

**PERANCANGAN SISTEM PENDETEKSI DDOS ATTACK PADA
ARSITEKTUR SDN MENGGUNAKAN IPS ATHENA DAN
NOTIFIKASI TELEGRAM BOT**

*Design of a DDoS Attack Detection System on SDN Architecture using IPS Athena and
Telegram Bot Notification*

PROPOSAL PROYEK AKHIR

Diajukan sebagai syarat untuk mengambil Mata Kuliah Proyek Akhir

oleh :

RINALDI MOHAMAD FARHAN

6705184138



D3 TEKNOLOGI TELEKOMUNIKASI

FAKULTAS ILMU TERAPAN

UNIVERSITAS TELKOM

2021

LEMBAR PENGESAHAN

Proposal Proyek Akhir dengan judul :

PERANCANGAN SISTEM PENDETEKSI DDOS ATTACK PADA ARSITEKTUR SDN MENGGUNAKAN IPS ATHENA DAN NOTIFIKASI TELEGRAM BOT

*Design of a DDoS Attack Detection System on SDN Architecture using IPS Athena and
Telegram Bot Notification*

oleh :

RINALDI MOHAMAD FARHAN
6705184138

Telah diperiksa dan disetujui untuk diajukan sebagai syarat mengambil
Mata Kuliah Proyek Akhir
pada Program Studi D3 Teknologi telekomunikasi Universitas Telkom

Bandung, 19 Januari 2021

Menyetujui,

Pembimbing I

22-Jan-21

Inui, Proposal PA
Rinaldi Mohamad Farhan

Rohmat Tulloh, S.T.,M.T.

NIP. 06830002

Pembimbing II



Agus Ganda Permana, Ir.,M.T.

NIP. 91620017

ABSTRAK

Serangan DDoS (*Distributed Denial of Service*) merupakan jenis serangan yang dilakukan dengan cara membanjiri lalu lintas jaringan internet pada *server*, sistem, atau jaringan. Umumnya serangan ini dilakukan menggunakan beberapa *computer host* penyerang sampai dengan computer target tidak bisa diakses. Serangan DDoS terhadap satu entitas di SDN (*Software Defined Network*) berpotensi berdampak terhadap entitas lain. Misalnya, jika *host* atau *server* dalam jaringan diserang dengan strategi DDoS tertentu, ada kemungkinan bahwa entitas lain, seperti switch dan controller juga terkena dampaknya.

Berdasarkan permasalahan diatas, maka pada penelitian ini akan dibuat system pendeteksi Serangan DDoS dengan IPS (*Intrusion Prevention System*) berbasis Athena dan Notifikasi Telegram Bot pada Arsitektur SDN. IPS juga dikenal sebagai IDPS (*Intrusion Detection Prevention System*), adalah aplikasi keamanan jaringan yang memantau perubahan jaringan dan kegiatan sistem jika ditemukan hal yang dianggap mencurigakan. Fungsi utama IPS adalah untuk mengidentifikasi aktivitas berbahaya, mencatat informasi tentangnya, dan berusaha untuk memblokir atau menghentikan aktivitas tersebut.

Dipilih IPS berbasis Athena karena *framework* ini bisa dikonfigurasi di *Controller* SDN. Pada penelitian ini diharapkan sistem pendeteksi serangan DDoS berbasis Athena ini berhasil mendeteksi serangan DDoS dan berhasil mengirimkan notifikasi serangan ke Telegram Bot.

kata kunci : Serangan DDoS, SDN, IPS, Athena, Telegram Bot

DAFTAR ISI

LEMBAR PENGESAHAN	i
ABSTRAK.....	ii
DAFTAR ISI	iii
DAFTAR GAMBAR.....	iv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	1
1.3 Tujuan dan Manfaat	1
1.4 Batasan Masalah	1
BAB II DASAR TEORI.....	2
2.1 <i>Software Defined Network (SDN)</i>	2
2.2 Mininet.....	2
2.3 <i>Open Network Operating System (ONOS) Controller</i>	3
2.4 <i>Distributed Denial of Service (DDoS)</i>	4
2.5 <i>Athena Framework</i>	5
2.6 Telegram Bot	5
BAB III MODEL SISTEM.....	7
3.1 Metodologi.....	8
3.2 Blok Diagram Sistem.....	8
3.3 Tahapan Perancangan	10
BAB IV BENTUK KELUARAN YANG DIHARAPKAN.....	11
4.1 Keluaran yang Diharapkan	11
4.2 Jadwal Pelaksanaan.....	11
DAFTAR PUSTAKA.....	12

DAFTAR GAMBAR

Gambar 2.1 Arsitektur Software Defined Network	3
Gambar 2.2 Mininet.....	3
Gambar 2.3 Arsitektur ONOS Controller.....	4
Gambar 2.4 Cara Kerja Serangan DDoS	5
Gambar 2.5 Arsitektur Athena.....	6
Gambar 2.6 Arsitektur Telegram Bot	6
Gambar 3.1 Metodologi Penelitian.....	8
Gambar 3.2 Model Sistem Perancangan	8
Gambar 3.3 Topologi Jaringan SDN	8
Gambar 3.4 Diagram Alir Pembuatan Sistem Pendeteksi Serangan DDoS	10

BAB I

PENDAHULUAN

1.1 Latar Belakang

Serangan *Distributed Denial of Service* (DDoS) merupakan jenis serangan yang dilakukan dengan cara membanjiri lalu lintas jaringan internet pada *server*, sistem, atau jaringan. Umumnya serangan ini dilakukan menggunakan beberapa *computer host* penyerang sampai dengan komputer target tidak bisa diakses. Serangan DDoS terhadap satu entitas di SDN berpotensi berdampak terhadap entitas lain. Misalnya, jika *host* atau *server* dalam jaringan diserang dengan strategi DDoS tertentu, ada kemungkinan bahwa entitas lain, seperti *switch* dan *controller* juga terkena dampaknya.

