Machine Learning Based Adaptive Cybersecurity Incident Detection

---

Progress report: 40%

Thanawat Tejapijaya
Krittawat Thongnoppakao
Punyawat Jaroensiripong

Karin Sumongkayothin, Ph.D (Main-Advisor)
Suratose Tritilanunt, Ph.D (Co-Advisor)
Konglit Hunchangsith, Ph.D (Co-Advisor)
Prarinya Siritanawan, Ph.D (JAIST-Advisor)

Introduction

- Research Papers Review
  - Machine Learning Anomaly detection Method Review
  - Anomaly detection using Hilbert's Curve flow-to-image and CNN method review
  - MAD-GAN review
  - Paper Implementation
- Proposed Method

Anomaly detection Method Review

- Classical Machine Learning (Supervised Learning)
  - Z. K. MASEER et al. have shown the comparison in the classical machine learning model on CIC-IDS2017 dataset with multi-attack classification. (Attack type e.g. Normal, Brute Fource, XSS, SQL Injection etc.)

	Model	Accuracy	F1-Score	Precision	Recall
1	K-Nearest Neighbors (KNN)	99.52%	99.49%	99.49%	99.52%
2	Decision tree (DT)	99.49%	99.42%	99.43%	99.49%
3	Naïve Bayes (NB)	98.86%	98.85%	99.01%	98.86%

Top 3 Supervised ML models with CIC-IDS2017

Anomaly detection Method Review

- Classical Machine Learning (Unsupervised Learning)
    - Z. K. MASEER et al. have shown the comparison in the classical machine learning model on CIC-IDS2017 dataset with multi-attack classification. (Attack type e.g. Normal, Brute Fource, XSS, SQL Injection, etc.)

	Model	Accuracy	F1-Score	Precision	Recall
1	Expectation-Maximization (EM)	60.06%	74.11%	86.88%	60.06%
2	Self Organizing Maps (SOM)	59.06%	74.11%	85.88%	60.00%
3	K-means	25.59%	39.96%	97.47%	25.59%

Top 3 Unsupervised ML models with CIC-IDS2017

Anomaly detection Method Review

- Deep Learning
  - J. Jose et al. have shown the comparison in Deep neural network, Long short-term memory (LSTM) and Convolutional Neural Network (CNN) on CIC-IDS2017 and other network attacks (e.g. NSL-KDD).

	Model	Accuracy	F1-Score	Precision	Recall
1	Long short-term memory (LSTM)	97.67%	93.55%	94.96%	95.95%
2	Convolutional Neural Network (CNN)	99.61%	93.09%	97.05%	95.00%
3	Deep neural network	90.61%	84.60%	80.85%	84.60%

