IDENTIFIKASI *DDOS* MENGGUNAKAN *KNN* PADA *SOFTWARE DEFINED NETWORK* DAN NOTIFIKASI BOT TELEGRAM BERBASIS RASPBERRY PI

Identification DDoS using KNN in Software Defined Network and Notification Bot Telegram on Raspberry Pi

PROPOSAL PROYEK AKHIR

Diajukan sebagai syarat untuk mengambil Mata Kuliah Proyek Akhir

oleh :

Faishal Nugraha Pratama

6705184098

D3 TEKNOLOGI TELEKOMUNIKASI

FAKULTAS ILMU TERAPAN

UNIVERSITAS TELKOM

2021

LEMBAR PENGESAHAN

Proposal Proyek Akhir dengan judul :

IDENTIFIKASI *DDOS* MENGGUNAKAN *KNN* PADA *SOFTWARE DEFINED NETWORK* DAN NOTIFIKASI BOT TELEGRAM BERBASIS RASPBERRY PI

Identification DDoS using KNN in Software Defined Network and Notification Bot Telegram on Raspberry Pi

oleh :

Faishal Nugraha Pratama

6705184098

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

Bandung, 13 Januari 2021

Menyetujui,

Pembimbing I

22-Jan-21
Untuk Proposal PA
Faishal Nugraha P

Rohmat Tulloh, S.T., M.T
NIP. 06830002

Pembimbing II

Dr. Indrarini Dyah Irawati, S.T., M.T
NIP. 07780053

ABSTRAK

Kebutuhan pada jaringan sangat mengutamakan performa untuk mendukung hasil yang sangat memuaskan dan fleksibel terutama pada konfigurasi serta kontrol jaringan. *Software Defined Network* muncul dengan menerapkan mekanisme konfigurasi yang mudah serta kontrol jaringn yang tidak rumit. Konsep dari SDN adalah memisahkan kontroler dan data forwarding plane. Dengan begitu kontroler yang terdapat pada SDN akan menjadi sasaran oleh penyerang yang tidak bertanggung jawab.

Berdasarkan pemaparan di atas, proyek akhir ini bertujuan untuk mengidentifikasi serangan *Distributed Denial of Service* yang dilakukan oleh pihak yang tidak bertanggung jawab. Penulis menggunakan Mininet untuk membuat topologi SDN dengan bahasa pemrograman Python yang akan di pasangkan pada Raspberry Pi guna untuk meringankan penggunaan laptop. Didalam SDN terdapat protocol *Sflow* dan *Openflow*. dikarenakan kontroler pada SDN keamanannya belum cukup tinggi. Sehingga penulis akan menambahkan *K-Nearest Neighbors* untuk meningkatkan akurasi dalam mendeteksi penyerang. Kontroler yang di gunakan pada penelitian ini adalah Ryu kontroler. Dan KNN digunakan untuk meningkatkan akurasi jika benar adanya penyerang, lalu akan mengirim notifikasi Bot Telegram.

Sistem ini digunakan untuk mendeteksi penyerang atau pihak yang tidak bertanggung jawab dalam menggunakan jaringan, seperti penggunaan DDoS untuk kepentingan pribadi. Sistem ini juga menggunakan Telegram untuk mengirim notifikasi serangan melalui bot Telegram.

Kata Kunci : *Distributed Denial of Service, K-Nearest Neigbors, Mininet, Ryu Kontroler, Software Defined Network*

DAFTAR ISI

BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini DDoS merupakan salah satu serangan di internet dimana penyerang melakukan serangan menggunakan beberapa *host* dengan cara membanjiri lalu lintas jaringan internet pada server, sistem atau suatu jaringan. Hal ini mengakibatkan kerusakan pada perangkat jaringan, yang menjadi salah satu faktor pendorong utama yang dilakukan oleh para penyerang [1].Mitigasi DDoS merupakan salah satu upaya untuk mengatasi masalah serangan DDoS. Mekanisme dari mitigasi DDoS adalah dengan memperkecil *bandwidth* dan *blocking* agar jumlah paket permintaan dapat berkurang durasinya, sehingga lalu lintas jaringan tidak terjadi kepadatan yang membuat kinerja *switch* dan *router* menjadi terbebani, karena hal ini berpengaruh terhadap kerusakan perangkat jaringan tersebut [2].

