**Deep Learning**

**Techniques in IDS**

Monday, June 09, 2025

Table of Contents

[1 CNN 2](#_Toc200812795)

[1.1 Structure 2](#_Toc200812796)

[1.2 Training Validation Result 3](#_Toc200812797)

[1.2.1 CIC\_IDS\_2017 3](#_Toc200812798)

[1.2.2 CIC\_TON\_IOT 4](#_Toc200812799)

[1.3 Test Result 5](#_Toc200812800)

[1.3.1 CIC\_IDS\_2017 5](#_Toc200812801)

[1.3.2 CIC\_TON\_IOT 6](#_Toc200812802)

[1.4 Confusion Matrix 8](#_Toc200812803)

[1.4.1 CIC\_IDS\_2017 8](#_Toc200812804)

[1.4.2 CIC\_TON\_IOT 11](#_Toc200812805)

[2 CNN LSTM 14](#_Toc200812806)

[2.1 Structure 14](#_Toc200812807)

[2.2 Training Validation Result 15](#_Toc200812808)

[2.2.1 CIC\_IDS\_2017 15](#_Toc200812809)

[2.2.2 CIC\_TON\_IOT 16](#_Toc200812810)

[2.3 Test Result 17](#_Toc200812811)

[2.3.1 CIC\_IDS\_2017 17](#_Toc200812812)

[2.3.2 CIC\_TON\_IOT 18](#_Toc200812813)

[2.4 Confusion Matrix 19](#_Toc200812814)

[2.4.1 CIC\_IDS\_2017 19](#_Toc200812815)

[2.4.2 CIC\_TON\_IOT 21](#_Toc200812816)

[3 conclusion 23](#_Toc200812817)

[3.1 CIC\_IDS\_2017 23](#_Toc200812818)

[3.2 CIC\_TON\_IOT 25](#_Toc200812819)

# CNN

## Structure

|  |  |
| --- | --- |
|  |  |
| Figure : CNN Structure 1. (original) | Figure 2: CNN Structure 2. (2 blocks) |
|  | |
| Figure 3: MLP Structure. | |