Deep Learning models with CIC-IDS2017 dataset

Anomaly detection Method Review

- P. S. Muhuri et al. have shown the performace of the LSTM on NSL-KDD

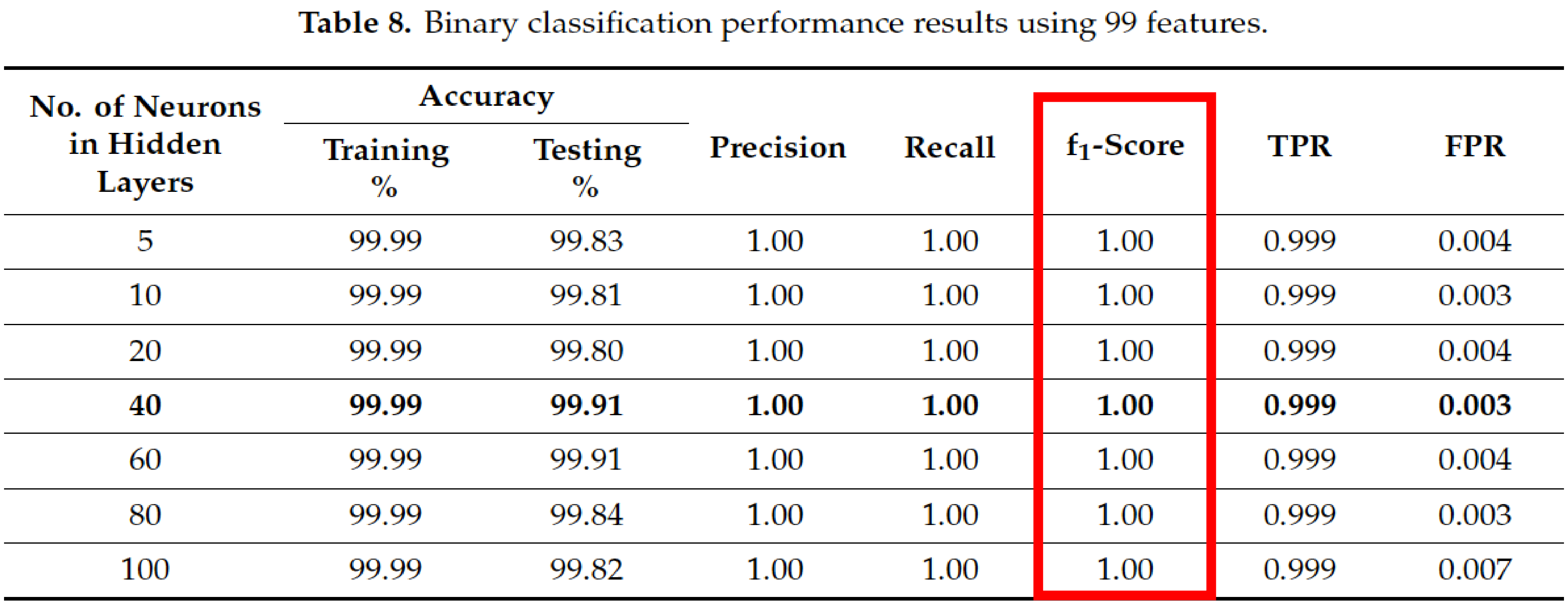
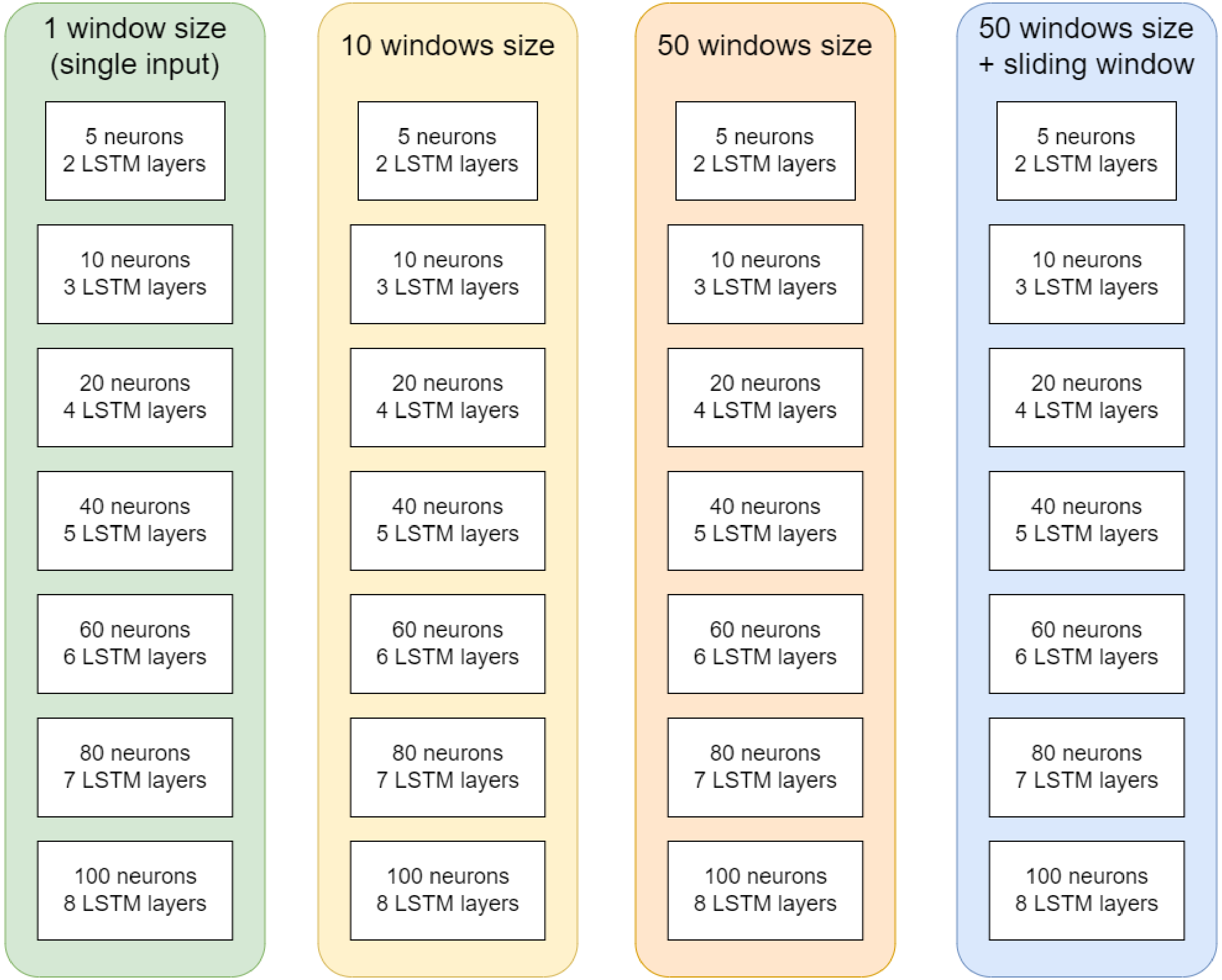


