

**DETEKSI DAN MITIGASI SERANGAN *DISTRIBUTED DENIAL OF SERVICE (DDOS)* PADA *SOFTWARE DEFINED NETWORK (SDN)* MENGGUNAKAN *MULTILAYER PERCEPTRON (MLP)***

**SKRIPSI**

Disusun sebagai salah satu syarat untuk memperoleh Sarjana Teknik (S.T.)



**Disusun oleh:**

**IVAN MUNANDAR PURNAMA**

**NPM. 3332190035**

**JURUSAN TEKNIK ELEKTRO  
FAKULTAS TEKNIK  
UNIVERSITAS SULTAN AGENG TIRTAYASA  
2023**

## LEMBAR PERNYATAAN KEASLIAN SKRIPSI

Dengan ini saya menyatakan bahwa:

Judul : Deteksi dan Mitigasi Serangan *Distributed Denial of Service* (DDoS) pada *Software Defined Network* (SDN) Menggunakan *Multilayer Perceptron* (MLP)

Nama Mahasiswa : Ivan Munandar Purnama

NPM : 3332190035

Fakultas/Jurusan : Teknik/Teknik Elektro

Saya dengan tegas dan jujur menyatakan bahwa skripsi ini adalah hasil karya saya sendiri. Tidak ada bagian di dalamnya yang merupakan plagiat dari karya orang lain dan saya tidak melakukan penjiplakan atau pengutipan dengan cara yang tidak sesuai dengan etika keilmuan yang berlaku. Saya memiliki kesadaran penuh tentang pentingnya menghormati hak cipta dan keaslian karya orang lain. Oleh karena itu, saya berkomitmen untuk tidak melakukan tindakan yang dapat merugikan integritas ilmiah dan keaslian karya saya sendiri. Saya bertanggung jawab atas keseluruhan isi skripsi ini serta keabsahan dan keaslian materi yang ada di dalamnya. Saya juga menyadari bahwa jika kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau jika ada klaim dari pihak lain terhadap keaslian karya saya ini, saya siap sepenuhnya menanggung resiko dan sanksi yang dijatuhkan kepada saya.

Cilegon, 22 Juli 2024



Ivan Munandar Purnama

NIM.3332190035

## LEMBAR PENGESAHAN

Dengan ini ditetapkan bahwa Skripsi berikut:

Judul : Deteksi dan Mitigasi Serangan *Distributed Denial of Service* (DDoS) pada *Software Defined Network* (SDN) Menggunakan *Multilayer Perceptron* (MLP)  
Nama Mahasiswa : Ivan Munandar Purnama  
NPM : 3332190035  
Fakultas/Jurusan : Teknik/Teknik Elektro

Telah di uji dan dipertahankan pada tanggal 15 Juli 2024 melewati Sidang Skripsi di Fakultas Teknik Universitas Sultan Ageng Tirtayasa Cilegon dan dinyatakan LULUS / TIDAK LULUS

### Dewan Penguji

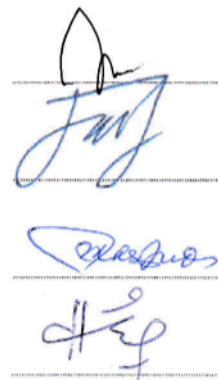
### Tanda Tangan

Pembimbing I : Rian Fahrizal, ST., MEng.

Pembimbing II : Fadil Muhammad, S.T., M.T.

Penguji I : Masjudin, S.T., M.Eng.

Penguji II : Dina Estining Tyas Lufianawati, S.T., M.T.



Mengetahui,

Ketua Jurusan Teknik Elektro



Dr. Eng. Rocky Alfanz, S.T., M.Sc.

NIP.198103282010121001

## PRAKATA

Puji syukur penulis panjatkan ke hadirat Allah SWT, karena dengan rahmat dan hidayah-Nya penulis dapat menyelesaikan penulisan skripsi ini dengan judul "Deteksi dan Mitigasi Serangan DDoS pada Lalu Lintas Jaringan *Software Defined Network* (SDN) Menggunakan *Multilayer Perceptron* (MLP)". Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik Elektro dari Universitas Sultan Ageng Tirtayasa.

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Orang tua tercinta, yang selalu memberikan dukungan, doa, dan kasih sayang tanpa henti. Terima kasih atas segala pengorbanan dan motivasi yang diberikan. Tanpa dukungan mereka, penulis tidak akan mampu menyelesaikan skripsi ini dengan baik.
2. Dr. Eng. Rocky Alfanz, S.T., M.Sc., selaku Ketua Jurusan Teknik Elektro, yang telah memberikan kesempatan dalam menjalankan penelitian ini. Bimbingan dari beliau sangat membantu penulis dalam memahami dan menyelesaikan masalah-masalah yang muncul selama penelitian.
3. Fadil Muhammad, S.T., M.T., selaku Pembimbing Akademik serta Pembimbing 2 skripsi, yang telah memberikan arahan, saran, dan motivasi yang sangat berarti dalam penyelesaian skripsi ini. Terima kasih atas kesabaran dan perhatian yang diberikan. Bimbingan dari beliau menginspirasi penulis untuk terus berkembang dan menghasilkan penelitian yang berkualitas.
4. Rian Fahrizal, S.T., M.Eng., selaku Pembimbing 1 skripsi, yang telah memberikan bimbingan, ilmu, dan pengalaman berharga dalam penulisan skripsi ini. Terima kasih atas bimbingan yang mendalam dan dukungan yang diberikan. Beliau telah membantu penulis dalam memahami konsep-konsep yang kompleks dan memberikan panduan yang jelas untuk mencapai tujuan penelitian.
5. Kepada teman-teman yang memberikan dukungan moral, semangat, dan persahabatan sepanjang perjalanan penulisan skripsi ini, penulis mengucapkan terima kasih yang sebesar-besarnya. Dukungan dan semangat dari teman-

teman sangat berarti bagi penulis dalam menghadapi tantangan dan melewati masa-masa sulit selama penulisan skripsi ini. Persahabatan yang terjalin juga memberikan motivasi dan kebahagiaan tersendiri dalam perjalanan ini.