Dalam penelitian ini, penulis sebelumnya menggunakan mininet untuk topologi SDN dikarenakan Mininet di anggap paling unggul dalam hal kemudahan pengguna, performansi, akurasi dan skabilitas serta mininet juga diciptakan dengan tujuan mendukung riset di bidang SDN dan *Openflow* [3]. Penulis sebelumnya mengusulkan kerangka kerja mitigasi serangan DDoS terhadap SDN yaitu FlowTrApp yang melakukan deteksi dan mitigasi dengan mengkombinasikan *sFlow* dan *OpenFlow*. *sFlow* adalah teknologi kolektor yang berfungsi sebagai mengumpulkan data pada lalu lintas jaringan yang ada pada *Switch* dan *Router*. *OpenFlow* merupakan protokol komunikasi yang berfungsi sebagai pemberi hak akses *forwarding* data pada *Switch* dan *Router* melalui jaringan.

Dalam penelitian ini penulis sebelumnya menggunakan DDoS dengan tipe *TCP Flood Attack* pada SDN, untuk melakukan mitigasi DDoS di SDN dengan menggunakan K-Nearest Neighbors pada controller. Dengan menggunakan KNN untuk mengenali pola serangan yang sudah dipelajari oleh KNN melalui dataset akan mempercepat membuat kesimpulan bahwa adanya penyerang. Ryu kontroler akan melakukan tindakan mitigasi terhadap penyerang yang telah dibenarkan oleh KNN. Penerapan KNN pada SDN bertujuan untuk meningkatkan akurasi dalam mendeteksi penyerang sehingga identitas penyerang dapat terlihat [2]. Telegram merupakan

salah satu aplikasi yang memberikan kemudahan bagi *administrator* untuk membangun sistem notifikasi dengan memanfaatkan fasilitas *Aplication Programing Interface* (API) yang disediakan oleh Telegram melalui bot yang dapat digunakan untuk mengirimkan pesan secara otomatis. [4].

Berdasarkan penelitian sebelumnya, penulis membuat sebuah sistem yang dapat mengidentifikasi serangan DDoS dengan judul "Identifikasi DDOS Menggunakan KNN pada Software Defined Network dan Notifikasi bot Telegram Berbasis Raspberry Pi". Penulis menggunakan Mininet untuk membuat topologi SDN dengan bahasa pemrograman Python yang akan di pasangkan pada Raspberry Pi guna untuk meringankan penggunaan laptop dan mengirim notifikasi serangan melalui bot telegram.

1.2 Tujuan dan Manfaat

Adapun tujuan dari Proyek akhir ini, sebagai berikut:

1. Dapat mengidentifikasi serangan DDoS menggunakan KNN pada *Software Defined Network* dan mengirim notifikasi serangannya melalui bot di Telegram berbasis Raspberry Pi.
2. Dapat membuat topologi *Software Defined Network* di Mininet.
3. Dapat mendeteksi penyerang.

1.3 Rumusan Masalah

Adapun rumusan masalah dari Proyek akhir ini, sebagai berikut:

1. Apa saja fungsi yang akan di terapkan pada identifikasi serangan DDoS menggunakan KNN pada *Sofware Defined Network*?
2. Bagaimana topologi yang akan diterapkan pada Identifikasi serangan DDoS menggunakan KNN pada *Software Defined Network*?
3. Bagaimana cara mendeteksi penyerang?

