BAB I

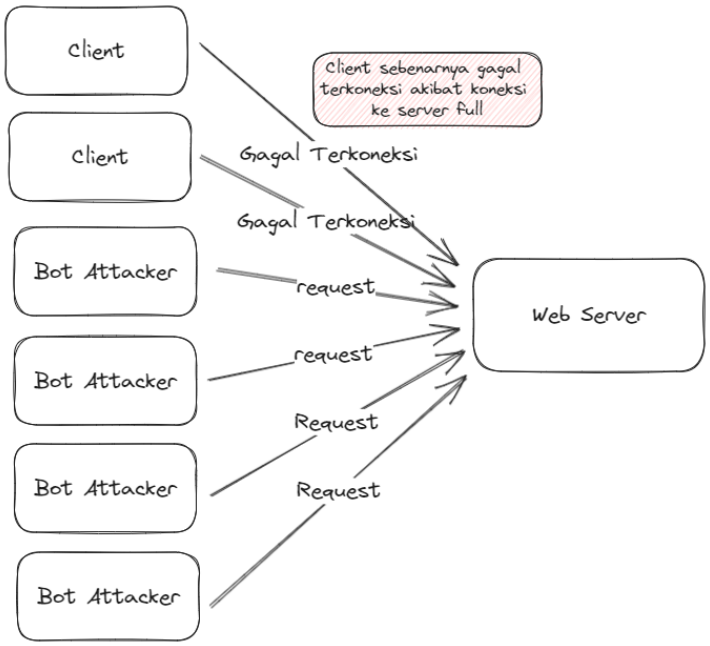
PENDAHULUAN

1.1 Latar Belakang

Penggunaan jaringan komputer sekarang ini semakin luas dan berkembang, ditambah dengan adanya berbagai teknologi layanan web (*web service*) di berbagai bidang kehidupan seperti contohnya adalah *financial technology*, *online game*, *Internet of Things*, *supply chain technology*, dan berbagai bentuk situs web. Layanan web adalah suatu perangkat lunak yang dirancang untuk mendukung interoperabilitas dan interaksi pertukaran data antar beberapa perangkat komputer yang berbeda melalui jaringan internet [1]. Layanan web menggunakan beberapa protokol jaringan komputer sebagai standar spesifikasi web server terlepas dari bahasa pemrogramannya dan sistem operasi yang digunakan oleh setiap perangkat yang berkomunikasi. Biasanya layanan web akan memakai protokol internet seperti layer 4 *transport layer* yaitu TCP / UDP dan layer 7 *application layer* yaitu HTTP / HTTPS. Layer ini dijabarkan dalam 7 OSI layer dalam jaringan komputer. Layanan web sering digunakan untuk integrasi aplikasi, akses jarak jauh, dan berbagi data antar sistem komputer.

Namun disisi lain jika semakin besar jaringan komputer yang dipakai maka akan semakin besar juga risiko yang dapat ditemukan dari suatu implementasi layanan web. Hal ini karena *hacker* dapat menyerang jaringan komputer yang memanfaatkan kelemahan dari jaringan komputer di antara ke 7 OSI layer. Yaitu suatu perangkat server yang menjalankan aplikasi layanan web dapat dengan mudah terserang dengan berbagai metode untuk menghabiskan *resource* atau sumber daya dari perangkat tersebut. Penyerangan ini dikenal dengan teknik *hacking Denial of Service* (DOS). Seiring perkembangan serangan ini, semakin meluas kapasitas serangannya, dimana sebelumnya menggunakan 1 komputer penyerang menjadi beberapa “bot” komputer penyerang dengan bertindak sebagai beberapa *client* terdistribusi yang me-*request* ke server tersebut dengan berulang kali dan bersamaan. Serangan ini dikenal dengan *Distributed Denial of Service*

(DDoS) [2]. Sebagai ilustrasi umum serangan DDoS, diilustrasikan pada gambar 1.1.



