Introduction

As the domain traffic is usually allowed to pass through enterprise firewalls without deep inspection the attackers exploit this to steal sensitive information. Therefore, our goal in these assignments builds a model that can classify the Fully qualified domain name (FQDN) into benign and malicious.

Implementation

Algorithms:

For this problem we used 3 Algorithms:

- Catboost classifier: is an ensemble machine learning strategy [1] in this paper they used catboost classifier in intrusion detection and achieved 99.46% in terms of accuracy. Therefore, we decided to test it in our problem as the two problems are under the umbrella of anomaly detection problems.
- Random Forest classifier:[2] in this paper they predict the existence of DNS tunnels using session behavior and achieved 99.97 in terms of accuracy.
- Logistic Regression: [3] In this paper logistic regression achieved high performance with F1-Score: 0.96 to detect Advanced Persistent Threat (APT) attacks.

Experiments:

We train the 3 classifiers to our model with and without hyperparameters tunning and compare the performance:

We note all the classifiers achieved the same accuracy which is 82%. Therefore, we will use another metric for comparison. Our goal to minimize the number of attacks will focus on False Positive (FP) of Confusion Matrix. We will select the random forest as the best classifier as it's the minim in the FP with 32 over the other classifiers.

1. CatBoost classifier:

Classification report:

	precision	recall	f1-score	support
0	1.00	0.60	0.75	72304
1	0.76	1.00	0.86	88538
accuracy			0.82	160842
macro avg	0.88	0.80	0.81	160842
weighted avg	0.87	0.82	0.81	160842

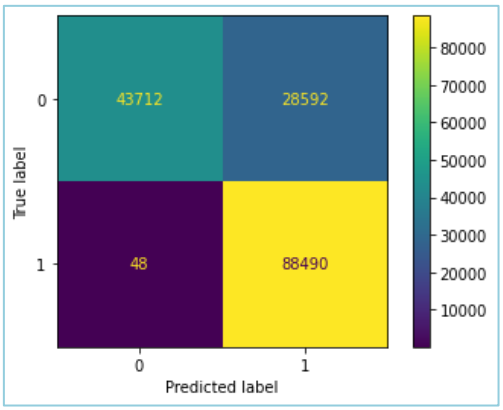

Figure 1: Basic classifier with 1500 iteration

Classification report:

	precision	recall	f1-score	support
0	1.00	0.60	0.75	72304
1	0.76	1.00	0.86	88538
accuracy			0.82	160842
macro avg	0.88	0.80	0.81	160842
weighted avg	0.86	0.82	0.81	160842

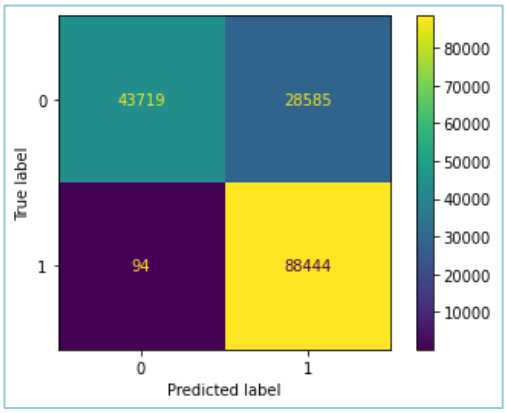

Figure 2: Classifier after changing the learning rate and loss_function

2. Random Forest Classifier:

Classification report:

	precision	recall	f1-score	support
0	1.00	0.60	0.75	72304
1	0.76	1.00	0.86	88538
accuracy			0.82	160842
macro avg	0.88	0.80	0.81	160842
weighted avg	0.87	0.82	0.81	160842

