**Deep Learning**

**Techniques in IDS (2)**

Monday, June 16, 2025

Table of Contents

[1 LSTM/BiLSTM/GRU 2](#_Toc202287028)

[1.1 Structure 2](#_Toc202287029)

[1.2 Training Validation Result 3](#_Toc202287030)

[1.2.1 CIC\_IDS\_2017 3](#_Toc202287031)

[1.2.2 CIC\_TON\_IOT 4](#_Toc202287032)

[1.3 Test Result 5](#_Toc202287033)

[1.3.1 CIC\_IDS\_2017 5](#_Toc202287034)

[1.3.2 CIC\_TON\_IOT 6](#_Toc202287035)

[1.3.3 CIC\_IDS\_2017 6](#_Toc202287036)

[2 Auto Encoder Decoder Classifier/ CNN\_LSTM 7](#_Toc202287037)

[2.1 Structure 7](#_Toc202287038)

[2.2 Train Validation Result 8](#_Toc202287039)

[2.2.1 CIC\_IDS\_2017 8](#_Toc202287040)

[2.2.2 CIC\_TON\_IOT 9](#_Toc202287041)

[2.3 Test Result 10](#_Toc202287042)

[2.3.1 CIC\_IDS\_2017 10](#_Toc202287043)

[2.3.2 CIC\_TON\_IOT 11](#_Toc202287044)

[3 FINAL RESULTS 12](#_Toc202287045)

[3.1 CIC\_IDS\_2017 12](#_Toc202287046)

[3.2 CIC\_TON\_IOT 13](#_Toc202287047)

[4 NOTES 14](#_Toc202287048)

# LSTM/BiLSTM/GRU

## Structure

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

## Training Validation Result

### CIC\_IDS\_2017

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

### CIC\_TON\_IOT

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

## Test Result

### CIC\_IDS\_2017

|  |
| --- |
|  |
|  |

### CIC\_TON\_IOT

|  |
| --- |
|  |
|  |

### CIC\_IDS\_2017

# Auto Encoder Decoder Classifier/ CNN\_LSTM

## Structure

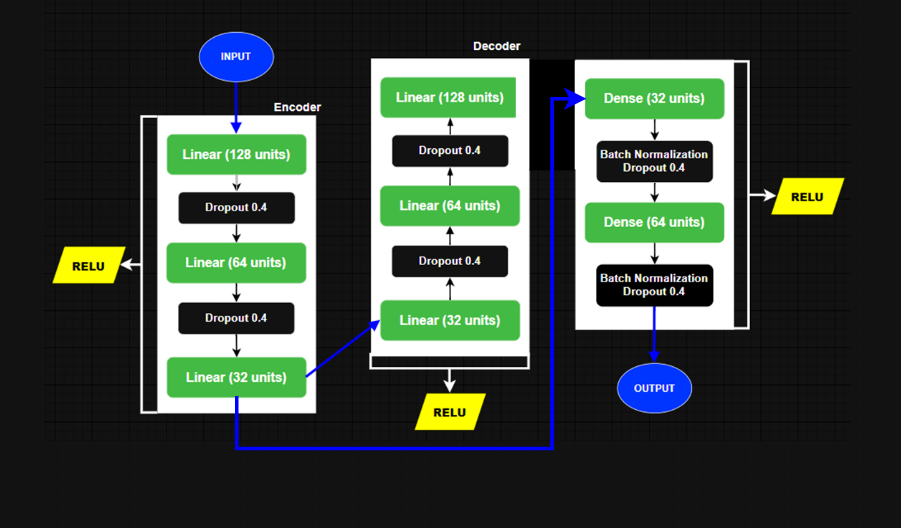


Figure 4: Auto Encoder Decoder Structure.

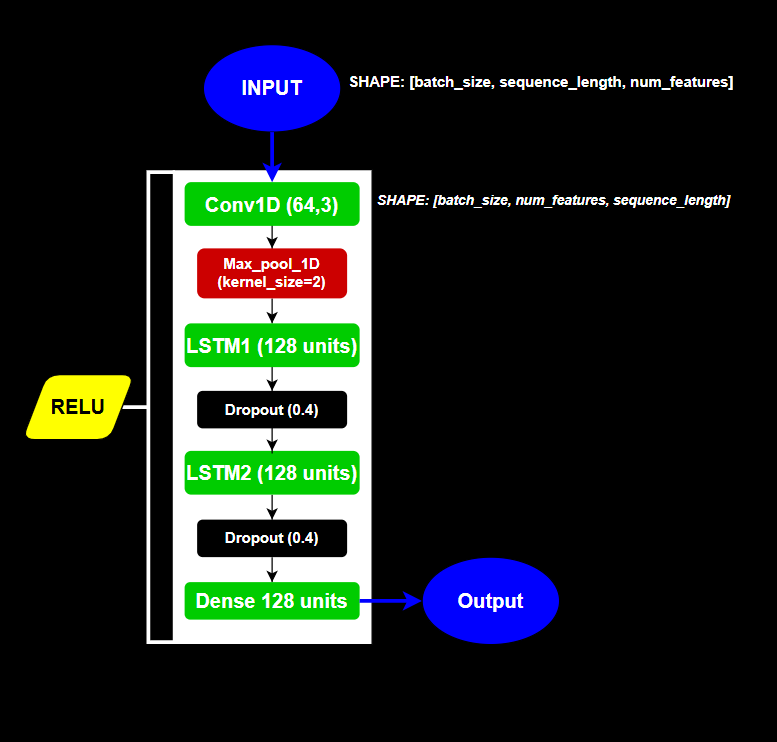


Figure 5: CNN\_LSTM\_UB Structure.

## Train Validation Result

### CIC\_IDS\_2017

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

### CIC\_TON\_IOT

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

## Test Result

### CIC\_IDS\_2017

|  |
| --- |
|  |
|  |

### CIC\_TON\_IOT

|  |
| --- |
|  |
|  |

# FINAL RESULTS

## CIC\_IDS\_2017

|  |
| --- |
|  |
|  |

## CIC\_TON\_IOT

|  |
| --- |
|  |
|  |

# NOTES

While searching for an AutoEncoderDecoder-based IDS model in recent research papers, I was unable to find one that directly fits our use case. Most models were either limited to encoders without a decoding component, or were developed for entirely different domains, making them unsuitable for adaptation to network intrusion detection. However, I did find an interesting CNN-LSTM architecture, which I evaluated under the name CNN\_LSTM\_UB.

The CNN\_LSTM\_2 is a model that we simulate from the research paper:

* IOT-BASED INTRUSION DETECTION SYSTEM USING NEW HYBRID DEEP LEARNING ALGORITHM

Similarly, the CNN\_LSTM\_UB is a model simulated from an existing one in the research paper:

* DDOS ATTACK DETECTION USING HYBRID (CCN AND LSTM) ML MODEL

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), which contains:

* Reports DL\_1, DL\_2 and the DL\_3.
* Notebook used.
* An excel that include the final results.

**Thank you for your Time.**