**Deep Learning**

**Techniques in IDS (2)**

Monday, June 16, 2025

Table of Contents

[1 LSTM/BiLSTM 3](#_Toc201484040)

[1.1 Structure 3](#_Toc201484041)

[1.2 Training Validation Result 4](#_Toc201484042)

[1.2.1 CIC\_IDS\_2017 4](#_Toc201484043)

[1.2.2 CIC\_TON\_IOT 5](#_Toc201484044)

[1.3 Test Result 6](#_Toc201484045)

[1.3.1 CIC\_IDS\_2017 6](#_Toc201484046)

[1.3.2 CIC\_TON\_IOT 7](#_Toc201484047)

[2 GRU / CNN\_GRU 8](#_Toc201484048)

[2.1 Structure 8](#_Toc201484049)

[2.2 Training Validation Result 9](#_Toc201484050)

[2.2.1 CIC\_IDS\_2017 9](#_Toc201484051)

[2.2.2 CIC\_TON\_IOT 10](#_Toc201484052)

[2.3 Test Result 11](#_Toc201484053)

[2.3.1 CIC\_IDS\_2017 11](#_Toc201484054)

[2.3.2 CIC\_TON\_IOT 12](#_Toc201484055)

[3 Auto Encoder Decoder Classifier 13](#_Toc201484056)

[3.1 Structure 13](#_Toc201484057)

[3.2 Train Validation Result 14](#_Toc201484058)

[3.2.1 CIC\_IDS\_2017 14](#_Toc201484059)

[3.2.2 CIC\_TON\_IOT 15](#_Toc201484060)

[3.3 Test Result 16](#_Toc201484061)

[3.3.1 CIC\_IDS\_2017 16](#_Toc201484062)

[3.3.2 CIC\_TON\_IOT 17](#_Toc201484063)

[4 Conclusion 18](#_Toc201484064)

[4.1 CIC\_IDS\_2017 18](#_Toc201484065)

[4.2 CIC\_TON\_IOT 19](#_Toc201484066)

[5 NOTES 20](#_Toc201484067)

# LSTM/BiLSTM

## Structure

|  |  |
| --- | --- |
| Figure 1: BiLSTM Structure 1. | Figure 2: BiLSTM Structure 2. |
| Figure 3: LSTM Structure. | |

## Training Validation Result

### CIC\_IDS\_2017

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

### CIC\_TON\_IOT

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

## Test Result

### CIC\_IDS\_2017

|  |
| --- |
|  |
|  |

### CIC\_TON\_IOT

|  |
| --- |
|  |
|  |

# GRU / CNN\_GRU

## Structure

|  |
| --- |
| Figure 4: GRU Structure. |
| Figure 5: CNN\_GRU Structure. |

## Training Validation Result

### CIC\_IDS\_2017

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

### CIC\_TON\_IOT

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

## Test Result

### CIC\_IDS\_2017

|  |
| --- |
|  |
|  |

### CIC\_TON\_IOT

|  |
| --- |
|  |
|  |

# Auto Encoder Decoder Classifier

## Structure

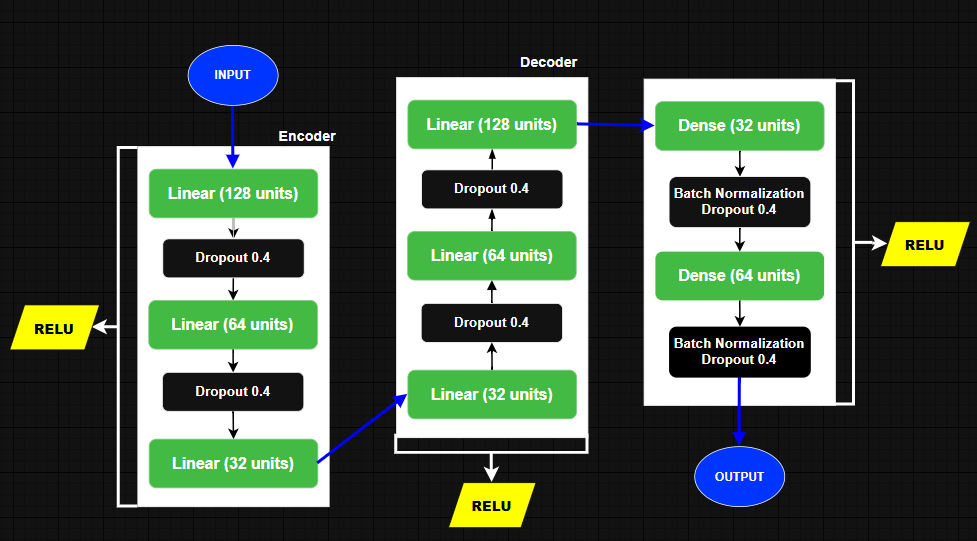


Figure 6: Auto Encoder Decoder Structure.