Table 8. Binary classification performance results using 99 features.

No. of Neurons in Hidden Layers	Accuracy		Precision	Recall	f_1-Score	TPR	FPR
	Training %	Testing %					
5	99.99	99.83	1.00	1.00	1.00	0.999	0.004
10	99.99	99.81	1.00	1.00	1.00	0.999	0.003
20	99.99	99.80	1.00	1.00	1.00	0.999	0.004
40	**99.99**	**99.91**	**1.00**	**1.00**	**1.00**	**0.999**	**0.003**
60	99.99	99.91	1.00	1.00	1.00	0.999	0.004
80	99.99	99.84	1.00	1.00	1.00	0.999	0.003
100	99.99	99.82	1.00	1.00	1.00	0.999	0.007

Reference : Using a long short-term memory recurrent neural network (LSTM-RNN) to classify network attacks (PS. Muhuri et al., 2020)

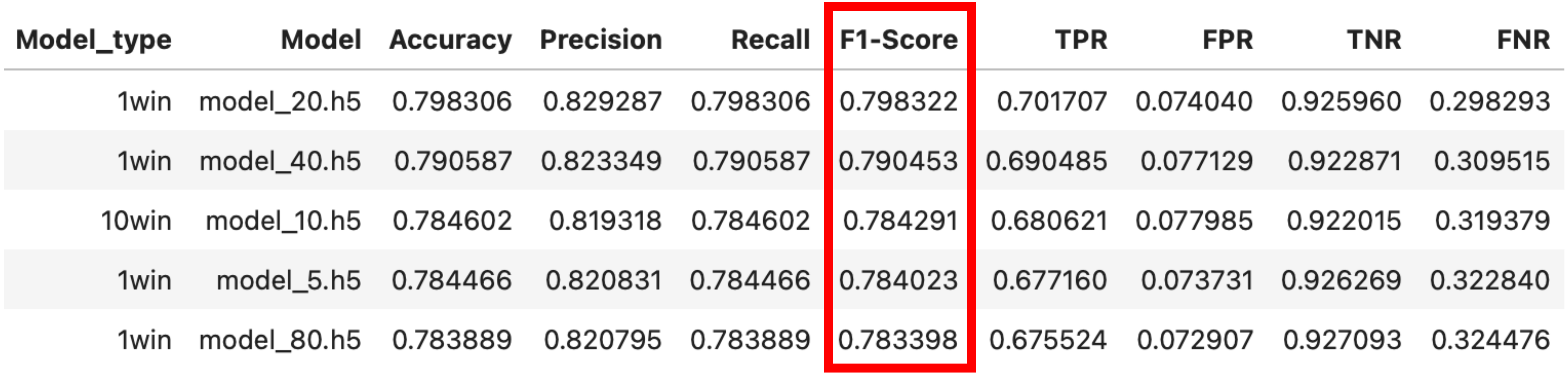


1 window size (single input)	10 windows size	50 windows size	50 windows size + sliding window
5 neurons 2 LSTM layers	5 neurons 2 LSTM layers	5 neurons 2 LSTM layers	5 neurons 2 LSTM layers
10 neurons 3 LSTM layers	10 neurons 3 LSTM layers	10 neurons 3 LSTM layers	10 neurons 3 LSTM layers
20 neurons 4 LSTM layers	20 neurons 4 LSTM layers	20 neurons 4 LSTM layers	20 neurons 4 LSTM layers
40 neurons 5 LSTM layers	40 neurons 5 LSTM layers	40 neurons 5 LSTM layers	40 neurons 5 LSTM layers
60 neurons 6 LSTM layers	60 neurons 6 LSTM layers	60 neurons 6 LSTM layers	60 neurons 6 LSTM layers
80 neurons 7 LSTM layers	80 neurons 7 LSTM layers	80 neurons 7 LSTM layers	80 neurons 7 LSTM layers
100 neurons 8 LSTM layers	100 neurons 8 LSTM layers	100 neurons 8 LSTM layers	100 neurons 8 LSTM layers

Overall detail with the implemented models

Paper Implementation- Result

- Top 5 models that have the best F1-Score
- F1-Score is the harmonic mean between Precision and Recall



Model_type	Model	Accuracy	Precision	Recall	F1-Score	TPR	FPR	TNR	FNR
1win	model_20.h5	0.798306	0.829287	0.798306	0.798322	0.701707	0.074040	0.925960	0.298293
1win	model_40.h5	0.790587	0.823349	0.790587	0.790453	0.690485	0.077129	0.922871	0.309515
10win	model_10.h5	0.784602	0.819318	0.784602	0.784291	0.680621	0.077985	0.922015	0.319379
1win	model_5.h5	0.784466	0.820831	0.784466	0.784023	0.677160	0.073731	0.926269	0.322840
1win	model_80.h5	0.783889	0.820795	0.783889	0.783398	0.675524	0.072907	0.927093	0.324476

The evaluation from the paper.