Intrusion Prevention System (IPS) juga dikenal sebagai *Intrusion Detection Prevention System* (IDPS), adalah aplikasi keamanan jaringan yang memantau perubahan jaringan dan kegiatan sistem jika ditemukan hal yang dianggap mencurigakan. Fungsi utama IPS adalah untuk mengidentifikasi aktivitas berbahaya, mencatat informasi tentangnya, dan berusaha untuk memblokir atau menghentikan aktivitas tersebut. *Intrusion Prevention System* (IPS) berbasis Athena diterapkan untuk mencegah dan mengurangi dampak serangan DDoS,

Berdasarkan uraian diatas, maka penulis membuat sebuah sistem yang dapat mencegah serangan DDoS dengan menggunakan IPS. Penulis memilih judul “Perancangan Sistem Pendeteksi DDoS Attack pada Arsitektur SDN Menggunakan IPS Athena dan Notifikasi Telegram Bot” dengan tujuan untuk mencegah serangan DDoS. Adapun penelitian yang terkait dengan proyek akhir ini bisa dilihat pada Tabel 1.1

Tabel 1.1 Hasil Studi Literatur

No	Judul Penelitian /Karya Ilmiah	Tahun	Keterangan
1.	Implementasi Intrusion Prevention System (IPS) Berbasis Athena Untuk Mencegah Serangan DDoS Pada Arsitektur Software-Defined Network (SDN) [1]	2019	Dalam penelitian ini penulis membuat system yang sama, yaitu pencegahan DDoS dengan IPS berbasis Athena, yang membedakannya adalah pada penelitian saya itu ada penambahan Telegram Bot yang berfungsi sebagai notifikasi serangan DDoS.
2.	Penerapan Intrusion Prevention System (IPS) Suricata Sebagai Pengaman dari Serangan Distributed Denial of Service (DDoS) [2]	2020	Dalam penelitian ini penulis membuat system pencegahan serangan Distributed Denial of Service (DDoS) menggunakan IPS Suricata yang dioperasikan menggunakan Linux Ubuntu untuk server, dan Arch Linux untuk penyerang.
3.	Penggunaan Bot Telegram Sebagai Announcement System pada Intansi Pendidikan [3]	2017	Dalam penelitian ini penulis membuat sebuah Bot Telegram untuk mengirimkan sebuah pengumuman tentang data siswa dan nilai – nilai yang sudah didapatkan oleh siswa tersebut.
4.	Analisis Perbandingan Performansi Kontroler Floodlight, Maestro, RYU, POX dan ONOS dalam Arsitektur Software Defined Network (SDN) [4]	2018	Dalam penelitian ini penulis membuat analisis tentang perbandingan performansi antara 5 Kontroler SDN, diantaranya adalah Floodlight, Maestro, RYU, POX, dan ONOS.

1.2 Rumusan Masalah

Adapun rumusan masalah dari Proyek akhir ini, sebagai berikut:

1. Bagaimana merancang sistem pendeteksi *DDoS Attack* pada arsitektur *Software-Defined Network (SDN)* dengan menggunakan IPS berbasis Athena.
2. Bagaimana agar ONOS Controller bisa terkonfigurasi dengan topologi jaringan SDN?
3. Bagaimana cara mengkonfigurasi Athena pada ONOS Controller?
4. Bagaimana cara mengirimkan notifikasi ke Telegram Bot?

1.3 Tujuan dan Manfaat

Adapun tujuan dari Proyek akhir ini, sebagai berikut:

1. Dapat merancang sistem pendeteksi *DDoS Attack* pada arsitektur *Software-Defined Network (SDN)* dengan menggunakan IPS berbasis Athena.
2. Dapat melakukan konfigurasi ONOS Controller pada topologi jaringan SDN.
3. Dapat mengkonfigurasi Athena pada ONOS Controller.
4. Dapat mengirimkan notifikasi serangan ke Telegram Bot.