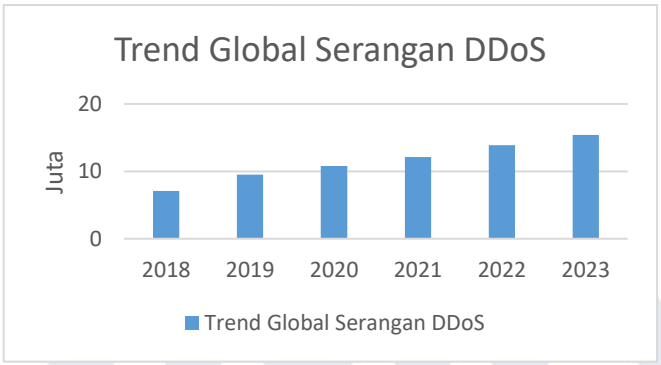
Gambar 1.1 Gambaran Umum Serangan DDoS

Dampak dari serangan DDoS ini menyebabkan aplikasi layanan web mengalami penurunan kinerja sampai gagalnya sistem yang mengakibatkan adanya *downtime* dan tidak bisa diaksesnya sistem tersebut. Oleh karena itu serangan DDoS merupakan ancaman dan masalah utama keamanan internet terlebih pada sistem yang memiliki *single point of failure* seperti penggunaan proxy server yang menjadi satu-satunya perantara antara *client* dan *server*. Jika proxy server atau web server yang memiliki *single point of failure* terserang DDoS maka akan melumpuhkan semua sistem di belakangnya. Hal ini karena akan bukan hanya melumpuhkan layanan web sehingga tidak bisa digunakan namun juga integritas dan kerahasiaan data yang tersimpan di server dapat menjadi rentan akibat serangan DDoS ini [3]. Misalnya seperti teknik *hacking brute-force*. Terlebih serangan DDoS cenderung mudah untuk diluncurkan dari pada serangan siber lainnya yaitu dengan melakukan akses secara berulang kali ke target yang dituju.

Secara umum tujuan dari serangan DDoS adalah menghabiskan *resource* atau sumber daya dari perangkat yang dituju, bisa sumber daya CPU, RAM, atau

network interface. Oleh karena itu metode yang digunakan bisa bermacam macam, penyerang akan melakukan serangan pada salah satu protokol komunikasi dalam jaringan komputer yaitu antara TCP, UDP, ICMP, HTTP, SSH, FTP, dan sebagainya. Karena metode dan teknik penyerangan DDoS sangat banyak dan terus berkembang, maka suatu serangan DDoS akan membentuk suatu pola stokastik. Pola stokastik ini adalah pola yang menghasilkan suatu kejadian yang acak dan tidak bersifat stasioner namun mempunyai *unit root* [4]. Terlebih dengan metode *IP Spoofing*, penyerang bisa saja menggunakan identitas atau alamat IP palsu sehingga akan cukup kompleks untuk mendeteksi dan mengidentifikasi serangan DDoS.

Kasus penyerangan jaringan komputer dengan metode DDoS sekarang ini semakin meningkat. Berdasarkan data statistik dari beberapa sumber seperti perusahaan Cloudflare dan Cisco. Menunjukkan bahwa pada kuartal 2 tahun 2022 terjadi peningkatan serangan DDoS pada layer 7 (*application layer*) sebesar 72% dan pada layer 4 (*transport layer*) meningkat hingga 109% per tahunnya [5]. Berikut merupakan grafik tren serangan DDoS yang ditampilkan pada gambar 1.2.



Gambar 1.2 Grafik Trend Global Serangan DDoS [5]

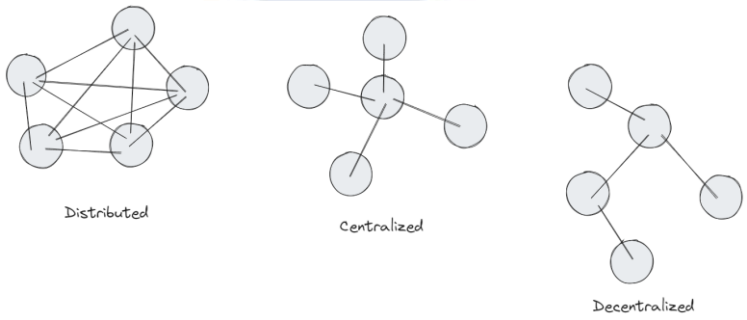
Ada beberapa solusi yang sudah ada untuk memitigasi serangan DDoS yaitu dengan menggunakan sistem *intrusion detection system* (IDS) dan *intrusion prevention system* (IPS). IPS dan IDS beberapanya menggunakan *signature based* dan *behavior based* dalam mendeteksi suatu anomali [6]. Dapat ditemukan banyak aplikasi IDS / IPS yang *open-source* dan sudah banyak dipakai, salah satunya adalah aplikasi yang bernama Snort. Namun untuk aplikasi ini metode