Penulis juga ingin menyampaikan terima kasih kepada semua pihak yang telah memberikan kontribusi, bantuan, dan dukungan dalam penyelesaian skripsi ini. Semoga skripsi ini dapat bermanfaat bagi pengembangan ilmu pengetahuan di bidang Teknik Elektro dan menjadi sumbangan positif bagi perkembangan dunia akademik. Akhir kata, penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan. Oleh karena itu, penulis menerima dengan tangan terbuka setiap saran, masukan, dan kritik membangun untuk peningkatan kualitas penelitian di masa yang akan datang.

Cilegon, 22 Juli 2024



Ivan Munandar Purnama

NIM.3332190035

# ABSTRAK

Ivan Munandar Purnama

Teknik Elektro

Deteksi dan Mitigasi Serangan *Distributed Denial of Service* (DDoS) pada *Software Defined Network* (SDN) Menggunakan *Multilayer Perceptron* (MLP)

Serangan *Distributed Denial of Service* (DDoS) pada *Software Defined Network* (SDN) telah menjadi ancaman yang semakin meningkat, mengakibatkan gangguan serius pada ketersediaan layanan dan keandalan infrastruktur. Saat ini, teknik deteksi serangan DDoS yang paling umum digunakan pada jaringan tradisional maupun SDN adalah metode deteksi berbasis statistik, namun metode ini memiliki kelemahan dalam mendeteksi serangan yang baru atau belum pernah terjadi sebelumnya. Hal tersebut dapat diatasi dengan menggunakan metode *deep learning* yang mampu untuk menangani data bersifat non-linier, heterogen, dan berdimensi tinggi, yang sering ditemukan pada data lalu lintas jaringan. Penelitian ini mengembangkan sistem deteksi dan mitigasi serangan DDoS pada lalu lintas jaringan SDN menggunakan algoritma *Multilayer Perceptron* (MLP). Pengujian yang dilakukan menunjukkan bahwa sistem deteksi dan mitigasi serangan DDoS yang dikembangkan dalam penelitian ini memiliki tingkat akurasi sebesar 71,17%. Sistem ini terbukti efektif dalam mendeteksi serangan DDoS. Analisis performa jaringan pasca-mitigasi menunjukkan peningkatan performa yang signifikan dibandingkan dengan kondisi sebelum mitigasi. Sebelumnya, *bottleneck* teridentifikasi pada jaringan. Namun, setelah dilakukan mitigasi, jaringan dapat kembali berfungsi secara optimal.

Kata kunci: DDoS, *Deep Learning*, SDN, MLP, deteksi, mitigasi.

## **ABSTRACT**

Ivan Munandar Purnama

Electrical Engineering

### Detection and Mitigation of Distributed Denial of Service (DDoS) Attacks on Software Defined Network (SDN) Using Multilayer Perceptron (MLP)

Distributed Denial of Service (DDoS) attacks on Software Defined Networks (SDNs) have become a growing threat, resulting in serious disruptions to service availability and infrastructure reliability. Currently, the most common DDoS attack detection technique used on both traditional and SDN networks is the statistical-based detection method. However, this method has the limitation of detecting new or unprecedented attacks. This can be overcome by using deep learning methods that are able to handle non-linear, heterogeneous, and high-dimensional data, characteristic of network traffic data. This research proposed a DDoS attack detection and mitigation system on SDN network traffic using the Multilayer Perceptron (MLP) algorithm. The tests show that the DDoS attack detection and mitigation system developed in this study has an accuracy of 71.17%. This system has demonstrated effectiveness in detecting DDoS attacks. Post-mitigation network performance analysis shows a significant improvement in performance compared to pre-mitigation conditions. Previously, bottlenecks were identified in the network. However, after mitigation, the network can regain optimal functionality.

Keywords: DDoS, Deep Learning, SDN, MLP, detection, mitigation.