Adapun manfaat dari Proyek akhir ini, sebagai berikut:

1. Dapat mencegah serangan *Distributed Denial of Service (DDoS)*

1.4 Batasan Masalah

Dalam Proyek akhir ini, dilakukan pembatasan masalah sebagai berikut:

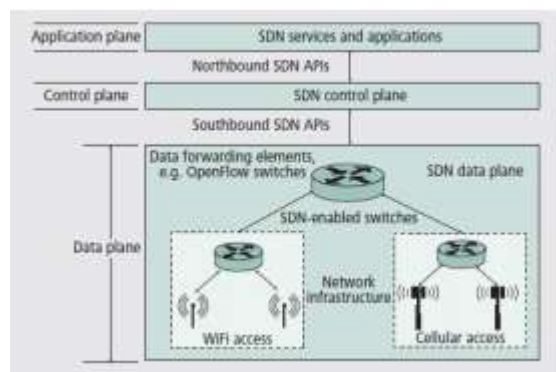
1. Perancangan sistem pendeteksi *DDoS Attack* pada arsitektur *Software-Defined Network (SDN)*
2. Menggunakan ONOS Controller sebagai kontroler SDN
3. Hanya mendeteksi *DDoS Attack*

BAB II

DASAR TEORI

2.1 *Software Defined Network (SDN)*

Software Defined Network merupakan paradigma jaringan yang memisahkan *control* dan *data plane*. Metode ini memungkinkan administrator jaringan untuk mengontrol kerja perangkat melalui sebuah kontroler, tanpa harus mengonfigurasi perangkatnya satu-satu. [5]. Gambar arsitektur *Software Defined Network (SDN)* bisa dilihat pada Gambar 2.1



Gambar 2.1 Arsitektur Software Defined Network

SDN adalah arsitektur yang bersifat dinamis, mudah dikelola, hemat biaya, dan mudah beradaptasi, sehingga cocok untuk digunakan pada jaringan yang memiliki bandwidth tinggi seperti aplikasi yang dinamis seperti saat ini. Arsitektur ini memisahkan antara kontrol jaringan dan fungsi forwarding untuk memungkinkan jaringan dapat diprogram secara langsung dan untuk menjadi sebuah pemisah dari aplikasi dan layanan jaringan. [6].

2.2 Mininet

Mininet adalah sebuah emulator untuk membuat *prototype* jaringan berskala besar secara cepat pada sumber daya yang terbatas (seperti pada *single* komputer atau laptop maupun *Virtual Machine*). Mininet diciptakan dengan tujuan untuk mendukung riset di bidang SDN dan OpenFlow. Emulator Mininet memungkinkan kita untuk menjalankan sebuah kode secara interaktif di atas laptop atau di atas

virtual hardware, tanpa harus memodifikasi kode tersebut. Artinya kode simulasi sama persis dengan kode pada *real network environment*.

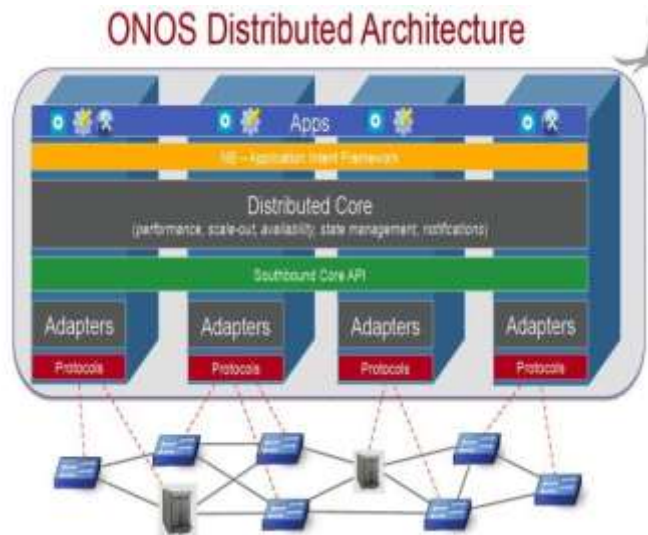


Gambar 2.2 Mininet

Mininet adalah solusi yang dianggap paling unggul dalam hal kemudahan penggunaan, performansi, akurasi, dan skalabilitas. Ia mampu menyediakan lingkungan yang realistis dan nyaman (*convenience*) dengan harga yang murah (*low cost*). Kita dapat menggunakan alternatif lain seperti *hardware test-bed* untuk simulasi jaringan, yang mana dapat berjalan cukup kencang dan akurat, namun harganya mahal dan harus di-*shared* dengan pengguna lain. Begitu pula, kita dapat menggunakan simulator yang harganya murah, namun seringkali kode simulasi akan harus dimodifikasi lagi bila akan dijalankan di *real network environment*. [7]

2.3 *Open Network Operating System (ONOS) Controller*

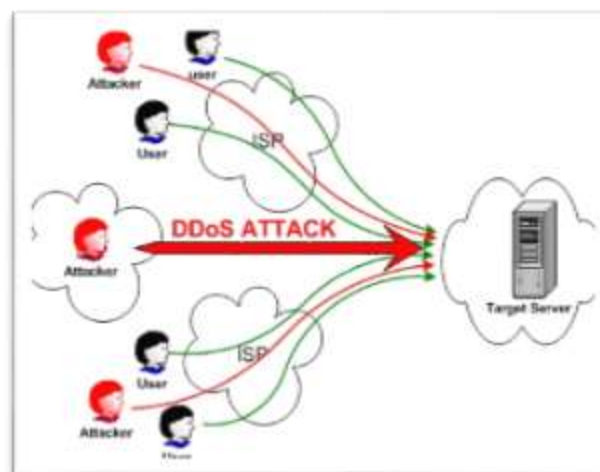
ONOS adalah sebuah sistem operasi (OS) yang dirancang untuk membantu penyedia layanan jaringan membangun jaringan berbasis *carrier-grade* yang dirancang untuk skalabilitas, ketersediaan dan kinerja tinggi. Meskipun dirancang khusus untuk memenuhi kebutuhan penyedia layanan, ONOS juga dapat bertindak sebagai pesawat kontrol SDN untuk jaringan area lokal (LAN) dan jaringan pusat data. [8]. Gambar arsitektur ONOS Controller bisa dilihat pada Gambar 2.3