pendeteksiannya masih menggunakan metode konvensional yaitu menggunakan algoritma statistika sederhana yaitu sistem "*Threshold*". Sistem *threshold* adalah membatasi suatu aktivitas jaringan komputer dengan menerapkan batasan tertentu pada interval waktu dan identitas tertentu secara statis. Misal sistem akan melimit suatu IP address hanya boleh memiliki *packet* berjumlah 100 buah setiap 10 detik. Ketika suatu IP address memiliki *packet* lebih dari 100 maka *packet* yang melebihi *threshold*-nya akan dianggap sebagai anomali dan dimitigasi sesuai dengan pengaturannya. Dengan metode tradisional ini memiliki beberapa kekurangan yaitu bisa saja terjadi kesalahan pendeteksian sehingga menghasilkan *false positive* dan *false negative*. Seperti jika lalu lintas jaringan memang sedang ramai pengguna yang normal akan menjadi masalah karena pengaturannya yang statis.

Teknologi *Machine learning* dapat digunakan untuk menangani masalah peristiwa pola stokastik. Dengan *machine learning* dapat membuat sistem IPS yang menggunakan metode *behavior based*. Setiap serangan DDoS memiliki pola dan variasi tersendiri yang bersifat kompleks dan sulit untuk didapatkan jika hanya menggunakan teori statistik dan observasi manusia. Dengan *machine learning* maka akan didapatkan *features* (informasi penting) tersendiri dari suatu data serangan DDoS. Beberapa metode *machine learning* yang dapat dilakukan yaitu untuk pendekatan secara individual dan *timeseries*, dan juga pendekatan secara *atomic* untuk identifikasi *packet* dan *composite* untuk deteksi DDoS pada *stream* (*flow*) packet jaringan [7]. 7 algoritma *machine learning* dan deep learning yang dipilih oleh penulis berdasarkan hasil tinjauan teori untuk klasifikasi data dapat digunakan dan dibandingkan untuk mendapatkan model *machine learning* yang sesuai untuk deteksi secara *realtime* dengan beberapa matriks pengujian. Hal ini karena setiap protokol memiliki *features*, karakteristik, dan penggunaan yang berbeda beda sehingga diperlukan perlakuan *machine learning* yang berbeda pula karena setiap algoritma *machine learning* memiliki metode kalkulasi matematis yang berbeda.

Seiring perkembangan teknologi, dibutuhkan arsitektur layanan web yang mendukung *redundancy*. Hal ini dapat dicapai dengan arsitektur terdistribusi dan terdesentralisasi yang akan bertumpu pada jaringan komputer. Dengan metode dan

arsitektur ini, layanan web memiliki kumpulan aplikasi dan perangkat yang berbeda beda dan memiliki tugasnya masing-masing. Setiap aplikasi dan perangkatnya saling bergantung satu sama lainnya dan digunakan untuk hal yang krusial dan penting sehingga dibutuhkan keamanan yang lebih agar tingkat ketersediaannya tinggi. Dengan ini, dimungkinkan bahwa suatu layanan web memiliki beberapa perangkat server yang terpisah satu dengan yang lainnya namun dikoneksikan dengan jaringan internet dikarenakan memiliki geolokasi yang berbeda beda. Contoh implementasi dari arsitektur ini adalah seperti *content delivery network, API services,* dan *regional game server*. Berdasarkan penelitian yang telah dilakukan oleh IBM Market Research yang diikuti oleh 1200 tenaga IT yang berpengalaman, bahwa lebih dari 80% perusahaan yang ada sudah beralih pada sistem *microservice* dan *decentralized computing* [8]. Adapun arsitektur sistem terdistribusi (*distributed*). Dimana walaupun sistem dibagi bagi menjadi beberapa *service* / *node* tertentu namun tetap ada *central control* untuk mengatur semuanya seperti melakukan konsensus dan lain lain [9]. Berikut merupakan ilustrasi arsitektur *centralized*, *decentralized,* dan *distributed* yang ditampilkan pada gambar 1.3.

