

**Pengenalan Pola Serangan TCP SYN Flood DDoS Pada  
Jaringan Internet Of Things (IoT) Dengan Menggunakan  
Metode Rule Based Signature Analysis**

**TUGAS AKHIR**

**Diajukan Untuk Melengkapi Salah Satu Syarat**

**Memperoleh Gelar Sarjana Komputer**



**OLEH :**

**Ahmad Ramdhoni Kusduandi**

**09011181823027**

**JURUSAN SISTEM KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**2022**

## **LEMBAR PENGESAHAN**

**Pengenalan Pola Serangan TCP SYN Flood DDoS Pada Jaringan Internet Of  
Things (IoT) Dengan Menggunakan Metode Rule Based Signature Analysis**

## **TUGAS AKHIR**

**Program Studi Sistem Komputer**  
**Jenjang S1**

**Oleh**

**Ahmad Ramdhoni Kusduandi**  
**09011181823027**

**Indralaya, Juli 2022**

**Mengetahui,**

**Ketua Jurusan Sistem Komputer**

  
Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

**Pembimbing Tugas Akhir 1**

  
Deris Stiawan, M.T., PH.D., IPU.

NIP. 197806172006041002

## HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Rabu  
Tanggal : 20 Juli 2022

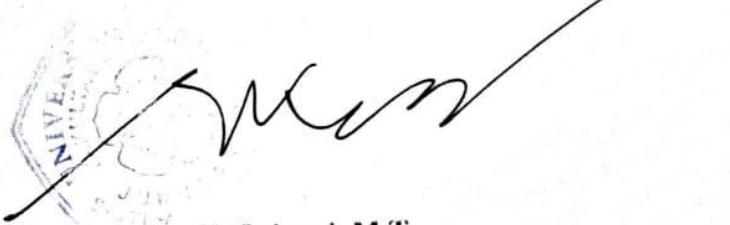
Tim Penguji :

1. Ketua Sidang : Ahmad Zarkasi, M.T.
2. Sekretaris Sidang : Tri Wanda Septian, M.Sc.
3. Penguji Sidang : Huda Ubaya, M.T.
4. Pembimbing : Deris Stiawan, M.T., Ph.D., IPU



Mengetahui, 2981,~

Ketua Jurusan Sistem Komputer



Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

## HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Ahmad Ramdhoni Kusdunadi

NIM : 09011181823027

Judul : Pengenalan Pola Serangan TCP SYN Flood DDoS Pada Jaringan Internet Of Things (IoT)  
Dengan Menggunakan Metode Rule Based Signature Analysis

### Hasil Pengecekan Software iThenticate/Turnitin : 15%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.



Palembang, Juli 2022



Ahmad Ramdhoni Kusduandi

NIM.09011181823027

## KATA PENGANTAR

Assalamu'alaikum Wr.Wb.

Puji syukur Alhamdulillah penulis panjatkan atas kehadiran Allah SWT yang telah memberikan karunia dan rahmat-Nya, sehingga penulis dapat menyelesaikan penulisan Proposal Tugas Akhir ini yang berjudul "**Pengenalan Pola Serangan TCP SYN Flood DDoS Pada Jaringan Internet Of Thing (IoT) Menggunakan Metode Rule Based Signature Analysis**".

Dalam laporan ini penulis menjelaskan mengenai pemodelan untuk identifikasi dan klasifikasi author terhadap suatu publikasi dengan disertai data-data yang diperoleh penulis saat melakukan penelitian dan pengujian data. Penulis berharap agar tulisan ini dapat bermanfaat bagi orang banyak.

Pada kesempatan ini penulis ingin mengucapkan terima kasih kepada beberapa pihak atas ide dan saran serta bantuannya dalam menyelesaikan penulisan Proposal Tugas Akhir ini. Oleh karena itu, penulis ingin mengucapkan rasa syukur kepada Allah SWT dan terimakasih kepada yang terhormat :

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga saya dapat menyelesaikan penulisan Proposal Tugas Akhir ini dengan baik dan lancar.
2. Orang tua saya tercinta yang telah membesarakan saya dengan penuh kasih sayang dan selalu mengajarkan saya dalam berbuat hal yang baik. Terimakasih untuk segala do'a, motivasi dan dukungannya baik moril, materil maupun spiritual selama ini.
3. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya

5. Bapak Deris Stiawan, M.T., PH.D., IPU. selaku Dosen Pembimbing Tugas Akhir 1 yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran dan motivasi serta bimbingan terbaik untuk penulis dalam menyelesaikan Tugas Akhir ini.