Gambar 2.3 Arsitektur ONOS Controller

2.4 *Distributed Denial of Service (DDoS)*

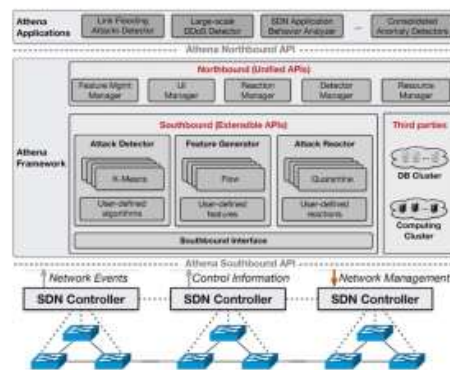
Serangan *Distributed Denial of Service* (DDoS) bertujuan untuk menghalangi ketersediaan sumber daya dalam jaringan bagi pengguna yang sah. Tugas ini dicapai oleh sekelompok perangkat yang secara sadar atau tidak sadar terlibat dalam serangan itu. Pengguna jahat membanjiri sumber daya jaringan dengan sejumlah besar *traffic* dengan paket yang tidak berguna untuk menghabiskan sumber daya tersebut. [9]. Gambar cara kerja serangan DDoS bisa dilihat pada Gambar 2.4



Gambar 2.4 Cara Kerja Serangan DDoS

2.5 Athena Framework

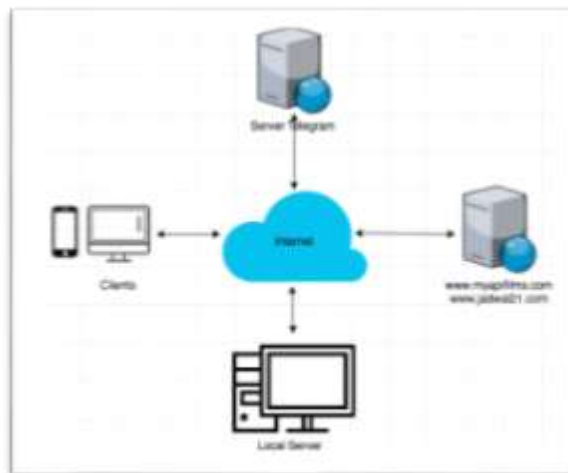
Athena adalah *framework* pendeteksi dan pencegah anomali jaringan yang memanfaatkan fungsionalitas SDN untuk secara eksplisit mendukung deteksi anomali jaringan berbasis *Machine Learning* (ML). Kelebihan Athena yakni ia mampu terintegrasi penuh pada komponen SDN dimana instansi di-*hosting* di atas *SDN controller*. Athena mencakup berbagai fitur jaringan dan algoritma deteksi untuk digunakan dalam menyederhanakan desain dan penyebaran aplikasi pendeteksi anomali. Bahkan, selain persyaratannya untuk mendukung standar OpenFlow, Athena menghindari kebutuhan akan perangkat keras khusus, sehingga secara dramatis meminimalisir kebutuhan untuk memodifikasi susunan SDN ketika memperkenalkan layanan pendeteksi anomali baru. [10]. Gambar arsitektur Athena bisa dilihat pada Gambar 2.5



Gambar 2.5 Arsitektur Athena Framework

2.6 Telegram Bot

Telegram Bot merupakan akun Telegram khusus yang didesain dapat meng-*handle* pesan secara otomatis. Pengguna dapat berinteraksi dengan Bot dengan mengirimkan pesan perintah (*Command*) melalui pesan *private* maupun *group*. Akun Telegram Bot tidak memerlukan tambahan nomor telepon pada pembuatannya. Akun ini hanya bertugas sebagai antarmuka dari kode yang berjalan di sebuah *Server*. Telegram Bot dapat dibangun sesuai dengan kebutuhan, semisal digunakan dengan mengintegrasikannya ke layanan lain untuk mengendalikan *smart home*, membangun *social services*, membangun *custom tools*, ataupun melakukan hal lain secara *virtual*. Gambar arsitektur Telegram Bot bisa dilihat pada Gambar 2.6



