



**PENDETEKSIAN SERANGAN
*IOT BOTNET TIDAK DIKENAL DENGAN
UNSUPERVISED COMPETITIVE LEARNING***



SAID FAUZUL RUSNAIDI

NIM: 55419110011

**PROGRAM MAGISTER TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS MERCU BUANA
2021**



**PENDETEKSIAN SERANGAN
IOT BOTNET TIDAK DIKENAL DENGAN
*UNSUPERVISED COMPETITIVE LEARNING***

TESIS

**Diajukan sebagai Salah Satu Syarat untuk Menyelesaikan
Program Studi Magister Teknik**

OLEH

SAID FAUZUL RUSNAIDI

NIM: 55419110011

PROGRAM MAGISTER TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS MERCU BUANA

2021

ABSTRAK

Pemanfaatan perangkat *IoT* sebagai *Robot Network (IoT Botnet)* merupakan ancaman serius pada *cybersecurity*. Hal tersebut tidak terlepas dari pertumbuhan perangkat *IoT* yang dilengkapi dengan teknologi komunikasi dan sistem komputasi yang canggih, namun tidak diiringi dengan kuatnya system keamanan yang diterapkan. Untuk mengantisipasi cepatnya pertumbuhan perangkat *IoT* dan/atau jenis *Botnet* di waktu yang akan datang, dibutuhkan penelitian untuk pendeteksian *IoT Botnet* pada perangkat *IoT* dan/atau jenis *Botnet* baru yang tidak dikenali sebelumnya (*Unknown Attack*). Dalam penelitian ini diusulkan pendeteksian *IoT Botnet* tidak dikenal menggunakan pendekatan *Unsupervised Learning* yang diterapkan pada metode pembelajaran berbasis *Competitive Learning* (pada penelitian ini disebut dengan *Unsupervised Competitive Learning*). Pengujian dilakukan dengan metode *Learning Vector Quantization (LVQ)* dan memanfaatkan dataset *N-BaIoT: Data for network based detection of IoT botnet attack*, yang menyediakan data *real traffic* dari 9 perangkat *IoT* komersial yang telah diinfeksi *Bashlite/Gafgyt* dan *Mirai Botnet*. Pengujian dilakukan dalam 257 *batch* yang terbagi pada 5 skenario pengujian, yaitu pendeteksian *IoT Botnet* yang menggunakan data gabungan dari keseluruhan perangkat *IoT* dan *IoT Botnet* sebagai *baseline scenario* (Skenario-0) dengan nilai akurasi tertinggi didapatkan sebesar 99,54%, pendeteksian *IoT Botnet* sudah dikenal pada perangkat *IoT* sudah dikenal (Skenario-1) dengan rata-rata total akurasi didapatkan sebesar 85,22%, pendeteksian *IoT Botnet* sudah dikenal pada perangkat *IoT* belum dikenal (Skenario-2) dengan rata-rata total akurasi didapatkan sebesar 83,06%, pendeteksian *IoT Botnet* belum dikenal pada perangkat *IoT* sudah dikenal (Skenario-3) dengan rata-rata total akurasi didapatkan sebesar 79,98% dan pendeteksian *IoT Botnet* belum dikenal pada perangkat *IoT* belum dikenal (Skenario-4) dengan rata-rata total akurasi didapatkan sebesar 75,07%.

Kata Kunci: *IoT Botnet, Unknown Attack, Unsupervised Learning, Competitive Learning, Learning Vector Quantization.*

ABSTRACT

The use of IoT devices as a Robot Network (IoT Botnet) is a serious threat to cybersecurity. This is inseparable from the growth of IoT devices equipped with advanced communication technology and computing systems, but not accompanied by a strong security system in place. To anticipate the rapid growth of IoT devices and/or types of Botnets in the future, research is needed to detect IoT Botnets on new IoT devices and/or new types of Botnets (Unknown Attack) which have never been involved in the training process. In this study, We proposed to detect unknown IoT Botnets using the Unsupervised Learning approach which is applied to Competitive Learning based method (hereinafter referred to as Unsupervised Competitive Learning). The test was carried out using Learning Vector Quantization (LVQ) method and the N-BaIoT dataset: Data for network based detection of IoT botnet attacks, which provides real traffic data from 9 commercial IoT devices that have been infected with Bashlite/Gafgyt and Mirai Botnet. Testing was carried out in 257 batches divided into 5 test scenarios, namely detection of IoT Botnet using combined data from all IoT devices and all kind of IoT Botnets as baseline scenario (Scenario-0) with the highest accuracy of 99.54%, detection of known IoT Botnets on known IoT devices (Scenario-1) with an average total accuracy of 85.22%, detection of known IoT Botnets on unknown IoT devices (Scenario-2) with an average total accuracy of 83.06%, detection of unknown IoT Botnet on known IoT devices (Scenario-3) with an average total accuracy of 79.98% and detection of unknown IoT Botnets on unknown IoT devices (Scenario-4) with an average total accuracy of 75.07%.