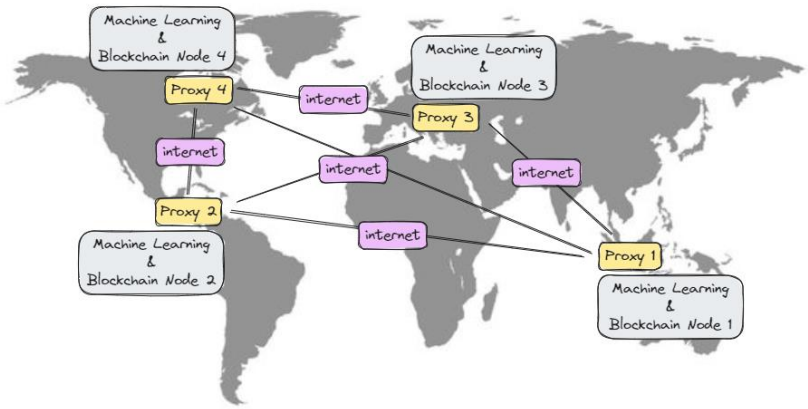


Gambar 1.3 Ilustrasi Perbedaan Sistem *Distributed*, *Centralized*, dan *Decentralized*

Oleh karena arsitektur terdesentralisasi dan terdistribusi maka antar IPS perlu membagi informasi penyerang agar menambah efektivitas dari keuntungan sistem terdesentralisasi. Agar jika suatu penyerang menyerang sistem 1, maka sistem 2, 3, dan 4 sudah memblokir penyerang sehingga *time to mitigate*-nya adalah 0. Namun karena antar IPS bisa saja menggunakan jalur komunikasi *public* internet karena perbedaan geolokasi maka perlu digunakan *database* yang terdistribusi dan

memiliki kemampuan *immutability* yaitu salah satunya adalah *database* berbasis *blockchain*. Kemampuan *immutability* penting agar tidak terjadi penyerangan pada sistem *database* dan mengubah konfigurasi *firewall*. Dibutuhkan juga sistem konsesus yang cepat agar informasi penyerang tersebar ke seluruh IPS sedini mungkin.

Oleh karena beberapa dasar permasalahan tersebut maka penelitian ini akan merancang dan membangun sistem proxy untuk memitigasi serangan DDoS dengan teknologi *machine learning* dan *blockchain*. Proxy akan bertindak sebagai penengah antara *client* dengan *webserver*, sehingga dapat menjadi *listener* dan juga *firewall*. Dengan begitu *webserver* tidak secara langsung terhubung dengan *public* internet. Proxy akan dirancang menjadi proxy terdistribusi yang berbeda secara geolokasi untuk memenuhi kebutuhan arsitektur *decentralized computing* dan *distributed computing*. Ilustrasi proxy terdistribusi dapat dilihat pada gambar 1.4.



Gambar 1.4 Ilustrasi Proxy Terdistribusi

Berdasarkan masalah dan rancangan solusi yang sudah dipaparkan, maka dengan latar belakang ini penulis akan melakukan penelitian dengan judul "*Rancang Bangun Sistem Proxy Mitigasi DDoS berbasis Machine Learning dan Blockchain*".

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang sudah dipaparkan, rumusan masalah pada penelitian ini terdiri dari beberapa poin, yaitu :

1.2.1 Apakah sistem proxy mitigasi DDoS berbasis *machine learning* dapat mengamankan layanan web dari serangan DDoS secara efektif, keseluruhan, dan akurat yang diukur dengan metrik pengujian tertentu jika dibandingkan dengan solusi IPS / IDS yang *open-source* dan banyak dipakai sekarang?

1.2.2 Model dan metode *machine learning* apakah yang cocok untuk diimplementasikan pada deteksi dan identifikasi serangan DDoS secara *realtime*?

1.2.3 Apakah dengan membuat sistem proxy mitigasi DDoS yang menggunakan *database* terdistribusi berbasis *blockchain* dapat menambah efektivitas pada sisi *time to mitigate* dari proxy terdistribusi?

1.3 Batasan Penelitian

Berdasarkan identifikasi masalah yang sudah disebutkan, berikut merupakan batasan masalah dari penelitian ini :

1.3.1 Jenis serangan DDoS yang diteliti hanya berjenis TCP Syn dan XMAS flood, UDP flood, ICMP ping dan Smurf flood, dan HTTP Get flood pada jaringan IPV4. Beberapa jenis metode DDoS ini dan aktivitas jaringan normal disimulasikan dengan *testbed*, kode, dan *tools* yang dipilih oleh penulis.