Gambar 2.6 Arsitektur Telegram Bot

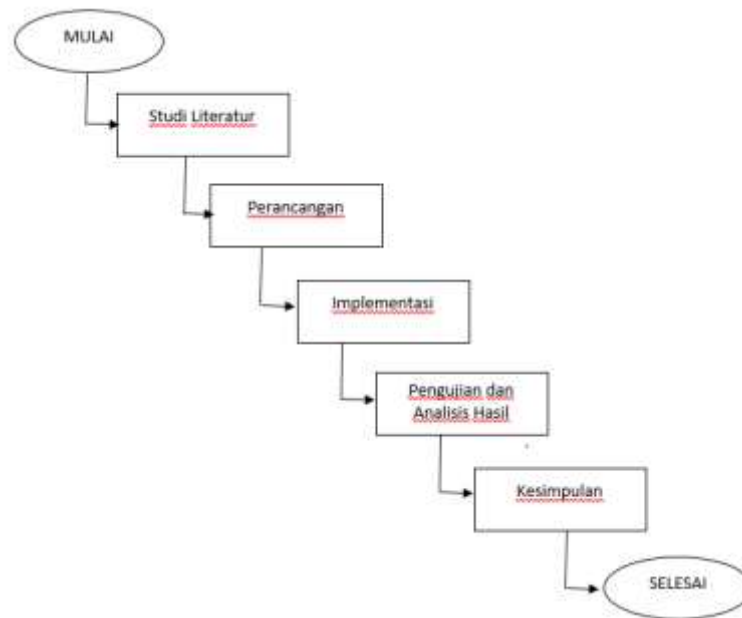
Program bot biasanya diprogram untuk berlaku seperti jika dioperasikan oleh seseorang. Bot bisa melakukan memberikan informasi tagihan, memberikan info atas request pengguna pada instansinya dan banyak hal lain seperti untuk mengajarkan sesuatu, bermain, nyari sesuatu, *broadcast*, mengingatkan sesuatu (*reminder*), bahkan dapat mengirim perintah/*command* ke perangkat *Internet of Things*. [11].