Keywords: *IoT Botnet, Unknown Attack, Unsupervised Learning, Competitive Learning, Learning Vector Quantization.*

PERNYATAAN *SIMILARITY CHECK*

Saya yang bertanda tangan di bawah ini menyatakan, bahwa karya ilmiah yang ditulis oleh

Nama : Said Fauzul Rusnaidi
NIM : 55419110011
Program Studi : Magister Teknik Elektro

dengan judul

“Unknown IoT Botnet Attack Detection Using Unsupervised Competitive Learning”,
telah dilakukan pengecekan *similarity* dengan sistem Turnitin pada tanggal 04/08/2021,
didapatkan nilai persentase sebesar 18 %.

Jakarta, 04 Agustus 2021
Administrator Turnitin


Arie Pangudi, A.Md

UNIVERSITAS
MERCU BUANA

PERNYATAAN

Saya yang bertandatangan di bawah ini menyatakan dengan sebenar-benarnya bahwa semua pernyataan dalam tesis ini :

Judul : Pendeteksian Serangan *IoT Botnet* Tidak Dikenal Dengan *Unsupervised Competitive Learning*
Bentuk Tesis : Penelitian Kuantitatif
Nama : Said Fauzul Rusnaidi
NIM : 55419110011
Program : Magister Teknik Elektro
Tanggal : 13 Agustus 2021

Merupakan hasil studi pustaka, penelitian lapangan, dan karya saya sendiri dengan bimbingan Dosen Pembimbing yang ditetapkan dengan Surat Keputusan Program Studi Magister Teknik Elektro Universitas Mercu Buana.

Karya ilmiah ini belum pernah diajukan untuk memperoleh gelar kesarjanaan pada program sejenis di perguruan tinggi lain. Semua informasi, data, dan hasil pengolahannya yang digunakan, telah dinyatakan secara jelas sumbernya dan dapat diperiksa kebenarannya.

UNIVERSITAS
MERCU BUANA

Jakarta, 13 Agustus 2021



Said Fauzul Rusnaidi

PENGESAHAN

Judul : Pendeteksian Serangan *IoT Botnet* Tidak Dikenal Dengan
Unsupervised Competitive Learning

Bentuk Tesis : Penelitian Kuantitatif

Nama : Said Fauzul Rusnaidi

NIM : 55419110011

Program : Magister Teknik Elektro

Tanggal : 14 Agustus 2021

Mengesahkan

Pembimbing



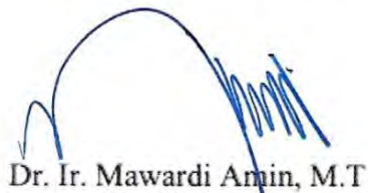
Dr. Marza Ihsan Marzuki, M.T.

UNIVERSITAS

MERCU BUANA

Dekan Fakultas Teknik

Ketua Program Studi
Magister Teknik Elektro



Dr. Ir. Mawardi Amin, M.T



Dr. Umairah, S.ST

KATA PENGANTAR

Alhamdulillah, puji syukur kehadiran Allah SWT yang senantiasa melimpahkan rahmat dan hidayah-Nya, sehingga tesis dengan judul “Pendeteksian Serangan *IoT Botnet* Tidak Dikenal Dengan *Unsupervised Competitive Learning*” ini dapat diselesaikan. Tesis ini disusun untuk memenuhi salah satu persyaratan menyelesaikan studi di Program Magister Teknik Elektro, Fakultas Teknik Universitas Mercu Buana.