6. Bapak DR. ERWIN, S.SI, M.SI selaku Pembimbing Akademik Jurusan Sistem Komputer.

7. Mbak Reni selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.

8. Dan semua pihak yang telah membantu.

Penulis menyadari bahwa laporan ini masih sangat jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangatlah diharapkan penulis. Akhir kata penulis berharap, semoga proposal tugas akhir ini bermanfaat dan berguna bagi khalayak.

Wassalamu'alaikum Wr. Wb.

Indralaya, Juli 2022  
Penulis,



Ahmad Ramdhoni Kusduandi  
NIM. 0901181823027

## ABSTRAK

### PENGENALAN POLA SERANGAN TCP SYN FLOOD DDoS PADA JARINGAN INTERNET OF THINGS (IoT) MENGGUNAKAN METODE RULE BASED SIGNATURE ANALYSIS

**Ahmad Ramdhoni Kusduandi (09011181283027)**

Jurusan Sistem Komputer, Fakultas Ilmu Komputer,

Universitas SriwijayaEmail : [ahmadramdhoni98@gmail.com](mailto:ahmadramdhoni98@gmail.com)

Keamanan pada jaringan *Internet of Thinngs* masih rentan terhadap banyaknya serangan yang di peruntukan untuk mengusik komunikasi jaringan. Serangan pada jaringan *Internet of Things* (IoT) bisa terjalin pada seluruh layer IoT, serangan dapat terjadi melalui komunikasi RFID, IEE 802.15.4 atau Zigbee, WiFi, serta Bluetooth, dan *node* (sensor). *Distribut Denial of Service* (DDoS) merupakan salah satu ancaman utama terhadap keamanan jaringan. Salah satu serangan *DDoS* pada jaringan *Internet of Things* (IoT) ialah *TCP SYN Flood DDoS*, serangan ini bekerja dengan memanfaatkan kelemahan pada protokol *TCP*, dengan membanjiri paket *Syn* ke server sehingga server kehabisan sumber daya dan membuat server akan bekerja tidak maksimal. Oleh karena itu, sangat penting untuk memahami pola serangan pada salah satunya serangan *TCP SYN Flood DDoS*. Salah satu metode yang berpotensi untuk melakukan pengenalan pola ialah dengan menggunakan metode *Rule Based Signature Analysis*. Metode ini mengenali pola serangan dengan mencari atribut unik pada paket serangan, sehingga antara paket serangan dan paket normal dapat dibedakan. Pada penelitian ini menggunakan dataset bernama *ToN\_IoT* yang dikembangkan oleh laboratorium Cyber Range di UNSW. Metode *Rule Based Signature Analysis* akan di implementasikan pada IDS menggunakan snort. Hasil dari metode ini memperoleh nilai *Ture Positive Rate* (TPR) sebesar 60.9844259%, nilai dari *False Positive Rate* (FPR) sebesar 0.037595%, nilai *True Negative Rate* (TNR) sebesar 99.9624045%, nilai dari *False Negative Rate* (FPR) sebesar 39.00212%, nilai dari presisi sebesar 99.971832%, nilai dari *Non-Precision* sebesar 53.952001% dan nilai akurasi mencapai 73.221971%.