BAB III

MODEL SISTEM

3.1 Metodologi

Adapun metodologi pada penelitian ini, bisa dilihat pada Gambar 3.1



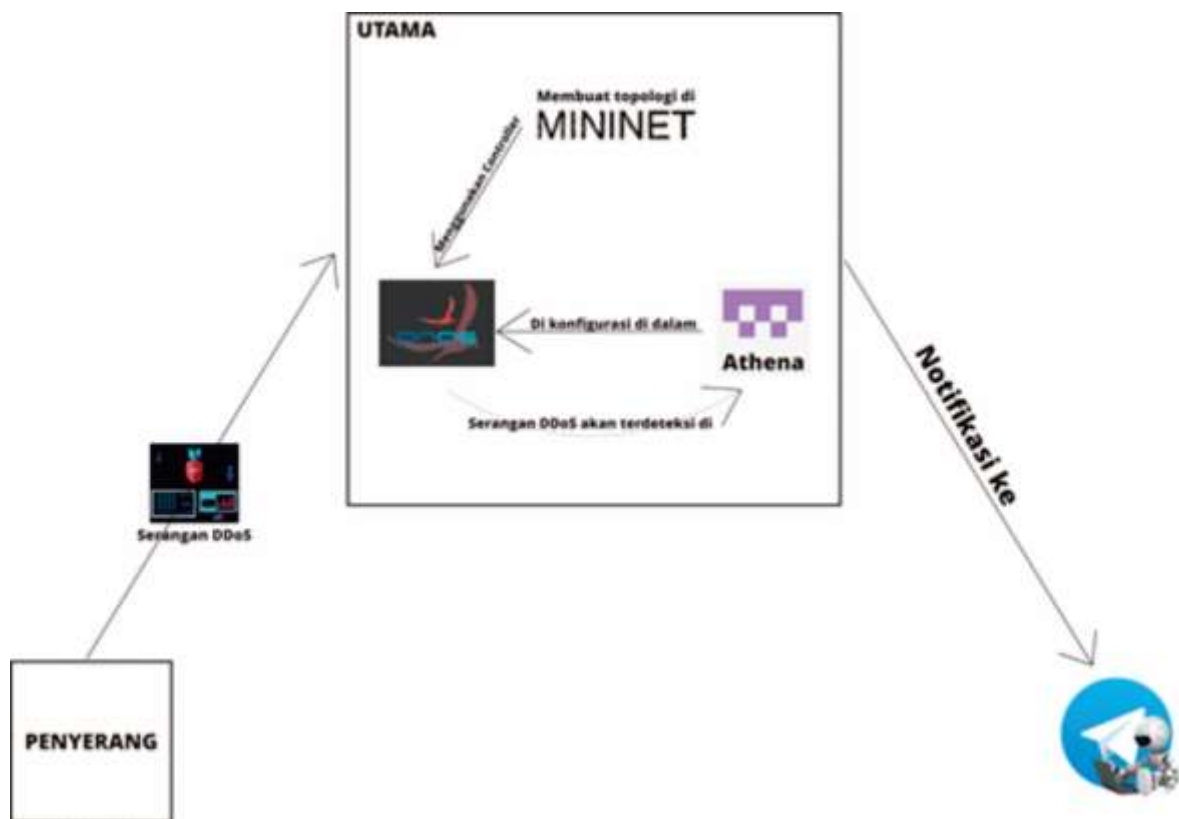
Gambar 3.1 Metodologi

3.2 Blok Diagram Sistem

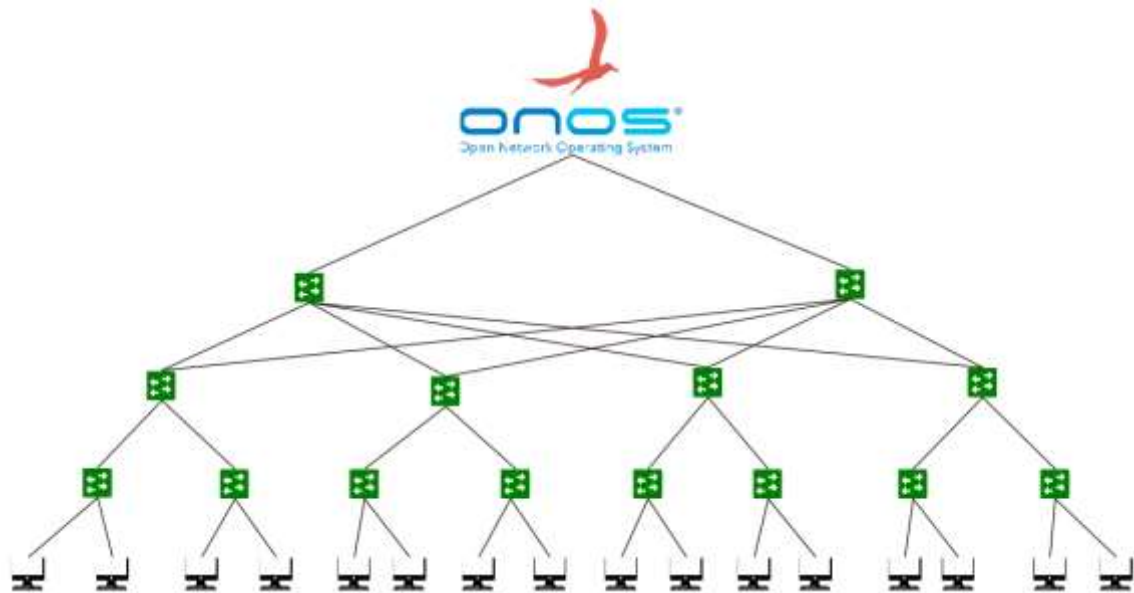
Pada bab ini akan dijelaskan mengenai perancangan sistem pencegahan serangan *Distributed Denial of Service* (DDoS) menggunakan *Intrusion Prevention System* (IPS) berbasis Athena pada *Software Defined Network* (SDN). Analisis ini dilakukan dengan tujuan untuk mendeteksi serangan DDoS atau upaya dimana penyerang berusaha menyerang pada suatu jaringan menggunakan tipe serangan DDoS. Penulis melakukan penelitian ini untuk memperkecil serangan DDoS

Dalam penelitian ini, penulis membuat sebuah topologi jaringan SDN pada Mininet dengan ONOS *Controller* sebagai kontroler SDN nya. Topologi tersebut memiliki model topologi dengan 16 *Host*, 32 *Link* dan 14 *Switch*. Metode pembuatan topologi SDN tersebut menggunakan bahasa pemrograman Python. Di dalam ONOS *Controller* tersebut akan di konfigurasi *Athena Framework*, yaitu

suatu sistem pendeteksi anomali jaringan yang akan di *hosting* pada ONOS *Controller*. Algoritma yang digunakan pada Athena Framework ini adalah Algoritma *K-Means*, yaitu salah satu algoritma *clustering* yang melakukan pemodelan tanpa *supervise*. Serangan yang dilakukan adalah serangan DDoS pada jaringan *Software-Defined Network* yang akan terdeteksi di *Athena Framework*. Setelah benar adanya tindakan penyerangan pada suatu jaringan, maka penulis akan mengirim notifikasi serangan ke Telegram Bot yang sudah diatur, sehingga penulis bisa me *monitoring* aktifitas jaringan secara *real time*. Adapun model sistem yang telah dibuat dapat dilihat pada Gambar 3.2 dibawah ini.



Gambar 3.2 Model Sistem Perancangan



Gambar 3.3 Topologi Jaringan SDN

3.3 Tahap Perancangan

Proses perancangan sistem pendeteksi serangan DDoS menggunakan *Athena Framework* pada Arsitektur SDN ini bisa dilihat pada Gambar 3.4, tahapan perancangannya adalah sebagai berikut:

1. Pembuatan Topologi Jaringan SDN

Langkah awal dalam merancang sistem pendeteksi serangan DDoS adalah dengan melakukan pembuatan topologi jaringan SDN. Topologi jaringan SDN dibuat menggunakan *software* Mininet yang memakai bahasa pemrograman Python. Topologi tersebut memiliki model topologi dengan 16 *Host*, 32 *Link*, dan 14 *Switch*.

2. Konfigurasi ONOS *Controller*

Arsitektur SDN harus mempunyai kontroler. Kontroler yang digunakan adalah ONOS *Controller*. ONOS *Controller* ini akan di konfigurasi pada Topologi jaringan SDN yang sudah dibuat di Mininet.