Tentunya penyelesaian tesis ini tidak terlepas dari dukungan berbagai pihak, yang pada kesempatan ini penulis secara khusus menyampaikan rasa hormat dan terima kasih yang sebesar-besarnya, kepada:

1. Kedua Orang Tua, Istri dan Anak-anak yang senantiasa mendoakan dan memberikan dukungan baik moril maupun materil.
2. Bapak Dr. Marza Ihsan Marzuki, M.T., selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran dalam membimbing penulis.
3. Bapak Dr. Setiyo Budiyanto, S.T., M.Sc. dan Ibu Dr. Umairah, S.ST. selaku penelaah dan penguji yang telah memberikan masukan dan saran membangun.
4. Bapak Prof. Dr. -Ing. Mudrik Alaydrus, Bapak Prof. Dr. Andi Andriansyah, M.Eng., serta semua dosen dan mahasiswa di Program Magister Teknik Elektro yang telah berbagi ilmu, pengalaman dan waktunya untuk berdiskusi.
5. Semua pihak yang telah membantu penyelesaian tesis ini, dengan tanpa mengurangi rasa hormat tidak dapat penulis sebutkan satu persatu.

Dengan keterbatasan ilmu dan pengalaman, penulis menyadari bahwa tesis ini masih banyak kekurangan dan membutuhkan pengembangan agar benar-benar dapat bermanfaat. Oleh sebab itu, penulis dengan senang hati menerima saran, kritik dan masukan yang membangun untuk kesempurnaan tesis ini.

Akhir kata, penulis berharap tesis ini dapat memberikan manfaat bagi kita semua terutama untuk pengembangan ilmu pengetahuan dan teknologi.

Jakarta, 14 Agustus 2021

Penulis

DAFTAR ISI

Abstrak	ii
Abstract	iii
Pernyataan <i>Similarity Check</i>	iv
Pernyataan	v
Pengesahan	vi
Kata Pengantar	vii
Daftar Isi	viii
Daftar Gambar	xii
Daftar Tabel	xiv
Daftar Notasi dan Istilah	xviii
BAB I PENDAHULUAN	1
A. Latar Belakang	1
B. Rumusan Masalah	4
C. Tujuan Penelitian	5
D. Kontribusi Penelitian	5
E. Batasan Masalah	6
BAB II KAJIAN PUSTAKA	8
A. <i>IoT Botnet</i>	8
B. Pendeteksian <i>IoT Botnet</i>	11
C. Dataset N-BaIoT	12
D. Standardisasi Z-Score	14
E. <i>K-Means Clustering</i>	15
F. <i>Unsupervised Learning</i>	16
G. <i>Competitive Learning</i>	17

1.	<i>Learning Vector Quantization (LVQ)</i>	19
2.	<i>Learning Vector Quantization 2.1 (LVQ-2.1)</i>	20
3.	<i>Learning Vector Quantization 3 (LVQ-3)</i>	21
H.	Penelitian Terdahulu	22
I.	Hipotesis.....	26
BAB III METODOLOGI.....		27
A.	Desain Penelitian.....	27
1.	Alur Penelitian	27
2.	Skenario Pengujian	28
B.	Persiapan Data.....	31
1.	Sampling Data	31
2.	Standardisasi Data	33
C.	Pembentukan <i>Initial Centroid</i>	35
D.	Pendeteksian <i>IoT Botnet</i>	37
E.	Evaluasi	39
BAB IV HASIL DAN PEMBAHASAN		41
A.	Data Pengujian	41
B.	Pembentukan <i>Initial Centroid</i>	45
C.	Hasil Pengujian Pendeteksian <i>IoT Botnet</i>	50
1.	Pendeteksian Gabungan Data Seluruh Perangkat <i>IoT dan IoT Botnet</i>	50
2.	Pendeteksian <i>IoT Botnet</i> Sudah Dikenal Pada Perangkat <i>IoT</i> Sudah Dikenal.....	51
2.1.	Pendeteksian <i>Gafgyt Attack</i>	52
2.2.	Pendeteksian <i>Mirai Attack</i>	54
3.	Pendeteksian <i>IoT Botnet</i> Sudah Dikenal Pada Perangkat <i>IoT</i> Belum Dikenal	56