1.4 Batasan Masalah

Dalam Proyek akhir ini, dilakukan pembatasan masalah sebagai berikut:

1. Mendeteksi serangan DDoS pada *Software Defined Network*
2. Menggunakan Ryu sebagai kontroler

3. Menggunakan serangan DDoS *TCP Flood Attack* untuk pengujian.

1.5 Metodologi

Metodologi pada penelitian ini, sebagai berikut:

1. Studi Literatur

   Studi literatur yang dilakukan penulis adalah mencari referensi dan memperdalam ilmu.

2. Analisis Kebutuhan

   Penulis mempersiapkan serta mengumpulkan *hardware* serta *software* apa saja yang dibutuhkan.

3. Perancangan dan simulasi

   Penulis melakukan perancangan serta melakukan simulasi dari proses yang sudah di buat.

4. *Troubleshooting*

   Penulis melakukan *troubleshooting* perihal masalah apa saja yang didapat kan saat merancang dan mensimulasikan.

5. Pengujian

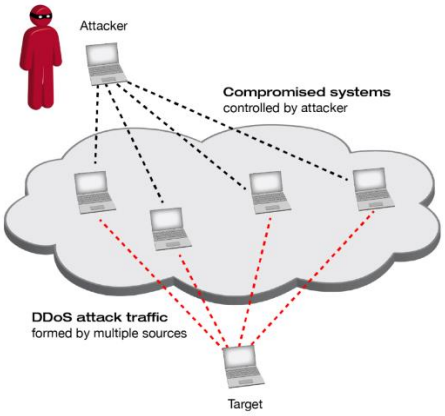
   Penulis melakukan pengujian dari hasil yang sudah di buat serta memastikan berjalan dengan baik dan semestrinya

6. Kesimpulan

   Penulis menyimpulkan dari semua rangkaian metodologi yang telah dilakukan.

BAB II
DASAR TEORI

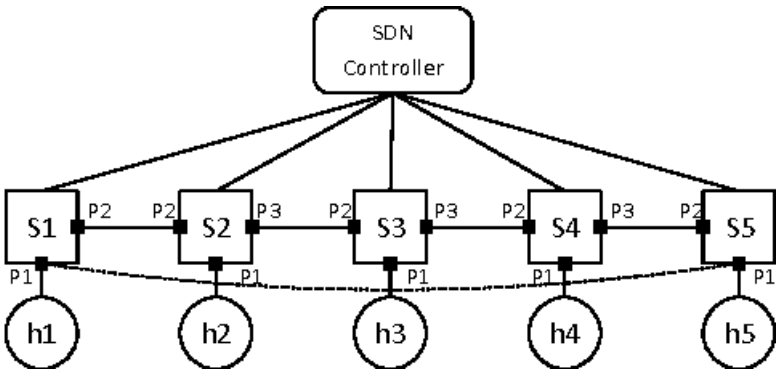
2.1 *Distributed Denial of Service (DDoS)*



Gambar 2. 1 Distributed Denial of Service

Apa itu DDoS? DDoS merupakan kependekan dari *Distributed Denial of Service* atau dalam bahasa Indonesia dapat diartikan sebagai Penolakan Layanan secara Terdistribusi. DDoS adalah jenis serangan yang dilakukan dengan cara membanjiri lalu lintas jaringan internet pada server, sistem, atau jaringan [1].