## Training Validation Result

### CIC\_IDS\_2017

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

### CIC\_TON\_IOT

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

## Test Result

### CIC\_IDS\_2017

|  |
| --- |
|  |
|  |
|  |

### CIC\_TON\_IOT

|  |
| --- |
|  |
|  |
|  |

## Confusion Matrix

### CIC\_IDS\_2017

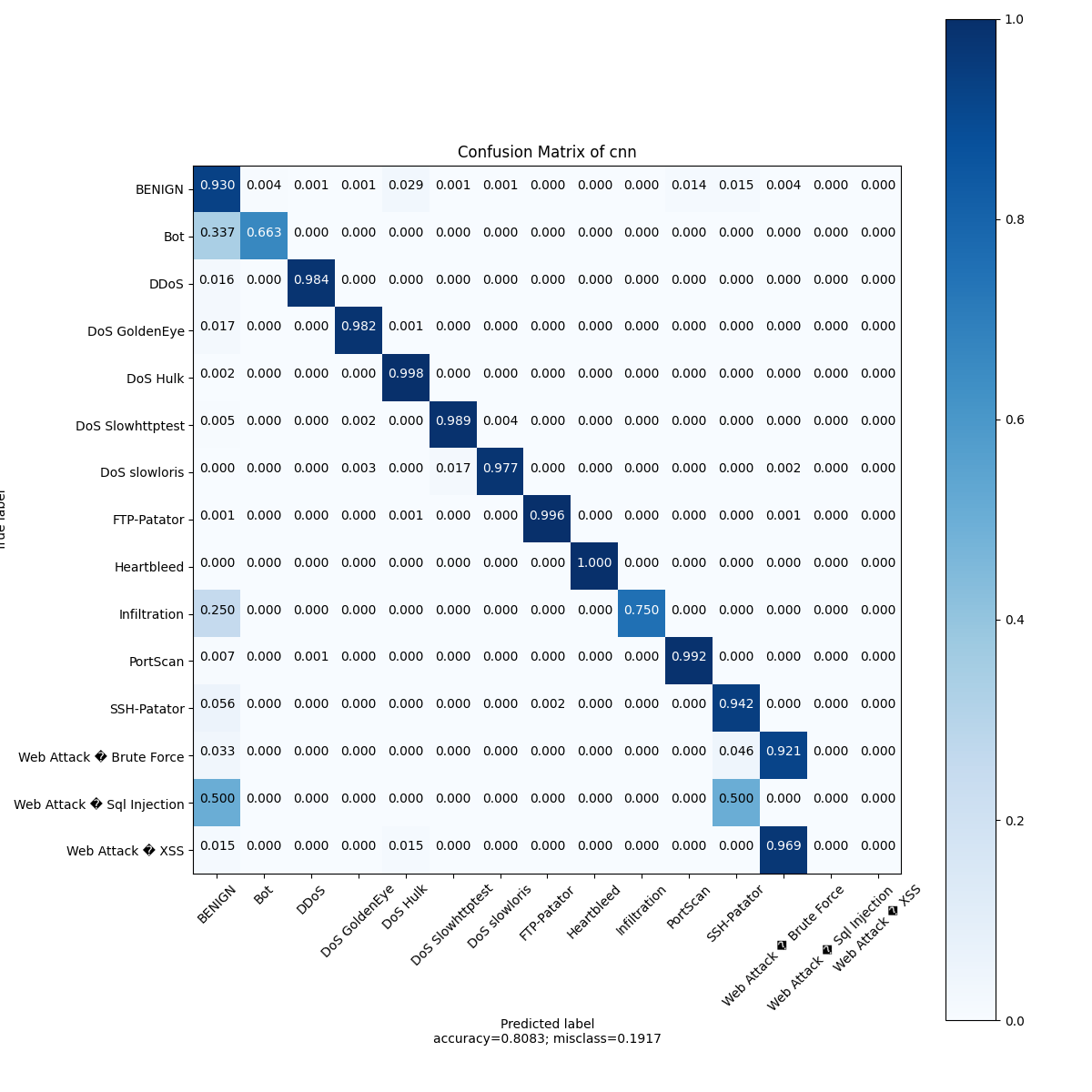


Figure 4: CNN orginal CFM.

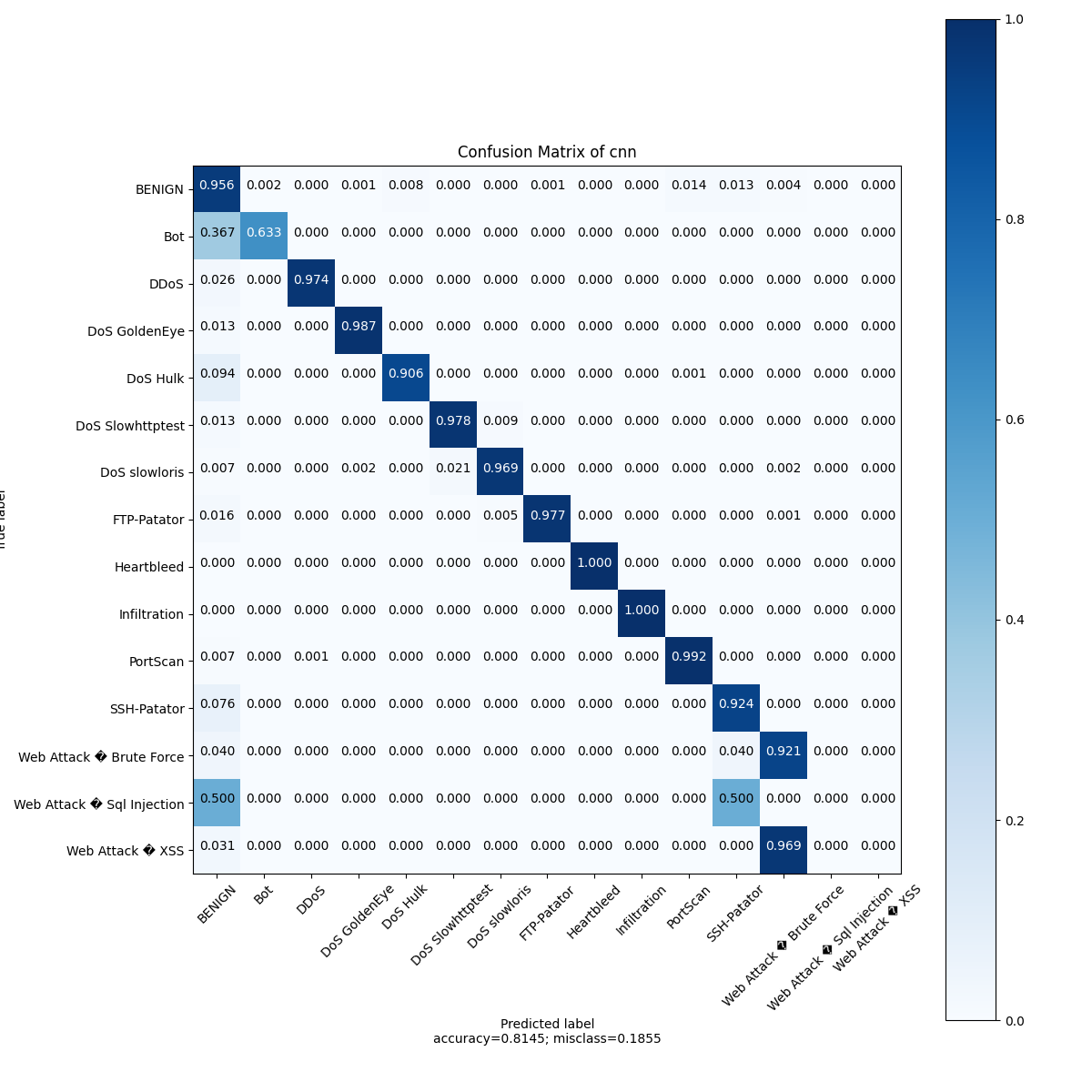


Figure 5: CNN 2 blocks CFM.