**Kata Kunci :** *Internet of Things, Distributed Denial of Service, Signature Based Analysis, TCP Syn Flood, Intrusion Detection System*

## **ABSTRACT**

### **PATTERN RECOGNITION OF TCP SYN FLOOD DDoS ATTACK ON INTERNET OF THINGS (IoT) NETWORK USING RULE BASED SIGNATURE ANALYSIS METHOD**

**Ahmad Ramdhoni Kusduandi (09011181823027)**

Department of Computer Engineering , Faculty of Computer Science,  
Sriwijaya University

Email: [ahmadramdhoni98@gmail.com](mailto:ahmadramdhoni98@gmail.com)

Security on the Internet of Thinngs network is still vulnerable to many attacks that are intended to disrupt network communications. Attacks on the Internet of Things (IoT) network can be established at all IoT layers, attacks can occur through RFID communication, IEE 802.15.4 or Zigbee, WiFi, as well as Bluetooth, and nodes (sensors). Distribution Denial of Service (DDoS) is one of the major threats to network security. One of the DDoS attacks on the Internet of Things (IoT) network is TCP SYN Flood DDoS, this attack works by exploiting weaknesses in the TCP protocol, by flooding Syn packets to the server so that the server runs out of resources and makes the server work optimally. Therefore, it is very important to understand the attack pattern on one TCP SYN Flood DDoS attack . One method that has the potential to do pattern recognition is to use the method of Rule Based Signature Analysis . This method recognizes attack patterns by looking for unique attributes on attack packets, so that between attack packets and normal packets can be distinguished. This study uses a dataset called ToN\_IoT developed by the Cyber Range Laboratory at UNSW. Rule Based Signature Analysis method will be implemented on IDS using snort. The results of this method obtain the value of Ture Positive Rate (TPR) of 60.9844259% , the value of False Positive Rate (FPR) of 0.037595%, the value of True Negative Rate (TNR) of 99.9624045%, the value of False Negative Rate (FPR) of 39.00212%, the value of precision of 99.971832%, the value of Non-Precision of 53.952001% the accuracy value reaches 73.221971%..

**Keywords :** Internet of Things, Distributed Denial of Service, Signature Based Analysis, TCP Syn Flood, Intrusion Detection System

## DAFTAR ISI

<b>LEMBAR PENGESAHAN .....</b>	ii
<b>HALAMAN PERSETUJUAN .....</b>	iii
<b>HALAMAN PERNYATAAN.....</b>	iv
<b>KATA PENGANTAR.....</b>	v
<b>ABSTRAK .....</b>	vii
<b>ABSTRACT .....</b>	viii
<b>DAFTAR ISI.....</b>	ix
<b>DAFTAR GAMBAR.....</b>	xi
<b>DAFTAR TABEL .....</b>	xiii
<b>BAB I PENDAHULUAN.....</b>	1
<b>1.1 Latar Belakang .....</b>	1
<b>1.2 Tujuan .....</b>	3
<b>1.3 Manfaat .....</b>	3
<b>1.4 Perumusan Masalah.....</b>	3
<b>1.5 Batasan Masalah.....</b>	4
<b>1.6 Metodelogi Penelitian .....</b>	4
<b>1.7 Sistematika Penulisan .....</b>	5
<b>BAB II TINJAUAN PUSTAKA.....</b>	7
<b>2.1 Penelitian Terkait.....</b>	7
<b>2.2 Internet of Things (IoT) .....</b>	9
<b>2.3 Transmission Control Protocol (TCP) .....</b>	10
<b>2.4 Distributed Denial of Service (DDoS) .....</b>	11
<b>2.5 Intrusion Detection Systems (IDS).....</b>	13
<b>2.5.1 Metode Deteksi Intrusion Detection System.....</b>	14
<b>2.6 Dataset .....</b>	15
<b>2.7 Snort .....</b>	18
<b>2.7.1 Rule Snort .....</b>	18
<b>2.8 Confussion Matrix .....</b>	18
<b>BAB III METODOLOGI PENELITIAN .....</b>	20
<b>3.1 Pendahuluan .....</b>	20
<b>3.2 Kerangka Kerja Penelitian .....</b>	20