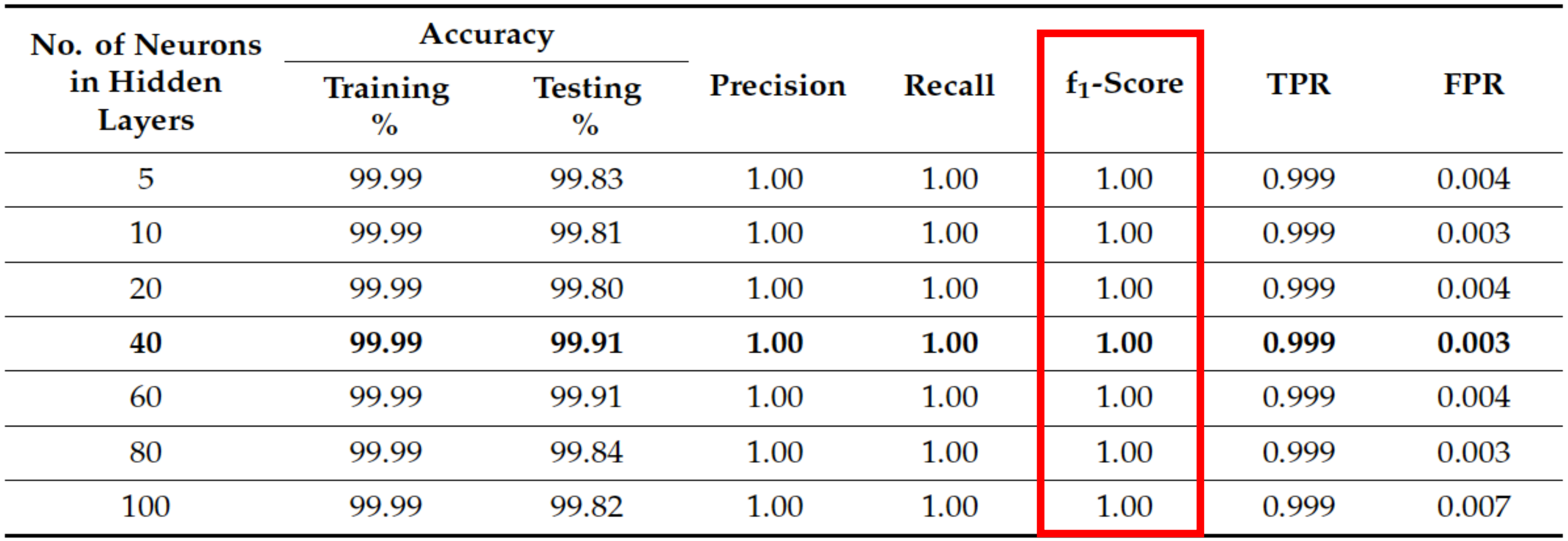
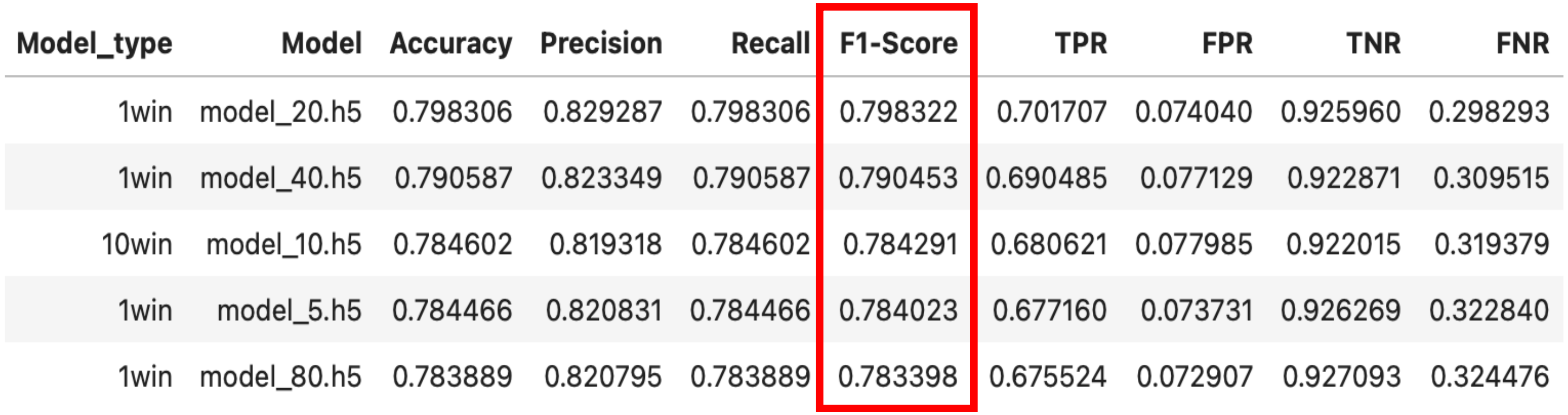


Table 8. Binary classification performance results using 99 features.