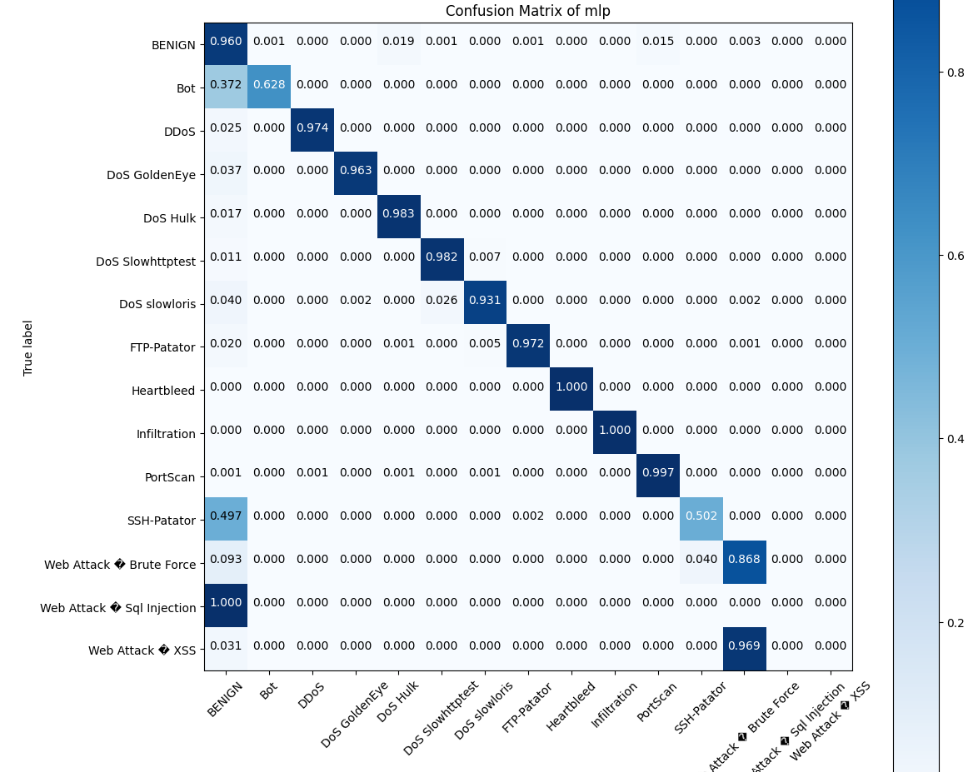


Figure 6: MLP model CFM.

