Bab I PENDAHULUAN.

I.1 Latar Belakang .

Sejak kemunculannya beberapa tahun lalu, Software Defined Network (SDN) menjadi salah satu isu yang menarik dalam dunia jaringan baik akademisi maupun praktisi. SDN dimunculkan untuk menggantikan jaringan yang sudah ada saat ini. Jaringan saat ini dianggap kaku dan sulit untuk dikembangkan. Pada jaringan saat ini, perangkatperangkat seperti switch, router dan perangkat jaringa lainnya, bagian kontrol dan data tergabung secara fisik sehingga tidak fleksibel. Dengan adanya SDN, maka kedua bagian dapat dipisahkan, sehingga secara fisik perangkat yang ada di jaringan adalah bagian data atau data plane (Demby Pratama, 2018)

Software Defined Network (SDN) adalah istilah yang merujuk pada konsep/paradigma baru dalam mendesain, mengelola dan mengimplementasikan jaringan, terutama untuk mendukung kebutuhan dan inovasi di bidang ini yang semakin lama semakin kompleks. Konsep dasar SDN adalah dengan melakukan pemisahan eksplisist antara control dan forwarding plane, serta kemudian melakukan abstraksi sistem dan mengisolasi kompleksitas yang ada pada komponen atau sub-sistem dengan mendefinisikan antar-muka (interface) yang standard. (Mulyana, 2014).

Konsep utama pada Software Defined Networking (SDN) adalah sentralisasi jaringan dengan semua pengaturan berada pada control plane. Pada jaringan konvensional administrator jaringan diharuskan menangani puluhan, ratusan atau babkan ribuan perangkat jaringan didalam sebuah organisasi. Permasalahan ini sering ditemukan dalam dunia industri (Farugi, ‘Nunwadi, Ismail & Maryanto, 2017)

Beberapa kelebihan *Software Defined Network* sebagai berikut. Karena semua jika administrasi jaringan terpusat dan otomatis, secara keseluruhan mengarah pada penghematan biaya di SDN. Pengguna mengurangi biaya yang tidak perlu menggunakan SDN dengan pemanfaatan server yang lebih baik dan virtualisasi yang ditingkatkan. Selain itu, SDN mengurangi operasi jaringan dengan mengaktifkan multi-tasking. Dengan demikian, persyaratan untuk perangkat keras yang mahal dihilangkan. SDN menyertakan pengontrol yang memberikan keamanan ke seluruh jaringan. Pengontrol ini memastikan bahwa kebijakan dan informasi keamanan yang tepat diterapkan dalam jaringan. Dan juga, SDN dilengkapi dengan sistem manajemen tunggal.

Satu entitas tunggal akan mengontrol keamanan dan fitur. SDN memungkinkan manajemen terpusat dari seluruh jaringan. Semua perangkat jaringan dapat dipantau dan dikelola dari lokasi pusat. Ini menghilangkan hambatan yang diciptakan oleh sistem tradisional dalam mengelola infrastruktur. Bahkan jika ada kebutuhan untuk mengelola sistem secara individual, SDN memungkinkan untuk melakukannya.

Kemudian berikut beberapa kekurangan dari Software Defined Network itu sendiri diantaranya. Setiap perangkat yang digunakan pada jaringan menempati ruang di dalamnya. Kecepatan interaksi antara perangkat dan jaringan tergantung pada jumlah sumber daya virtual. Jika ada kebutuhan yang lebih cepat, lebih banyak sumber daya virtual dapat diperkenalkan. Sekarang memvirtualisasikan sumber daya dapat menghasilkan latensi yang signifikan. Pemeliharaan merupakan aspek yang sangat penting dari jaringan untuk menjalankan operasinya. SDN kurang di sisi pemeliharaan. Itu membuat hampir tidak mungkin untuk mengelola perangkat yang sebenarnya. Terutama saat meningkatkan jaringan. Tidak ada protokol keamanan standar untuk SDN. Meskipun ada beberapa penyedia layanan pihak ketiga, masih ada masalah keamanan. Hanya mereka yang ahli dalam menangani sistem SDN yang mampu mencegah serangan besar.