## DAFTAR ISI

<b>HALAMAN JUDUL</b> .....	i
<b>LEMBAR PERNYATAAN KEASLIAN SKRIPSI</b> .....	ii
<b>LEMBAR PENGESAHAN</b> .....	iii
<b>PRAKATA</b> .....	iv
<b>ABSTRAK</b> .....	vi
<b>ABSTRACT</b> .....	vii
<b>DAFTAR ISI</b> .....	viii
<b>DAFTAR TABEL</b> .....	xiv
<b>BAB I PENDAHULUAN</b> .....	1
1.1. Latar Belakang .....	1
1.2. Rumusan Masalah.....	3
1.3. Tujuan penelitian .....	3
1.4. Manfaat Penelitian .....	4
1.5. Batasan Masalah .....	4
1.6. Sistematika Penulisan .....	5
<b>BAB II TINJAUAN PUSTAKA</b> .....	6
2.1. Artificial Intelligence .....	6
2.2. <i>Machine Learning</i> .....	6
2.3. <i>Deep Learning</i> .....	7
2.4. Matriks Evaluasi pada <i>artificial intelligence</i> Model.....	7
2.4.1 Matriks Konfusi.....	8
2.4.2 Akurasi .....	8
2.4.3 Presisi .....	8
2.4.4 <i>Recall</i> .....	9
2.4.5 <i>F1 Score</i> .....	9
2.4.6 <i>Loss Function</i> .....	9



2.4.7	<i>Receiver Operating Characteristic Curve (ROC Curve)</i> .....	9
2.5.	<i>Multilayer Perceptron (MLP)</i> .....	9
2.6.	Jaringan Komputer.....	10
2.7.	<i>Software-Defined Networks</i> .....	12
2.7.2	Mininet .....	13
2.7.3	<i>Ryu controller</i> .....	14
2.8.	<i>Quality of Service</i> .....	14
2.8.2	<i>Throughput</i> .....	15
2.8.3	<i>Delay</i> .....	15
2.8.4	<i>Jitter</i> .....	15
2.8.5	<i>Packet loss</i> .....	16
2.9.	<i>Cyber Security</i> .....	16
2.10.	Serangan DDoS.....	17
2.11.	Python .....	20
2.12.	Kajian Pustaka .....	20
<b>BAB III</b>	<b>METODOLOGI PENELITIAN</b> .....	<b>23</b>
3.1.	Alur Penelitian .....	23
3.2.	Komponen Penelitian.....	24
3.2.1	Python.....	24
3.2.2	Sistem Operasi Ubuntu 22.04.....	24
3.2.3	<i>Traffict Generator</i> .....	24
3.2.4	Wireshark .....	24
3.2.5	<i>S-flow</i> RT.....	24
3.2.6	Jupyter Notebook.....	25
3.2.7	Mininet .....	25
3.2.8	<i>Ryu controller</i> .....	25

3.2.9	Hardware .....	25
3.3.	Metode Penelitian .....	26
3.3.1	Studi Literatur.....	26
3.3.2	Perancangan Topologi <i>Software Defined Network</i> (SDN).....	27
3.3.3	Akuisisi Data .....	30
3.3.4	Pra-pemrosesan data.....	32
3.3.5	Perancangan Algoritma .....	33
3.3.6	Training <i>Dataset</i> .....	34
3.3.7	Uji Keandalan Model .....	34
3.3.8	Analisis <i>Quality of Service</i> (QoS) .....	35
3.4.	Perancangan Sistem .....	36
<b>BAB IV</b>	<b>HASIL DAN PEMBAHASAN</b> .....	<b>37</b>
4.1.	Analisis Jaringan.....	37
4.2.	Analisis Hasil Deteksi dan Mitigasi.....	41
4.2.1	Lalu lintas Normal.....	41
4.2.2	ICMP <i>flood</i> .....	43
4.2.3	UDP <i>flood</i> .....	45
4.2.4	TCP SYN <i>flood</i> .....	46
4.2.5	Rata -Rata Efektivitas Deteksi.....	49
4.3.	Analisis Performa Jaringan .....	50
4.3.1	<i>Jitter</i> .....	50
4.3.2	<i>Delay</i> .....	52
4.3.3	<i>Throughput</i> .....	54
4.3.4	<i>Packet Loss</i> .....	55
4.3.5	<i>Resource Utilization</i> .....	57
4.4.	Hasil dan Analisis Pembuatan <i>Dataset</i> .....	60

4.5. Evaluasi Model MLP .....	62
4.6. Efektivitas Pelatihan Model .....	67
<b>BAB V PENUTUP</b> .....	<b>70</b>
5.1. Kesimpulan .....	70
5.2. Saran. ....	71
<b>LAMPIRAN A HASIL SIMULASI PERCOBAAN</b> .....	<b>A-1</b>
<b>LAMPIRAN B KODE PROGRAM</b> .....	<b>B-1</b>

