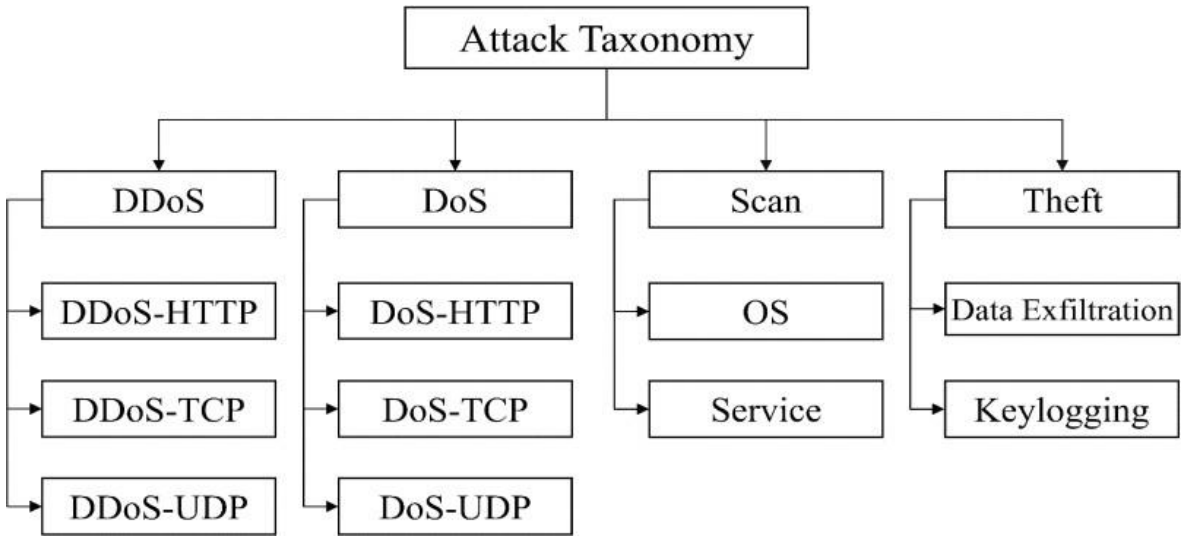
Detecting Anomaly Activity in IoT Networks Using Deep Learning-Based Model

Various Phases and Result

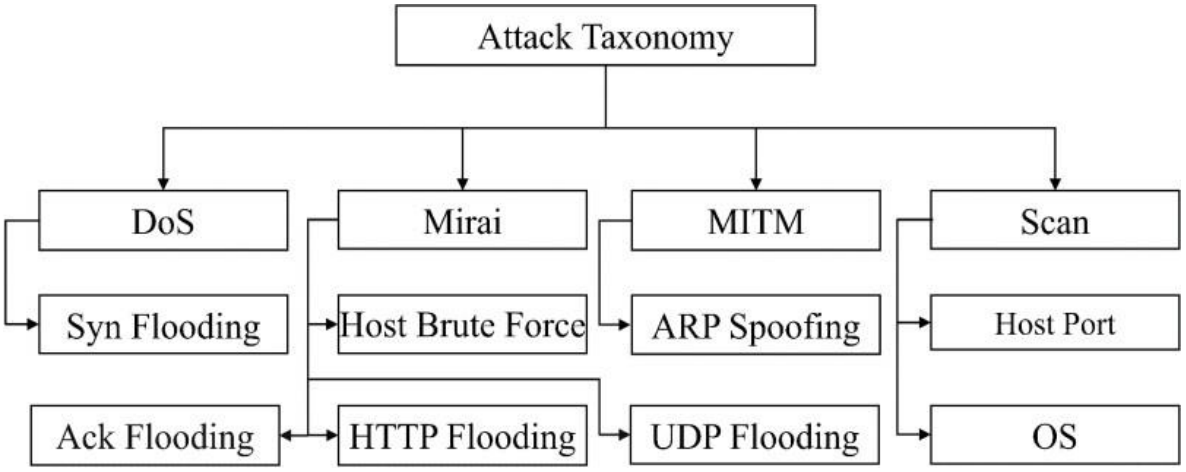
Step 1: Collecting Dataset and Combining it

In this we used four publicly available datasets:

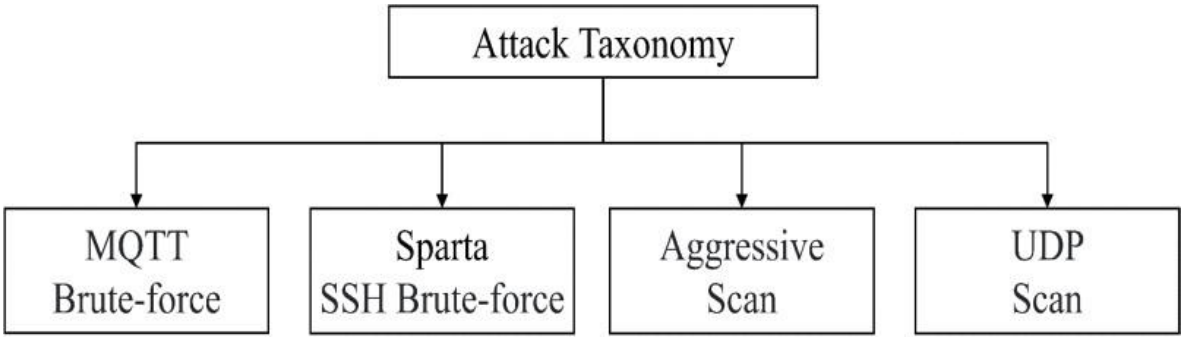
1) BoT-IoT Dataset



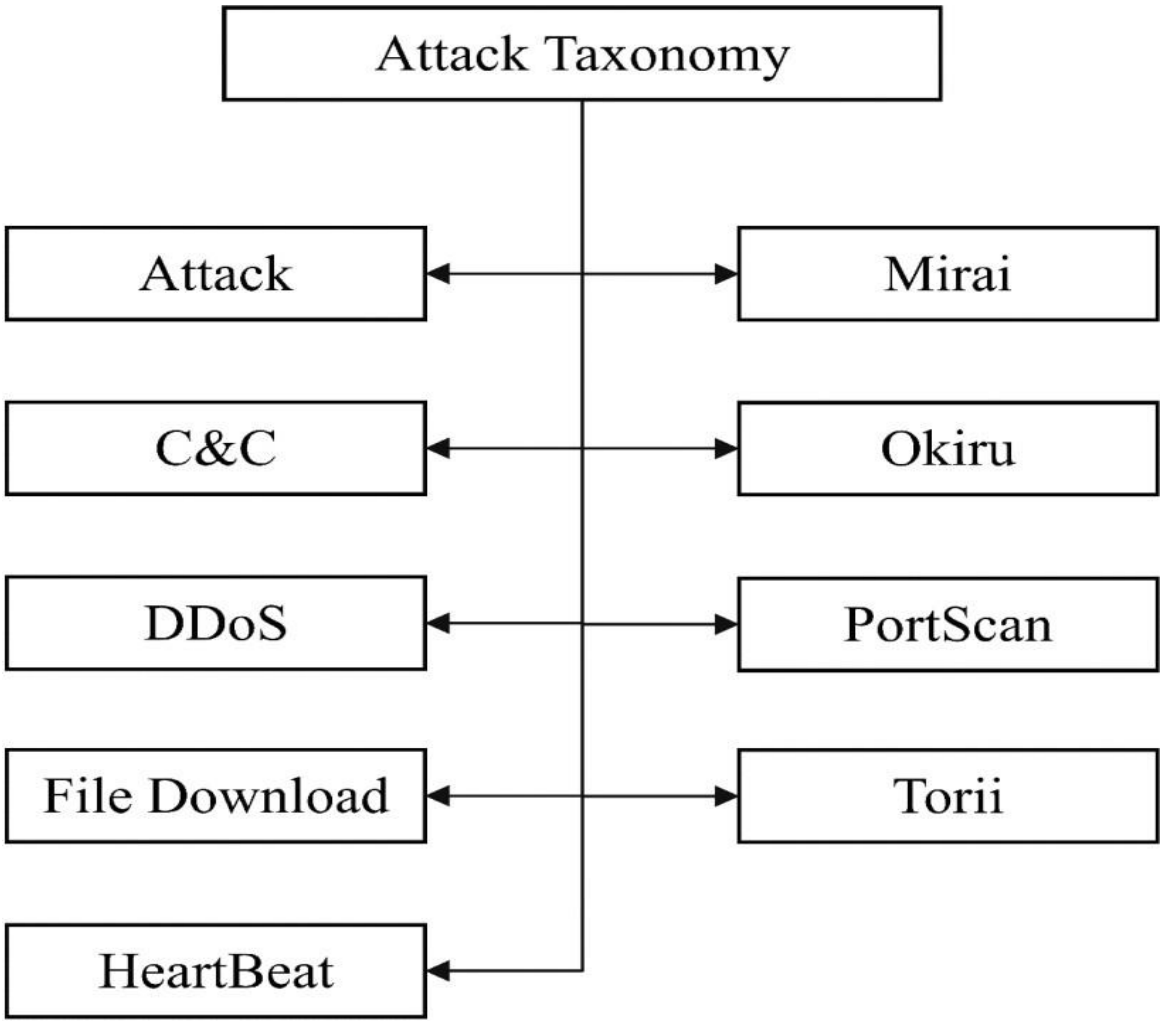
2) IoT Intrusion Detection Dataset



3) MQTT-IoT-IDS2020 Dataset



4) IoT-23 Dataset



Created a new IOT-DS2 Dataset:

we combined BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, and IoT-23 datasets further to increase the number of attacks in the dataset. Table below shows the new dataset named IoT-DS-2, which contains 16 attack classes and a normal class. The IoT-DS-2 dataset multiclass was labelled 0 for normal and 1-16 for attack categories.

```
iot_ds2['Cat'].unique()
```

```
array(['DDoS', 'DoS', 'MITM ARP Spoofing', 'Mirai', 'MQQT_bruteforce',
       'Reconnaissance', 'Sparta', 'Theft', 'Normal', 'Attack', 'C&C',
       'FileDownload', 'HeartBeat', 'Okiru', 'PortScan', 'Torii', 'Flood'],
      dtype=object)
```

```
Cat_map = {
    'Normal' : 0,
    'DDoS' : 1,
    'DoS' : 2,
    'MITM ARP Spoofing' : 3,
    'Mirai' : 4,
    'MQTT_bruteforce' : 5,
    'Sparta' : 6,
    'Theft' : 7,
    'Attack' : 8,
    'C&C' : 9,
    'FileDownload' : 10,
    'HeartBeat' : 11,
    'Okiru' : 12,
    'Reconnaissance' : 13,
    'Port Scan' : 14,
    'Torii' : 15,
    'Flood' : 16
}
```

IOT Network intrusion dataset:

This dataset is also a publicly available dataset and we are going to use this to train our model. The new dataset consists of 4 attack classes and a normal class. The new dataset, named IOT Network intrusion dataset, is described below. The IOT Network intrusion dataset multiclass was labelled 0 for normal and 1 to 4 for attack categories.

```
    intrusion['Cat'].unique()
```

```
array(['Mirai', 'DoS', 'Scan', 'Normal', 'MITM ARP Spoofing'],
      dtype=object)
```

```
Cat_map = {
    'Normal' : 0,
    'Mirai' : 1,
    'DoS' : 2,
    'Scan' : 3,
    'MITM ARP Spoofing' : 4,
}
```

Here is the link for both Dataset that we are using. Click here

Step 2: Feature Processing:

1. After extracting the features, the network features flow ID, source IP, destination IP, source port, and timestamp were removed from all datasets.
2. The non-numeric category features in the datasets were converted to a numeric field, with NaN values filled with 0.
3. Input feature columns were normalized within the range of -1 to 1 to remove extreme values and improve calculation efficiency.

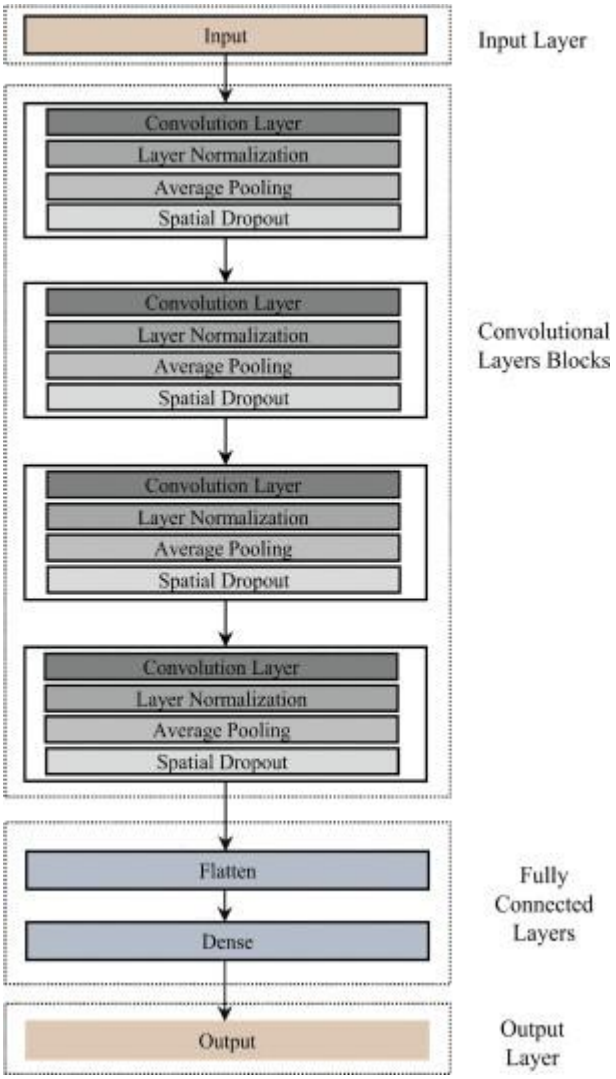
Step 3: Feature Selection:

1. Feature selection is a crucial step in deep learning model development, aiming to enhance prediction by choosing relevant features and minimizing overfitting.
2. The RFE (Recursive Feature Elimination) technique was employed to extract 64 significant features from the IoT-DS-2 dataset, using accuracy, precision, recall, and F1 score for ranking.

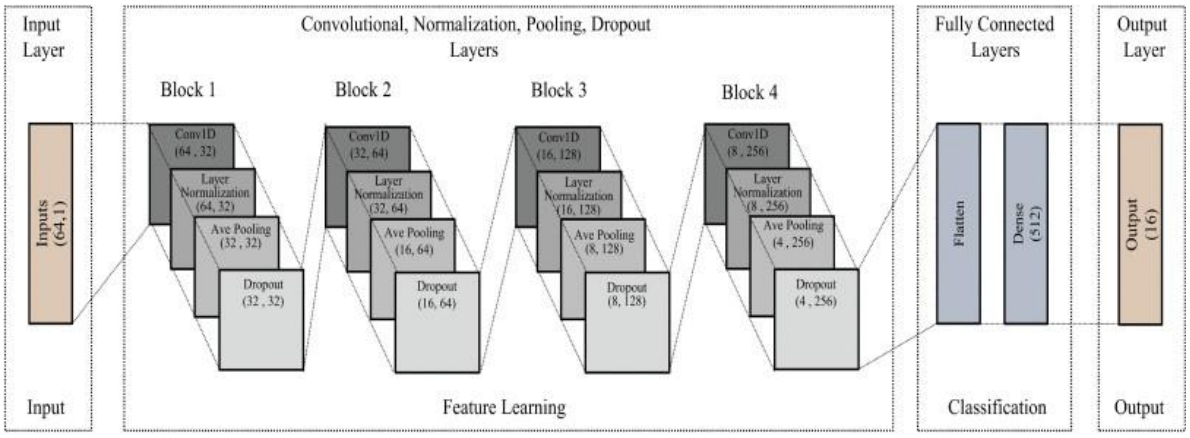
Step 4: Model Design:

An input layer, four blocks of convolutional layers, a fully connected dense layer, and an output layer make up the model we used in this article. Our proposed architecture is implemented using CNN1D, CNN2D, and CNN3D models. The IoT Network Intrusion Dataset and IoT-DS-2 datasets are used to evaluate the CNN model's performance.

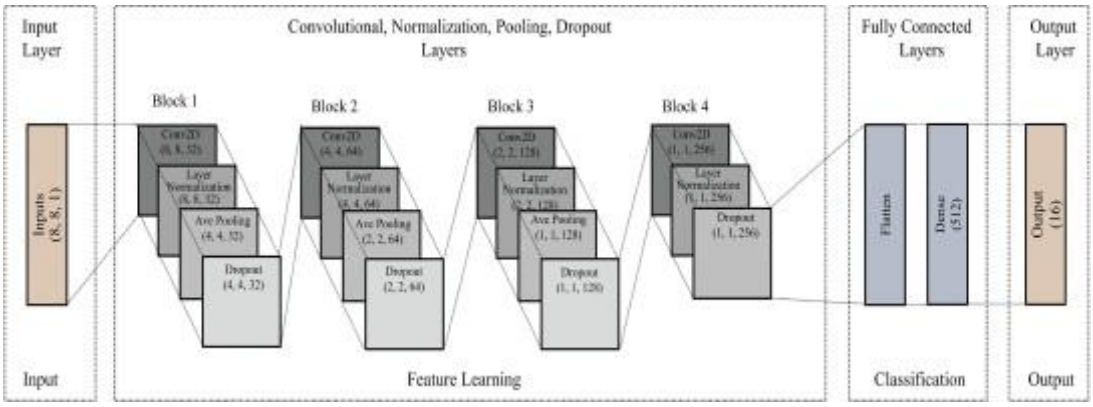
First, we trained these models for multiclass classification using IOT-Ds2 dataset in *'IOT_DS2.ipynb'* file.