1.3.2 Keseluruhan sistem yang dibangun hanya diuji coba pada *testbed* dan uji skenario yang sudah ditetapkan oleh penulis yang dijabarkan pada bab analisis dan perancangan sistem untuk mendapatkan hasil dan analisa pengujian.

1.3.3 *Hyper-parameter* model *machine learning* yang digunakan merupakan pilihan penulis berdasarkan penelitian terdahulu, dasar teori, dan hasil observasi penulis.

1.4 Tujuan Penelitian

Berikut beberapa tujuan dari penelitian ini, yaitu :

1.4.1 Merancang dan membangun sistem proxy mitigasi DDoS berbasis *machine learning* dan *blockchain*.

1.4.2 Membandingkan sistem proxy mitigasi DDoS yang sudah dibangun dengan solusi IPS / IDS *open-source* dan banyak digunakan sekarang dengan uji skenario dan metrik pengujian tertentu.

1.4.3 Menguji coba beberapa metode dan algoritma *machine learning* untuk mengklasifikasi data deteksi dan identifikasi serangan DDoS berdasarkan protokol TCP, UDP, ICMP, dan HTTP pada jaringan IPV4.

1.4.4 Merancang, membangun, dan menganalisis proxy yang terdistribusi untuk menunjang perkembangan sistem *distributed computing*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut :

1.5.1 Menyediakan sistem proxy mitigasi DDoS berbasis *machine learning* dan *blockchain* sebagai solusi dan referensi untuk mengatasi masalah serangan DDoS yang semakin meningkat.

1.5.2 Dapat digunakan sebagai sumber referensi dan acuan dalam hasil penelitian dan analisis untuk modul *machine learning* yang digunakan untuk mendeteksi dan mengidentifikasi serangan DDoS secara *realtime*.

1.5.3 Dapat digunakan sebagai sumber informasi dalam pembuatan sistem terdistribusi dengan *distributed database* berbasis *blockchain*

1.5.4 Mendorong perkembangan dan penggunaan teknologi internet, *machine learning*, dan *blockchain* pada berbagai bidang.

1.6 Sistematika Penulisan

Laporan penelitian ini disusun dengan beberapa bagian untuk mempermudah pembacaan dan pemahaman pada bahasan penelitian ini.

1.6.1 Bab 1 Pendahuluan

Pada bab ini akan membahas tentang latar belakang, rumusan masalah, batasan penelitian, tujuan penelitian, dan manfaat penelitian dari penelitian yang akan dilakukan oleh penulis.

1.6.2 Bab 2 Tinjauan Pustaka

Pada bab ini akan membahas tentang penulis melakukan pencarian dan mempelajari penelitian terdahulu serta teori terkait pada penelitian yang akan dilakukan guna untuk referensi penelitian dan perbaikan untuk mengoptimalkan sistem yang akan dibuat oleh penulis seperti karakteristik serangan DDoS, *features* dataset, dan metode *machine learning* apa saja yang dapat digunakan untuk deteksi dan identifikasi serangan DDoS. Selain itu akan dibahas juga deskripsi dari teknologi yang akan dipakai penulis seperti NetfilterQueue, Python, Socket, BigchainDB, Bidirectional LSTM, SVM, Linear Regresion, dan lain lain.

1.6.3 Bab 3 Analisis dan Perancangan Sistem

Pada bab ini akan membahas tentang penulis melakukan perancangan umum dari keseluruhan sistem yang akan dibuat oleh penulis, mulai dari arsitektur sistem, cara kerja, sub sistem dan modul yang akan diimplementasikan, skenario uji coba, dan penentuan metrik pengujian.

1.6.4 Bab 4 Implementasi dan Pengujian Sistem

Pada bab ini akan membahas tentang penulis melakukan implementasi dan pengujian berupa hasil penelitian dan analisa berdasarkan skenario uji coba dan metrik pengujian pada sistem yang dibangun. Berisi juga tentang kendala dan solusi terhadap masalah saat proses implementasi yang dilakukan oleh penulis.

1.6.5 Bab 5 Simpulan dan Saran

Pada bab ini akan membahas tentang kesimpulan pengujian beserta saran terhadap penelitian terkait selanjutnya berdasarkan penelitian yang telah dilakukan oleh penulis.