## DAFTAR GAMBAR

Gambar 2.1	Arsitektur jaringan berdasarkan model OSI .....	11
Gambar 2.2	Jenis serangan siber .....	12
Gambar 2.3	Jenis serangan siber .....	16
Gambar 3.1	Diagram alir penelitian.....	23
Gambar 3.2	Topologi jaringan SDN .....	28
Gambar 3.3	Blok diagram pembuatan <i>dataset</i> .....	30
Gambar 3.4	Alur pra-pemrosesan data.....	32
Gambar 3.5	Alur proses training data .....	34
Gambar 3.6	Perancangan sistem .....	36
Gambar 4.1	Topologi jaringan linear .....	38
Gambar 4.2	Koneksi antara <i>host</i> dan <i>switch</i> .....	39
Gambar 4.3	Aktivitas <i>port</i> saat pertama kali terhubung .....	40
Gambar 4.4	Hasil pengujian <i>pingall</i> pada terminal mininet .....	41
Gambar 4.5	Hasil monitoring lalu lintas normal.....	42
Gambar 4.6	Hasil deteksi lalu lintas normal .....	42
Gambar 4.7	Hasil monitoring lalu lintas ICMP <i>flood</i> .....	43
Gambar 4.8	Hasil deteksi dan mitigasi lalu lintas ICMP <i>flood</i> .....	44
Gambar 4.9	Hasil monitoring lalu lintas UDP <i>flood</i> .....	45
Gambar 4.10	Hasil deteksi dan mitigasi lalu lintas UDP <i>flood</i> .....	46
Gambar 4.11	Hasil monitoring lalu lintas TCP SYN.....	47
Gambar 4.12	Lalu lintas TCP SYN <i>flood</i> pada Wireshark .....	47
Gambar 4.13	Hasil deteksi dan mitigasi lalu lintas TCP SYN <i>flood</i> .....	48
Gambar 4.14	<i>Jitter</i> pada jaringan lalu lintas normal.....	50
Gambar 4.15	Hasil <i>dataset</i> berdasarkan ekstraksi jaringan SDN .....	60
Gambar 4.16	Distribusi jumlah paket lalu lintas dalam <i>dataset</i> .....	61
Gambar 4.17	Hasil <i>pre-processing Dataset</i> .....	62
Gambar 4.18	Akurasi model MLP .....	63
Gambar 4.19	Grafik <i>loss</i> model MLP .....	64
Gambar 4.20	Grafik <i>Receiver Operating Characteristic (ROC)</i> .....	65
Gambar 4.21	Grafik presisi- <i>recall</i> .....	65

Gambar 4.22 Kurva pembelajaran model .....	66
Gambar 4.23 Laporan hasil klasifikasi .....	67
Gambar 4.24 <i>Confusion matrix</i> model .....	68
Gambar 4.25 Dataframe hasil prediksi.....	69

## DAFTAR TABEL

Tabel 2.1 Standar TIPHON .....	14
Tabel 3.1 Tabel spesifikasi <i>hardware</i> .....	26
Tabel 3.2 Tabel konfigurasi SDN .....	29
Tabel 3.3 Tabel parameter lingkungan simulasi .....	31
Tabel 3.4 Tabel arsitektur MLP .....	33
Tabel 4.1 Hasil deteksi sistem.....	49
Tabel 4.2 <i>Jitter</i> selama serangan dan setelah mitigasi DDoS .....	51
Tabel 4.3 <i>Delay</i> jaringan pada lalu lintas normal .....	52
Tabel 4.4 <i>Delay</i> selama serangan dan setelah mitigasi DDoS.....	53
Tabel 4.5 <i>Throughput</i> jaringan pada lalu lintas normal .....	54
Tabel 4.6 <i>Throughput</i> selama serangan dan setelah mitigasi DDoS.....	54
Tabel 4.7 <i>Packet loss</i> pada lalu lintas normal .....	55
Tabel 4.8 <i>Packet loss</i> selama serangan dan setelah mitigasi DDoS .....	56
Tabel 4.9 <i>Resource utilization</i> pada lalu lintas normal .....	58
Tabel 4.10 <i>Resource utilization</i> pada lalu lintas DDoS .....	58

# BAB I

## PENDAHULUAN

### 1.1. Latar Belakang

Dalam era digital saat ini, jaringan komputer telah menjadi salah satu infrastruktur penting bagi organisasi maupun individu. Kemajuan pesat dalam jaringan dan teknologi informasi telah memungkinkan koneksi tanpa batas untuk menyimpan dan mengkomunikasikan informasi dalam skala besar dalam bentuk teks dan suara yang sensitif [1]. Namun, kemajuan teknologi ini juga membawa ancaman terhadap keamanan jaringan. Salah satu serangan utama yang paling dominan menyebabkan penolakan layanan kepada pengguna adalah *Distributed Denial of Service* (DDoS) [2], [3].

Serangan DDoS adalah salah satu ancaman utama terhadap keamanan sistem informasi dan infrastruktur jaringan yang meningkat pesat baik frekuensi maupun intensitasnya setiap tahun. Dalam laporan internet tahunan Cisco, 2018–2023 menunjukkan bahwa tren lonjakan serangan DDoS dari tahun 2018 sebanyak 7,09 juta hingga tahun 2023 diperkirakan serangan DDoS akan meningkat sebanyak 15,4 juta [4]. Serangan DDoS bekerja dengan cara membanjiri paket data secara besar-besaran. Tujuan serangan DDoS adalah untuk menghabiskan *bandwidth* jaringan dan menolak layanan untuk pengguna yang sah dari sistem target [5], [6]. Penelitian dalam deteksi dan pencegahan serangan DDoS dalam transaksi jaringan streaming telah menjadi fokus utama selama lebih dari satu dekade [7]. Penyerang biasanya mengeksploitasi kerentanan dalam *transportasi* data, jaringan, dan protokol lapisan aplikasi seperti *Transmission Control Protocol* (TCP), *User Datagram Protocol* (UDP), dan *Internet Control Message Protocol* (ICMP) [8]. Oleh karena itu, keamanan jaringan menjadi aspek yang sangat penting untuk diperhatikan guna mencegah terjadinya serangan DDoS yang tidak hanya merugikan dari segi keuangan dan operasional, tetapi juga dapat merugikan reputasi suatu entitas atau bisnis. Sayangnya deteksi serangan terbilang kompleks dan sulit dilakukan karena meniru permintaan asli pengguna [9]. Evolusi serangan DDoS dan kompleksitasnya menekankan perlunya terus-menerus mengembangkan

metode deteksi yang lebih canggih dan solusi pencegahan yang adaptif guna mengatasi tantangan yang terus berkembang di dunia siber yang dinamis.