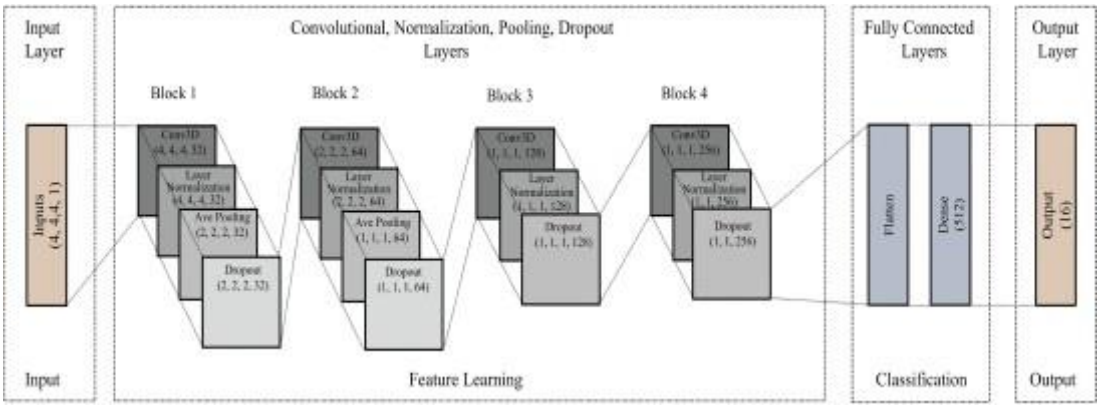
- Convolution1D Model Design



- Convolution2D Model Design



- Convolution3D Model Design



Transfer Learning:

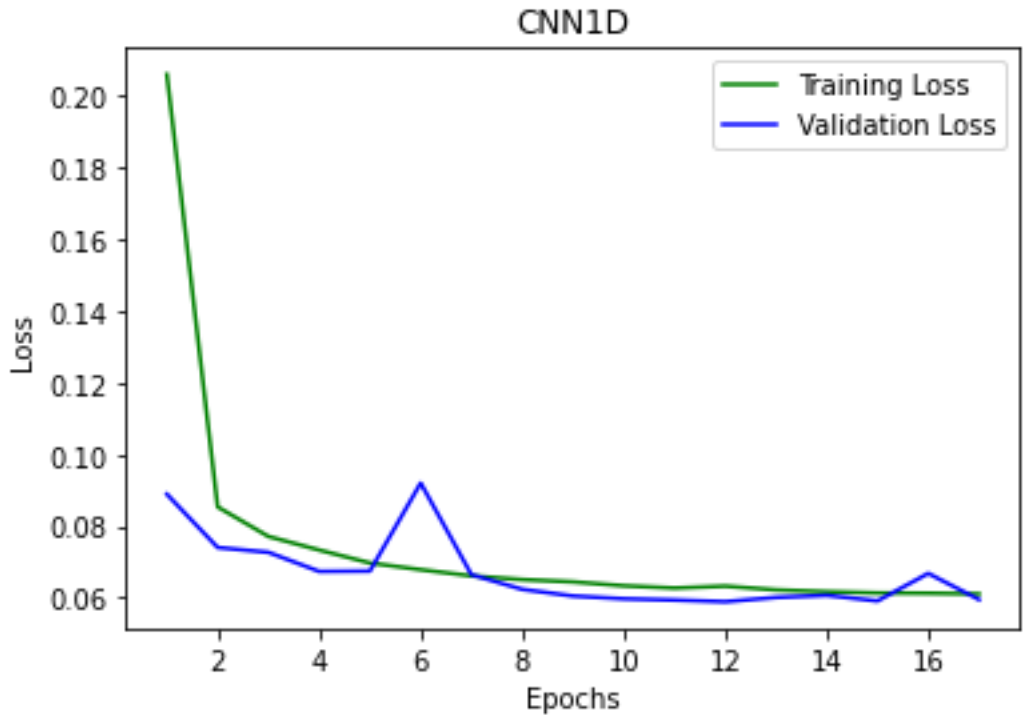
In the first phase, we used IoT-DS-2 pre-trained multiclass classification CNN1D, CNN2D, CNN3D models for the binary classification of the IoT-DS-2 dataset via the transfer learning principle in *'IOT_DS2.ipynb'* file. In the next phase, we used the same pre-trained learning model for multiclass classification of IoT Network Intrusion Dataset and binary classification of IoT Network Intrusion Dataset in *'Intrusion.ipynb'* file.

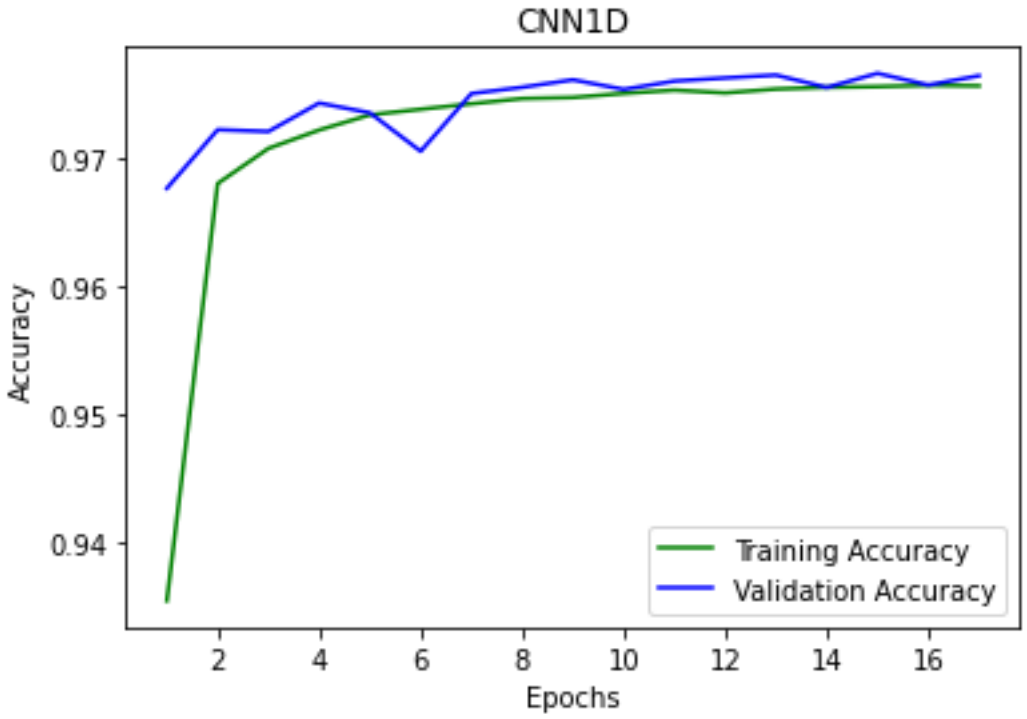
The output layer was removed from the pre-trained multiclass CNN model. we add two new dense layers to the model.

Step 5: Evaluation Results:

❖ Multiclass Classification IoT-DS-2 :-

1. **CNN1D:**



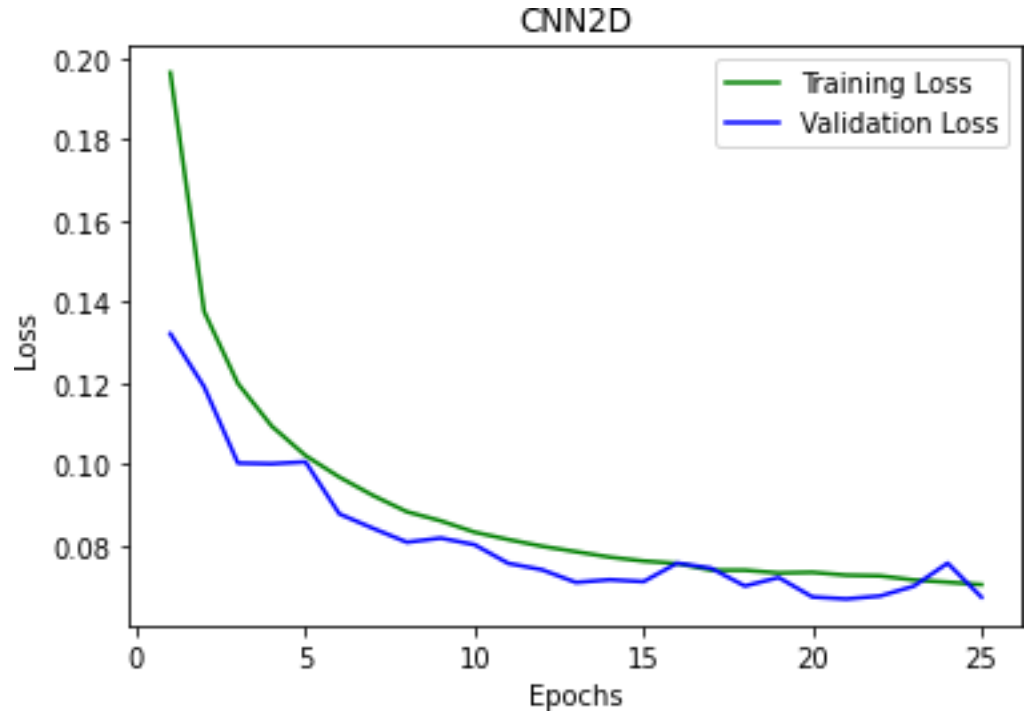


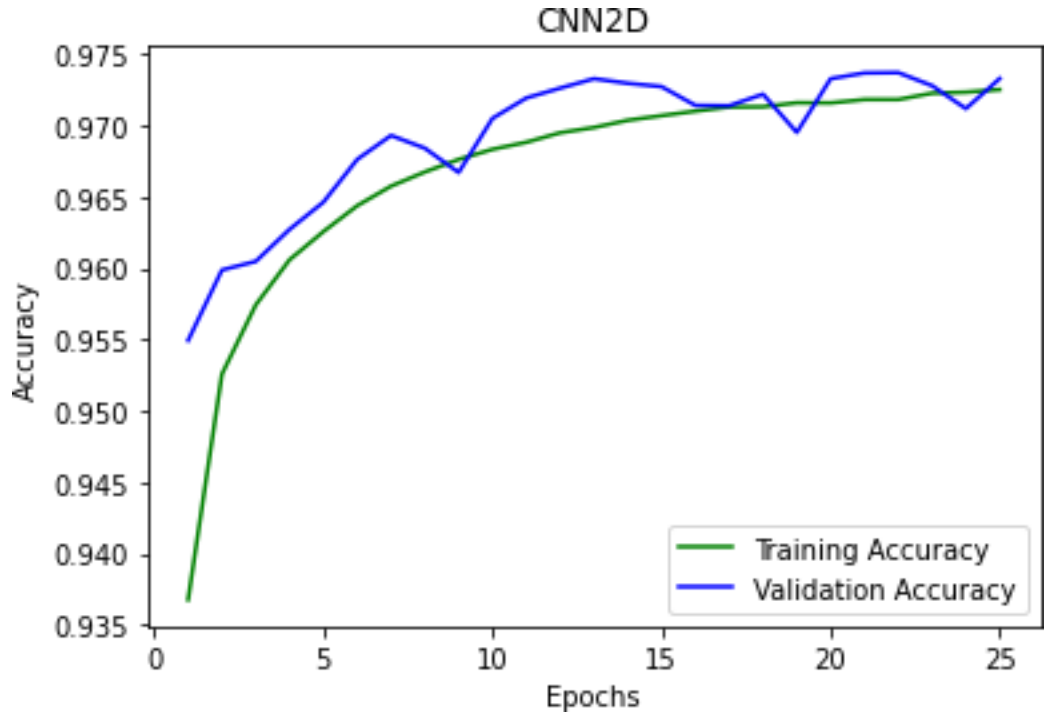

```
Testing Accuracy: 97.66

Precision: 97.28
Recall: 97.66
F1-score: 97.17
```

	precision	recall	f1-score	support
Normal	0.99	0.99	0.99	55122
DDoS	1.00	1.00	1.00	80742
DoS	0.97	0.99	0.98	4038
MITM ARP Spoofing	0.69	0.16	0.26	2035
Mirai	0.91	0.99	0.95	18424
Sparta	1.00	0.99	1.00	16458
Theft	0.99	0.98	0.98	1251
Attack	0.91	0.90	0.90	3739
C&C	0.81	0.87	0.84	4122
FileDownload	0.36	0.03	0.06	1587
HeartBeat	0.66	0.96	0.78	2530
Okiru	0.82	0.33	0.47	27
Reconnaissance	1.00	0.99	1.00	27656
Torii	1.00	1.00	1.00	414
Flood	1.00	1.00	1.00	2747
accuracy			0.98	220892
macro avg	0.87	0.81	0.81	220892
weighted avg	0.97	0.98	0.97	220892

	Category	Accuracy	TPR	TNR	FPR	FNR
0	Normal	0.996075	54705.0	165320.0	450.0	417.0
1	DDoS	0.999864	80720.0	140142.0	8.0	22.0
2	DoS	0.999307	3997.0	216742.0	112.0	41.0
3	MITM ARP Spoofing	0.991571	319.0	218711.0	146.0	1716.0
4	Mirai	0.991222	18235.0	200718.0	1750.0	189.0
5	Sparta	0.999289	16370.0	204365.0	69.0	88.0
6	Theft	0.999828	1231.0	219623.0	18.0	20.0
7	Attack	0.996759	3376.0	216800.0	353.0	363.0
8	C&C	0.993807	3603.0	215921.0	849.0	519.0
9	FileDownload	0.992634	49.0	219216.0	89.0	1538.0
10	HeartBeat	0.993843	2423.0	217109.0	1253.0	107.0
11	Okiru	0.999909	9.0	220863.0	2.0	18.0
12	Reconnaissance	0.999009	27516.0	193157.0	79.0	140.0
13	Torii	1.000000	414.0	220478.0	0.0	0.0
14	Flood	1.000000	2747.0	218145.0	0.0	0.0

2. CNN2D:





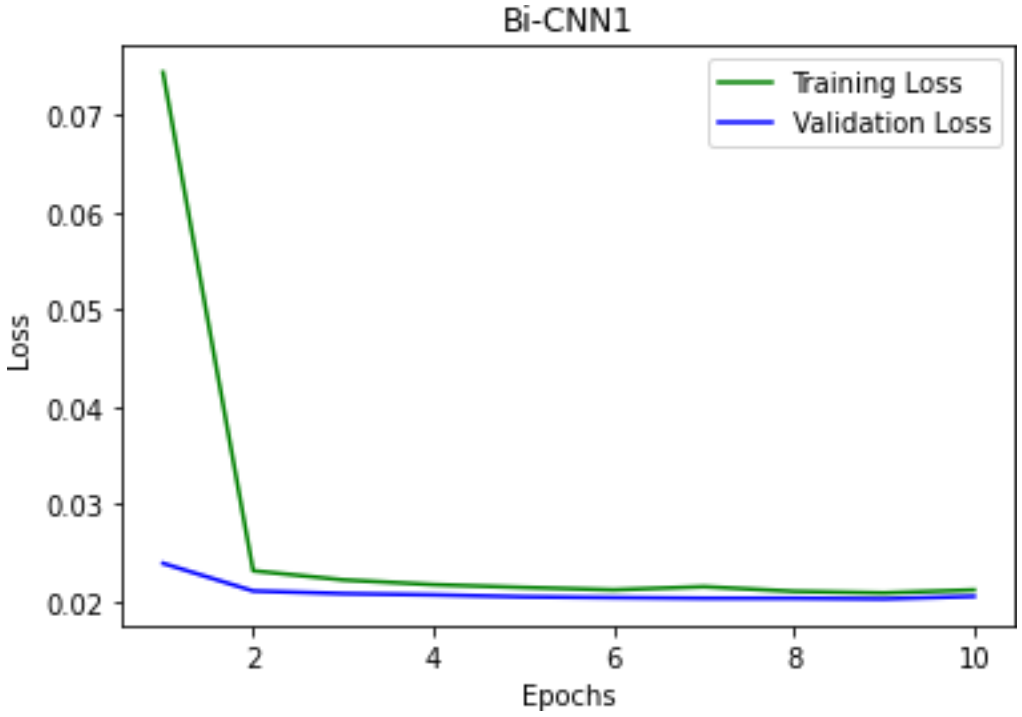

```
Testing Accuracy: 97.31

Precision: 96.96
Recall: 97.31
F1-score: 96.99
```

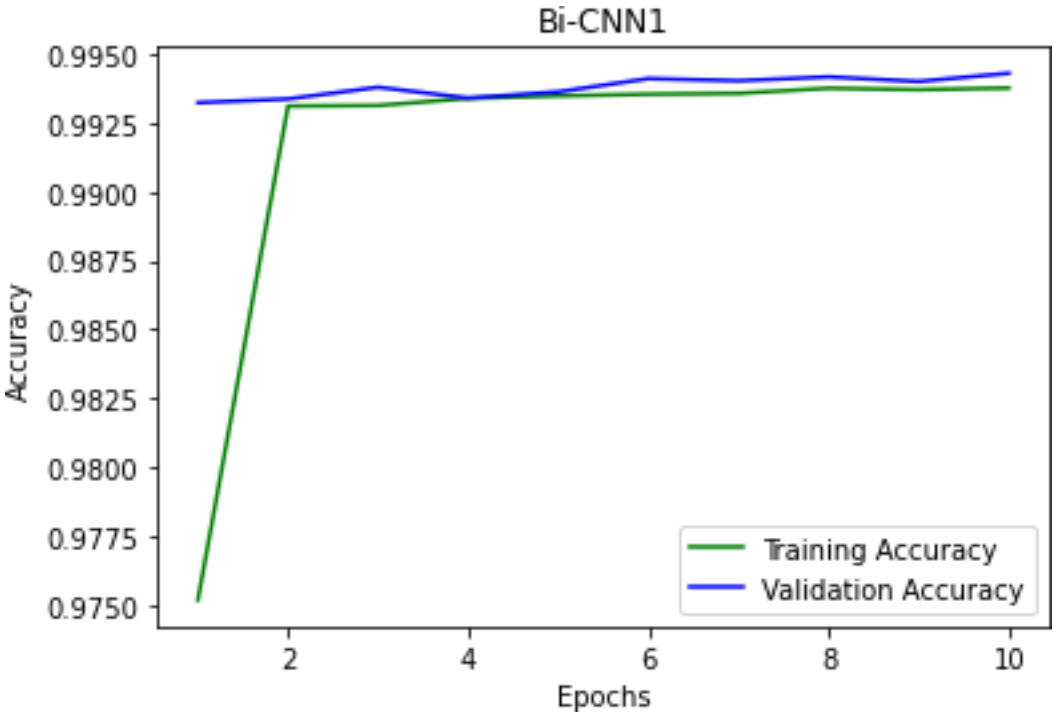
	precision	recall	f1-score	support
Normal	0.99	0.99	0.99	55122
DDoS	1.00	1.00	1.00	80742
DoS	0.93	0.98	0.95	4038
MITM ARP Spoofing	0.51	0.24	0.32	2035
Mirai	0.92	0.97	0.94	18424
Sparta	0.99	1.00	0.99	16458
Theft	0.98	0.93	0.95	1251
Attack	0.91	0.90	0.90	3739
C&C	0.81	0.87	0.84	4122
FileDownload	0.40	0.09	0.15	1587
HeartBeat	0.65	0.90	0.75	2530
Okiru	0.82	0.52	0.64	27
Reconnaissance	0.99	0.99	0.99	27656
Torii	1.00	1.00	1.00	414
Flood	1.00	1.00	1.00	2747
accuracy			0.97	220892
macro avg	0.86	0.82	0.83	220892
weighted avg	0.97	0.97	0.97	220892