<b>3.3</b>	<b>Kebutuhan Perangkat Keras dan Perangkat Lunak .....</b>	<b>21</b>
<b>3.3.1</b>	<b>Kebutuhan Perangkat keras .....</b>	<b>21</b>
<b>3.3.2</b>	<b>Kebutuhan Perangkat Lunak .....</b>	<b>22</b>
<b>3.4</b>	<b>Studi Pustaka .....</b>	<b>22</b>
<b>3.5</b>	<b>Persiapan Dataset .....</b>	<b>23</b>
<b>3.6</b>	<b>Ekstraksi Data .....</b>	<b>23</b>
<b>3.7</b>	<b>Analisis Dataset.....</b>	<b>24</b>
<b>3.8</b>	<b>Deteksi Serangan Dengan Snort Sebagai IDS .....</b>	<b>25</b>
<b>3.9</b>	<b>Korelasi dan Evaluasi .....</b>	<b>27</b>
<b>3.10</b>	<b>Analisa dan Kesimpulan .....</b>	<b>27</b>
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>		<b>28</b>
<b>4.1</b>	<b>Pendahuluan .....</b>	<b>28</b>
<b>4.2</b>	<b>Analisa Dataset .....</b>	<b>28</b>
<b>4.3</b>	<b>Hasil Ekstraksi Data .....</b>	<b>33</b>
<b>4.4</b>	<b>Analisa Pola Serangan <i>DDoS SYN Flood</i> .....</b>	<b>35</b>
<b>4.5</b>	<b>Hasil Pengujian Snort sebagai IDS .....</b>	<b>37</b>
<b>4.5.1</b>	<b>Pengujian Menggunakan <i>Rule Default</i> Snort.....</b>	<b>37</b>
<b>4.5.2</b>	<b>Identifikasi Pola Serangan Sebagai Rules .....</b>	<b>39</b>
<b>4.5.3</b>	<b>Pengujian Snort Menggunakan <i>Rule Based Signatured</i> .....</b>	<b>40</b>
<b>4.6</b>	<b>Hasil Perhitungan <i>Confussion Matrix</i>.....</b>	<b>43</b>
<b>4.6.1</b>	<b>Perhitungan Confusion matrix <i>Snort rule default</i> .....</b>	<b>43</b>
<b>4.6.2</b>	<b>Perhitungan Confusion Matrix Penerapan Rule Based Signature Analysis .....</b>	<b>45</b>
<b>4.7</b>	<b>Perbandingan Snort IDS dan Rule Based Signatured Analysis.....</b>	<b>48</b>
<b>BAB V KESIMPULAN DAN SARAN .....</b>		<b>50</b>
<b>5.1</b>	<b>Kesimpulan .....</b>	<b>50</b>
<b>5.2</b>	<b>Saran .....</b>	<b>50</b>
<b>DAFTAR PUSTAKA .....</b>		<b>52</b>

## DAFTAR GAMBAR

<b>Gambar 2.1</b> TCP Header .....	10
<b>Gambar 2.2</b> Arsitektur DDoS Attack .....	12
<b>Gambar 2.3</b> Topologi dari IDS .....	14
<b>Gambar 2.4</b> Arsitektur Testbed pada Dataset ToN_IoT .....	16
<b>Gambar 2.5</b> Contoh Rule Snort .....	18
<b>Gambar 2.6</b> Confusion Matrix.....	18
<b>Gambar 3.1</b> Kerangkatan Kerja Penelitian.....	21
<b>Gambar 3.2</b> Struktur Dari Rule Snort.....	25
<b>Gambar 3.3</b> Tahapan Deteksi Menggunakan Snort.....	26
<b>Gambar 3.4</b> Contoh Serangan Terdeteksi Oleh Snort .....	27
<b>Gambar 4.1</b> Data Mentah Normal .....	29
<b>Gambar 4.2</b> Protokol Pada Dataset Normal .....	30
<b>Gambar 4.3</b> Data Mentah Gabungan .....	31
<b>Gambar 4.4</b> Protokol Pada Dataset Gabungan .....	33
<b>Gambar 4.5</b> Hasil Ekstraksi Dataset Normal .....	33
<b>Gambar 4.6</b> Hasil Ekstraksi Dataset Gabungan .....	34
<b>Gambar 4.7</b> Korelasi Dataset Normal .....	35
<b>Gambar 4.8</b> Korelasi Dataset Gabungan .....	35
<b>Gambar 4.9</b> Paket Data Normal.....	36
<b>Gambar 4.10</b> Paket Data Serangan .....	36
<b>Gambar 4.11</b> Hasil Deteksi Pada Dataset Normal.....	38
<b>Gambar 4.11</b> Hasil Deteksi Pada Dataset Gabungan .....	38