## Train Validation Result

### CIC\_IDS\_2017

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

### CIC\_TON\_IOT

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

## Test Result

### CIC\_IDS\_2017

|  |
| --- |
|  |
|  |

### CIC\_TON\_IOT

|  |
| --- |
|  |
|  |

# Conclusion

## CIC\_IDS\_2017

|  |
| --- |
|  |
|  |

**DISCUSSION:**

Based on the test loss results, we can conclude that the **MLP model** continues to be the best performer, achieving the lowest test loss among all models. It is closely followed by the **cnn\_gru** and **cnn\_lstm\_new** architectures, which also show competitive results. These models demonstrate a strong balance between high test accuracy and low test loss.

In contrast, the **Auto Encoder Decoder** model performs poorly in comparison, exhibiting the highest test loss by a significant margin. This suggests that it may not be well-suited for the current task or dataset.

Overall, except for the Auto Encoder Decoder, **all other models achieved a test accuracy greater than 90% and a test loss below 0.25**, indicating reliable performance across the board.

## CIC\_TON\_IOT

|  |
| --- |
|  |
|  |

**DISCUSSION:**

When evaluating performance on the **CIC-TON-IoT dataset**, the results differ significantly from the previous dataset. In this case, **BiLSTM**, **LSTM**, and **GRU** models outperform the others, achieving **over 90% accuracy and less than 0.25 test loss**. These are followed by the **MLP model**, while the **Auto Encoder Decoder** model demonstrates the poorest performance with the highest test loss.

It is important to note that the data preparation process for this dataset involved **data sampling techniques**, primarily due to computing resource constraints. This may have impacted models differently, especially those like autoencoders that are sensitive to the quality and balance of input distributions.

Comparing results across both datasets, we can infer that **MLP**, **cnn\_gru**, and **cnn\_lstm** are consistently strong performers. However, on the CIC-TON-IoT dataset specifically, **sequence-based models (BiLSTM, LSTM, GRU)** showed superior generalization and robustness.

**Why BiLSTM, LSTM, and GRU Performed Better**

1. **Temporal Awareness**: These models are designed to capture **temporal dependencies** in sequential data, which is highly relevant in IoT network traffic where the order and timing of packets are critical for intrusion patterns.
2. **Context Preservation**: **LSTM and GRU** can retain important information over longer sequences, while **BiLSTM** benefits from looking at the input in both forward and backward directions, providing a richer context and better pattern recognition.
3. **Noise Robustness**: These architectures are often more **robust to noise and irregularities** in time-series data, making them well-suited for real-world, less-clean datasets like CIC-TON-IoT.
4. **Efficient Memory Control**: The internal gating mechanisms of LSTM and GRU help them **filter out irrelevant information**, which can reduce overfitting and lead to lower loss values.

# NOTES

The **BiLSTM** [**Structure 1**](#_Structure_1) was applied to the **CIC-IDS-2017** dataset, while a simplified [**Structure 2**](#_Structure_1) was used for the **CIC-TON-IoT** dataset due to computational resource limitations. These constraints also led to adjustments in several training parameters—such as **batch size, maximum number of epochs, and sequence length**—for the CIC-TON-IoT dataset in order to ensure successful training, validation, and testing on the larger and more complex dataset.

Additionally, visualizations and performance graphs are available on **Weights & Biases** at the following links:

* [CIC-IDS-2017 Results](•%09https:/wandb.ai/mohammad-fleity-lebanese-university/DL-NIDS-2--cic-ids-2017?nw=nwusermohammadfleity)
* [CIC-TON-IoT Results](https://wandb.ai/mohammad-fleity-lebanese-university/DL-NIDS-2--cic-ton-iot/workspace?nw=nwusermohammadfleity)

All notebooks (excluding the one shared by Mr. Thermos) are available on [**GitHub**](https://github.com/Mohammad-Fleity2002/DL_IDS.git).

**Thank you for your Time.**