3.1.	Pendeteksian <i>Gafgyt Attack</i>	56
3.2.	Pendeteksian <i>Mirai Attack</i>	77
4.	Pendeteksian <i>IoT Botnet</i> Belum Dikenal Pada Perangkat <i>IoT</i> Sudah Dikenal.....	89
4.1.	Pendeteksian <i>Gafgyt Attack</i>	90
4.2.	Pendeteksian <i>Mirai Attack</i>	92
5.	Pendeteksian <i>IoT Botnet</i> Belum Dikenal Pada Perangkat <i>IoT</i> Belum Dikenal	94
5.1.	Pendeteksian <i>Gafgyt Attack</i>	94
5.2.	Pendeteksian <i>Mirai Attack</i>	110
D.	Pembahasan Hasil Pengujian Pendeteksian <i>IoT Botnet</i>	127
1.	Pendeteksian Gabungan Data Seluruh Perangkat <i>IoT</i> dan <i>IoT</i> <i>Botnet</i>	127
2.	Pendeteksian <i>IoT Botnet</i> Sudah Dikenal Pada Perangkat <i>IoT</i> Sudah Dikenal.....	128
3.	Pendeteksian <i>IoT Botnet</i> Sudah Dikenal Pada Perangkat <i>IoT</i> Belum Dikenal	129
3.1.	Pendeteksian <i>Gafgyt Attack</i>	130
3.2.	Pendeteksian <i>Mirai Attack</i>	132
3.3.	Generalisasi Hasil Pendeteksian <i>IoT Botnet</i> Pada Perangkat <i>IoT</i> Belum Dikenal	134
4.	Pendeteksian <i>IoT Botnet</i> Belum Dikenal Pada Perangkat <i>IoT</i> Sudah Dikenal.....	135
5.	Pendeteksian <i>IoT Botnet</i> Belum Dikenal Pada Perangkat <i>IoT</i> Belum Dikenal	137
5.1.	Pendeteksian <i>Gafgyt Attack</i>	138
5.2.	Pendeteksian <i>Mirai Attack</i>	140

5.3. Generalisasi Hasil Pendeteksian <i>IoT Botnet</i> Belum Dikenal Pada Perangkat <i>IoT</i> Belum Dikenal.....	142
E. Sintesa Hasil Studi	143
BAB V KESIMPULAN DAN SARAN.....	145
A. Kesimpulan	145
B. Saran.....	147
DAFTAR PUSTAKA	148



DAFTAR GAMBAR

Gambar 2.1	Ilustrasi K-Means Clustering.....	16
Gambar 2.2	Arsitektur Jaringan Syaraf <i>Competitive Learning</i>	18
Gambar 3.1	Alur penelitian	27
Gambar 3.2	Diagram alur normalisasi data.....	34
Gambar 3.3	Diagram alur pembentukan <i>Initial Centroids</i>	36
Gambar 3.4	Diagram alur <i>Testing</i>	38
Gambar 4.1	Komposisi Data Pengujian	42
Gambar 4.2	Sebaran nilai atribut sebelum normalisasi	44
Gambar 4.3	Sebaran nilai atribut setelah normalisasi	44
Gambar 4.4	Sebaran nilai atribut sebelum normalisasi (<i>zoom in</i>).....	44
Gambar 4.5	Sebaran nilai atribut setelah normalisasi (<i>zoom in</i>).....	45
Gambar 4.6	Perbandingan akurasi K-Means Clustering <i>Gafgyt Attack</i> berdasarkan <i>Time Window</i>	49
Gambar 4.7	Perbandingan akurasi K-Means Clustering <i>Mirai Attack</i> berdasarkan <i>Time Window</i>	49
Gambar 4.8	Perbandingan hasil pendeteksian <i>IoT Botnet</i> dengan Skenario-1	129
Gambar 4.9	Perbandingan Perangkat <i>IoT</i> sebagai basis dan obyek pendeteksian <i>Gafgyt Attack</i> dengan Skenario-2	132
Gambar 4.10	Perbandingan Perangkat <i>IoT</i> sebagai basis dan obyek pendeteksian <i>Mirai Attack</i> dengan Skenario-2.....	134
Gambar 4.11	Perbandingan <i>IoT Botnet</i> sebagai basis dan obyek pendeteksian dengan Skenario-3	137
Gambar 4.12	Perbandingan Perangkat <i>IoT</i> sebagai basis dan obyek pendeteksian <i>Gafgyt Attack</i> dengan Skenario-4	138

Gambar 4.13 Perbandingan Perangkat *IoT* sebagai basis dan obyek pendeteksian
Mirai Attack dengan Skenario-4.....142