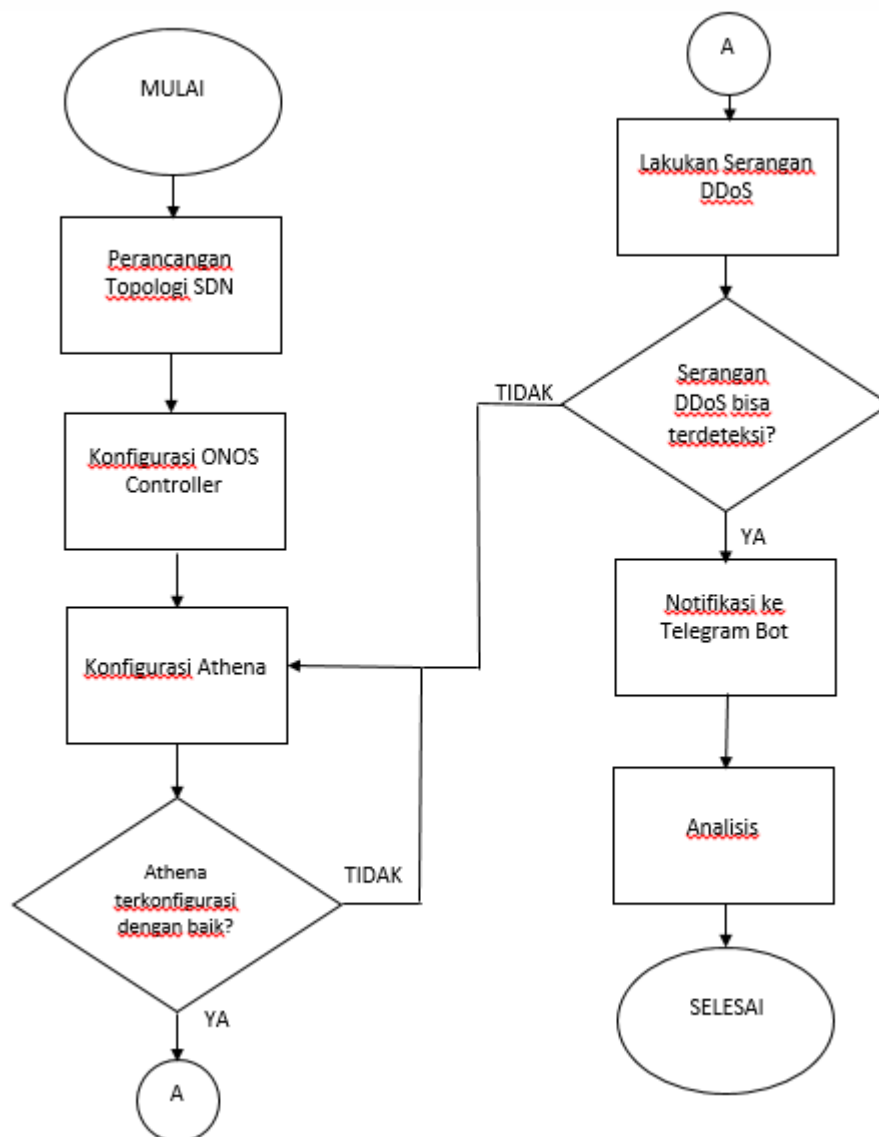
3. Konfigurasi *Athena Framework*

Athena ini akan dikonfigurasi pada ONOS *Controller*. Algoritma yang digunakan pada Athena ini adalah Algoritma *K-Means*. Untuk menampilkan grafik deteksi serangan di *Athena Framework*, maka model yang digunakan adalah model *Athena Framework GUI (Graphical User Interface)*. Ada 5 hal yang harus diperhatikan dalam melakukan konfigurasi *Athena Framework*

yaitu *Query* (q), *Preprocessor* (f), *Algorithm* (a), *Reaction* (r), dan *Operation* (o). Masukkan *code* untuk membuat sistem pendeteksi DDoS di Athena untuk ke 5 parameter. Cek apakah konfigurasi sudah berhasil atau tidak. Jika tidak berhasil, cek lagi apakah ada yang salah pada konfigurasinya.

4. Pengujian dan Analisis Sistem

Pengujian dan Analisis Sistem dilakukan serangan DDoS untuk memastikan apakah *Athena Framework* bisa mendeteksi serangan tersebut atau tidak. Jika tidak terdeteksi, cek kembali pada *Athena Framework* apakah ada yang salah dengan konfigurasinya atau tidak. Jika terdeteksi, kirim notifikasi ke Telegram Bot.



Gambar 3.4 Diagram Alir Pembuatan Sistem Pendeteksi Serangan DDoS

BAB IV

BENTUK KELUARAN YANG DIHARAPKAN

4.1 Keluaran yang Diharapkan

Adapun keluaran yang diharapkan pada Perancangan system pendeteksi serangan DDoS pada Arsitektur SDN menggunakan Athena adalah sebagai berikut :

- a) Dapat membuat topologi jaringan SDN
- b) Dapat melakukan konfigurasi Athena pada topologi jaringan SDN
- c) Dapat melakukan dan mendeteksi serangan DDoS
- d) Dapat mengirimkan notifikasi serangan melalui Telegram Bot

4.2 Jadwal Pelaksanaan

Adapun jadwal pengerjaan Proyek akhir bisa dilihat pada Tabel 4.1 sebagai berikut :

Tabel 4.1 Jadwal Pelaksanaan

Judul Kegiatan	Waktu							
	Des	Jan	Feb	Mar	Apr	Mei	Jun	Jul
Studi Literatur								
Perancangan dan Simulasi								
Pengujian								
Analisa								
Pembuatan Laporan								