### CIC\_TON\_IOT

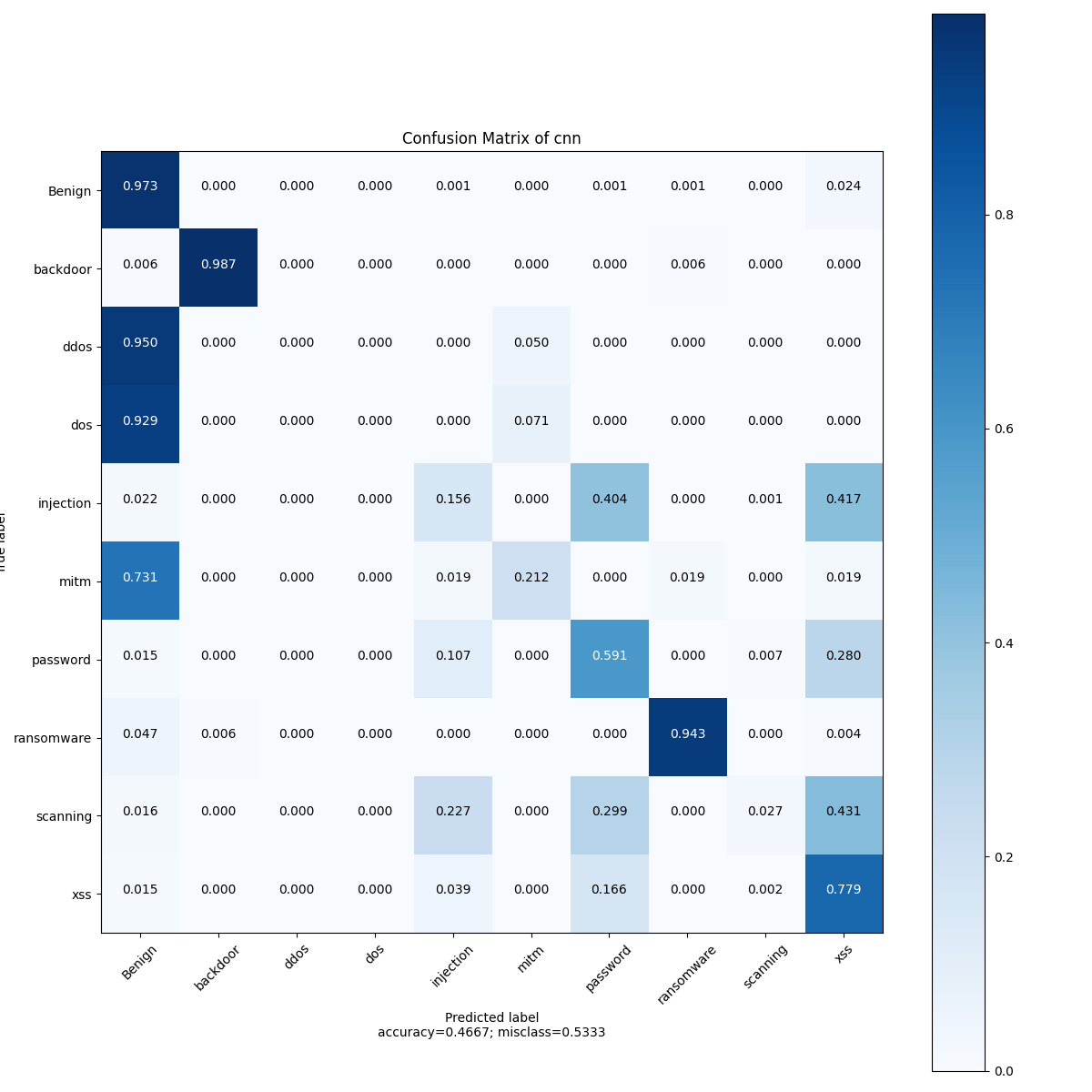


Figure 7: CNN orginal Strucuture CFM.

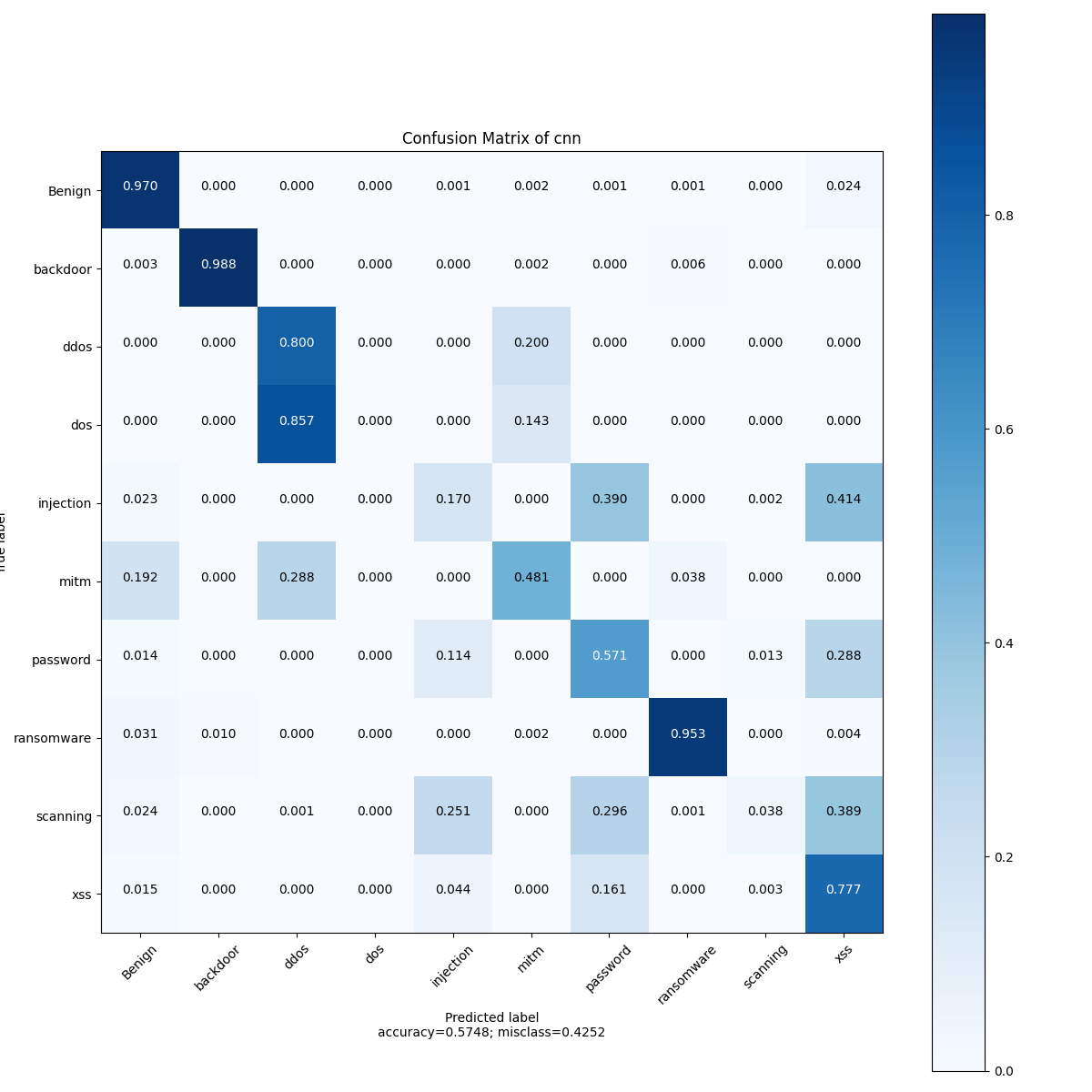


Figure 8: CNN 2 blocks structure CFM.