No. of Neurons in Hidden Layers	Accuracy		Precision	Recall	f_1-Score	TPR	FPR
	Training %	Testing %					
5	99.99	99.83	1.00	1.00	1.00	0.999	0.004
10	99.99	99.81	1.00	1.00	1.00	0.999	0.003
20	99.99	99.80	1.00	1.00	1.00	0.999	0.004
40	**99.99**	**99.91**	**1.00**	**1.00**	**1.00**	**0.999**	**0.003**
60	99.99	99.91	1.00	1.00	1.00	0.999	0.004
80	99.99	99.84	1.00	1.00	1.00	0.999	0.003
100	99.99	99.82	1.00	1.00	1.00	0.999	0.007

The evaluation by implementation.



Model_type	Model	Accuracy	Precision	Recall	F1-Score	TPR	FPR	TNR	FNR
1win	model_20.h5	0.798306	0.829287	0.798306	0.798322	0.701707	0.074040	0.925960	0.298293
1win	model_40.h5	0.790587	0.823349	0.790587	0.790453	0.690485	0.077129	0.922871	0.309515
10win	model_10.h5	0.784602	0.819318	0.784602	0.784291	0.680621	0.077985	0.922015	0.319379
1win	model_5.h5	0.784466	0.820831	0.784466	0.784023	0.677160	0.073731	0.926269	0.322840
1win	model_80.h5	0.783889	0.820795	0.783889	0.783398	0.675524	0.072907	0.927093	0.324476

Anomaly detection using Hilbert Curve technique and Convolutional Neural Network (CNN) method review

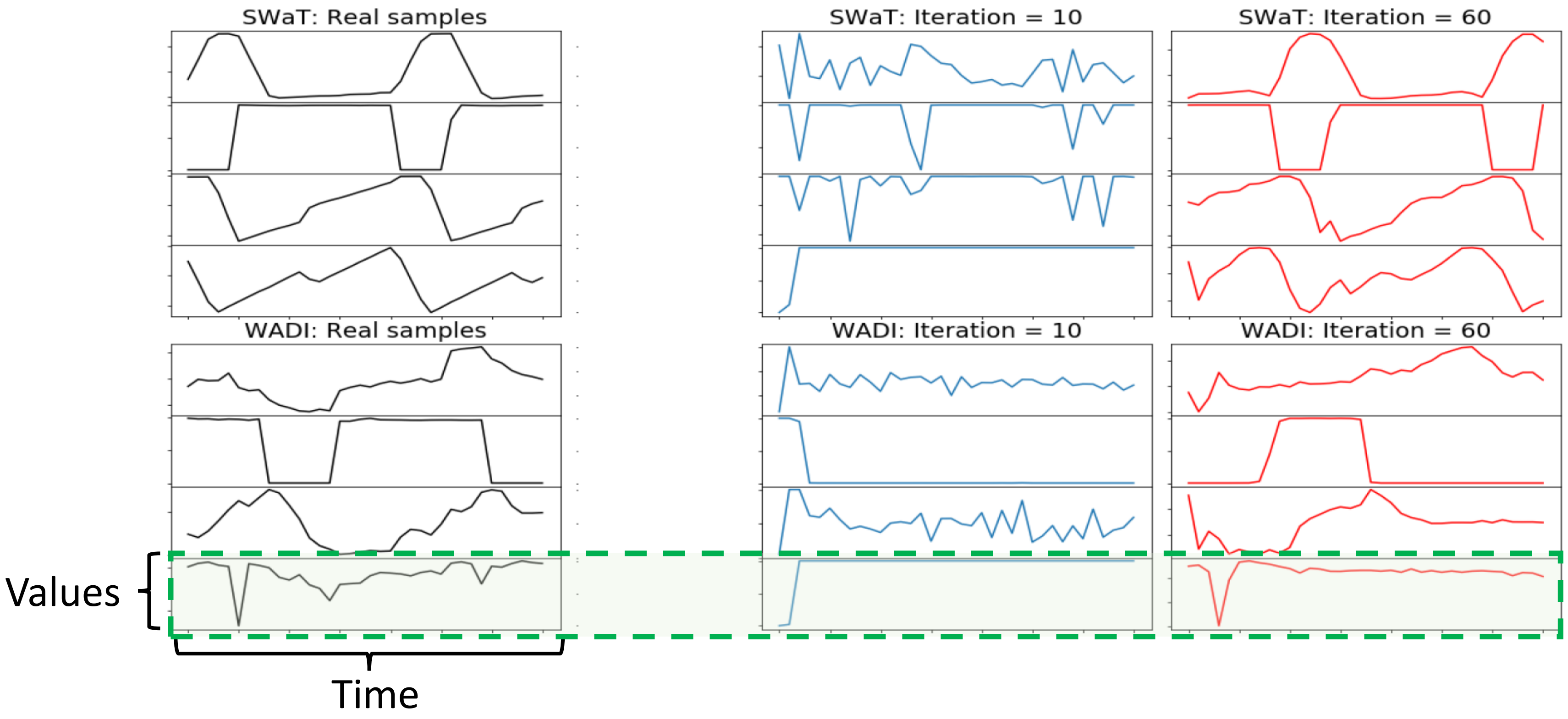
- P. Jaroensiripong has shown the potential of CNN, the image classification model to detect intrusion from image of network flow which training on 2 dataset

