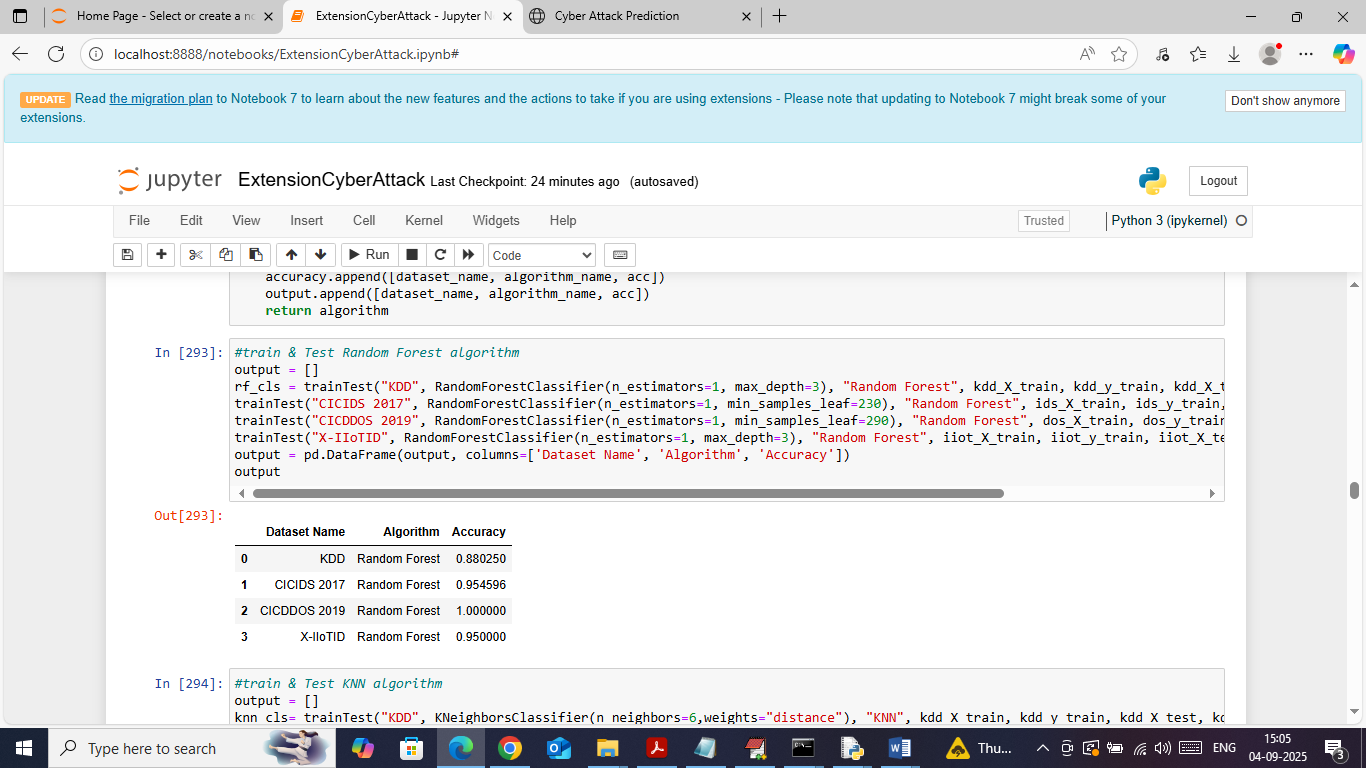
In above screen applying label encoding on 4 datasets to convert non-numeric data to numeric data and then displaying clean data values



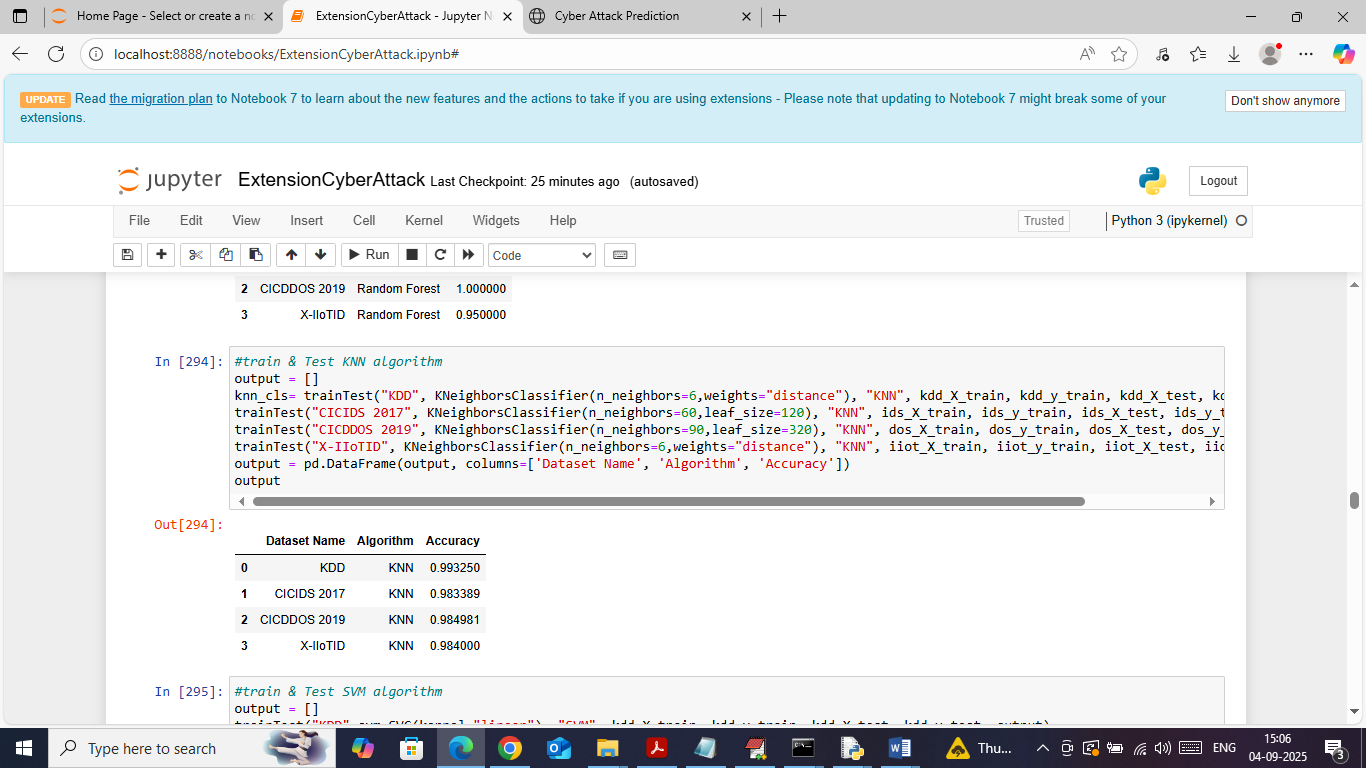
In above screen defining function to normalize and shuffle values from all dataset values