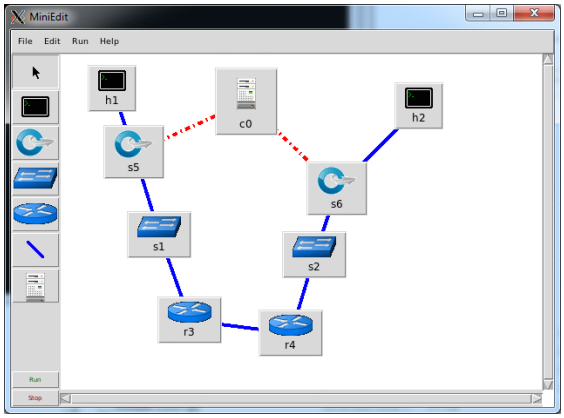
2.2 *Software Defined Network*



Gambar 2. 2 SDN

Software Defined Network adalah kemampuan dalam menyediakan virtualisasi jaringan, membuat aturan jaringan yang dinamis, dan kontrol yang lebih besar atas entitas jaringan di seluruh struktur jaringan dengan mengurangi biaya operasional. SDN memberikan beban yang besar pada *administrator* untuk secara manual menjamin keamanan dan fungsi yang benar dari seluruh jaringan, dimana *administrator* membuat aplikasi pada kontroler untuk mengatur dan memberi keamanan pada seluruh jaringan karena SDN bersifat terpusat [2].

2.3 Mininet



Gambar 2. 3 Mininet

Mininet adalah sebuah *emulator* untuk membuat *prototype* jaringan berskala besar secara cepat pada sumberdaya yang terbatas (seperti pada *single* komputer atau laptop maupun *Virtual Machine*). Mininet diciptakan dengan tujuan untuk mendukung riset di bidang SDN dan *OpenFlow* [3].

2.4 *Ryu Controller*

Gambar 2. 4 *Ryu Controller*

Ryu adalah kerangka kerja jaringan yang mendukung S*oftware Defined Network*. Ryu menyediakan komponen perangkat lunak dengan API yang terdefinisi dengan baik yang memudahkan pengembang untuk membuat manajemen jaringan baru dan pada kontroler. Ryu mendukung berbagai protokol untuk mengelola perangkat jaringan, seperti *OpenFlow*, *Netconf*, *OF-config*, dll [5].

2.5 *SFlow*

Gambar 2. 5 *sFlow*

sFlow merupakan salah satu protokol yang digunakan untuk menangkap trafik jaringan di *switch* atau *router*. Protokol *sFlow* menggunakan *packet sampling technology* untuk mengumpulkan atau menangkap trafik data [6].

2.6 *OpenFlow*

Gambar 2. 6 *OpenFlow*

OpenFlow merupakan suatu protokol komunikasi yang menghubungkan antara perangkat jaringan dengan sebuah kontroler. Dapat melakukan pemrograman pada *data plane* dan memberikan akses pada *forwarding plane* dari *switch* atau *router* melalui jaringan. Dengan menerapkan *OpenFlow* pada *switch* atau *router* maka dapat mengatur sebuah paket yang masuk secara terpusat pada Kontroler [2].

2.7 Telegram

Gambar 2. 7 Telegram

Telegram bot adalah sebuah bot atau robot yang diprogram dengan berbagai perintah untuk menjalankan serangkaian instruksi yang diberikan oleh pengguna [7].

Dalam perancangan *notification alert* via Telegram yang harus disiapkan adalah aplikasi Telegram dengan membuat akun Telegram dan membuat bot Telegram untuk melakukan pengriman notifikasi nya [8].

2.8 Raspberry Pi

Gambar 2. 8 Raspberry Pi

Raspberry Pi (juga dikenal sebagai RasPi) adalah sebuah SBC (*Single Board Computer*) seukuran kartu kredit yang dikembangkan oleh Yayasan Raspberry Pi di Inggris (UK) dengan maksud untuk memicu pengajaran ilmu komputer dasar di sekolah-sekolah. [9]