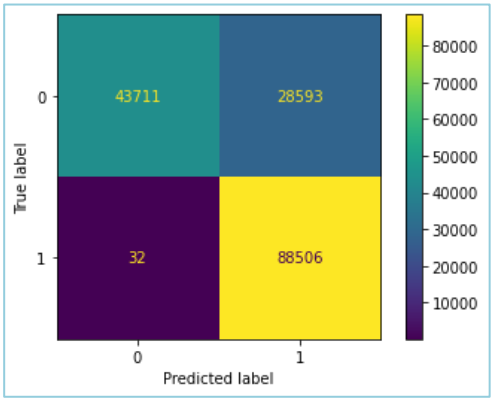

Figure 3: Basic classifier with 250 estimators

Classification report:

	precision	recall	f1-score	support
0	1.00	0.60	0.75	72304
1	0.76	1.00	0.86	88538
accuracy			0.82	160842
macro avg	0.88	0.80	0.81	160842
weighted avg	0.87	0.82	0.81	160842

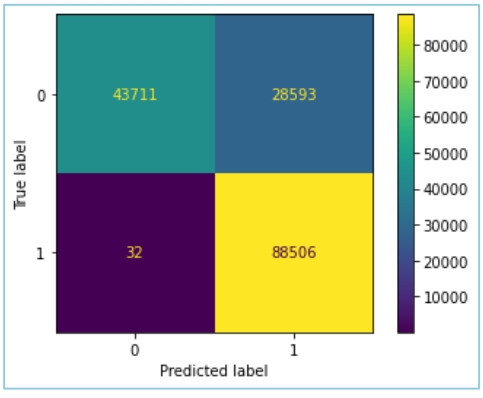

Figure 4: Classifier after changing class weight attribute

3. Logistics Regression

```
Classification report:
              precision    recall  f1-score   support

           0       0.99      0.60      0.75     72304
           1       0.76      1.00      0.86     88538

    accuracy                           0.82    160842
   macro avg       0.87      0.80      0.81    160842
weighted avg       0.86      0.82      0.81    160842
```

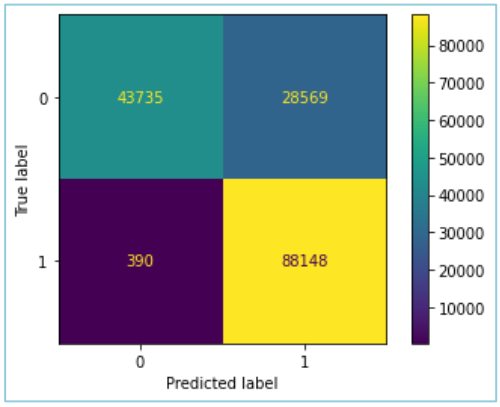

Figure 5: Basic classifier

```
Classification report:
              precision    recall  f1-score   support

           0       0.99      0.60      0.75     72304
           1       0.76      1.00      0.86     88538

    accuracy                           0.82    160842
   macro avg       0.87      0.80      0.81    160842
weighted avg       0.86      0.82      0.81    160842
```

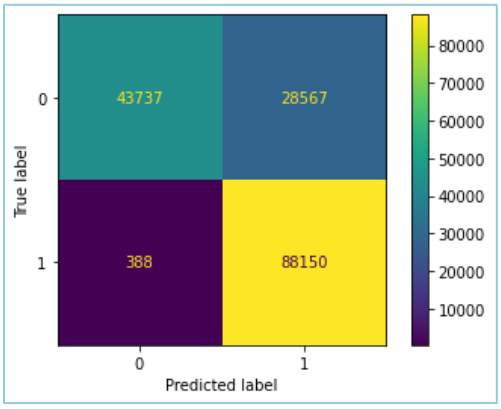

Figure 6: Classifier after changing solver attribute

References:

[1] Bhati, N. S., & Khari, M. (2021). A New Intrusion Detection Scheme Using CatBoost Classifier. In E. Ever & F. Al-Turjman (Eds.), Forthcoming Networks and Sustainability in the IoT Era (pp. 169–176). Springer International Publishing.

[2] Z. Yang, Y. Hongzhi, L. Lingzi, H. Cheng and Z. Tao, "Detecting DNS Tunnels Using Session Behavior and Random Forest Method," 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC), 2020, pp. 45-52, doi: 10.1109/DSC50466.2020.00015.

[3] A. Das, M. Shen, M. Shashanka and J. Wang, "Detection of Exfiltration and Tunneling over DNS," 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), 2017, pp. 737-742, doi: 10.1109/ICMLA.2017.00-71.