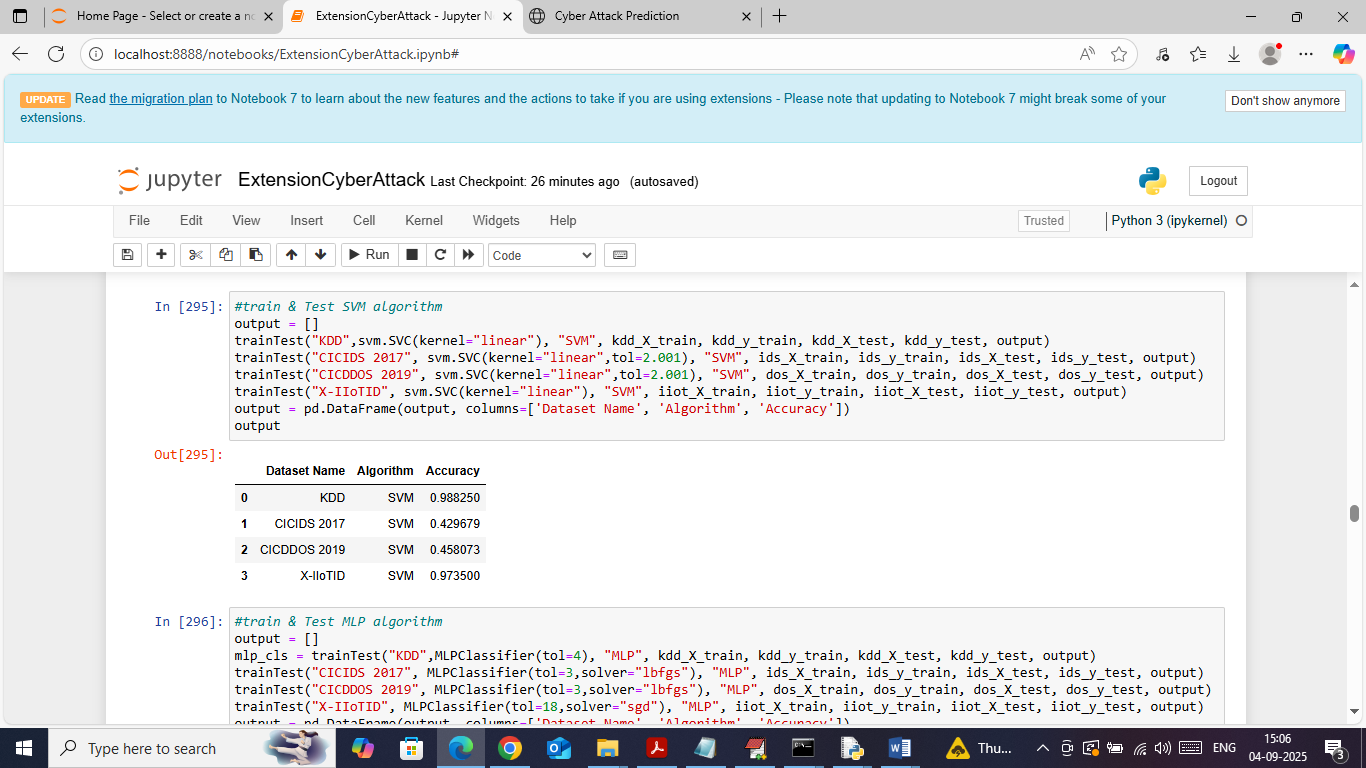
In above screen splitting all 4 datasets into train and test where application using 80% data for training and 20% for testing. In table format can see dataset names along with train and test size



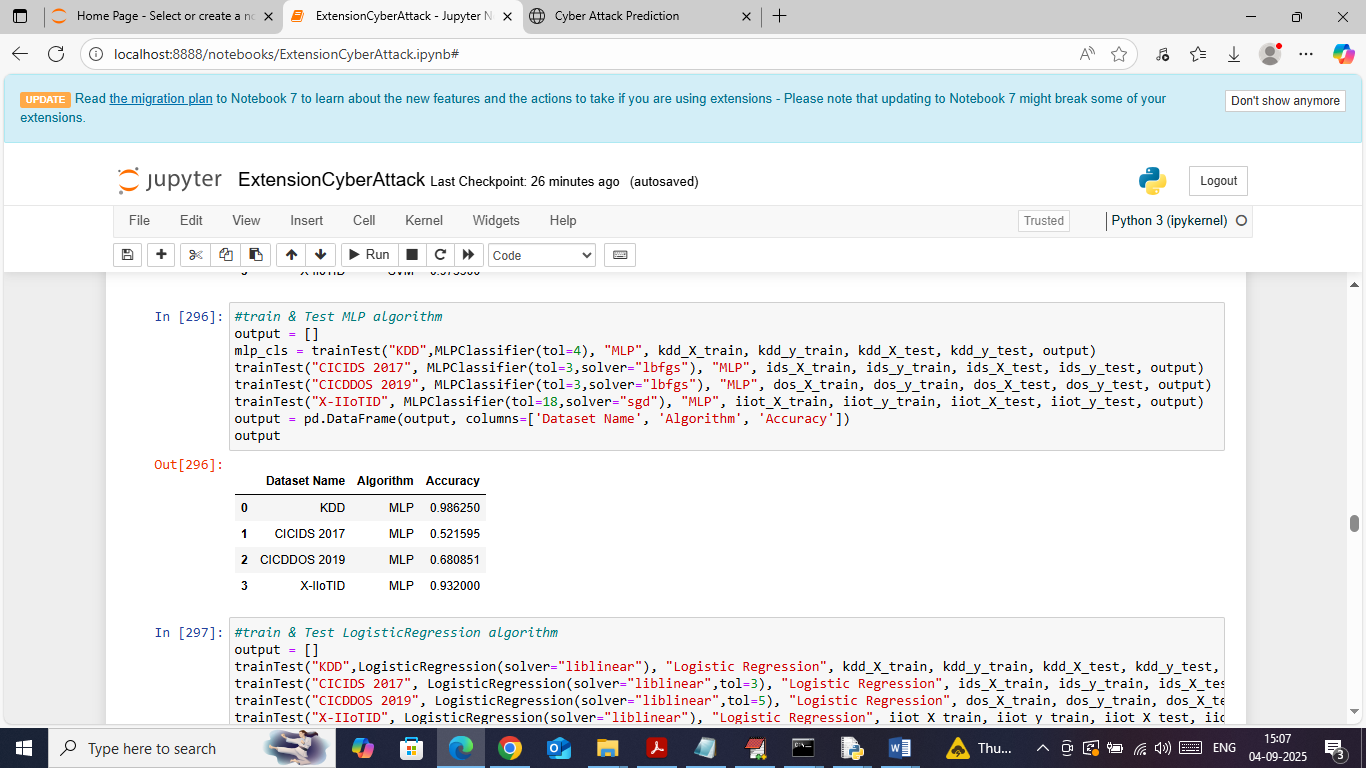
In above screen training Random Forest on all 4 datasets and then performing prediction on 20% test data and then in table format can see Random Forest accuracy on each dataset