DAFTAR PUSTAKA

- [1] Muhammad Farradhika Muntaha, Primantara Hari Trisnawan, and Rakhmadany Primananda, "Implementasi Intrusion Prevention System (IPS) berbasis Athena untuk Mencegah Serangan DDoS pada Arsitektur Software-Defined Network (SDN)," in *2019 Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, Malang, Indonesia , 2019.
- [2] Istiana Adesty, Wahyu Adi Prabowo, and Muhammad Fajar Sidiq, " Penerapan Intrusion Prevention System (IPS) Suricata Sebagai Pengamanan Dari Serangan Distributed Denial of Service (DDoS)," in *2020 Implementation of Intrusion Prevention System (IPS) as a Security from DDoS (Distributed Denial of Service) Attacks*, Institut Teknologi Telkom Purwokerto, 2020.
- [3] Moh Wahyudi Putra, Eko Sakti Pramukantoro, and Widhi Yahya, "Analisis Perbandingan Performansi Kontroler Floodlight, Maestro, RYU, POX, dan ONOS dalam Arsitektur Software Defined Network (SDN)," in *2018 Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, Malang, Indonesia , 2018.
- [4] Hariyanto Soeroso, Afif Zuhri Arfianto, Novi Eka Mayangsari, and Muhammad Taali, "Penggunaan Bot Telegram Sebagai Announcement System pada Intansi Pendidikan," in *2017 Seminar MASTER*, Madiun, Indonesia , 2017.
- [5] Fahry Adnantlya, Sofia Naning Hertiana, ST.,MT. , and Leanna Vidya Yovita, ST.,MT., "Simulasi dan Analisis Performansi Protokol Routing EBGp pada SDN (Software Defined Network)," in *2015 e-Proceeding of Engineering*, Bandung, Indonesia , 2015.
- [6] Moh Wahyudi Putra, Eko Sakti Pramukantoro, and Widhi Yahya, "Analisis Perbandingan Performansi Kontroler Floodlight, Maestro, RYU, POX, dan ONOS dalam Arsitektur Software Defined Network (SDN)," in *2018 Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, Malang, Indonesia , 2018.
- [7] Izzatul Ummah, and Desianto Abdillah, "Perancangan Simulasi Jaringan Virtual Berbasis Software-Define Networking," in *2016 Indonesian Journal on Computing*, Bandung, Indonesia, 2016.
- [8] Faizal Ramadhan, Rakhmadhany Primananda, and Widhi Yahya, "Implementasi Routing berbasis Algoritme Dijkstra pada Software Defined Networking

Menggunakan Kontroler Open Network Operating System," in *2018 Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, Malang, Indonesia , 2018.

- [9] Rudi Hermawan, "Analisis Konsep dan Cara Kerja Serangan Komputer Distributed Denial of Service," in *2015 Faktor Exacta*, Jakarta, Indonesia , 2015.
- [10] Muhammad Farradhika Muntaha, Primantara Hari Trisnawan, and Rakhmadany Primananda, "Implementasi Intrusion Prevention System (IPS) berbasis Athena untuk Mencegah Serangan DDoS pada Arsitektur Software-Defined Network (SDN)," in *2019 Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, Malang, Indonesia , 2019.
- [11] Hariyanto Soeroso, Afif Zuhri Arfianto, Novi Eka Mayangsari, and Muhammad Taali, "Penggunaan Bot Telegram Sebagai Announcement System pada Intansi Pendidikan," in *2017 Seminar MASTER*, Madiun, Indonesia , 2017.



UNIVERSITAS TELKOM

FAKULTAS ILMU TERAPAN

KARTU KONSULTASI

SEMINAR PROPOSAL PROYEK TINGKAT

NAMA / PRODI : Rinaldi Mohamad Farhan / D3TT

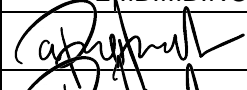

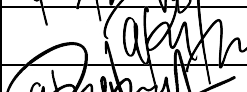
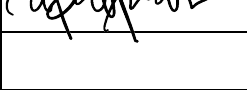
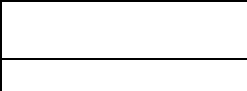
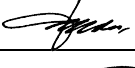

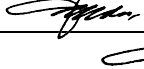
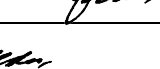
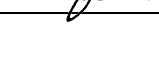
NIM : 6705184138

JUDUL PROYEK TINGKAT :

Perancangan Sistem Pendeteksi DDoS Attack pada Arsitektur SDN Menggunakan IPS Athena dan Notifikasi Telegram Bot

CALON PEMBIMBING : I. Rohmat Tulloh, S.T., M.T.

II. Agus Ganda Permana, Ir., M.T.

NO	TANGGAL	CATATAN HASIL KONSULTASI	TANDA TANGAN CALON PEMBIMBING I
1	22/01/2021	BAB 1 (SELESAI)	
2	22/01/2021	BAB 2 (SELESAI)	
3	22/01/2021	BAB 3 (SELESAI)	
4	22/01/2021	BAB 4 (SELESAI)	
5	22/01/2021	FINALISASI PROPOSAL	
6			
7			
8			
9			
10			
NO	TANGGAL	CATATAN HASIL KONSULTASI	TANDA TANGAN CALON PEMBIMBING II
1	21/01/2021	BAB 1 (SELESAI)	
2	21/01/2021	BAB 2 (SELESAI)	
3	21/01/2021	BAB 3 (SELESAI)	
4	21/01/2021	BAB 4 (SELESAI)	
5	21/01/2021	FINALISASI PROPOSAL	
6			
7			
8			
9			
10			