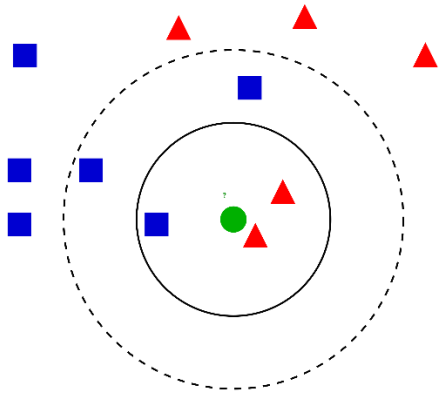
Raspberry Pi menggunakan *system on a chip* (SoC) dari *Broadcom BCM2835*, juga sudah termasuk prosesor *ARM1176JZF-S 700 MHz*, GPU VideoCore IV dan RAM sebesar 256 MB (untuk Rev. B). Tidak menggunakan *hard disk*, namun menggunakan SD Card untuk proses *booting* dan penyimpanan data jangka-panjang. [9]

2.9 Python

Gambar 2. 9 Python

Python adalah bahasa pemrograman interpretatif yang dapat digunakan di berbagai platform dengan filosofi perancangan yang berfokus pada tingkat keterbacaan kode dan merupakan salah satu bahasa populer yang berkaitan dengan *Data Science*, *Machine Learning*, dan *Internet of Things* (IoT). Keunggulan Python yang bersifat interpretatif juga banyak digunakan untuk *prototyping*, *scripting* dalam pengelolaan infrastruktur. [10]

2.10 *K-Nearest Neighbors*



Gambar 2. 10 K-Nearest Neighbors

Algoritma *K-Nearest Neighbor* (KNN) adalah sebuah metode untuk melakukan klasifikasi terhadap objek yang berdasarkan dari data pembelajaran yang jaraknya paling dekat dengan objek tersebut. KNN merupakan algoritma *supervised learning* dimana hasil dari *query instance* yang baru diklasifikan berdasarkan mayoritas dari kategori pada algoritma KNN. Dimana kelas yang paling banyak muncul yang nantinya akan menjadi kelas hasil dari klasifikasi [11].

$$distance = \sqrt{\sum_{i=1}^{n}(X^i_{training} - X_{testing})^2}$$

dengan

$X^i_{training}$: data training ke-*i*,
$X_{testing}$: data testing,
i : record (baris) ke-*i* dari tabel,
n : jumlah data training.

Gambar 2. 11 Rumus KNN

Langkah-langkah untuk menghitung metode K *Nearest Neighbor* antara lain :

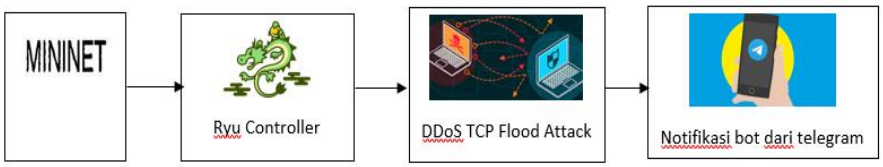
a) Menentukan parameter *K* (jumlah tetangga paling dekat).
b) Menghitung kuadrat jarak *Euclid* (*queri instance*) masing-masing objek
c) Kemudian mengurutkan objek-objek tersebut ke dalam kelompok yang mempunyai jarak *Euclid* terkecil.
d) Mengumpulkan kategori *Y* (Klasifikasi *Nearest Neighbor*)
e) Dengan menggunakan kategori *Nearest Neighbor* yang paling mayoritas maka dapat diprediksi nilai *query instance* yang telah dihitung [11].

BAB III
MODEL SISTEM

3.1 Blok Diagram Sistem

Pada bab ini akan dijelaskan mengenai perancangan identifikasi serangan DDoS menggunakan KNN pada *Software Defined Network* menggunakan Ryu Controller dan notifikasi bot dari Telegram berbasis Raspberry Pi. Analisis ini digunakan untuk mendeteksi serangan DDoS atau upaya dimana penyerang berusuha menyerang pada suatu jaringan menggunakan tipe serangan DDoS. Penulis melakukan penelitian ini guna untuk memperkecil serangan DDoS dengan menggunakan mekanisme Mitigasi DDoS dimana penulis menggunakan metode *FlowTrApp*, metode ini mengkombinasikan *sFlow* dan *OpenFlow*.