Tidak seperti jaringan tradisional dimana kontrol dan manajemen jaringan terdistribusi di dalam perangkat keras jaringan seperti router dan *switch*, *Software-Defined Networks* (SDN) adalah jenis jaringan berbeda dengan pengaturannya terpusat pada perangkat lunak sehingga memungkinkan SDN menjadi solusi yang dapat diandalkan dalam melindungi dari serangan DDoS dengan kontrol lebih fleksibel dan adaptif [10]. Selama beberapa tahun terakhir, SDN telah terbukti mampu menghasilkan pertahanan yang efektif terhadap berbagai jenis serangan DDoS berbasis jaringan [11]. Saat ini, teknik deteksi serangan DDoS yang paling umum digunakan pada jaringan SDN adalah metode deteksi berbasis statistik, namun metode ini memiliki kelemahan dalam mendeteksi serangan yang baru atau belum pernah terjadi sebelumnya [12]. Pada penelitian yang dilakukan oleh [13] menggunakan metode deteksi DDoS berbasis statistik memiliki beberapa kekurangan. Salah satu kekurangan utamanya adalah kinerjanya yang buruk pada serangan DDoS yang sangat besar seperti serangan berjuta-juta paket yang terjadi dalam waktu yang singkat. Selain itu, metode ini juga dapat menghasilkan banyak *false positive* dan *false negative*. Untuk mengatasi kekurangan ini, beberapa penelitian menggunakan metode berbasis *machine learning*. Metode ini mampu meningkatkan akurasi dan kinerja deteksi DDoS pada serangan yang sangat besar dan kompleks [14]. Dengan kemajuan teknik *deep learning* dan peningkatan kinerja *Graphics Processing Unit* (GPU), terdapat potensi besar untuk mempercepat pengembangan detektor serangan DDoS yang semakin kompleks [12], [15].

*Dataset* yang digunakan pada penelitian ini dibuat pada jaringan SDN dengan menggunakan simulasi *hping3* melibatkan serangkaian langkah untuk merekam data lalu lintas yang dihasilkan oleh perangkat lunak simulasi ini. Dengan memanfaatkan *hping3*, skenario serangan dapat disimulasikan, dan data yang dihasilkan selama simulasi tersebut kemudian direkam untuk membentuk *dataset*. *Dataset* yang dihasilkan dapat mencakup berbagai jenis serangan serangan *Distributed Denial of Service* (DDoS) yang direplikasi dalam simulasi. *Dataset* ini dapat digunakan untuk melatih model deteksi intrusi dan mengembangkan strategi pencegahan yang efektif dalam jaringan SDN. Selain itu, *dataset* ini juga dapat



digunakan untuk menguji keandalan dan kinerja algoritma deteksi intrusi yang ada, serta melakukan penelitian lebih lanjut dalam bidang keamanan jaringan SDN.

Dalam penelitian ini, diajukan sebuah metode deteksi serangan DDoS berbasis *deep learning* untuk jaringan berbasis SDN. Model *multilayer perceptron* (MLP) digunakan untuk mempelajari pola lalu lintas jaringan yang normal dan mengidentifikasi anomali yang mengindikasikan serangan DDoS. Dengan menggunakan *deep learning*, metode ini diharapkan dapat meningkatkan akurasi dan kecepatan deteksi serangan DDoS pada jaringan berbasis SDN. Selain itu, penelitian ini juga diharapkan dapat memberikan kontribusi pada pengembangan teknik *machine learning* dalam deteksi serangan DDoS pada jaringan komputer. Selain itu, hasil penelitian ini juga dapat memberikan panduan bagi organisasi atau perusahaan dalam mengamankan infrastruktur jaringan mereka dari serangan DDoS.

## **1.2. Rumusan Masalah**

Pada penelitian ini terdapat empat permasalahan utama yang diharapkan dapat diselesaikan diantaranya:

1. Bagaimana cara melakukan deteksi dan mitigasi yang cepat dan efektif terhadap serangan DDoS?
2. Bagaimana cara melatih dan menyesuaikan parameter model MLP agar dapat mengklasifikasikan serangan DDoS?
3. Bagaimana mempersiapkan *environment* yang tepat untuk pelatihan dan pengujian model?
4. Bagaimana performa penggunaan algoritma MLP untuk deteksi dan mitigasi serangan DDoS?

## **1.3. Tujuan penelitian**

Pada penelitian ini memiliki beberapa tujuan yang diharapkan tercapai, diantaranya:

1. Mengetahui cara membuat sistem deteksi dan mitigasi DDoS yang cepat dan efektif dengan menggunakan model *Multilayer Perceptron* (MLP).
2. Melatih dan menyesuaikan model MLP agar mampu mengklasifikasikan serangan DDoS.

3. Memilih dan mempersiapkan *environment* dan topologi yang tepat serta relevan untuk melatih dan menguji serangan DDoS.
4. Menganalisis performa *deep learning* khususnya model MLP dalam mendeteksi serangan DDoS untuk mengetahui apakah model *deep learning* mampu untuk mendeteksi dan memitigasi serangan DDoS.