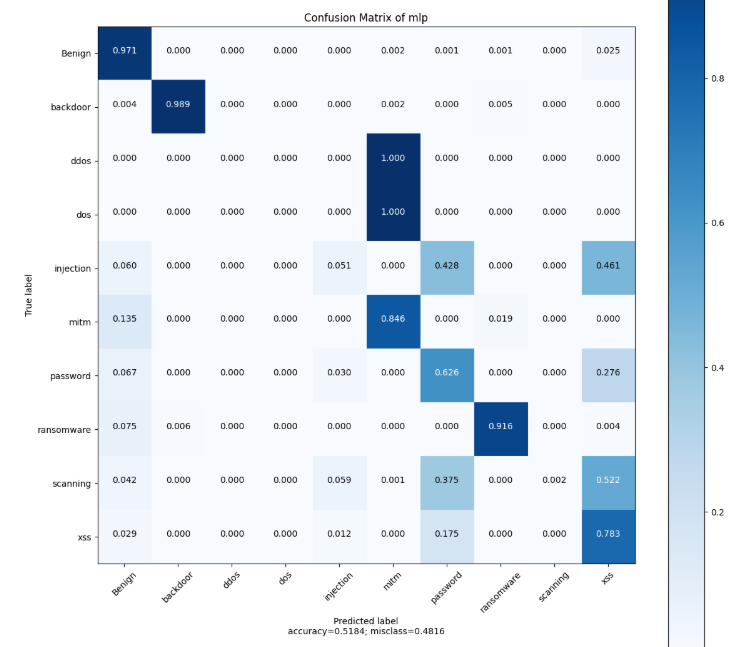


Figure 9: MLP CFM.

# CNN LSTM

## Structure

|  |  |
| --- | --- |
|  |  |
| *Figure 10: CNN\_LSTM STRUCTURE 1. (original)* | *Figure 11: CNN\_LSTM STRUCTURE 2. (new)* |