Dataset	Accuracy	F1-Score	Precision	Recall
NSL-KDD	77.87%	77.82%	90.63%	68.18%
CIC-IDS2017	91.52%	92.01%	93.73%	90.36%

Result of the CNN image classification model by Hilbert curve network flow to image technique

Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks review

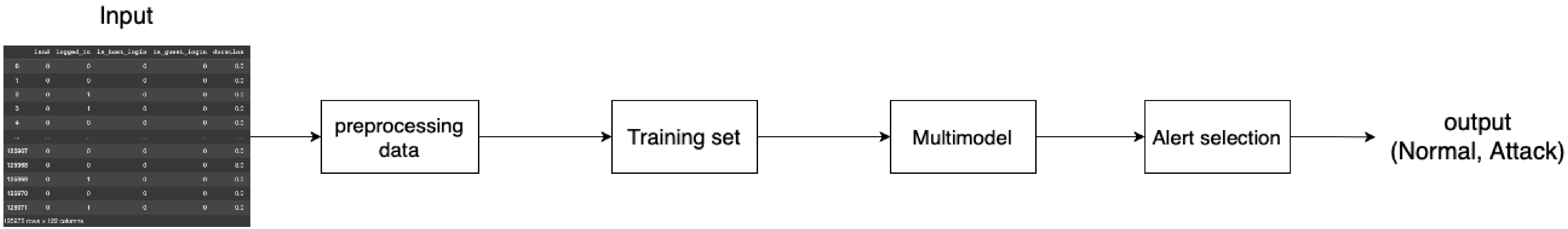
- To generate data samples and to detect anomalies in Cyber-Physical Systems (CPSs) with Generative Adversarial Networks (GANs) based on LSTM-RNN using multivariate time series data generated by the systems.



Comparison between generated samples at different training stages

Proposed Anomaly detection Method

- Idea came from ensemble machine learning method
- Each model will be trained by different type of cyber attack
- Integrate every trained model to predict one result