#### 1.4. Manfaat Penelitian

Berikut adalah beberapa manfaat yang dapat diperoleh dari penelitian yang dilakukan, di antaranya adalah sebagai berikut:

1. Bagi pengembangan teknologi keamanan jaringan, penelitian ini diharapkan dapat menciptakan sistem deteksi dan klasifikasi DDoS yang cepat dan efektif menggunakan model MLP, yang dapat meningkatkan respons terhadap ancaman keamanan di jaringan.
2. Bagi akademisi dan peneliti keamanan siber, penelitian ini diharapkan dapat memberikan wawasan baru mengenai penerapan model *Multilayer Perceptron* (MLP) dalam deteksi dan mitigasi serangan DDoS, serta mendukung penelitian selanjutnya dalam pengembangan metode deteksi serta mitigasi yang lebih baik di masa depan.
3. Bagi pengelola jaringan, penelitian ini diharapkan dapat membantu mengurangi waktu dan biaya yang dibutuhkan untuk mengembangkan sistem deteksi dan mitigasi serangan DDoS sehingga lebih efisien dalam implementasinya.

#### 1.5. Batasan Masalah

Mengingat luasnya pembahasan sistem deteksi dan mitigasi serangan DDoS menggunakan metode *deep learning* dengan MLP, maka dalam penelitian ini permasalahan perlu di batasi pada:

1. Penelitian ini hanya berfokus pada kinerja model MLP dalam mendeteksi dan mitigasi serangan DDoS tanpa mempertimbangkan faktor lain yang dapat mempengaruhi kinerja model, seperti kecepatan lalu lintas jaringan dan arsitektur jaringan.
2. Penelitian ini hanya membahas sistem deteksi serangan DDoS menggunakan model *deep learning* pada jaringan SDN tanpa mempertimbangkan mengimplementasikannya pada sistem keamanan lainnya.

3. Data yang digunakan dalam penelitian ini terbatas pada data serangan DDoS yang dihasilkan melalui simulasi pada jaringan SDN.
4. Membangun jaringan SDN lokal dengan menggunakan mininet dan *Ryu controller* yang terdiri dari 15 PC, 5 *switch*, dan 1 *controller*.
5. Parameter *delay*, *throughput*, *packet loss*, dan *resource utilization* digunakan sebagai indikator untuk mengukur kualitas jaringan SDN ketika dilintasi *flow* data normal dan DDoS.

## 1.6. Sistematika Penulisan

Sistematika penulisan skripsi ini terdiri dari lima bab, yaitu di susun sebagai berikut.

### BAB I

Bab ini akan membahas mengenai latar belakang, identifikasi masalah, tujuan penelitian, manfaat penelitian, ruang lingkup penelitian, dan sistematika penulisan.

### BAB II

Bab ini akan membahas mengenai teori-teori dan penelitian terkait yang relevan dengan topik penelitian ini. Bab ini berisi tentang teori jaringan komputer, serangan DDoS, jaringan *Software Defined Network* (SDN), teknik deteksi serangan DDoS, Python, *deep learning*, dan *MLP*.

### BAB III

Bab ini akan menjelaskan mengenai rancangan dan metode penelitian yang digunakan pada penelitian ini, seperti teknik *pre-processing* data, pembuatan jaringan virtual, teknik klasifikasi serangan DDoS menggunakan algoritma *MLP*, alur *training*, dan pengujian hasil penelitian.

### BAB IV

Bab ini akan membahas mengenai hasil penelitian yang telah dilakukan, serta analisis terhadap hasil tersebut.

### BAB V

Bab ini akan berisi kesimpulan dari hasil penelitian yang telah dilakukan, serta saran untuk penelitian selanjutnya yang dapat dilakukan untuk pengembangan lebih lanjut.

## Daftar Pustaka

- [1] P. A and S. S, “DDOS ATTACK DETECTION IN TELECOMMUNICATION NETWORK USING MACHINE LEARNING,” *Journal of Ubiquitous Computing and Communication Technologies*, vol. 01, no. 01, pp. 33–44, Sep. 2019, doi: 10.36548/jucct.2019.1.004.
- [2] F. J. Abdullayeva, “Distributed denial of service attack detection in E-government cloud via data clustering,” *Array*, vol. 15, Sep. 2022, doi: 10.1016/j.array.2022.100229.
- [3] P. Khuphiran, P. Leelaprute, P. Uthayopas, K. Ichikawa, and W. Watanakeesuntorn, “Performance Comparison of Machine Learning Models for DDoS Attacks Detection,” in *2018 22nd International Computer Science and Engineering Conference (ICSEC)*, IEEE, Nov. 2018, pp. 1–4. doi: 10.1109/ICSEC.2018.8712757.
- [4] “Cisco Annual Internet Report - Cisco Annual Internet Report (2018–2023) White Paper - Cisco.” Accessed: Mar. 30, 2023. [Online]. Available: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html>
- [5] F. J. Abdullayeva, “Convolutional Neural Network-Based Automatic Diagnostic System for AL-DDoS Attacks Detection,” *International Journal of Cyber Warfare and Terrorism*, vol. 12, no. 1, pp. 1–15, Jul. 2022, doi: 10.4018/IJCWT.305242.
- [6] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, “DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison,” *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 2, pp. 930–939, Apr. 2023, doi: 10.11591/eei.v12i2.4466.
- [7] P. K. Kishore, S. Ramamoorthy, and V. N. Rajavarman, “AN IMPROVED BIO-INSPIRED BAT ALGORITHM FOR DETECTION AND PREVENTION OF HTTP FLOOD DDOS ATTACK USING MACHINE LEARNING METRICS,” 2020.
- [8] H. S. Obaid and E. H. Abeed, “Abeed,-DoS and DDoS Attacks at OSI Layers,” *International Journal of Multidisciplinary Research and Publications Hadeel S. Obaid and Esamaddin H*, vol. 2, no. 8, pp. 1–9, 2020.
- [9] M. S. Mahmoud and Y. Xia, “Distributed denial-of-service attacks,” in *Cloud Control Systems*, S. Ison, Ed., Elsevier, 2020, pp. 51–76. doi: 10.1016/B978-0-12-818701-2.00011-1.
- [10] B. Nugraha and R. N. Murthy, “Deep Learning-based Slow DDoS Attack Detection in SDN-based Networks,” in *2020 IEEE Conference on Network*