Serangan DDoS (Distributed Denial of Service) adalah tipe serangan jaringan berskala besar dengan cara terkoordinasi, yang biasanya diluncurkan secara tidak langsung dengan memanfaatkan komputer lain di Internet yang biasa dinamakan botnet. DDoS bekerja dengan mengirimkan sejumlah paket data secara bersamaan untuk membuat resource target sistem terkuras habis untuk merespon paket data ini. Dengan banyaknya paket data yang masuk maka jaringan komputer akan mengalami overload. (Ahmad Ismail, 2018)

Serangan *denial of service* telah dikenal untuk komunitas jaringan sejak awal 1980. Dampak akhir dari aktifitas ini mengakibatkan terhambatnya aktifitas korban sebagai pengguna layanan komunikasi data. Target serangan DDoS attack bisa ditujukan ke berbagai bagian jaringan. Bisa ke *routing devices, web, electronic mail, atau server Domain Name System*. Serangan ini bertujuan membuat *server shutdown, reboot, crash,* atau"*not responding*". Server adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer (Oetomo, 2003).

Berdasarkan permasalahan keamanan jaringan tersebut, perlunya sebuah studi yang bertujuan untuk mengetahui lebih banyak lagi tentang metode yang digunakan dalam penyerangan DDoS dimana efek yang ditimbulkan oleh DDoS dan pengamanan yang perlu dilakukan untuk mencegah terjadinya DDoS Attack. Selain itu untuk mengetahui apakah serangan DDoS pada suatu sistem jaringan komputer menimbulkan kerugian sistem pada suatu *web server* (Sutarti, 2016).

Disini dijelaskan Self-Organizing Map (SOM) atau sering disebut topology-preserving map pertama kali diperkenalkan oleh Teuvo Kohonen pada tahun 1996. SOM merupakan salah satu teknik dalam Neural Network yang bertujuan untuk melakukan visualisasi data dengan cara mengurangi dimensi data melalui penggunaan Self-organizing neural networks sehingga manusia dapat mengerti

Pada penelitian ini akan dilakukan mitigasi serangan DDoS pada *Software Defined Network* di aplikasi mininet menggunakan metode *Self-Organizing Map* (SOM). Diharapkan penelitian ini dapat mendapatkan hasil penelitian yang mumpuni sehingga dapat bermanfaat terhadap pencegahan serangan DDoS.

I.2 **Perumusan** Masalah

Berdasarkan latar belakang tersebut, penelitian ini dapat merumuskan beberapa permasalahan yaitu:

1. Bagaimana dektesi dan mitigasi Serangan DDoS pada jaringan SDN menggunakan Self-Organizing Map?
2. Bagaimana akurasi deteksi serangan DDoS menggunakan Self-Organizing Map?

I.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah menjawab beberapa masalah yang telah peneliti uraikan sebelumnya pada perumusan maslah, yaitu :

1. Memanfaatkan dan mengimplementasikan metode Self-Organizing Map untuk melakukan deteksi dan mitigasi penyerangan DDoS terhadap SDN
2. Menghasilkan hasil akurasi deteksi serangan DDoS menggunakan Self-Organizing Map

I.4 Batasan Penelitian

Mengingat luasnya pembahasan masalah yang akan dilakukan, maka penelitian ini membatasi ruang lingkup masalah agar pembahasan dapat lebih terfokus dan tujuan penulisan dapat tercapai. Pembatasan ruang lingkup permasalah dalam penelitian ini meliputi:

1. Metode algoritma yang digunakan adalah algoritma Self-Organizing Map
2. Penyerangan yang diujicobakan adalah ICMP flood DDoS attack
3. Dataset yang digunakan adalah data yang digenerate
4. Penggunaan model konseptual NDLC

I.5 Manfaat Penelitian

Manfaat dari penelitian

1. Bagi civitas, penelitian ini bermanfaat dalam meningkatkan efisiensi perkembangan penelitian untuk pengujian serangan DDoS terhadap sebuah jaringan menggunakan *Software Defined Network* sehingga dapat membantu mahasiswa dan dosen agar lebih membantu penelitian selanjutnya dalam pengembangan *Software Defined Network* dalam penelitian kegiatan akademis selanjutnya.
2. Bagi peneliti lain yang bergerak dalam sistem informasi pendidikan tinggi, penelitian ini bermanfaat dalam menjelaskan pendekatan yang paling tepat dalam pengembangan lebih lanjut mengenai pengujian serangan DDoS terhadap sebuah jaringan menggunakan *Software Defined Network* dengan metode *Self-Organizing Map*.