	Category	Accuracy	TPR	TNR	FPR	FNR
0	Normal	0.995591	54572.0	165346.0	424.0	550.0
1	DDoS	0.999697	80694.0	140131.0	19.0	48.0
2	DoS	0.998257	3971.0	216536.0	318.0	67.0
3	MITM ARP Spoofing	0.990842	480.0	218389.0	468.0	1555.0
4	Mirai	0.990090	17849.0	200854.0	1614.0	575.0
5	Sparta	0.998660	16379.0	204217.0	217.0	79.0
6	Theft	0.999479	1160.0	219617.0	24.0	91.0
7	Attack	0.996754	3349.0	216826.0	327.0	390.0
8	C&C	0.993716	3596.0	215908.0	862.0	526.0
9	FileDownload	0.992471	145.0	219084.0	221.0	1442.0
10	HeartBeat	0.993246	2272.0	217128.0	1234.0	258.0
11	Okiru	0.999928	14.0	220862.0	3.0	13.0
12	Reconnaissance	0.997524	27314.0	193031.0	205.0	342.0
13	Torii	1.000000	414.0	220478.0	0.0	0.0
14	Flood	1.000000	2747.0	218145.0	0.0	0.0

❖ Binary Classification IOT-DS-2:

1. CNN1D:



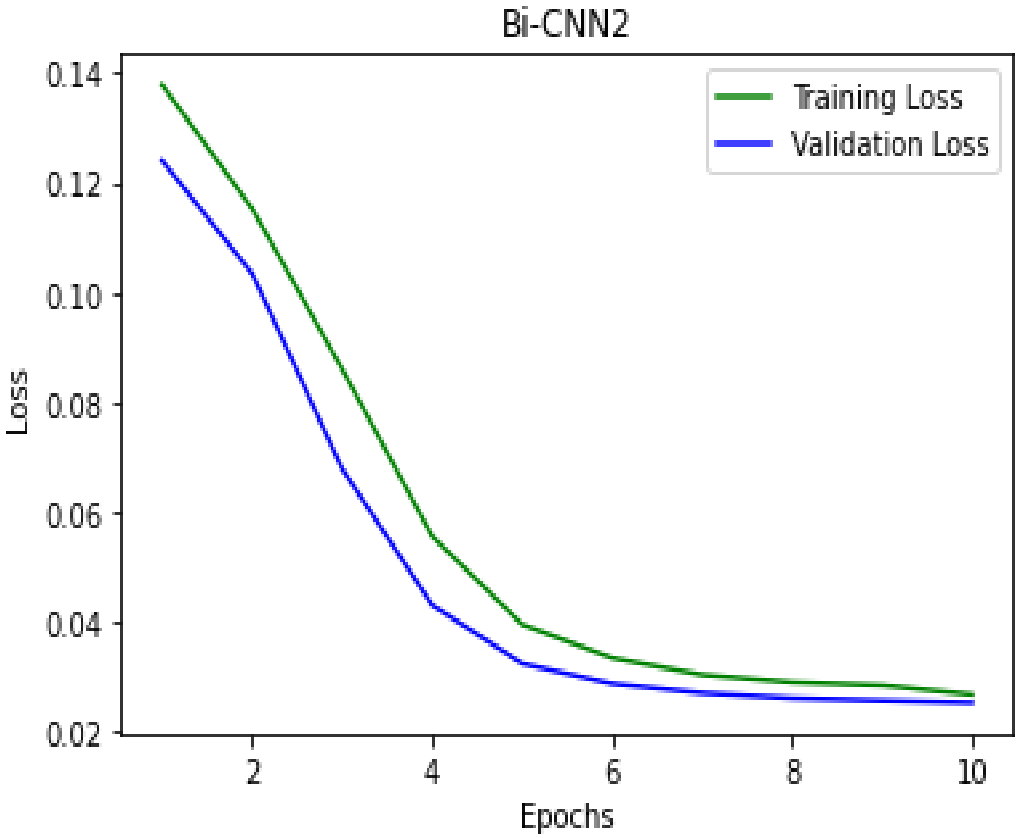


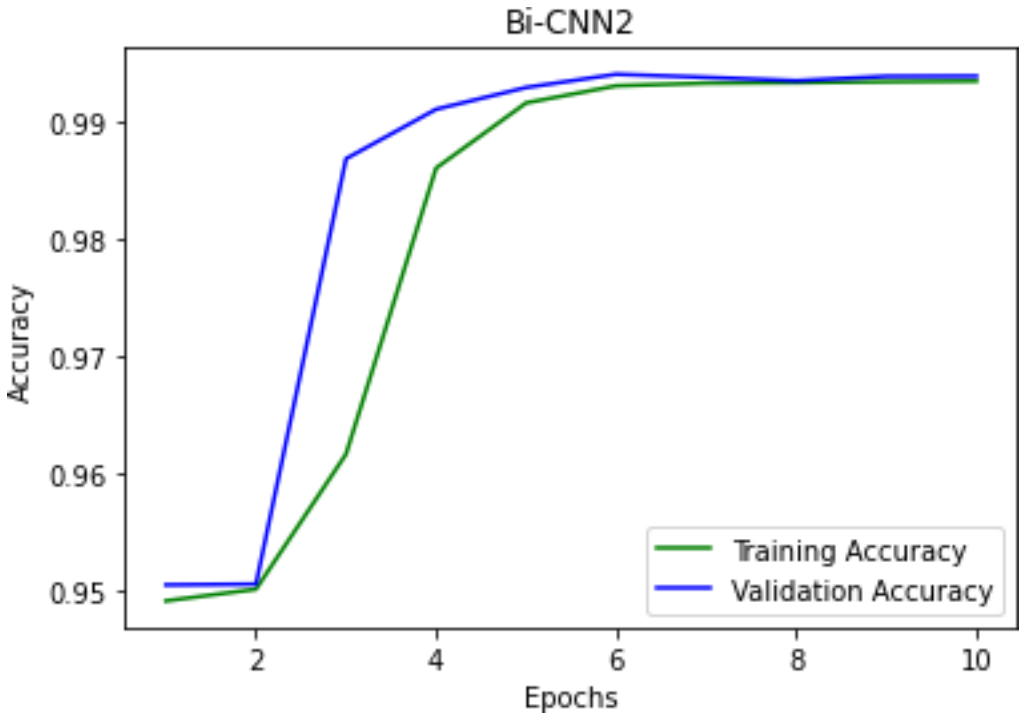

```
Testing Accuracy: 99.44

Precision: 99.44
Recall: 99.44
F1-score: 99.44
```

	precision	recall	f1-score	support
Normal	0.99	0.99	0.99	44970
Anamoly	1.00	1.00	1.00	175920
accuracy			0.99	220890
macro avg	0.99	0.99	0.99	220890
weighted avg	0.99	0.99	0.99	220890

	Category	Accuracy	TPR	TNR	FPR	FNR
0	Normal	0.994445	44315.0	175348.0	572.0	655.0
1	Anomaly	0.994445	175348.0	44315.0	655.0	572.0