Dalam penelitian ini penulis membuat topologi jaringan di Mininet dengan Ryu sebagai kontroler nya serta menggunakan serangan DDoS berupa TCP Flood Attack pada jaringan SDN dengan menggunakan KNN pada Kontroler. Setelah benar adanya tindakan serangan pada suatu jaringan, maka penulis mengirim notifikasi serangan ke Telegram dengan fitur bot yang sudah di atur.



Gambar 3. 1 Blok Diagram Sistem

3.2 Tahapan Perancangan

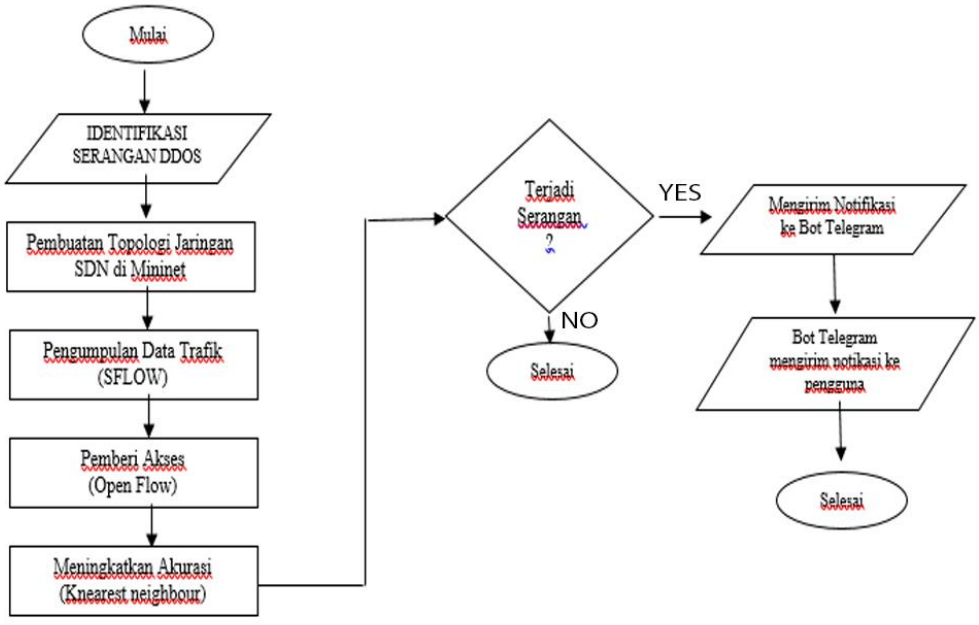
Proses perancangan ini dilakukan dengan metode eksperimental dan tahapan pembuatanya adalah sebagai berikut:

1. Penentuan spesifikasi

   Langkah awal dalam pembuatan sistem ini adalah dengan membuat topologi *Software Defined Network* di *Mininet* dimana didalam jaringan SDN tersebut terdapat *sFlow* dan *OpenFlow*. *K-Nearest Neighbors* bertujuan untuk meningkatkan akurasi dalam mendeteksi penyerang dan bisa di atur oleh Raspberry Pi

2. Perancangan Sistem

   Perancangan sistem dilakukan untuk merealisasikan dari model simulasi ke dalam bentuk aslinya, dari tahapan utama diatas untuk tahapan penyusunan sistemnya dapat dibuat *flowchart* sebagai berikut.