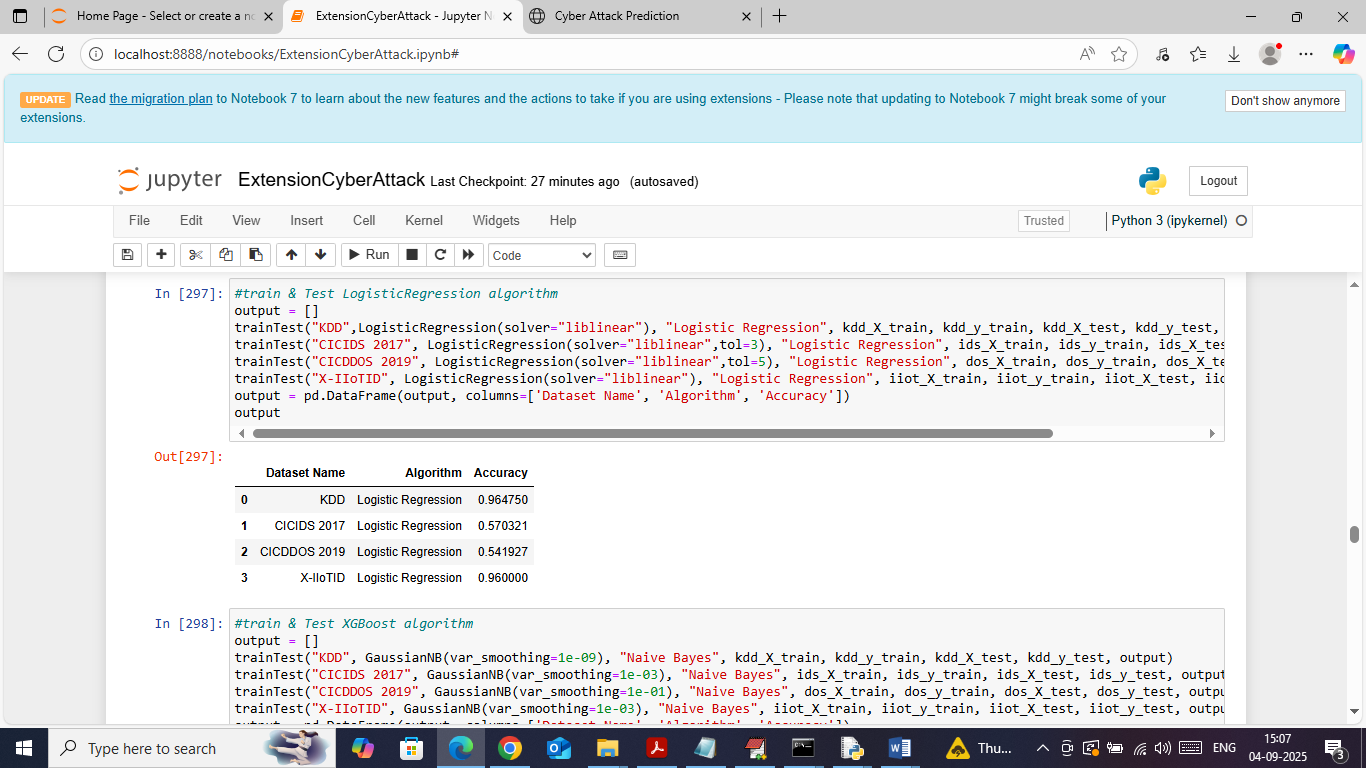
In above screen can see KNN accuracy on all 4 datasets



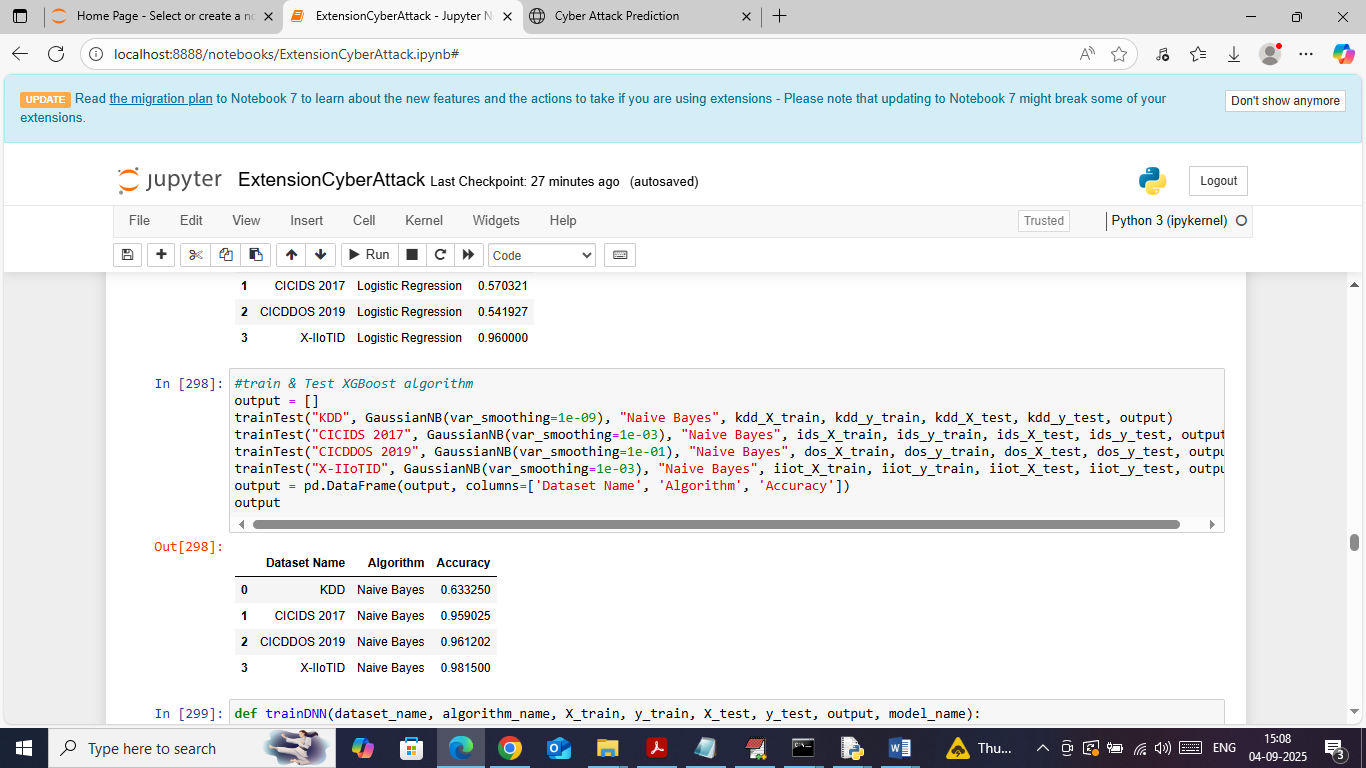
In above screen can see SVM performance on all 4 datasets