DAFTAR TABEL

Tabel 2.1	Perbandingan <i>Botnet</i> tradisional dan <i>IoT Botnet</i> [1].....	10
Tabel 2.2	Konten Dataset N-BaIoT	12
Tabel 2.3	Ekstraksi Atribut Trafik [13]	14
Tabel 2.4	Hubungan antar penelitian	25
Tabel 3.1	Skenario Pengujian	29
Tabel 3.2	Detail Komposisi Dataset	31
Tabel 3.3	Proporsi Sampling Data IoT Botnet.....	33
Tabel 3.4	<i>Confusion Matrix</i> [29]	39
Tabel 3.5	<i>Performance measures for classification</i> [29].....	40
Tabel 4.1	Komposisi Data Pengujian.....	41
Tabel 4.2	Contoh Atribut dengan perbedaan rentang nilai paling dominan	43
Tabel 4.3	Hasil Pembentukan <i>Initial Centroid</i>	46
Tabel 4.4	Hasil Pengujian Skenario-0 dengan Data Gabungan	51
Tabel 4.5	Hasil Pengujian Skenario-1 untuk <i>Gafgyt Attack</i>	52
Tabel 4.6	Hasil Pengujian Skenario-1 untuk <i>Mirai Attack</i>	54
Tabel 4.7	Hasil Pengujian Skenario-2 perangkat <i>Danmini Doorbell</i> dan <i>Gafgyt Attack</i>	57
Tabel 4.8	Hasil Pengujian Skenario-2 perangkat <i>Ecobee Thermostat</i> dan <i>Gafgyt Attack</i>	59
Tabel 4.9	Hasil Pengujian Skenario-2 perangkat <i>Ennio Doorbell</i> dan <i>Gafgyt Attack</i>	61
Tabel 4.10	Hasil Pengujian Skenario-2 perangkat <i>Philips B120N10 Baby Monitor</i> dan <i>Gafgyt Attack</i>	63

Tabel 4.11	Hasil Pengujian Skenario-2 perangkat <i>Provision PT 737E Security Camera</i> dan <i>Gafgyt Attack</i>	66
Tabel 4.12	Hasil Pengujian Skenario-2 perangkat <i>Provision PT 838 Security Camera</i> dan <i>Gafgyt Attack</i>	68
Tabel 4.13	Hasil Pengujian Skenario-2 perangkat <i>Samsung SNH 1011 N Webcam</i> dan <i>Gafgyt Attack</i>	70
Tabel 4.14	Hasil Pengujian Skenario-2 perangkat <i>SimpleHome XCS7 1002 WHT Security Camera</i> dan <i>Gafgyt Attack</i>	72
Tabel 4.15	Hasil Pengujian Skenario-2 perangkat <i>SimpleHome XCS7 1003 WHT Security Camera</i> dan <i>Gafgyt Attack</i>	75
Tabel 4.16	Hasil Pengujian Skenario-2 perangkat <i>Danmini Doorbell</i> dan <i>Mirai Attack</i>	77
Tabel 4.17	Hasil Pengujian Skenario-2 perangkat <i>Ecobee Thermostat</i> dan <i>Mirai Attack</i>	79
Tabel 4.18	Hasil Pengujian Skenario-2 perangkat <i>Philips B120N10 Baby Monitor</i> dan <i>Mirai Attack</i>	81
Tabel 4.19	Hasil Pengujian Skenario-2 perangkat <i>Provision PT 737E Security Camera</i> dan <i>Mirai Attack</i>	82
Tabel 4.20	Hasil Pengujian Skenario-2 perangkat <i>Provision PT 838 Security Camera</i> dan <i>Mirai Attack</i>	84
Tabel 4.21	Hasil Pengujian Skenario-2 perangkat <i>SimpleHome XCS7 1002 WHT Security Camera</i> dan <i>Mirai Attack</i>	86
Tabel 4.22	Hasil Pengujian Skenario-2 perangkat <i>SimpleHome XCS7 1003 WHT Security Camera</i> dan <i>Mirai Attack</i>	88
Tabel 4.23	Hasil Pengujian Skenario-3 untuk <i>Gafgyt Attack</i>	90
Tabel 4.24	Hasil Pengujian Skenario-3 untuk <i>Mirai Attack</i>	92