## Training Validation Result

### CIC\_IDS\_2017

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

### CIC\_TON\_IOT

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

## Test Result

### CIC\_IDS\_2017

|  |
| --- |
|  |
|  |
|  |

### CIC\_TON\_IOT

|  |
| --- |
|  |
|  |
|  |

## Confusion Matrix

### CIC\_IDS\_2017

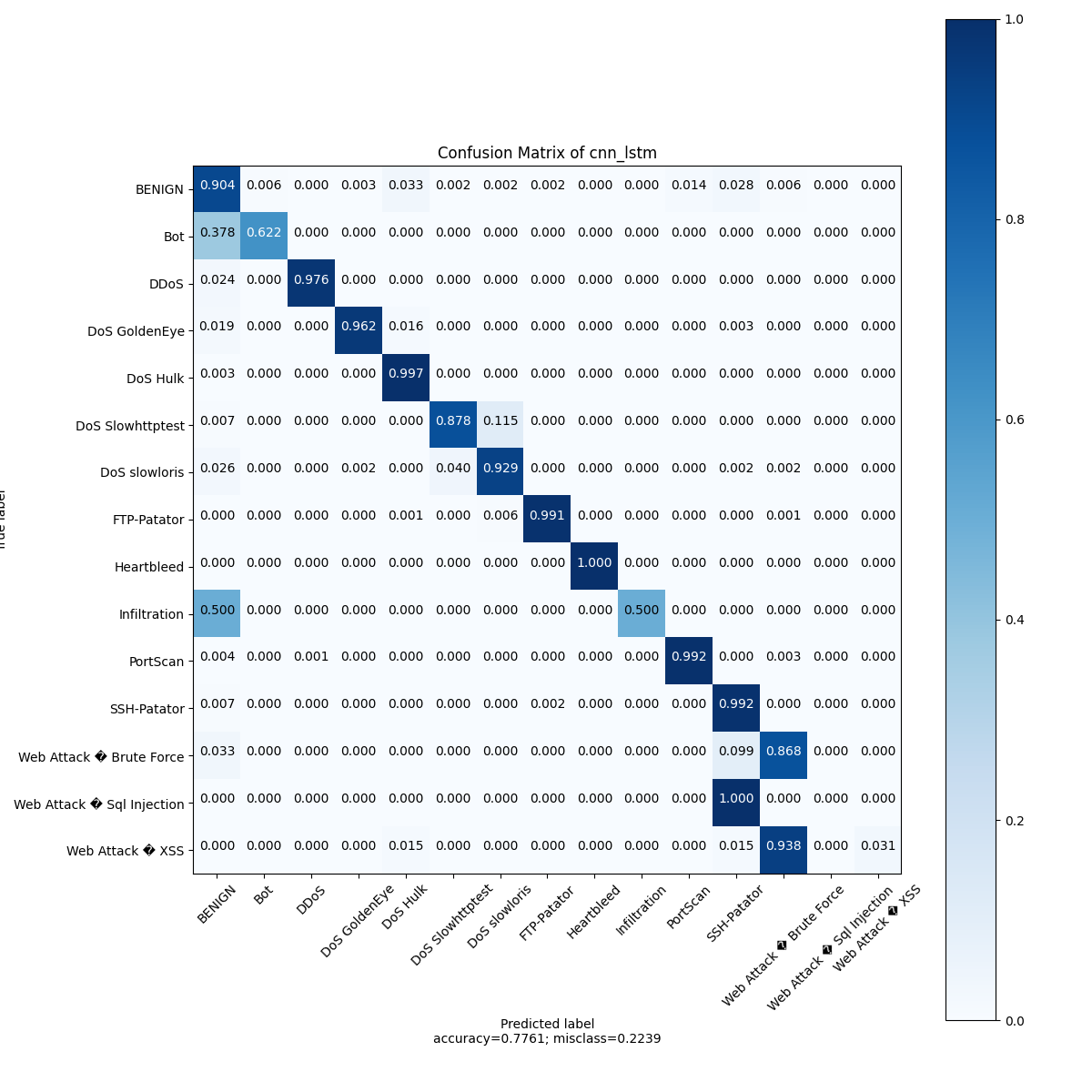


Figure 12: CNN\_LSTM STRUCTURE 1 CFM.

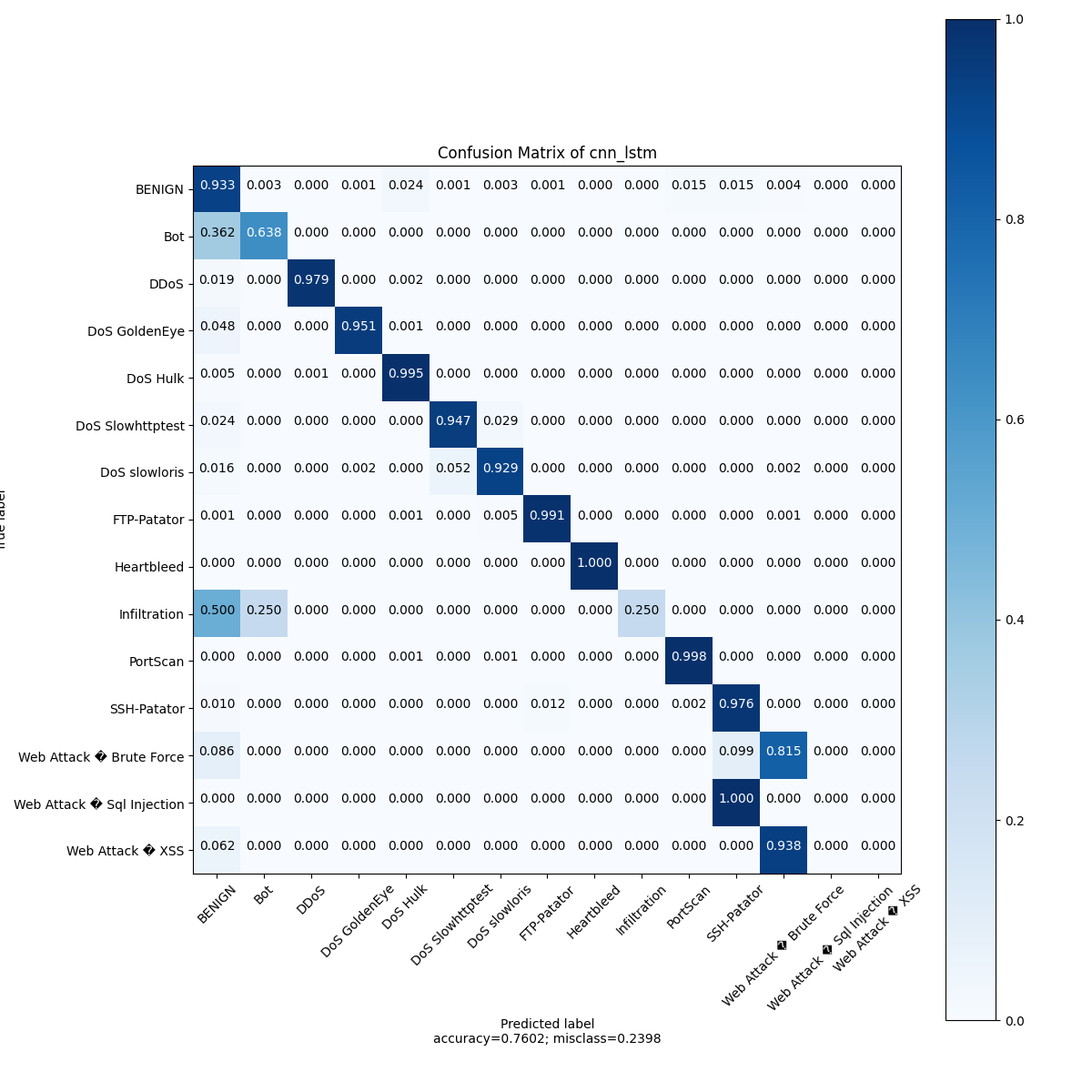


Figure 13: CNN\_LSTM STRUCTURE 2 CFM.