<b>Gambar 4.13</b>	Hasil Deteksi Pada Dataset Normal.....	40
<b>Gambar 4.14</b>	Hasil Deteksi Pada Dataset Gabungan .....	41
<b>Gambar 4.15</b>	Korelasi Hasil Deteksi Dengan Dataset Gabungan .....	42

## DAFTAR TABEL

<b>Tabel 2.1</b> Penelitian Terkait Serangan DoS Maupun DDoS .....	8
<b>Tabel 2.2</b> Jenis Paket Pada Dataset ToN_IoT .....	17
<b>Tabel 3.1</b> Kebutuhan Perangkat Keras .....	22
<b>Tabel 3.2</b> Kebutuhan Perangkat Lunak .....	22
<b>Tabel 3.3</b> Atribut Data Ekstraksi.....	23
<b>Tabel 4.1</b> Statistik Protokol Data Normal .....	29
<b>Tabel 4.2</b> Statistik Protokol Dataset Gabungan.....	32
<b>Tabel 4.3</b> Atribut Serangan SYN Flood .....	37
<b>Tabel 4.4</b> Hasil Pengujian Dengan Rule Standar .....	39
<b>Tabel 4.5</b> Hasil Pengujian Dengan Rule Based Signature .....	41
<b>Tabel 4.6</b> Binary Classification Matrix Snort Rule Default .....	43
<b>Tabel 4.7</b> Perhitungan Detection Rate Dengan Rule Default .....	45
<b>Tabel 4.8</b> Binary Classification Dengan Rule Based Signature Analysis .....	46
<b>Tabel 4.9</b> Confusion Matrix Dan Detection Rate Rule Based Siganture Analysis .....	47
<b>Tabel 4.10</b> Perbandingan Nilai Detection Rte .....	48

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Internet Of Things (IoT) adalah sebuah kemampuan dari jaringan yang mampu menghubungkan satu sama lain antara berbagai objek cerdas sekaligus dapat memungkinkan semua objek tersebut untuk saling berkomunikasi ataupun berinteraksi dengan objek lain, dengan lingkungan, maupun dengan peralatan komputasi cerdas lainnya melalui jaringan internet[1]. Setiap objek dalam jaringan IoT mampu berinteraksi, bekerja sama, memproses, mengolah dan menyampaikan informasi secara otonom untuk menghasilkan layanan, seperti informasi statistik, monitoring dan sistem kontrol[2]. IoT pada dasarnya memiliki tiga lapisan *layer* yang mempunyai tiga fungsi yang berbeda. Lapisan pertama, disebut sebagai *perceptron layer*, Lapisan kedua disebut sebagai *network layer*. Lapisan terakhir disebut sebagai *application layer* [3].

Keamanan pada jaringan Internet Of Things (IoT) menjadi salah satu yang utama yang harus diperhatikan. Karena Internet Of Things (IoT) rentan terhadap banyaknya serangan yang di peruntukan untuk mengusik komunikasi jaringan. Serangan keamanan bisa terjalin pada seluruh layer IoT, serangan dapat terjadi melalui komunikasi RFID, IEE 802.15.4 atau Zigbee, WiFi, serta Bluetooth, dan node (sensor) . Sehingga permasalahan keamanan, seperti privasi, otorisasi, verifikasi, control akses, konfigurasi system, penyimpanan serta manajemen data dapat aman[4].

Distribut Denial of Service (DDoS) merupakan salah satu ancaman utama terhadap keamanan jaringan. Serangan DDoS memakai banyak *host* untuk menyerang membanjiri paket ke sistem , sehingga sistem tidak dapat bekerja dengan semestinya. Sangat susah untuk mengenali sumber dari serangan itu, karena penyerang menyembunyikan identitasnya dengan memalsukan alamat IP mereka[5]. Adapun beberapa jenis serangan DDoS seperti serangan ACK dan SYN

Flood, Domain name server (DNS) amplification, Network time protocol (NTP) amplification, UDP fragment, UDP Flood, HTTP Flood, ICMP Flood, Zero-Day DDoS[6].