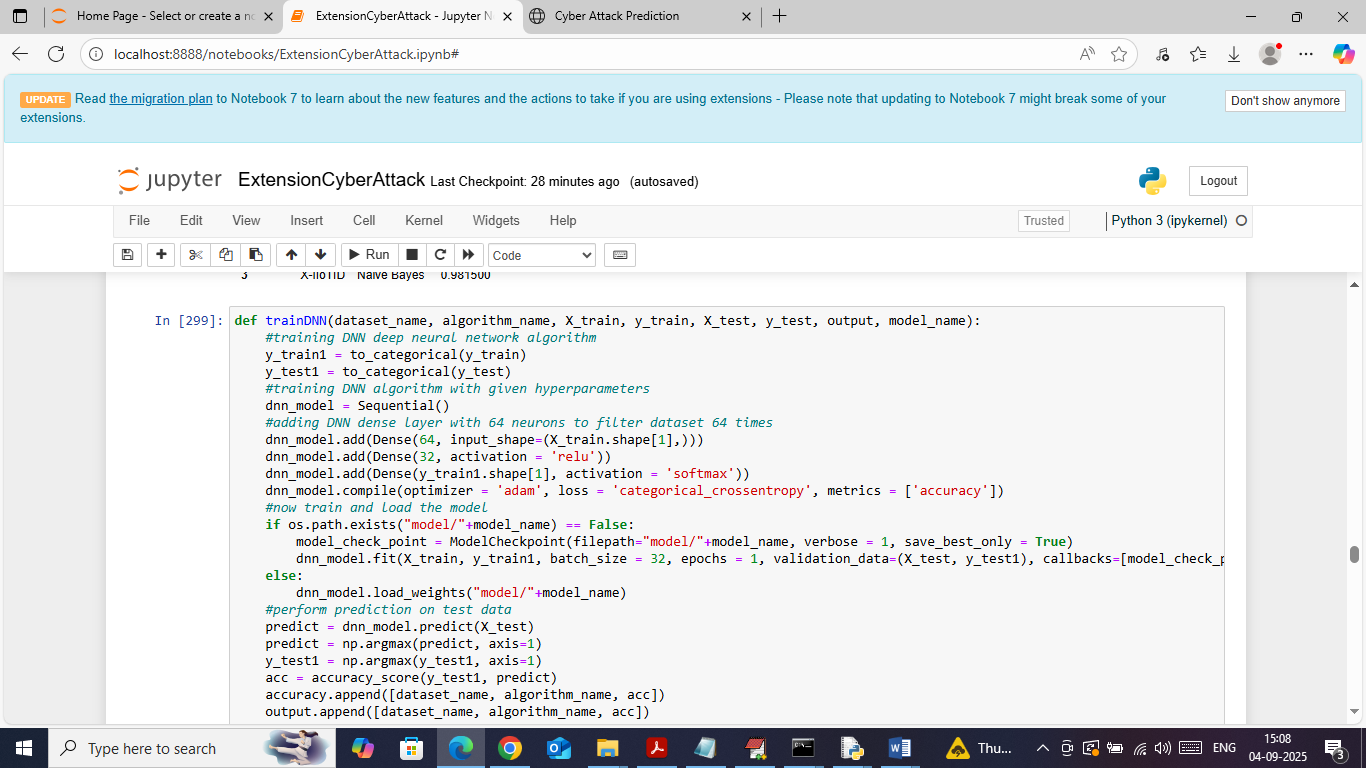
In above screen can see MLP performance on all 4 datasets



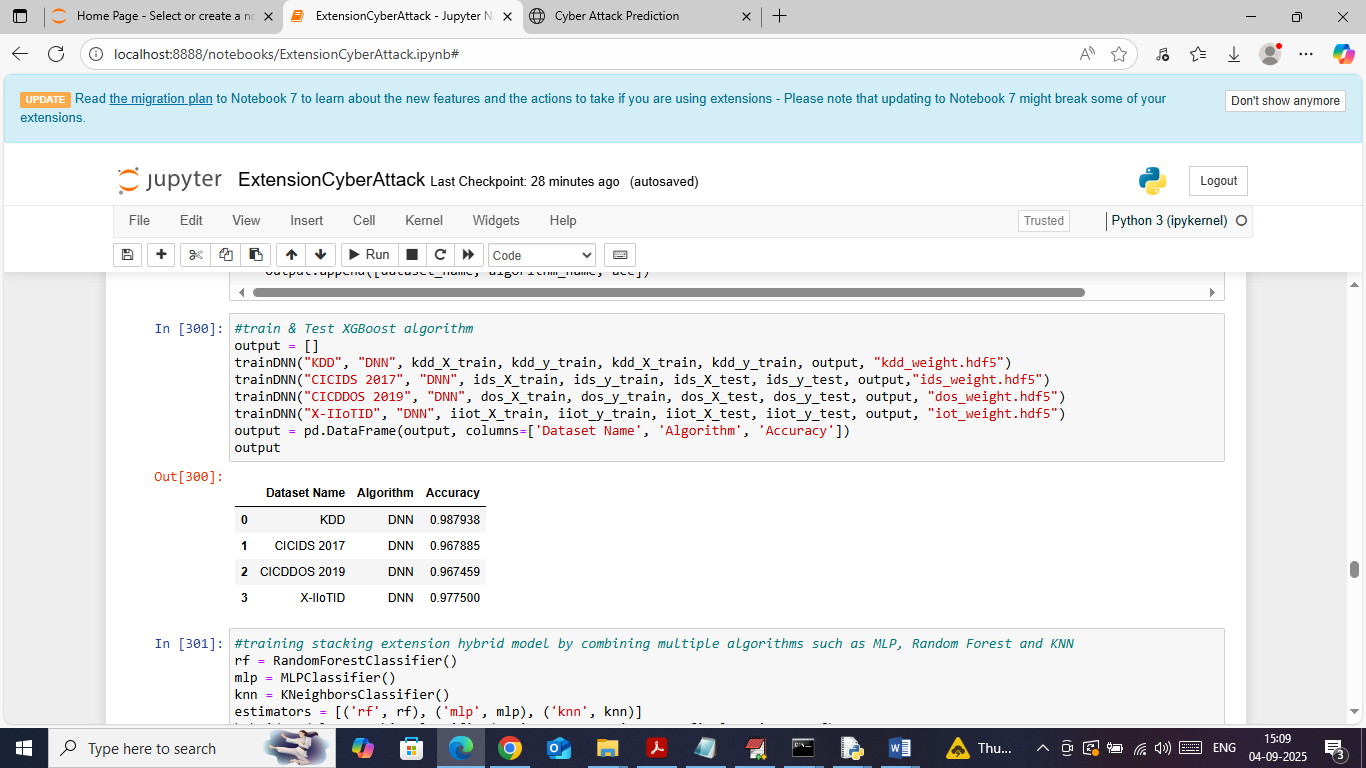
In above screen can see Logistic Regression performance on all 4 datasets