### CIC\_TON\_IOT

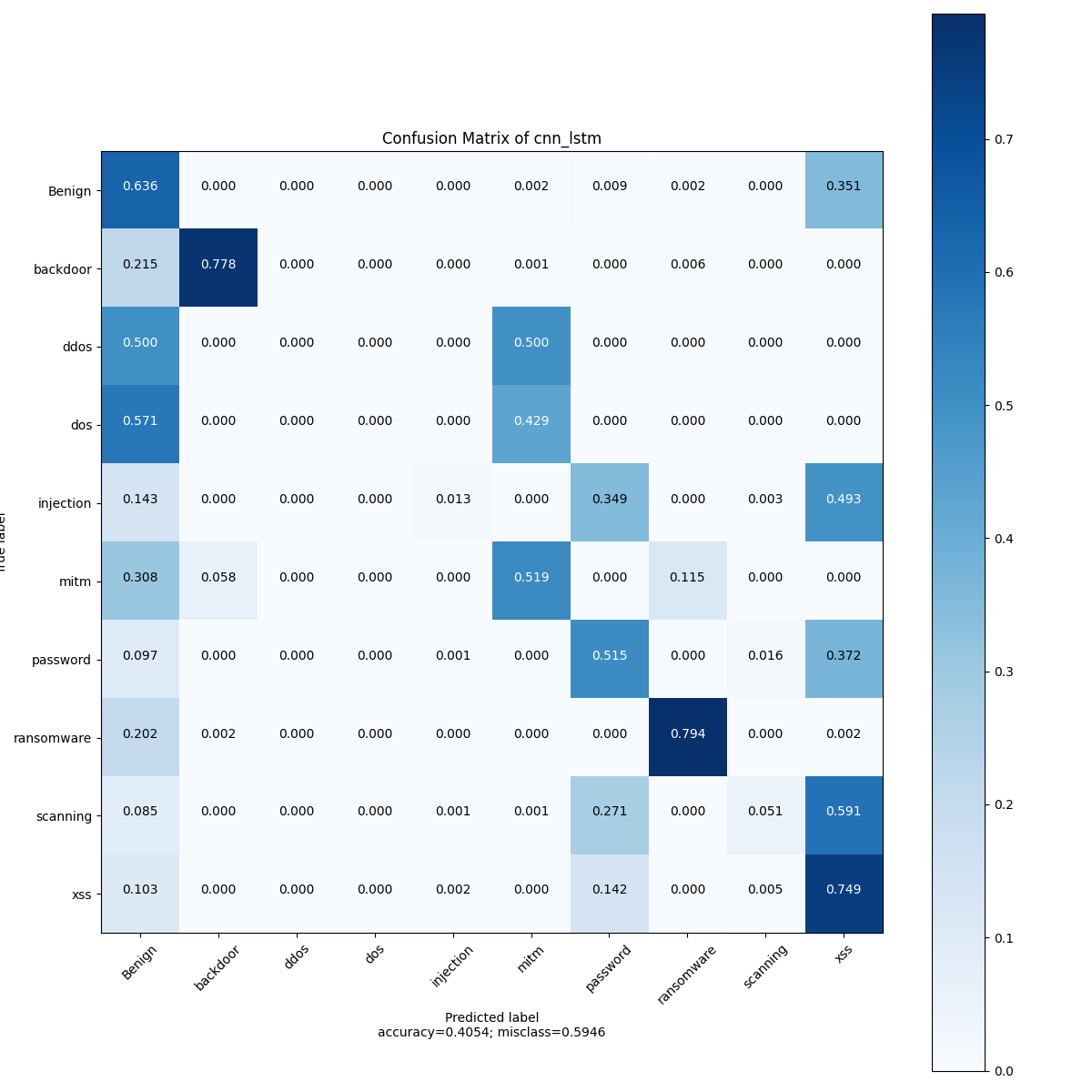


Figure 14: CNN\_LSTM STRUCTURE 1 CEM.