*Function Virtualization and Software Defined Networks, NFV-SDN 2020 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020, pp. 51–56. doi: 10.1109/NFV-SDN50289.2020.9289894.

- [11] P. Karthika and K. Arockiasamy, “Simulation of SDN in mininet and detection of DDoS attack using machine learning,” *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 3, pp. 1797–1805, Jun. 2023, doi: 10.11591/eei.v12i3.5232.
- [12] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, “IoT DoS and DDoS Attack Detection using ResNet,” in *Proceedings - 2020 23rd IEEE International Multi-Topic Conference, INMIC 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020. doi: 10.1109/INMIC50486.2020.9318216.
- [13] H. Majed, H. N. Noura, O. Salman, M. Malli, and A. Chehab, “Efficient and secure statistical DDoS detection scheme,” in *ICETE 2020 - Proceedings of the 17th International Joint Conference on e-Business and Telecommunications*, SciTePress, 2020, pp. 153–161. doi: 10.5220/0009873801530161.
- [14] S. Hosseini and M. Azizi, “The hybrid technique for DDoS detection with supervised learning algorithms,” *Computer Networks*, vol. 158, pp. 35–45, Jul. 2019, doi: 10.1016/j.comnet.2019.04.027.
- [15] Q. Zhang, L. T. Yang, Z. Chen, and P. Li, “A survey on deep learning for big data,” Jul. 01, 2018, *Elsevier B.V.* doi: 10.1016/j.inffus.2017.10.006.
- [16] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, “Harnessing artificial intelligence capabilities to improve cybersecurity,” *IEEE Access*, vol. 8, pp. 23817–23837, 2020, doi: 10.1109/ACCESS.2020.2968045.
- [17] A. Aljuhani, “Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments,” *IEEE Access*, vol. 9, pp. 42236–42264, 2021, doi: 10.1109/ACCESS.2021.3062909.
- [18] Naveen Bindra and Manu Sood, “Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset,” *Automatic Control and Computer Sciences*, vol. 53, no. 5, pp. 419–428, Sep. 2019, doi: 10.3103/S0146411619050043.
- [19] A. R. Shaaban, E. Abd-Elwanis, and M. Hussein, “DDoS attack detection and classification via Convolutional Neural Network (CNN),” *2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS)*.

- [20] A. Voulodimos, N. Doulamis, A. Doulamis, and E. Protopapadakis, “Deep Learning for Computer Vision: A Brief Review,” 2018, *Hindawi Limited*. doi: 10.1155/2018/7068349.
- [21] *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*. IEEE, 2018.
- [22] P. P. Shinde, *A Review of Machine Learning and Deep Learning Applications*.
- [23] C. Janiesch, P. Zschech, and K. Heinrich, “Machine learning and deep learning”, doi: 10.1007/s12525-021-00475-2/Published.
- [24] T. Thomas, A. P. Vijayaraghavan, and S. Emmanuel, *Machine Learning Approaches in Cyber Security Analytics*. Singapore: Springer Singapore, 2020. doi: 10.1007/978-981-15-1706-8.
- [25] C. Janiesch, P. Zschech, and K. Heinrich, “Machine learning and deep learning,” *The International Journal On Networked Bussines*, vol. 31, pp. 685–695, 2021, doi: 10.1007/s12525-021-00475-2/Published.
- [26] N. Buduma and N. Locascio, “Deep Learning DESIGNING NEXT-GENERATION MACHINE INTELLIGENCE ALGORITHMS Nikhil Buduma with contributions by Nicholas Locascio,” 2017.
- [27] L. L. Minku, G. Cabral, M. Martins, and M. Wagner, “Introduction to Computational Intelligence,” vol. 1, pp. 105–110, 2023, doi: 10.5281/zenodo.7537827.
- [28] E. Bisong, *Building Machine Learning and Deep Learning Models on Google Cloud Platform*. Apress, 2019. doi: 10.1007/978-1-4842-4470-8.
- [29] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, “A Survey on Machine Learning Techniques for Cyber Security in the Last Decade,” *IEEE Access*, vol. 8, pp. 222310–222354, 2020, doi: 10.1109/ACCESS.2020.3041951.
- [30] G. Howser, *Computer Networks and the Internet*. Cham: Springer International Publishing, 2020. doi: 10.1007/978-3-030-34496-2.
- [31] C. Panek, *Networking fundamentals*. Canada: John Wiley & Sons, Inc, 2020.
- [32] L. Yang, B. Ng, W. K. G. Seah, L. Groves, and D. Singh, “A survey on network forwarding in Software-Defined Networking,” Feb. 15, 2021, *Academic Press*. doi: 10.1016/j.jnca.2020.102947.
- [33] S. Saraswat, V. Agarwal, H. P. Gupta, R. Mishra, A. Gupta, and T. Dutta, “Challenges and solutions in Software Defined Networking: A survey,” *Journal of Network and Computer Applications*, vol. 141, pp. 23–58, Sep. 2019, doi: 10.1016/j.jnca.2019.04.020.