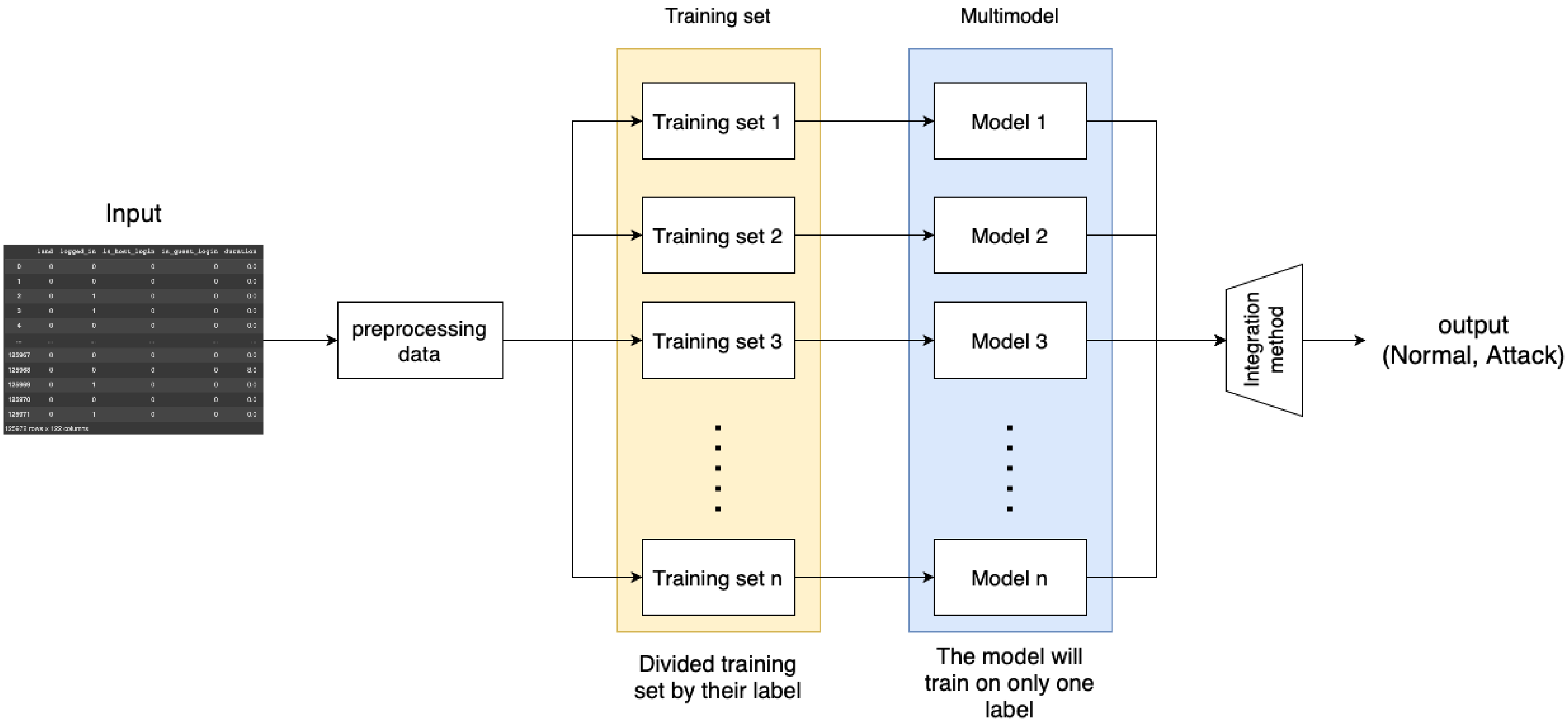


	land	logged_in	is_host_login	is_guest_login	duration
0	0	0	0	0	0.0
1	0	0	0	0	0.0
2	0	1	0	0	0.0
3	0	1	0	0	0.0
4	0	0	0	0	0.0
...	...	...	...	...	...
125967	0	0	0	0	0.0
125968	0	0	0	0	0.0
125969	0	1	0	0	0.0
125970	0	0	0	0	0.0
125971	0	1	0	0	0.0

125973 rows × 122 columns

Model training methodology

Overall Model



	land	logged_in	is_host_login	is_guest_login	duration
0	0	0	0	0	0.0
1	0	0	0	0	0.0
2	0	1	0	0	0.0
3	0	1	0	0	0.0
4	0	0	0	0	0.0
...	...	...	...	...	...
125967	0	0	0	0	0.0
125968	0	0	0	0	0.0
125969	0	1	0	0	0.0
125970	0	0	0	0	0.0
125971	0	1	0	0	0.0

125972 rows × 122 columns

Divided training set by their label

The model will train on only one label

Thank You