Tabel 4.25	Hasil Pengujian Skenario-4 perangkat <i>Danmini Doorbell</i> dan <i>Mirai Attack</i>	95
Tabel 4.26	Hasil Pengujian Skenario-4 perangkat <i>Ecobee Thermostat</i> dan <i>Mirai Attack</i>	97
Tabel 4.27	Hasil Pengujian Skenario-4 perangkat <i>Philips B120N10 Baby Monitor</i> dan <i>Mirai Attack</i>	99
Tabel 4.28	Hasil Pengujian Skenario-4 perangkat <i>Provision PT 737E Security Camera</i> dan <i>Mirai Attack</i>	102
Tabel 4.29	Hasil Pengujian Skenario-4 perangkat <i>Provision PT 838 Security Camera</i> dan <i>Mirai Attack</i>	104
Tabel 4.30	Hasil Pengujian Skenario-4 perangkat <i>SimpleHome XCS7 1002 WHT Security Camera</i> dan <i>Mirai Attack</i>	106
Tabel 4.31	Hasil Pengujian Skenario-4 perangkat <i>SimpleHome XCS7 1003 WHT Security Camera</i> dan <i>Mirai Attack</i>	108
Tabel 4.32	Hasil Pengujian Skenario-4 perangkat <i>Danmini Doorbell</i> dan <i>Gafgyt Attack</i>	111
Tabel 4.33	Hasil Pengujian Skenario-4 perangkat <i>Ecobee Thermostat</i> dan <i>Gafgyt Attack</i>	113
Tabel 4.34	Hasil Pengujian Skenario-4 perangkat <i>Ennio Doorbell</i> dan <i>Gafgyt Attack</i>	114
Tabel 4.35	Hasil Pengujian Skenario-4 perangkat <i>Philips B120N10 Baby Monitor</i> dan <i>Gafgyt Attack</i>	116
Tabel 4.36	Hasil Pengujian Skenario-4 perangkat <i>Provision PT 737E Security Camera</i> dan <i>Gafgyt Attack</i>	118
Tabel 4.37	Hasil Pengujian Skenario-4 perangkat <i>Provision PT 838 Security Camera</i> dan <i>Gafgyt Attack</i>	120

Tabel 4.38	Hasil Pengujian Skenario-4 perangkat <i>Samsung SNH 1011 N Webcam dan Gafgyt Attack</i>	122
Tabel 4.39	Hasil Pengujian Skenario-4 perangkat <i>SimpleHome XCS7 1002 WHT Security Camera dan Gafgyt Attack</i>	124
Tabel 4.40	Hasil Pengujian Skenario-4 perangkat <i>SimpleHome XCS7 1003 WHT Security Camera dan Gafgyt Attack</i>	126
Tabel 4.41	Perbandingan Akurasi Terbaik Hasil Pendeteksian <i>IoT Botnet</i> Dengan Skenario-1	128
Tabel 4.42	Perbandingan Akurasi Terbaik Hasil Pendeteksian <i>Gafgyt Attack</i> Dengan Skenario-2	131
Tabel 4.43	Perbandingan Akurasi Terbaik Hasil Pendeteksian <i>Mirai Attack</i> Dengan Skenario-2	133
Tabel 4.44	Perbandingan Akurasi Terbaik Hasil Pendeteksian <i>IoT Botnet</i> Dengan Skenario-3	136
Tabel 4.45	Perbandingan Akurasi Terbaik Hasil Pendeteksian <i>Gafgyt Attack</i> Dengan Skenario-4	139
Tabel 4.46	Perbandingan Akurasi Terbaik Hasil Pendeteksian <i>Mirai Attack</i> Dengan Skenario-4	141