- [34] P. Ferdiansyah and U. Amikom Yogyakarta, “Analisis Perbandingan Parameter QoS Standar TIPHON Pada Jaringan Nirkabel Dalam Penerapan Metode PCQ,” 2022.
- [35] R. A. R. Q. Y. Putri, Anhar, and A. Al Nazen, “Analysis of LTE Network Quality of Service on Streaming Application,” *International Joournal of Electrical, Energy and Power System Engineering (IJEPPSE)*, vol. 6, no. 2, pp. 151–155, 2023.
- [36] M. Snehi and A. Bhandari, “Vulnerability retrospection of security solutions for software-defined Cyber-Physical System against DDoS and IoT-DDoS attacks,” May 01, 2021, *Elsevier Ireland Ltd.* doi: 10.1016/j.cosrev.2021.100371.
- [37] Y. Li and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments,” *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egy.2021.08.126.
- [38] A. M. Abdul and S. Umar, “Attacks of Denial-of-Service on Networks Layer of OSI Model and Maintaining of Security,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 5, no. 1, pp. 181–186, 2017, doi: 10.11591/ijeecs.v5.i1.pp.
- [39] S. Pande, A. Khamparia, D. Gupta, and D. N. H. Thanh, “DDOS Detection Using Machine Learning Technique,” 2021, pp. 59–68. doi: 10.1007/978-981-15-8469-5\_5.
- [40] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, “IoT DoS and DDoS Attack Detection using ResNet,” in *Proceedings - 2020 23rd IEEE International Multi-Topic Conference, INMIC 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020. doi: 10.1109/INMIC50486.2020.9318216.
- [41] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abdulllah, “Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods,” *IEEE Access*, vol. 7, pp. 51691–51713, 2019, doi: 10.1109/ACCESS.2019.2908998.
- [42] A. Bhati, A. Bouras, U. Ahmed Qidwai, and A. Belhi, “Deep learning based identification of DDoS attacks in industrial application,” in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, IEEE, Jul. 2020, pp. 190–196. doi: 10.1109/WorldS450073.2020.9210320.
- [43] “Hacktivists step back giving way to professionals: a look at DDoS in Q3 2022 | Kaspersky.” Accessed: May 03, 2023. [Online]. Available: [https://www.kaspersky.com/about/press-releases/2022\\_hacktivists-step-back-giving-way-to-professionals-a-look-at-ddos-in-q3-2022](https://www.kaspersky.com/about/press-releases/2022_hacktivists-step-back-giving-way-to-professionals-a-look-at-ddos-in-q3-2022)

- [44] J. A. Perez-Diaz, I. A. Valdovinos, K.-K. R. Choo, and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," *IEEE Access*, vol. 8, pp. 155859–155872, 2020, doi: 10.1109/ACCESS.2020.3019330.
- [45] S. H. Islam, P. Vijayakumar, M. Z. A. Bhuiyan, R. Amin, V. Rajeev M., and B. Balusamy, "A Provably Secure Three-Factor Session Initiation Protocol for Multimedia Big Data Communications," *IEEE Internet Things J*, vol. 5, no. 5, pp. 3408–3418, Oct. 2018, doi: 10.1109/JIOT.2017.2739921.
- [46] A. R. Shaaban, E. Abd-Elwanis, and M. Hussein, "DDoS attack detection and classification via Convolutional Neural Network (CNN)," in *2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS)*, IEEE, Dec. 2019, pp. 233–238. doi: 10.1109/ICICIS46948.2019.9014826.
- [47] M. S. Khaing, Y. M. Thant, T. Tun, C. S. Htwe, and M. M. S. Thwin, "IoT Botnet Detection Mechanism Based on UDP Protocol," in *2020 IEEE Conference on Computer Applications (ICCA)*, IEEE, Feb. 2020, pp. 1–7. doi: 10.1109/ICCA49400.2020.9022832.
- [48] "Top 10 Python Libraries untuk Machine Learning - Algoritma." Accessed: Apr. 27, 2023. [Online]. Available: <https://algorit.ma/blog/python-libraries-machine-learning-2022/>
- [49] N. K. Manaswi, *Deep Learning with Applications Using Python*. Berkeley, CA: Apress, 2018. doi: 10.1007/978-1-4842-3516-4.
- [50] Y. Cui *et al.*, "Towards DDoS detection mechanisms in Software-Defined Networking," Sep. 15, 2021, *Academic Press*. doi: 10.1016/j.jnca.2021.103156.
- [51] Institute of Electrical and Electronics Engineers, *2020 IEEE International Conference on Communications Workshops (ICC) : proceedings : Dublin, Ireland, 7-11 June 2020*. 2020.
- [52] R. M. A. Ujjan, Z. Pervez, K. Dahal, A. K. Bashir, R. Mumtaz, and J. González, "Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN," *Future Generation Computer Systems*, vol. 111, pp. 763–779, Oct. 2020, doi: 10.1016/j.future.2019.10.015.