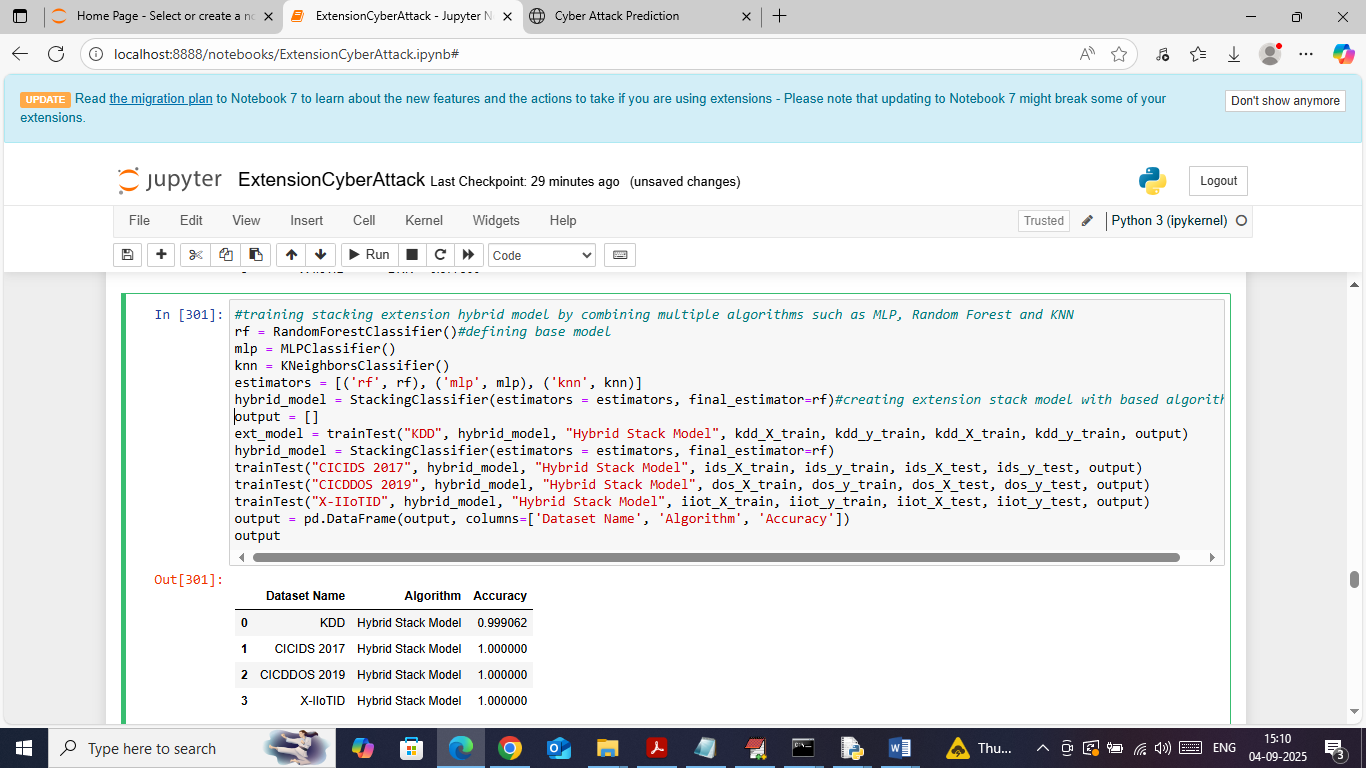
In above screen can see Naïve Bayes algorithm performance on all 4 datasets



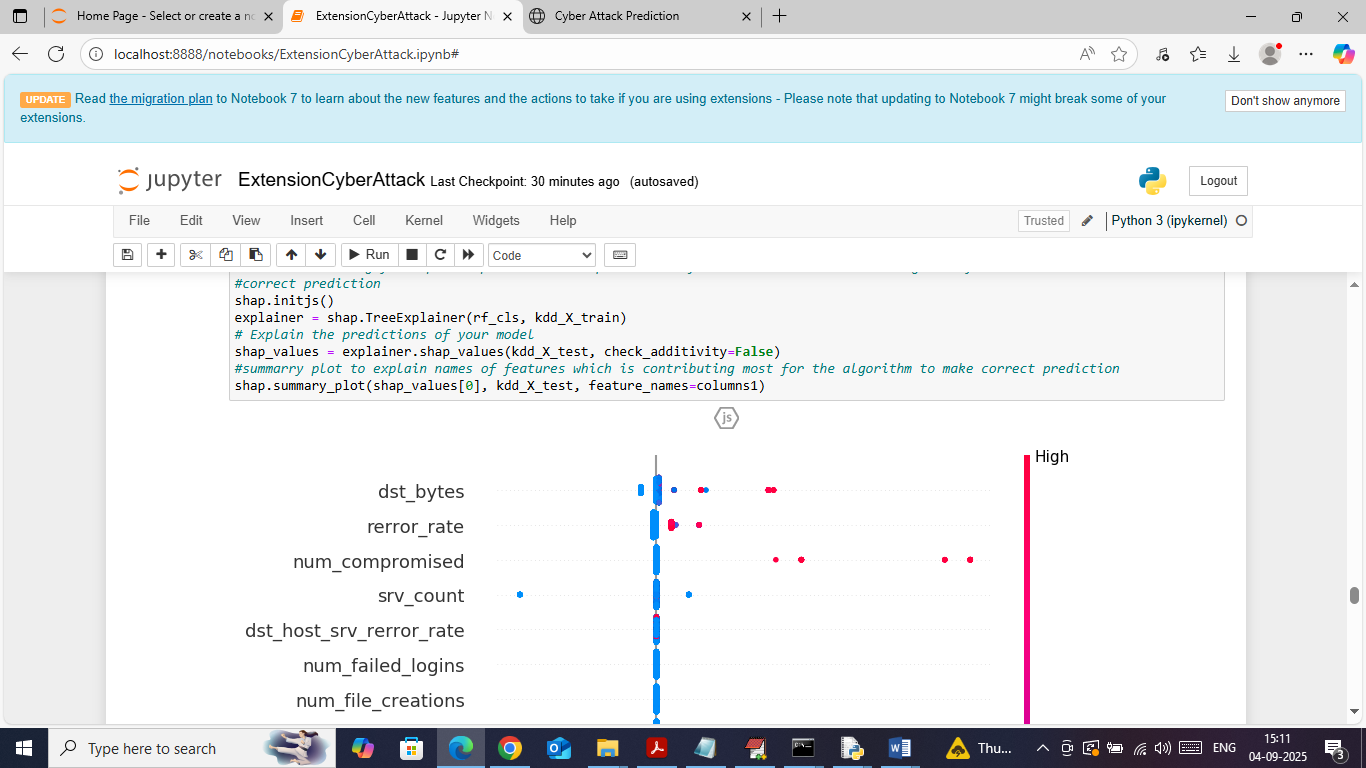
In above screen defining and training DNN algorithm on all 4 datasets and after executing above model will get below output