2. CNN2D:





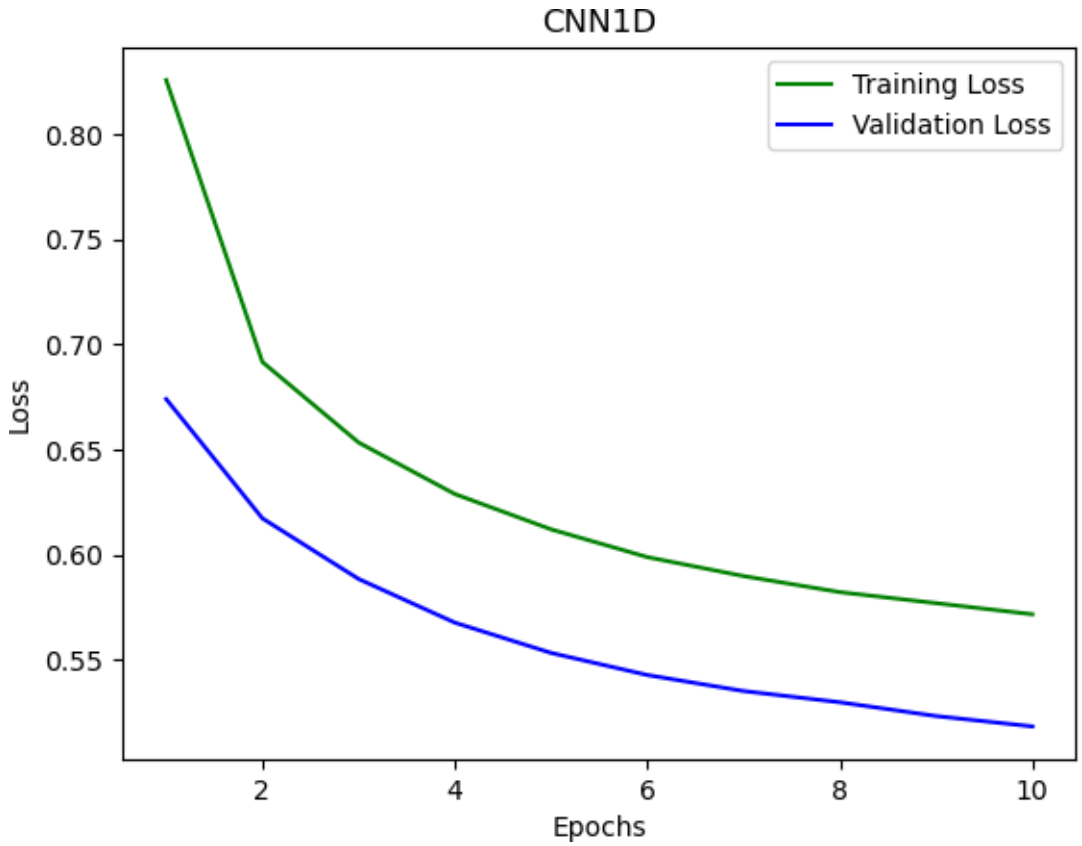

```
Testing Accuracy: 99.42

Precision: 99.41
Recall: 99.42
F1-score: 99.41
```

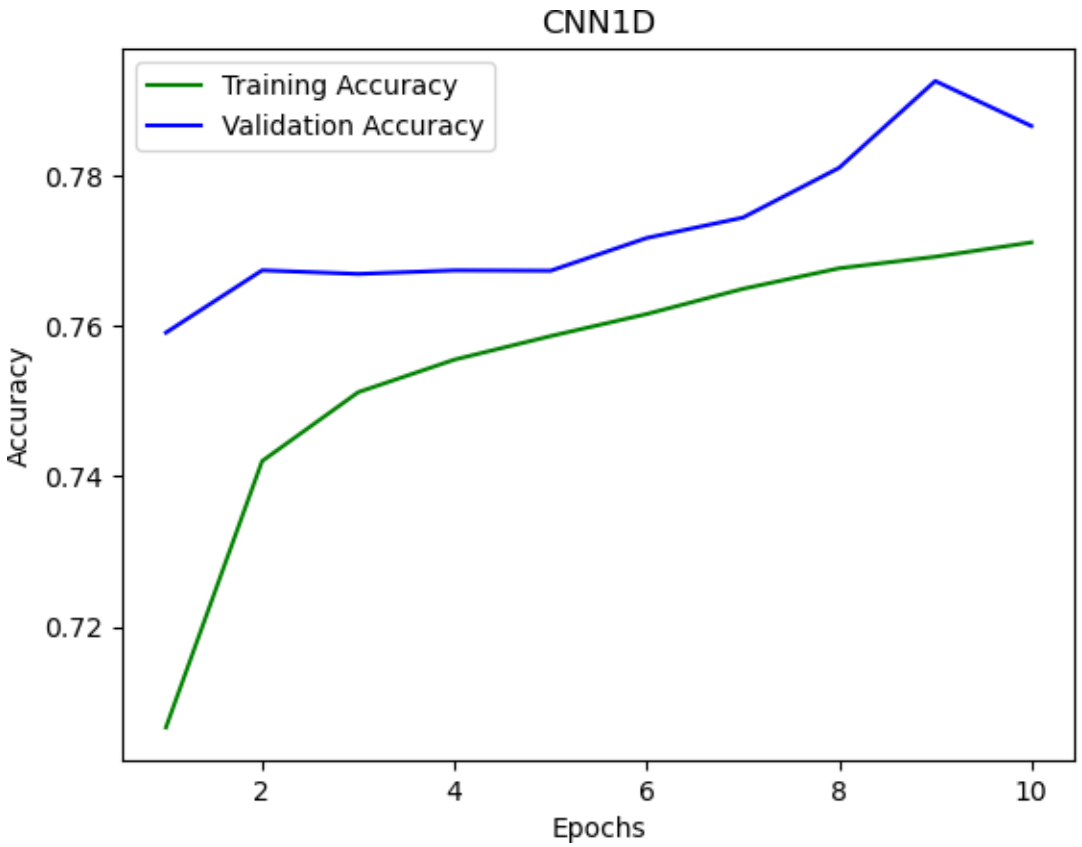
	precision	recall	f1-score	support
Normal	0.99	0.98	0.99	44970
Anamoly	1.00	1.00	1.00	175920
accuracy			0.99	220890
macro avg	0.99	0.99	0.99	220890
weighted avg	0.99	0.99	0.99	220890

	Category	Accuracy	TPR	TNR	FPR	FNR
0	Normal	0.994151	44145.0	175453.0	467.0	825.0
1	Anomaly	0.994151	175453.0	44145.0	825.0	467.0

❖ Multiclass Classification IOT Network intrusion dataset:

1. CNN1D:



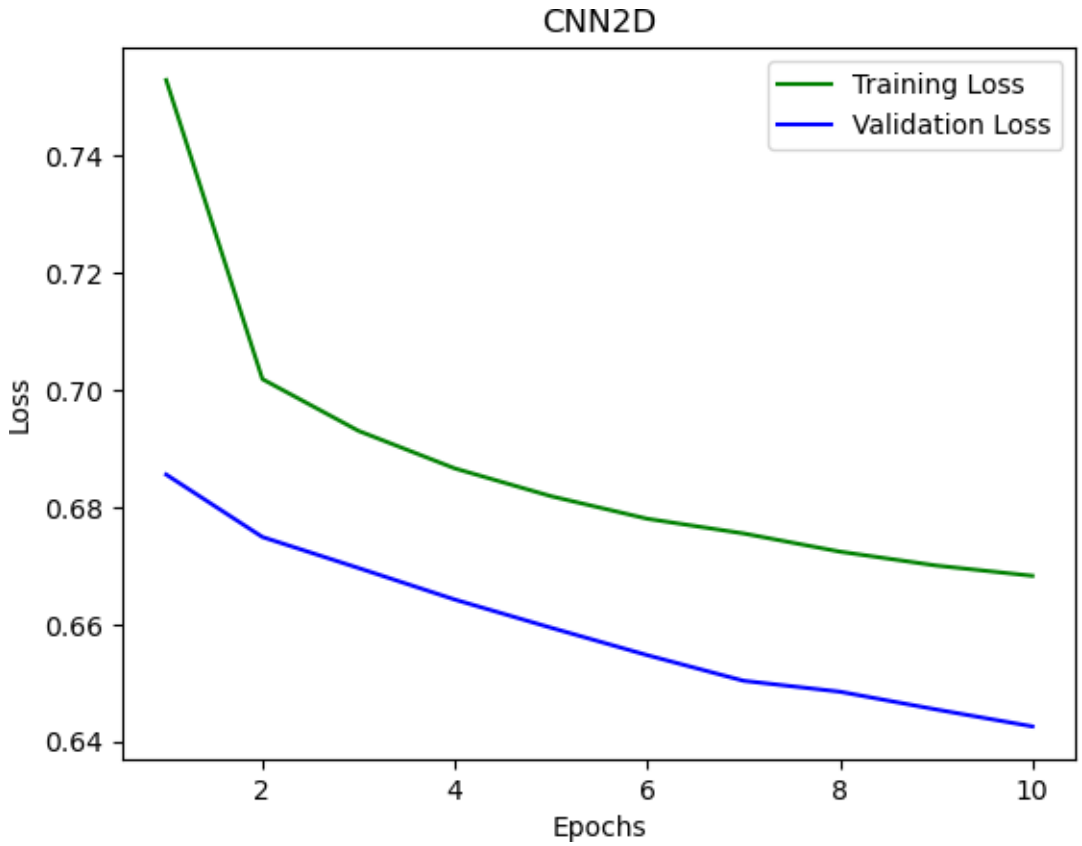


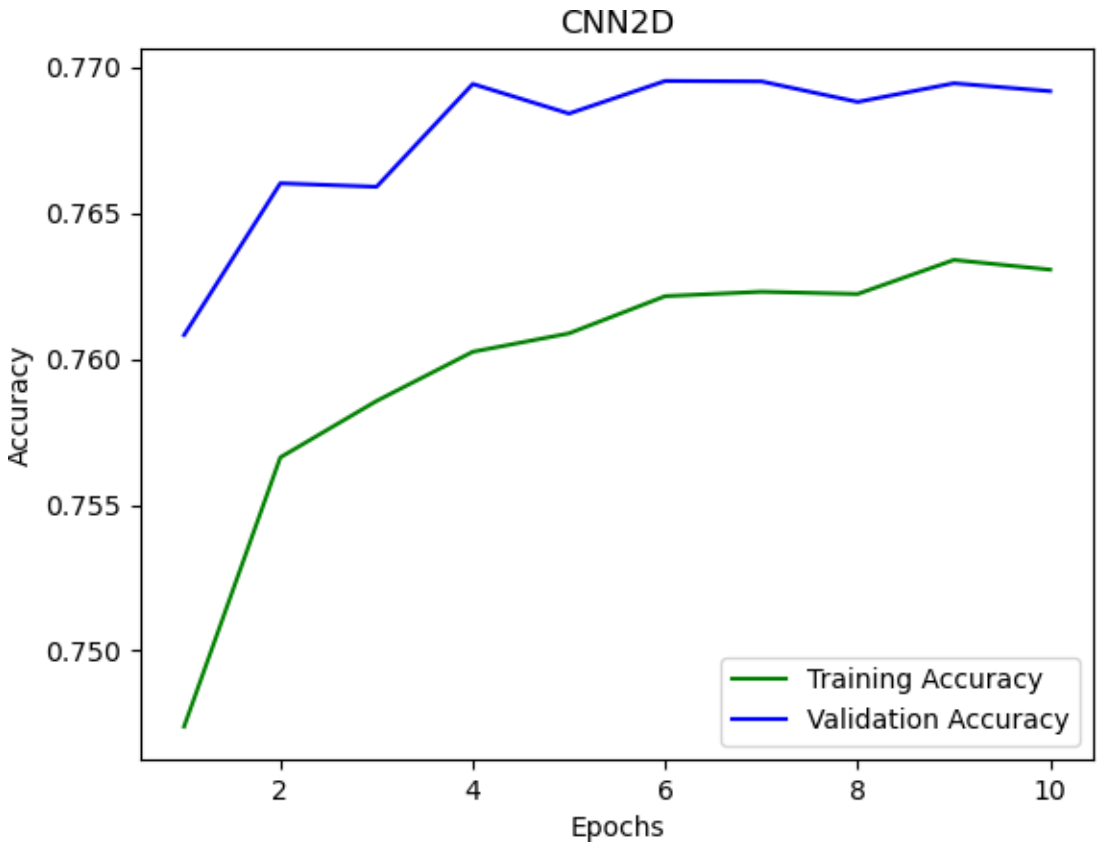
```
Testing Accuracy: 78.58

Precision: 77.76
Recall: 78.58
F1-score: 75.27
```

	precision	recall	f1-score	support
Normal	0.79	0.41	0.54	8015
Mirai	0.79	0.94	0.86	83136
DoS	1.00	0.94	0.97	11878
Scan	0.50	0.32	0.39	15053
MITM ARP Spoofing	0.86	0.08	0.15	7075
accuracy			0.79	125157
macro avg	0.79	0.54	0.58	125157
weighted avg	0.78	0.79	0.75	125157

	Category	Accuracy	TPR	TNR	FPR	FNR
0	Normal	0.955144	3296.0	116247.0	895.0	4719.0
1	Mirai	0.795529	78545.0	21021.0	21000.0	4591.0
2	DoS	0.994183	11155.0	113274.0	5.0	723.0
3	Scan	0.879312	4764.0	105288.0	4816.0	10289.0
4	MITM ARP Spoofing	0.947346	583.0	117984.0	98.0	6492.0

2. CNN2D:


CNN2D
Training Loss
Validation Loss
Loss
0.74
0.72
0.70
0.68
0.66
0.64
2
4
6
8
10
Epochs


CNN2D
Accuracy
0.770
0.765
0.760
0.755
0.750
Training Accuracy
Validation Accuracy
2
4
6
8
10
Epochs

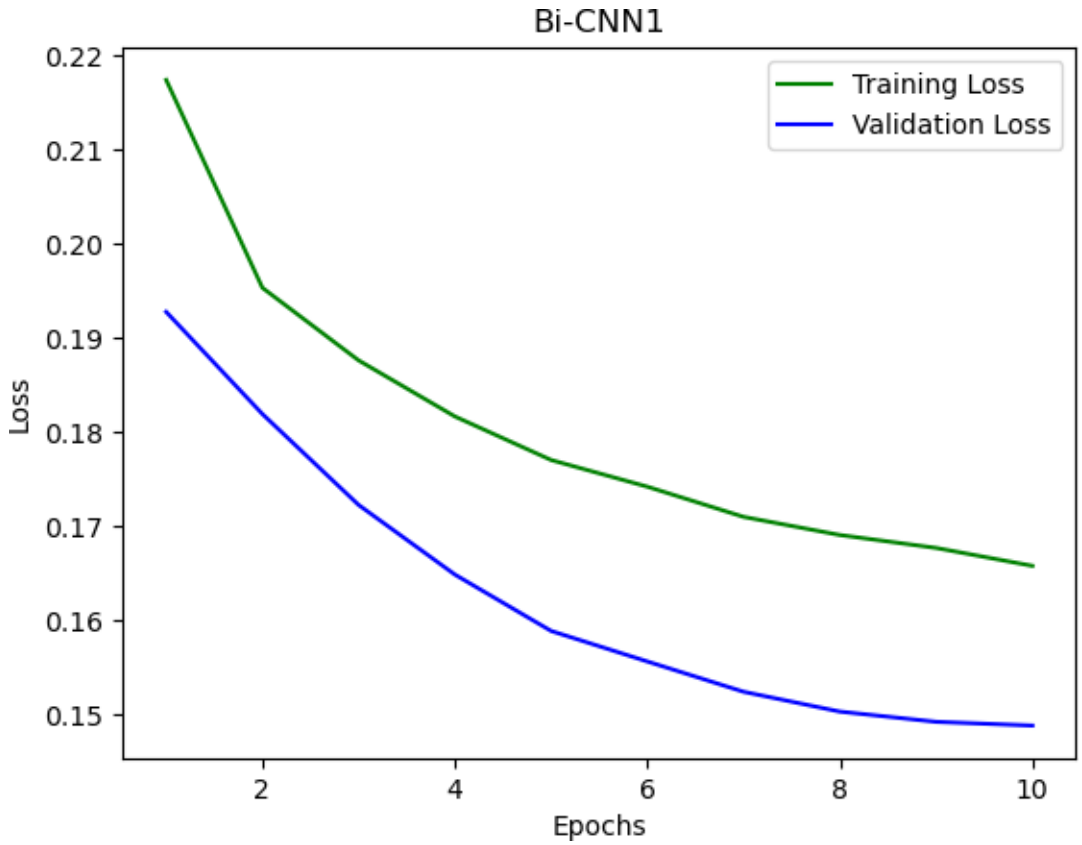
```
Testing Accuracy: 76.79

Precision: 70.15
Recall: 76.79
F1-score: 71.54
```

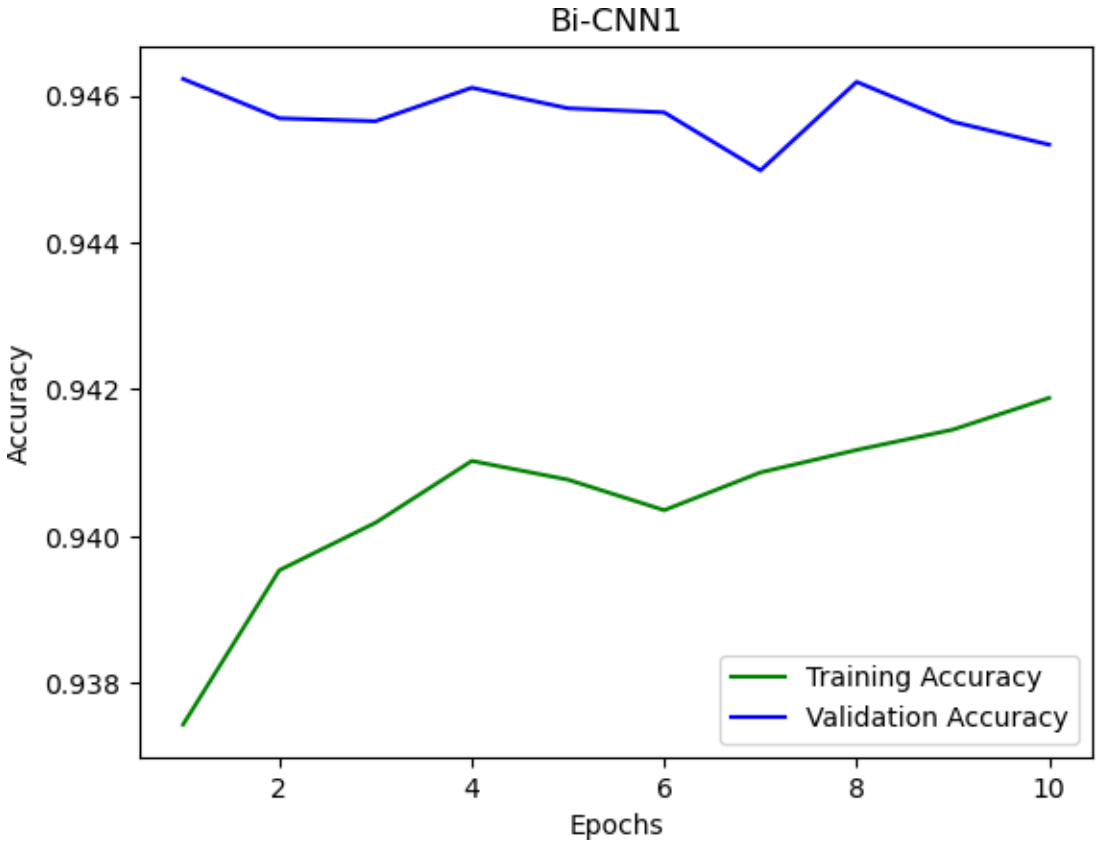
	precision	recall	f1-score	support
Normal	0.02	0.00	0.00	8015
Mirai	0.77	0.95	0.85	83136
DoS	0.99	0.99	0.99	11878
Scan	0.47	0.27	0.34	15053
MITM ARP Spoofing	0.69	0.17	0.28	7075
accuracy			0.77	125157
macro avg	0.59	0.48	0.49	125157
weighted avg	0.70	0.77	0.72	125157