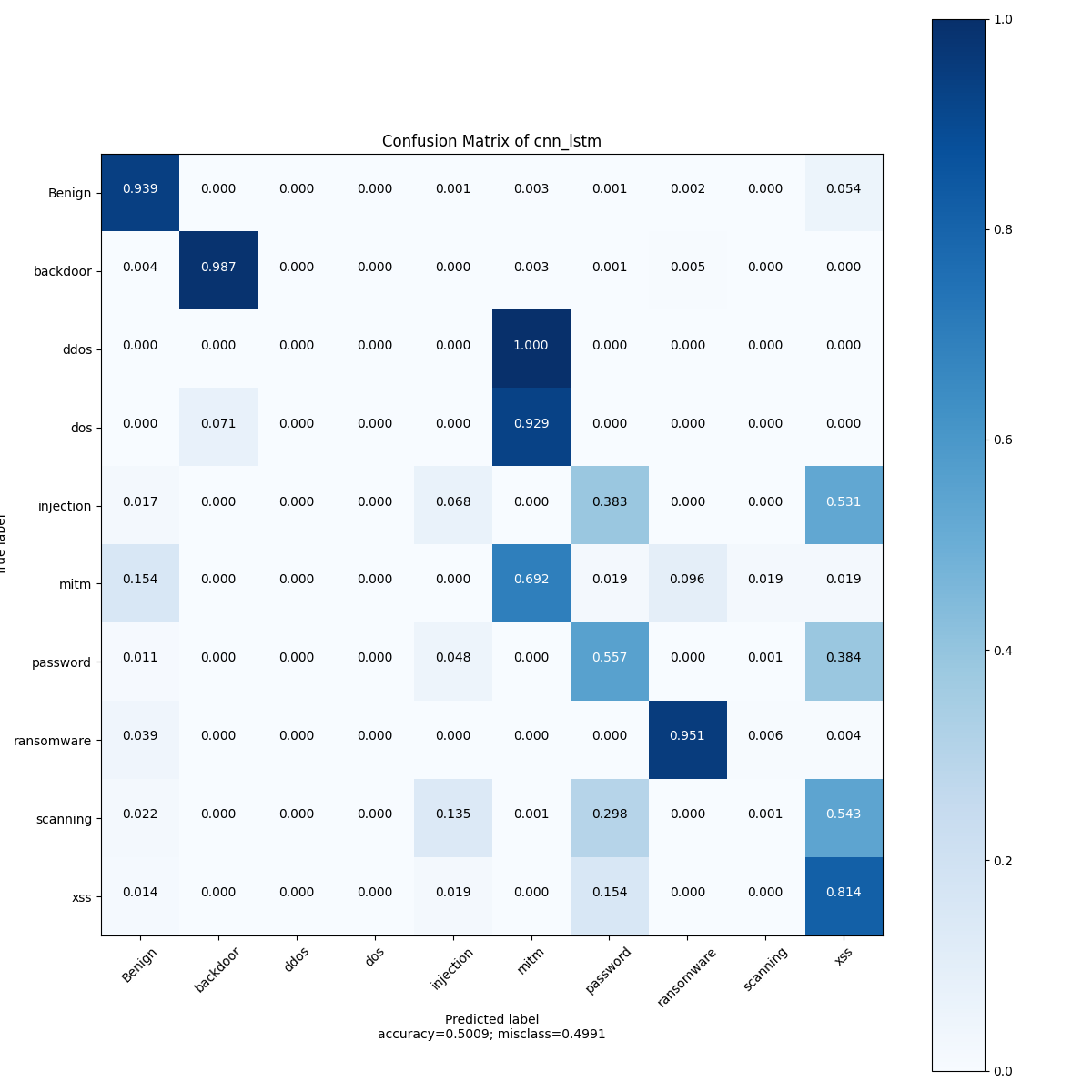


Figure 15: CNN\_LSTM STRUCTURE 2 CFM

# conclusion

## CIC\_IDS\_2017

|  |
| --- |
|  |
|  |
|  |

For the CIC\_IDS\_2017 dataset, [the MLP model](#_Structure_1) achieved the highest performance among all evaluated models, closely followed by the [CNN model (CNN Structure 2)](#_Structure_1). All models recorded accuracy and F1-scores exceeding 90%, which can be attributed to the dataset's relatively small size and clean nature. However, the key differentiator lies in the test loss values, where the MLP and CNN models demonstrated significantly lower losses—less than 12%—highlighting their superior generalization capabilities.

To better understand the sources of error, we analyzed the [confusion matrices](#_CIC_IDS_2017_1), which revealed that most misclassifications occurred in detecting SQL Injection, SSH-Patator, and Bot attacks. These categories contributed the most to the residual test loss and warrant further attention for model refinement.

## CIC\_TON\_IOT

|  |
| --- |
|  |
|  |
|  |

For the CIC\_TON\_IoT dataset—which is larger and noisier than CIC\_IDS\_2017—the [**CNN models**](#_Structure_1) (both single-block and 2-block structures) now outperform the MLP, which drops to third place and exhibits slightly higher test loss. All models see degraded performance overall. The [**confusion matrices**](#_CIC_TON_IOT) show that misclassifications primarily involve **DoS**, **injection**, **MITM**, and **scanning** attacks.

**Two key reasons** for this performance decline may be:

1. **Data volume and noise**: TON‑IoT is larger with more real-world, heterogeneous traffic, making it harder for models to generalize.
2. **Class imbalance and attack diversity**: The presence of more varied and less-represented attack types increases misclassification, particularly for rare attacks.

**Thank you for your Time.**