Serangan SYN Flood merupakan tipe serangan DDoS yang bekerja dengan memanfaatkan kelemahan pada TCP. Penyerang membanjiri dengan mengirimkan banyak paket SYN ke sistem. Umumnya, saat sistem menerima paket SYN, sistem akan mengirim balik paket SYN ACK ke pengirim dan sistem akan menerima paket ACK dari pengirim untuk menyelesaikan komunikasi. Pada serangan SYN Flood, penyerang membanjiri sistem dengan mengirim banyak paket SYN, sistem tetap akan mengirim paket SYN ACK, namun dikarenakan informasi dari yang dikirim dari paket SYN tidak valid, maka sistem tidak akan mendapatkan paket ACK dan sistem akan terus menunggu paket ACK tersebut sampai waktu koneksi habis. Karena banyaknya komunikasi yang belum terselesaikan menyebabkan kinerja sistem menjadi sangat lambat [7].

Salah satu konsep yang sangat baik dalam keamanan data adalah pendekatan defense in depth yang menggunakan desain struktural multilayer, dimana firewall, anti-virus, serta Intrusion Detection and Prevention System (IDPS) digunakan untuk menghindari seluruh upaya penyerangan pada sistem jaringan dan juga server[8].

Pada penelitian [9], membahas mengenai pengenalan pola serangan TCP FIN Flood serta Zbassocflood / Association Flood pada jaringan Internet Of Things (IoT) memakai metode Rule Based Signature Analysis. Riset tersebut dilakukan pada komunikasi WiFi serta IEEE 802.15.4. Pengujian dilakukan dengan memakai dua parameter Instrusion Detection System (IDS), pengujian pertama memakai Snort serta pengujian kedua menggunakan metode Rule Based Signature Analysis. Pengujian memakai Snort bertujuan selaku pembanding dari metode Rule Based Signature Analysis. Hasil dari pengujian tersebut menampilkan kalau pengujian memakai metode Rule Based Signature Analysis lebih baik, dengan tingkatan persentase rata- rata akurasi 99,9199%, sebaliknya Snort hanya memiliki tingkatan persentase rata- rata akurasi 26,3268%.

Selanjutnya pada penelitian [10], membahas cara menerapkan mekanisme deteksi serangan memakai Intrusion Detection (IDS) pada jaringan IoT memakai rule basaed, contohnya petri nets, state machine dan signature analysis. IDS didistribusikan untuk menghindari serangan yang berkaitan dengan sumber daya yang terdapat pada IoT.

Merujuk dari latar belakang tersebut, penelitian ini akan membahas mengenai pengenalan pola pada salah satu serangan DDoS yaitu SYN Flood pada jaringan Internet Of Things (IoT) yang diberi judul “Pengenalan Pola Serangan TCP SYN Flood DDoS Pada Jaringan Internet of Things (IoT) Menggunakan Metode *Rule Based Signature*”

## 1.2 Tujuan

Adapun tujuan dari penelitian ini adalah :

1. Membedakan pola paket serangan SYN Flood Distributed Denial of Service (DDoS) pada jaringan Internet of Things (IoT)
2. Mengimplementasikan *Intrusion Detection System* (IDS) pada jaringan Internet of Things (IoT) menggunakan rule based signatured analysis.
3. Memahami pattern dari serangan *SYN Flood Distributed Denial of Service* (DDoS) pada jaringan *Internet of Things* (IoT)

## 1.3 Manfaat

Adapun Manfaat yang bisa diambil dari penelitian ini :

1. Dapat mengenali pola serangan *DDoS SYN Flood*.
2. Dapat mengetahui atribut unik dari paket serangan *DDoS SYN Flood*.
3. Sebagai referensi bagi peneliti lain mengenai serangan *DDoS SYN Flood*.

## 1.4 Perumusan Masalah

Berikut merupakan rumusan masalah pada penelitian ini :

1. Bagaimana cara menentukan atribut untuk mengetahui pola serangan *DDoS SYN Flood* ?
2. Bagaimana cara menggunakan metode *signature rule based* untuk mendeteksi serangan *DDoS SYN Flood* ?