	Category	Accuracy	TPR	TNR	FPR	FNR
0	Normal	0.935585	1.0	117094.0	48.0	8014.0
1	Mirai	0.777647	79170.0	18158.0	23863.0	3966.0
2	DoS	0.998098	11712.0	113207.0	72.0	166.0
3	Scan	0.875772	4008.0	105601.0	4503.0	11045.0
4	MITM ARP Spoofing	0.948776	1222.0	117524.0	558.0	5853.0

❖ Binary Classification IOT Network intrusion dataset:

1. CNN1D:



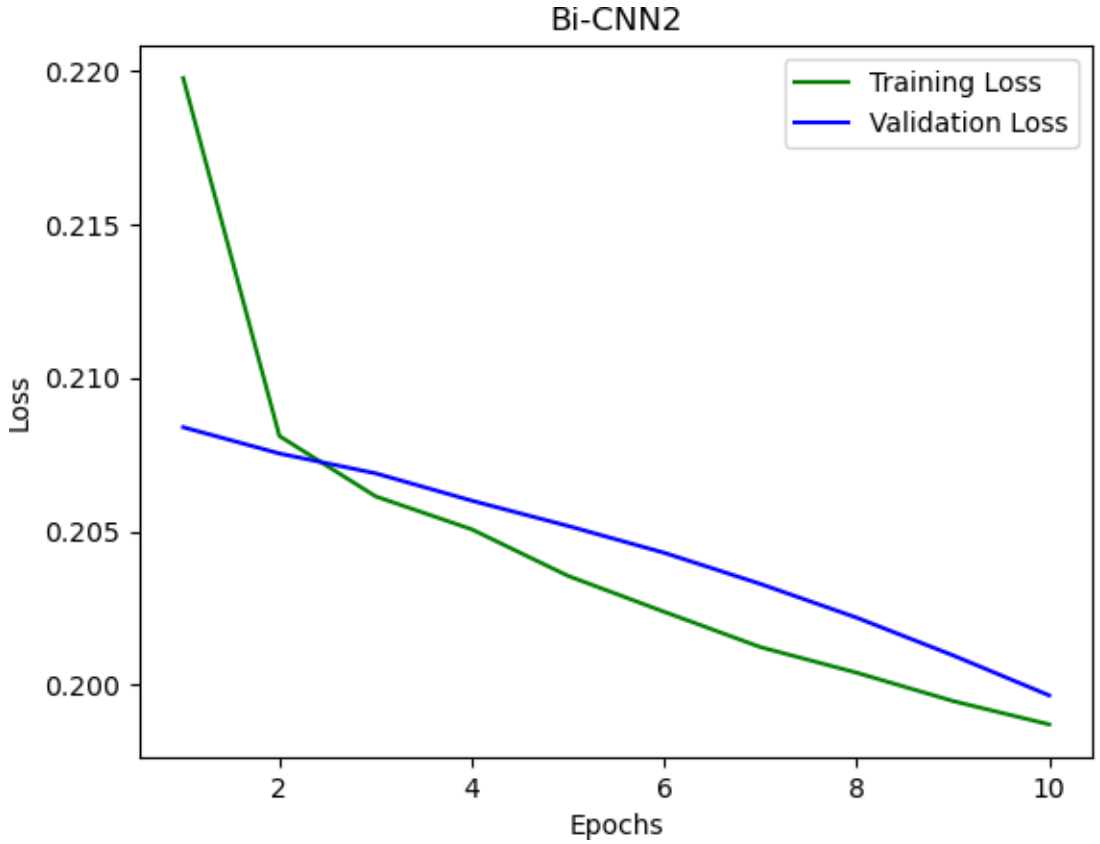


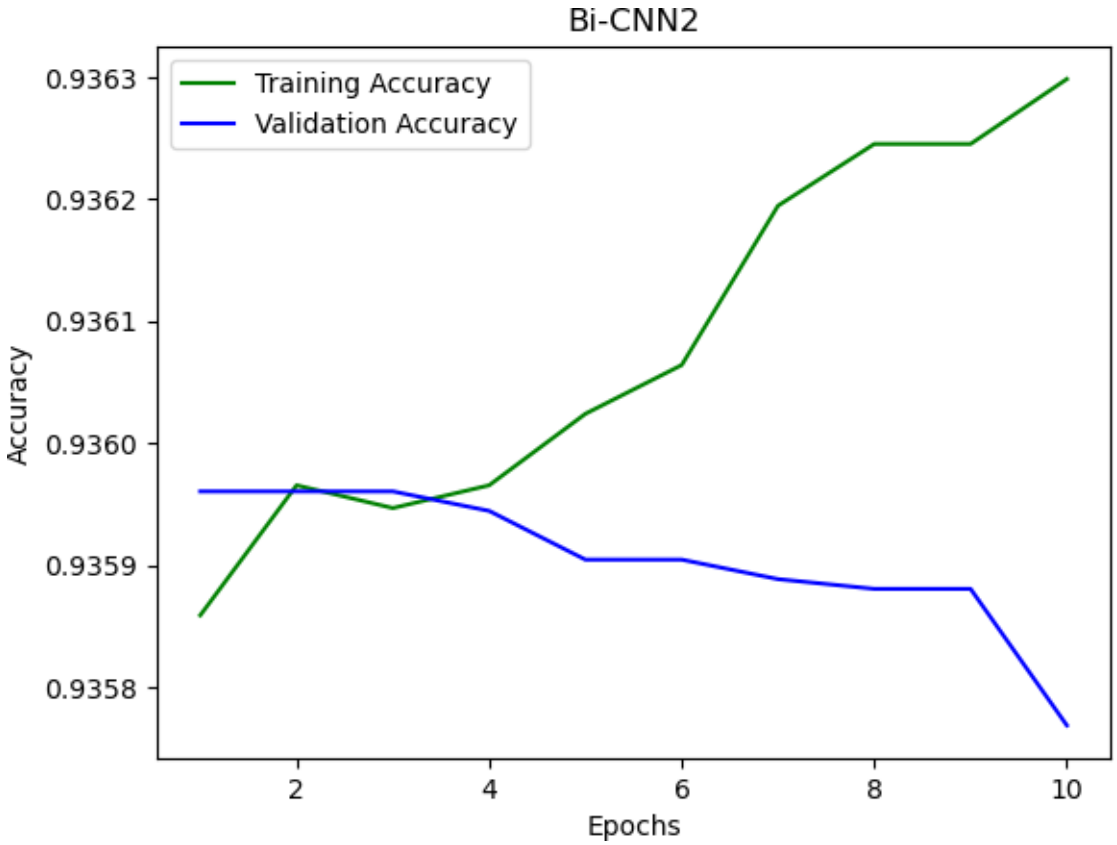
```
Testing Accuracy: 94.55

Precision: 93.60
Recall: 94.55
F1-score: 93.21
```

	precision	recall	f1-score	support
Normal	0.73	0.23	0.36	8015
Anamoly	0.95	0.99	0.97	117142
accuracy			0.95	125157
macro avg	0.84	0.61	0.66	125157
weighted avg	0.94	0.95	0.93	125157

	Category	Accuracy	TPR	TNR	FPR	FNR
0	Normal	0.9455	1878.0	116458.0	684.0	6137.0
1	Anomaly	0.9455	116458.0	1878.0	6137.0	684.0

2. CNN2D:


Bi-CNN2
Training Loss
Validation Loss
Loss
0.220
0.215
0.210
0.205
0.200
2
4
6
8
10
Epochs


Bi-CNN2
Training Accuracy
Validation Accuracy
Accuracy
0.9363
0.9362
0.9361
0.9360
0.9359
0.9358
2
4
6
8
10
Epochs

```
Testing Accuracy: 93.57

Precision: 87.60
Recall: 93.57
F1-score: 90.49
```

	precision	recall	f1-score	support
Normal	0.00	0.00	0.00	8015
Anamoly	0.94	1.00	0.97	117142
accuracy			0.94	125157
macro avg	0.47	0.50	0.48	125157
weighted avg	0.88	0.94	0.90	125157

	Category	Accuracy	TPR	TNR	FPR	FNR
0	Normal	0.935665	0.0	117105.0	37.0	8015.0
1	Anomaly	0.935665	117105.0	0.0	8015.0	37.0