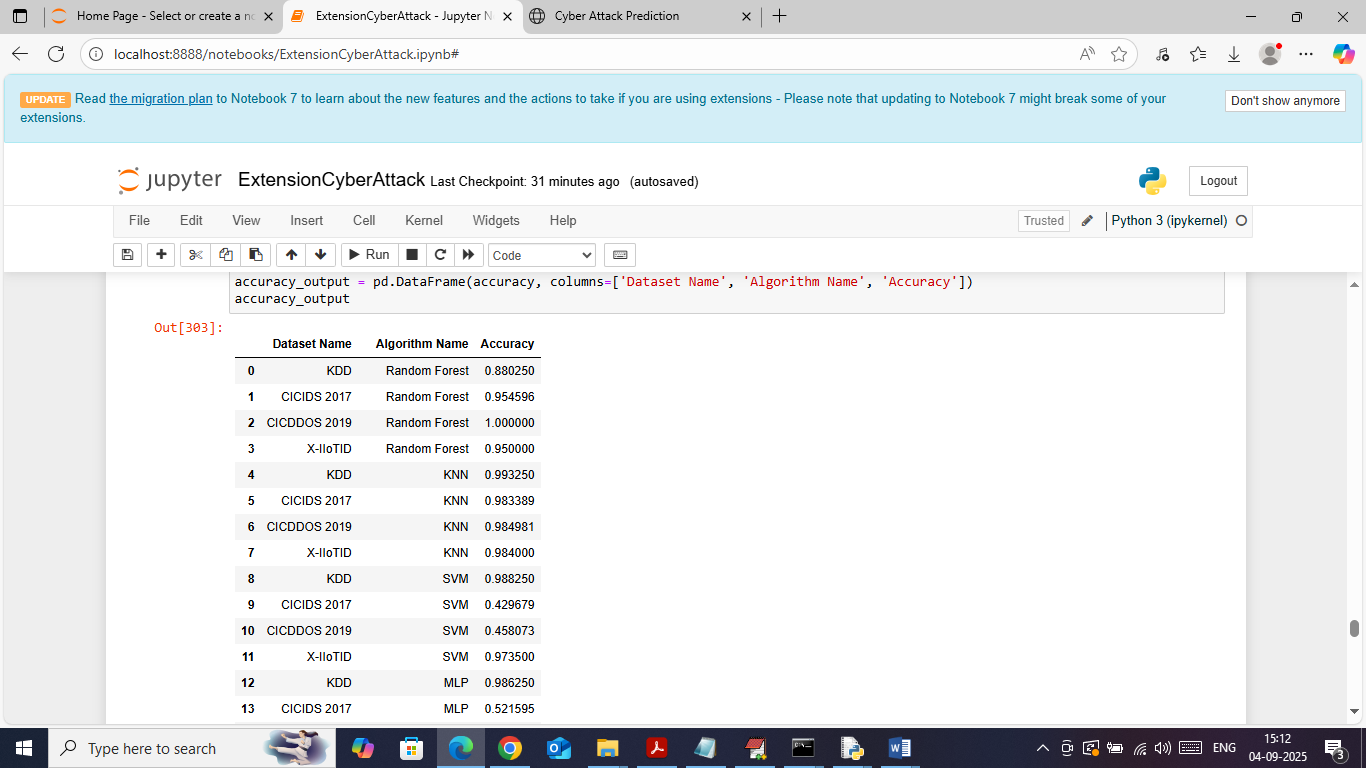
In above screen can see DNN accuracy on all 4 datasets



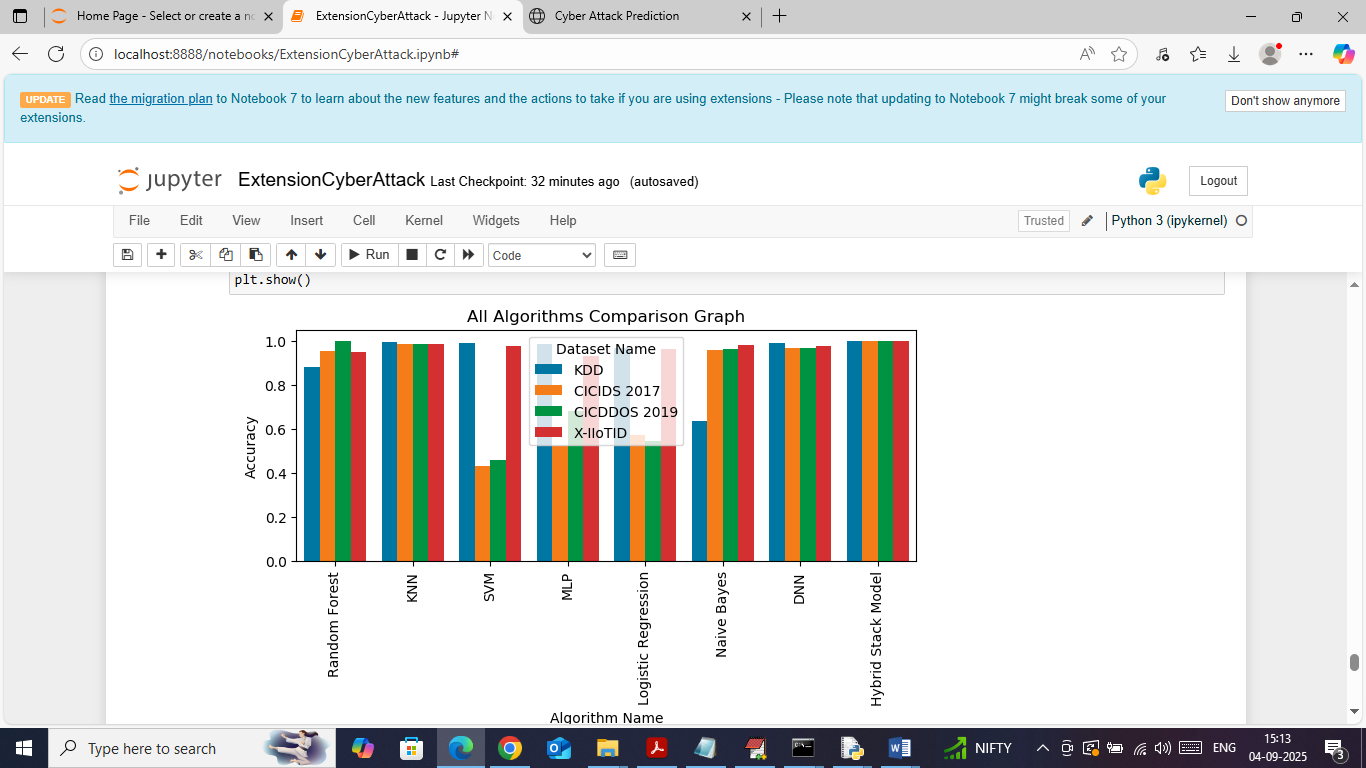
In above screen training extension hybrid algorithms and after training extension model got 99 and 100% accuracy on all 4 datasets