Gambar 3. 2 *Flowchart*

3.3 Perancangan

Pada Proyek akhir ini akan dirancang topologi *Software Defined Network* menggunakan *software* Mininet dan Ryu sebagai kontrolernya serta jika benar terdapat serangan maka notifikasi tersebut akan di kirimkan melalui *Telegram* dimana didalamnya sudah dibuatkan bot Telegram. Tahapan perancangan sistem ini menggunakan beberapa *software* dan bahan lainnya yaitu sebagai berikut:

1. *Software*

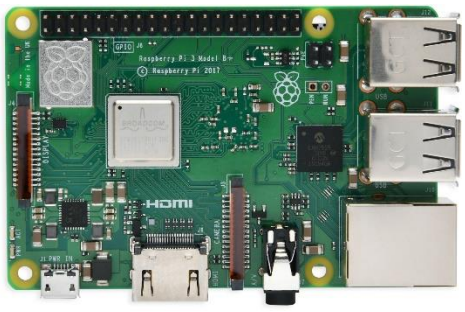
   Software yang digunakan untuk merancang sistem ini menggunakan Mininet, dan Telegram dimana Mininet digunakan untuk merancang topologi *Software Defined Network*, dan Telegram untuk memberikan notifikasi seranganya.

2. Bahasa Pemrograman

Gambar 3. 3 Python

Bahasa pemrograman yang digunakan untuk merancang sistem ini menggunakan bahasa pemrograman Python yang akan di gunakan di Mininet.

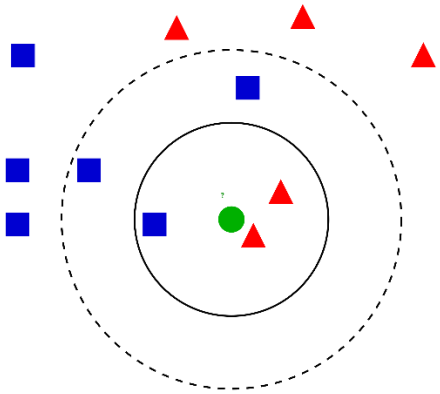
3. *Hardware*



Gambar 3. 4 Raspberry Pi

Hardware yang digunakan untuk mendukung merancang sistem ini menggunakan Raspberry Pi.

4. Algoritma



Gambar 3. 5 Algoritma *K-Nearest Neighbors*

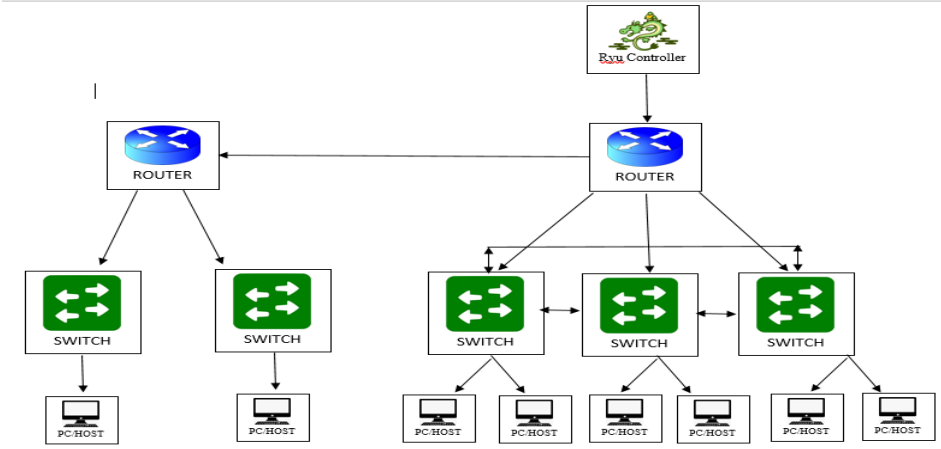
Algoritma yang digunakan oleh penulis adalah *K-Nearest Neighbors* digunakan untuk meningkatkan akurasi dalam mendeteksi penyerang.

5. *Protocol*

Protocol yang digunakan oleh penulis adalah *sFlow* dan *OpenFlow*. *sFlow* digunakan untuk menangkap trafik jaringan pada *switch* dan *router*, sedangkan *OpenFlow* digunakan untuk memberi hak akses *forwarding data*.