### **1.5 Batasan Masalah**

Berikut batasan masalah dari tugas akhir ini, yaitu :

1. Pengujian dilakukan hanya pada serangan TCP SYN Flood.
2. Tidak dilakukan pada lalu lintas jaringan real-time.
3. Metode yang digunakan untuk mengenali pola serangan TCP SYN Flood Distributed Denial of Service (DDoS) pada jaringan Internet of Things (IoT) adalah Rule Based Signature Analysis.
4. Tidak membahas cara mencegah serangan tersebut.

### **1.6 Metodelogi Penelitian**

Pada tugas akhir ini menggunakan metodelogi sebagai berikut :

#### **1. Metode Studi Pustaka dan Literature**

Pada metode ini mencari dan mengumpulkan referensi yang berupa literature yang terdapat pada buku, jurnal ilmiah, dan internet yang berkaitan dengan pembahasan Tugas Akhir ini.

#### **2. Metode Konsultasi**

Pada metode ini melakukan konsultasi kepada pihak-pihak yang memiliki pengetahuan serta wawasan yang baik dalam mengatasi permasalahan yang ditemui pada penulisan tugas akhir ini.

#### **3. Metode Perancangan Software**

Dalam tahap ini dilakukan perancangan serta pembuatan sistem untuk mengenali pola serangan *TCP SYN Flood Distributed Denial of Service* (DDoS) pada jaringan *Internet of Things* (IoT).

#### 4. Metode Pengujian

Pada metode ini akan dilakukan pengujian sistem dengan Batasan masalah dengan parameter – parameter yang telah di tentukan.

#### 5. Metode Analisa dan Kesimpulan

Hasil dari pengujian pada metode sebelumnya kemudian dianalisa untuk mengetahui kekurangan dari hasil perancangan dan factor penyebabnya, sehingga dapat dilakukan pengembangan pada penelitian selanjutnya.

### **1.7 Sistematika Penulisan**

Pada penelitian ini digunakan sistematika sebagai berikut untuk mendeskripsikan bab – bab penelitian yang tersusun. Berikut susunan penelitian yang digunakan yaitu :

### **BAB I PENDAHULUAN**

Pada bab ini menjelaskan latar belakang, tujuan, manfaat, rumusan masalah, batasan masalah, metodologi penelitian dan sistematika penelitian mengenai pengenalan pola serangan *DDoS SYN Flood* pada jaringan *Internet of Things* (*IoT*) menggunakan metode *Signature based analysis*.

### **BAB II TINJAUAN PUSTAKA**

Pada bab ini menjelaskan mengenai teori yang berasal dari berbagai sumber yang dijadikan sebagai referensi penelitian. Bab ini berisikan *literature review* yang berkaitan mengenai pengenalan pola serangan *DDoS SYN Flood* pada jaringan *Internet of Things* (*IoT*) menggunakan metode *Signature based analysis*.

### **BAB III METODOLOGI PENELITIAN**

Pada bab ini berisikan penjelasan tahapan - tahapan secara rinci dan rangkaian kerja untuk melakukan pengenalan pola serangan *DDoS SYN Flood* pada jaringan *IoT*.

### **BAB IV HASIL DAN PEMBAHASAN**

Pada bab ini berisikan hasil dari pengujian yang telah dilakukan dan data yang diuji akan dianalisa dengan menggunakan teknik yang sesuai dan selanjutnya akan dilakukan validasi hasil.

### **BAB V KESIMPULAN**

Pada bab ini berisikan kesimpulan dan saran yang didapatkan dari hasil penelitian yang telah dilakukan.