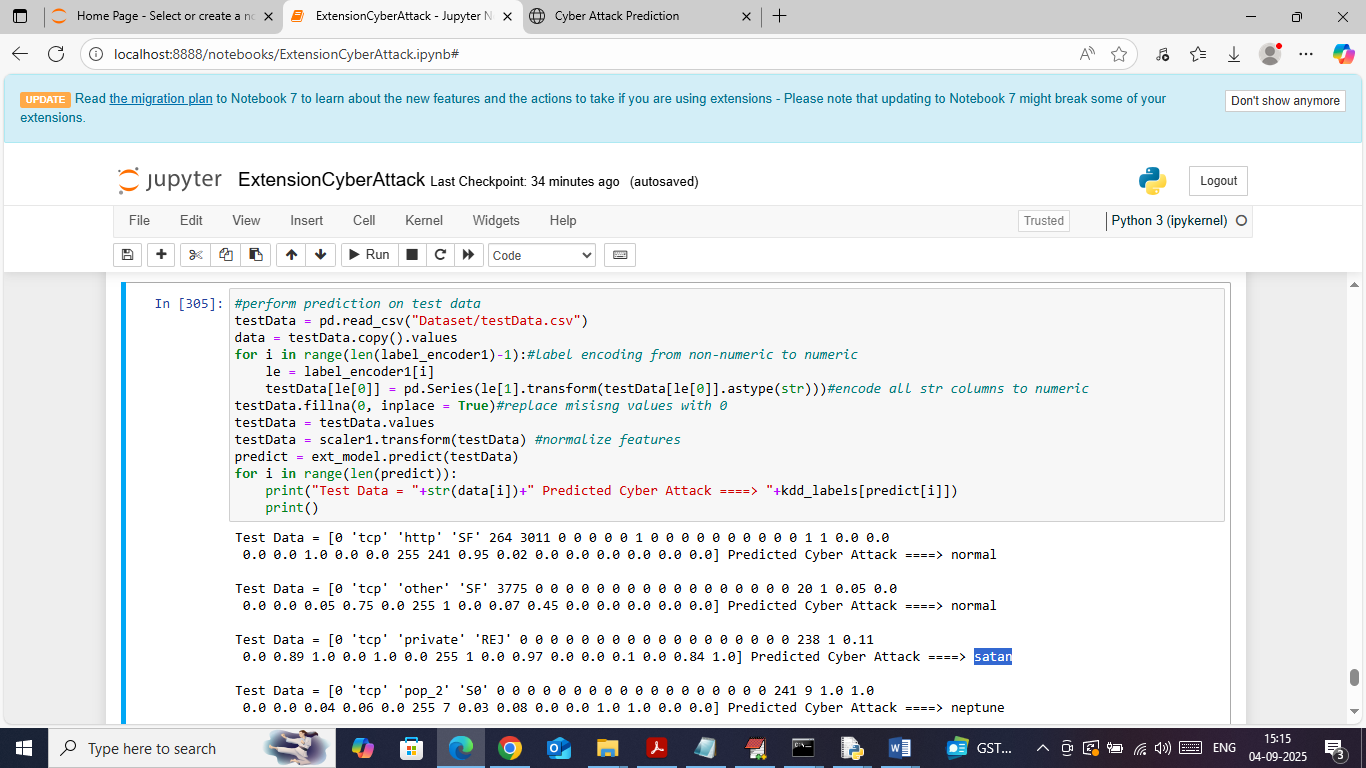
In above screen defining SHAP explanation tool on trained and test data and then SHAP explaining which features contributing most for correct class label prediction, in above graph feature names on left side with most number of dots will be consider as high relevant features



In above screen in table format showing all algorithms accuracy on each dataset



In above screen showing comparison graph between all algorithms with all datasets. In above graph x-axis represents ‘algorithm names’ and y-axis represents accuracy and different colour bars represents different dataset names. In above graph can see Extension Hybrid model got high accuracy



In above screen loading and processing test data values and then applying extension model to predict attack type. In above output area in square bracket can see test data values and after =🡺 symbol can see predicted attack type

WEB OUTPUT

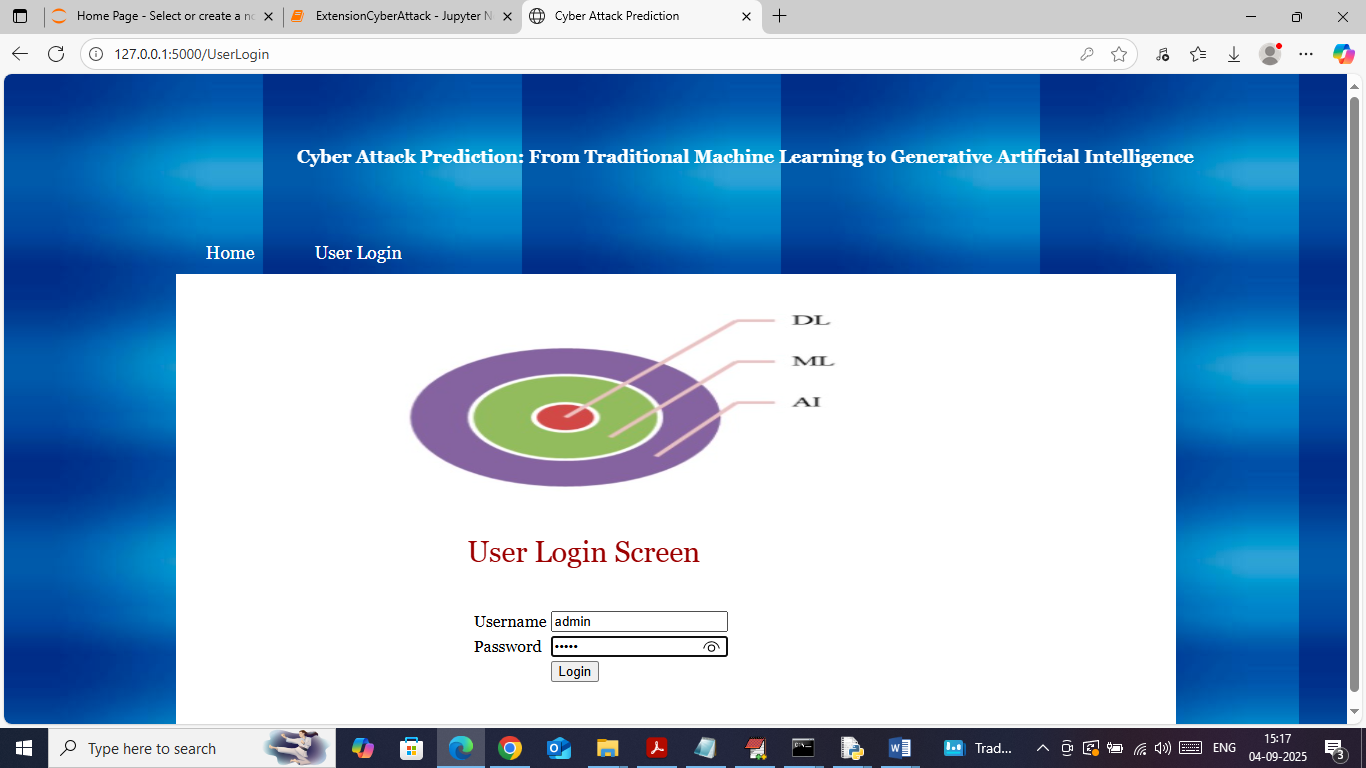
To run web prediction double click on ‘runFlask.bat’ file to start flask server and then will get below page