6. Topologi

Adapun topologi yang akan digunakan oleh penulis sebagai berikut :



Gambar 3. 6 Topologi SDN

BAB IV
BENTUK KELUARAN YANG DIHARAPKAN

4.1 Keluaran yang Diharapkan

Perancangan pada Proyek akhir akan dibuat reflektor sudut dengan spesifikasi sebagai berikut :

a. Dapat membuat topologi jaringan *Software Defined Network*
b. Dapat mendeteksi serangan DDoS
c. Dapat mengirimkan notifikasi serangan melalui bot Telegram
d. Dapat berfungsi dengan baik dan semestrinya.

4.2 Jadwal Pelaksanaan

Adapun jadwal pengerjaan Proyek akhir bisa dilihat pada tabel sebagai berikut :

Table 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] Niagahoster, "Niagahoster," Pengertian DDOS dan Bagaimana Menanggulanginya, 1 May 2018. [Online]. Available: https://www.niagahoster.co.id/blog/ddos-adalah/. [Accessed 18 January 2021].

[2] M. M. Azis, A. Yufis and Saifuddin, "Analisa Sistem Identifikasi DDoS Menggunakan KNN Pada Jaringan Software Defined Network(SDN)," p. 8, 2020.

[3] I. Ummah and D. Abdillah, "Perancangan Simulasi Jaringan Virtual Berbasis Software-Define Networking," *Ind. Journal on Computing,* p. 11, 2016.

[4] J. Fahana, R. Umar and R. Faizin, "Pemanfaatan Telegram Sebagai Notifikasi Serangan untuk Keperluan Forensik Jaringan," p. 9, 2017.

[5] Ryu SDN Framework Community, WHAT'S RYU?, 2017. [Online]. Available: https://ryu-sdn.org/. [Accessed 18 January 2021].

[6] R. Taufik, "Protokol sFlow untuk Network Monitoring," p. 4.

[7] Ariskisaputri, "Bukugue," Pengertian, fungsi dan cara menggunakan bot telegram, 18 Mei 2019. [Online]. Available: https://www.bukugue.com/apa-itu-bot-telegram/#:~:text=Telegram%20bot%20adalah%20sebuah%20bot,lunak%20yang%20memiliki%20fitur%20AI.. [Accessed 18 January 2021].

[8] B. Rifai, N. Nuryadi and A. Ripai, "IMPLEMENTASI TELEGRAM NOTIFICATION ALERT PADA NETWORK MONITORING SYSTEM DENGAN NAGIOS," *Jurnal Mantik Penusa,* p. 7, 2019.

[9] A. E. Putra, "DSP & Embedded Electronic," Mengenal Raspberry Pi, 30 August 2012. [Online]. Available: http://agfi.staff.ugm.ac.id/blog/index.php/2012/08/mengenal-raspberry-pi/. [Accessed 19 January 2021].

[10] D. Indonesia, Memulai Pemrograman Dengan Python, 2021. [Online]. Available: https://www.dicoding.com/academies/86. [Accessed 20 January 2021].

[11] A. J. T, D. Yanosma and K. Anggriani, "IMPLEMENTASI METODE K-NEAREST NEIGHBOR (KNN) DAN SIMPLE ADDITIVE WEIGHTING (SAW) DALAM PENGAMBILAN KEPUTUSAN SELEKSI PENERIMAAN ANGGOTA PASKIBRAKA," p. 15, 2016.

UNIVERSITAS TELKOM
FAKULTAS ILMU TERAPAN
KARTU KONSULTASI
SEMINAR PROPOSAL PROYEK AKHIR

NAMA / PRODI : Faishal Nugraha Pratama / D3 Teknologi Telekomunikasi NIM : 6705184098

JUDUL PROYEK AKHIR :

IDENTIFIKASI DDOS MENGGUNAKAN KNN PADA *SOFTWARE DEFINED NETWORK* DAN NOTIFIKASI BOT TELEGRAM BERBASIS RASPBERRY PI

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

II. Dr. Indrarini Dyah Irawari,S.T.,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	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			