DAFTAR NOTASI DAN ISTILAH

- Perangkat *IoT* Tidak Dikenal : Perangkat *IoT* yang tidak digunakan dalam proses *training*, untuk mensimulasikan bahwa perangkat *IoT* tersebut saat ini belum tersedia di pasaran (baru akan hadir di waktu yang akan datang)
- Perangkat *IoT* Sudah Dikenal : Perangkat *IoT* yang digunakan dalam proses *training*, untuk mensimulasikan bahwa perangkat *IoT* tersebut saat ini sudah tersedia di pasaran, sehingga dapat dipelajari pola/*patern* dari data trafiknya
- IOT Botnet* Tidak Dikenal : *IoT Botnet* yang tidak digunakan dalam proses *training*, untuk mensimulasikan bahwa *IoT Botnet* tersebut belum ada saat ini (baru akan hadir di waktu yang akan datang)
- IOT Botnet* Sudah Dikenal : *IoT Botnet* yang digunakan dalam proses *training*, untuk mensimulasikan bahwa *IoT Botnet* tersebut saat ini sudah ada dan diketahui keberadaannya (dalam hal ini *Mirai* dan *Gafgyt*), sehingga dapat dipelajari pola/*patern* dari data trafiknya
- Basis pendeteksian : Perangkat *IoT* dan/atau *IoT Botnet* yang digunakan dalam proses *training*, dimana hasil *training* tersebut digunakan untuk pendeteksian *IoT Botnet* pada tahap *testing* sesuai dengan skenario yang ditetapkan
- Obyek pendeteksian : Perangkat *IoT* dan/atau *IoT Botnet* yang dijadikan obyek pendeteksian *IoT Botnet* pada tahap *testing* sesuai dengan skenario yang ditetapkan
- IoT* : *Internet of Think*
- Botnet* : *Robot Network*

<i>LVQ</i>	: <i>Learning Vector Quantization</i>
<i>PRCL</i>	: <i>Pursuit Reinforcement Competitive Learning</i>
<i>SVM</i>	: <i>Support Vector Machine</i>
<i>LOF</i>	: <i>Local Outlier Factor</i>
<i>NB</i>	: <i>Naïve Bayes</i>
<i>KNN</i>	: <i>K-Nearest Neighbours</i>
<i>RF</i>	: <i>Random Forest</i>
<i>LR</i>	: <i>Logistic Regression</i>
<i>DOS</i>	: <i>Denial of Service</i>
<i>DDOS</i>	: <i>Distributed Denial of Service</i>
<i>H</i>	: <i>Host Device</i>
<i>MI</i>	: <i>MAC and IP address</i>
<i>HH</i>	: <i>Source Host and Destination Host</i>
<i>HH_jit</i>	: <i>HH Jitter</i>
<i>HpHp</i>	: <i>Host and Port dari source dan destination</i>
\mathbb{R}	: Anggota bilangan real
<i>StdDev</i>	: Standar deviasi
x_i	: <i>Data vector x ke i</i>
x_1, \dots, x_n	: <i>Data vector x ke i sampai dengan vector x ke n</i>
y^1, \dots, y^5	: <i>Subvector dari x yang ke 1 sampai subvector ke 5</i>
w_i	: <i>Weight atau bobot dari neuron yang ke i</i>
w_{i1}, \dots, w_{id}	: <i>Weight yang ke i untuk amatan vector/subvector ke 1 sampai ke d</i>
m_i	: <i>Titik tengah dari neuron (centroid) yang ke i</i>

$\ x - m_i\ $: Jarak antara <i>vector</i> x dan m yang ke i
c_p	: <i>Class neuron</i> pemenang
c_r	: <i>Class neuron</i> runner up
w_p	: <i>Weight</i> neuron pemenang
w_r	: <i>Weight</i> neuron runner up
$w^{(t-1)}$: <i>Weight</i> pada iterasi sebelumnya (<i>before</i>)
$w^{(t)}$: <i>Weight</i> pada iterasi terakhir (<i>current</i>)
$w^{(t+1)}$: <i>Weight</i> pada iterasi berikutnya (<i>next</i>)
α	: <i>Parameter learning rate</i> , yaitu nilai yang menentukan berapa besar pengaruh hasil proses pendeteksian terhadap proses pendeteksian berikutnya (proses pembelajaran)
ε	: <i>Parameter window</i> , yaitu nilai yang menentukan rentang area/daerah yang harus dipenuhi untuk memperbaharui <i>weight</i> dari <i>vector</i> pemenang dan <i>runner up</i>
o_1, \dots, o_n	: Output yang ke i sampai dengan output ke n
TP	: <i>True Positive</i> , Hasil pendeteksian yang benar, dimana <i>IoT Botnet</i> terdeteksi sebagai <i>IoT Botnet</i>
TN	: <i>True Negative</i> , Hasil pendeteksian yang benar, dimana data <i>benign</i> terdeteksi sebagai <i>benign</i>
FP	: <i>False Positive</i> , Hasil pendeteksian yang salah, dimana data <i>benign</i> terdeteksi sebagai <i>Iot Botnet</i>
FN	: <i>False Negative</i> , Hasil pendeteksian yang salah, dimana <i>IoT Botnet</i> terdeteksi sebagai data <i>benign</i>