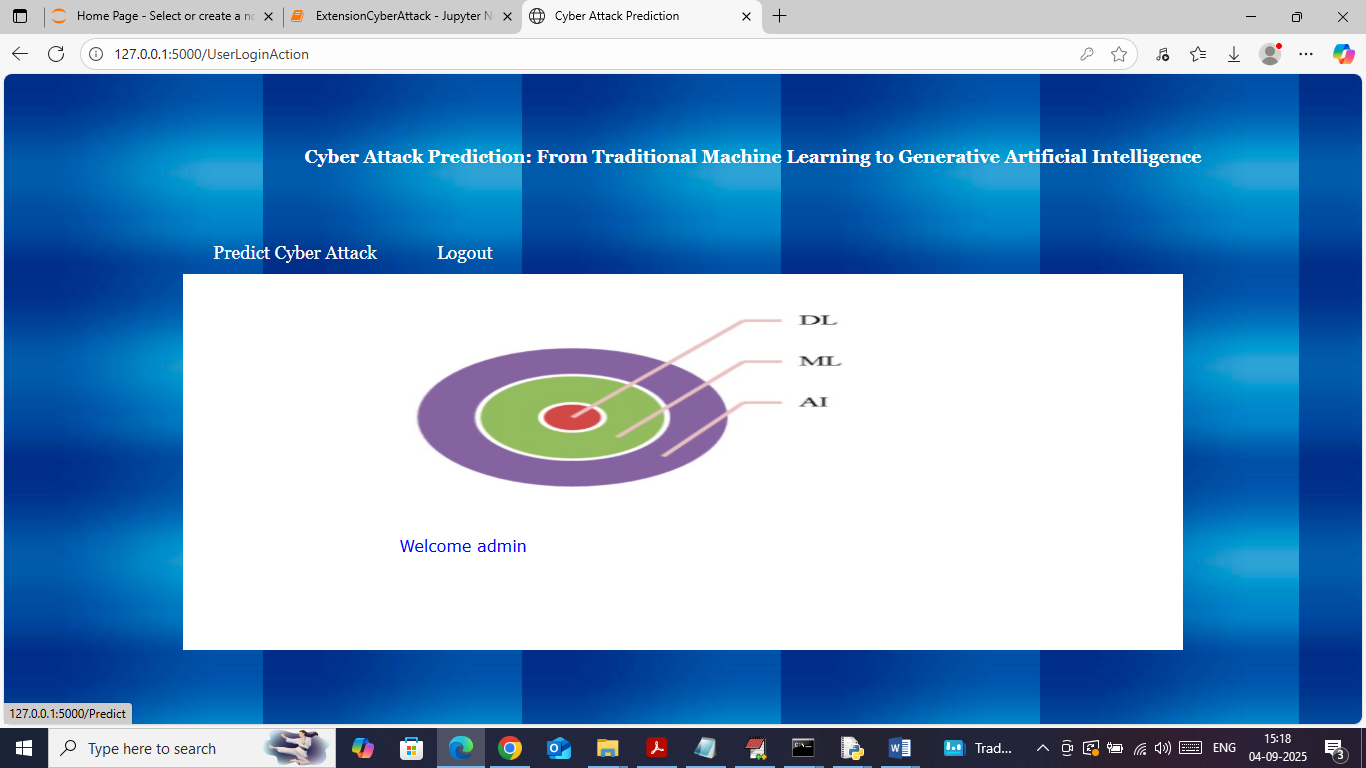
In above screen flask server started and now open browser and enter URL as <http://127.0.0.1:5000/index> and then press enter key to get below page



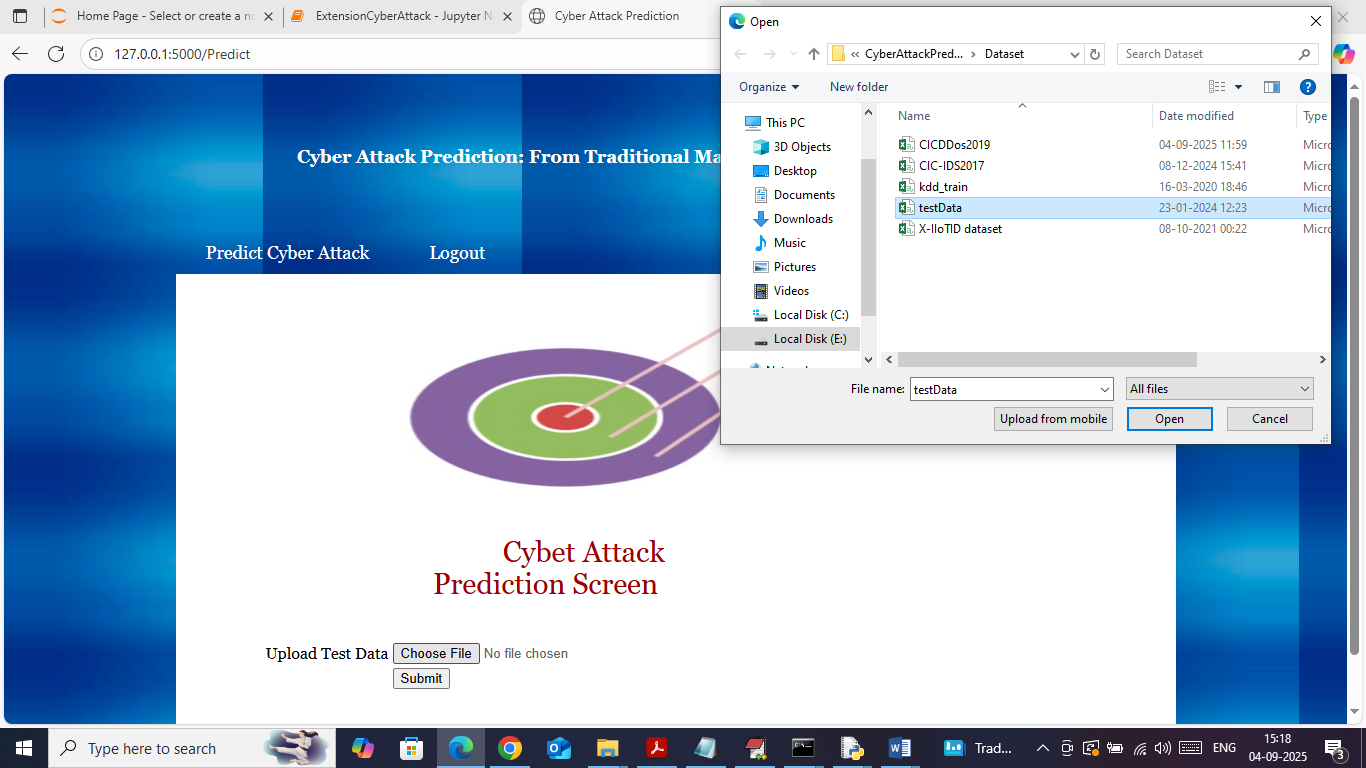
In above screen click on ‘User Login’ link to get below page



In above screen user is login by entering username and password as ‘admin and admin’. After login will get below page



In above screen click on ‘Predict Cyber Attack’ link to get below page



In above screen selecting and uploading test data file and then click on buttons to get below page



In above screen in first column can see test data values and in second column can see predicted attack type.