## DAFTAR PUSTAKA

- [1] W. Najib, S. Sulistyo, and Widyawan, “Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things,” *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 9, no. 4, pp. 375–384, 2020, doi: 10.22146/jnteti.v9i4.539.
- [2] A. Botta, W. De Donato, V. Persico, and A. Pescapé, “Integration of Cloud computing and Internet of Things: A survey,” *Futur. Gener. Comput. Syst.*, vol. 56, pp. 684–700, 2016, doi: 10.1016/j.future.2015.09.021.
- [3] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, 2017, doi: 10.1109/JIOT.2017.2683200.
- [4] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, “Internet of Things security: A survey,” *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, 2017, doi: 10.1016/j.jnca.2017.04.002.
- [5] P. Kamboj, M. C. Trivedi, V. K. Yadav, and V. K. Singh, “Detection techniques of DDoS attacks: A survey,” *2017 4th IEEE Uttar Pradesh Sect. Int. Conf. Electr. Comput. Electron. UPCON 2017*, vol. 2018-Januari, pp. 675–679, 2017, doi: 10.1109/UPCON.2017.8251130.
- [6] R. Vishwakarma and A. K. Jain, “A survey of DDoS attacking techniques and defence mechanisms in the IoT network,” *Telecommun. Syst.*, vol. 73, no. 1, pp. 3–25, 2020, doi: 10.1007/s11235-019-00599-z.
- [7] G. Ramadhan, Y. Kurniawan, and Chang-Soo Kim, “Design of TCP SYN Flood DDoS attack detection using artificial immune systems,” pp. 72–76, 2017, doi: 10.1109/icsengt.2016.7849626.
- [8] W. Bul’ajoul, A. James, and S. Shaikh, “A New Architecture for Network Intrusion Detection and Prevention,” *IEEE Access*, vol. 7, pp. 18558–18573, 2019, doi: 10.1109/ACCESS.2019.2895898.

- [9] D. Wahyudi and D. Stiawan, “Deteksi Serangan Denial of Service Menggunakan Rule Based Signature Analysis Pada Jaringan Internet of Things,” *eJournal Sriwij. Univ.*, 2018, [Online]. Available: <https://repository.unsri.ac.id/47903/>.
- [10] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. De, “Author ’ s Accepted Manuscript A Survey of Intrusion Detection in I nternet of Things Reference ;,” *J. Netw. Comput. Appl.*, 2017, doi: 10.1016/j.jnca.2017.02.009.
- [11] Dr. S. Smys, Dr. Abul Basar, and Dr. Haoxiang Wang, “Hybrid Intrusion Detection System for Internet of Things (IoT),” *J. ISMAC*, vol. 2, no. 4, pp. 190–199, 2020, doi: 10.36548/jismac.2020.4.002.
- [12] D. I. J. Sdn, “Deteksi Serangan Ddos Udp Flood Dengan Metode Rule-Based Signature Secara Real-Time,” no. 09011281419046, pp. 1–2, 2019.
- [13] A. SETIAWAN, D. Stiawan, and A. Heryanto, “VISUALISASI SERANGAN DDOS FIN FLOOD DENGAN METODE ARTIFICIAL IMMUNE SYSTEM PADA JARINGAN INTERNET OF THINGS (IoT),” 2021.
- [14] Walter, *The Illustrated Network*. 2014.
- [15] T. M. Booij, I. Chiscop, E. Meeuwissen, N. Moustafa, and F. T. H. D. Hartog, “ToN\_IoT: The Role of Heterogeneity and the Need for Standardization of Features and Attack Types in IoT Network Intrusion Data Sets,” *IEEE Internet Things J.*, vol. 9, no. 1, pp. 485–496, 2022, doi: 10.1109/JIOT.2021.3085194.
- [16] A. R. Gad, A. A. Nashat, and T. M. Barkat, “Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset,” *IEEE Access*, vol. 9, pp. 142206–142217, 2021, doi: 10.1109/ACCESS.2021.3120626.
- [17] N. Moustafa, “A new distributed architecture for evaluating AI-based

security systems at the edge: Network TON\_IoT datasets,” *Sustain. Cities Soc.*, vol. 72, no. June, 2021, doi: 10.1016/j.scs.2021.102994.

- [18] D. Stiawan *et al.*, “Ping Flood Attack Pattern Recognition Using a K-Means Algorithm in an Internet of Things (IoT) Network,” *IEEE Access*, vol. 9, pp. 116475–116484, 2021, doi: 10.1109/ACCESS.2021.3105517.