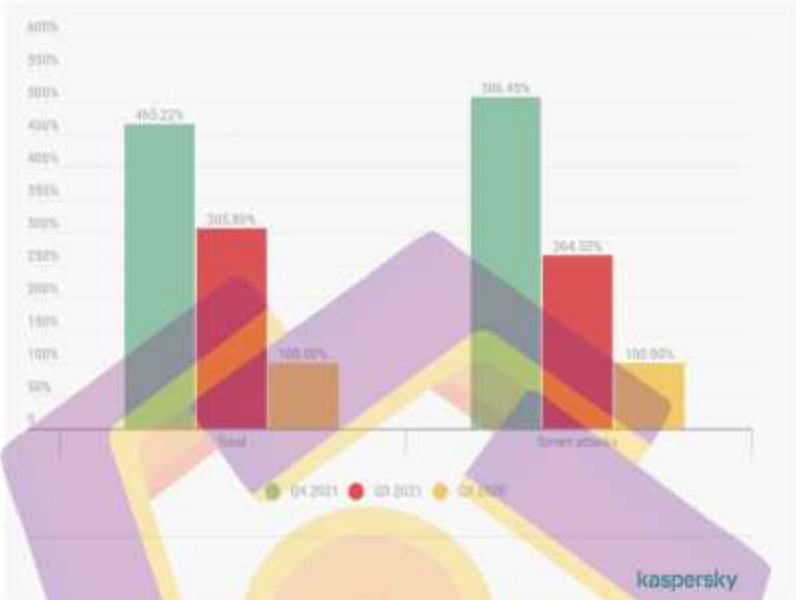
BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

(DDoS) adalah salah satu serangan Internet yang paling berbahaya, dengan kemampuan untuk membanjiri server web, sehingga memperlambat dan berpotensi melumpuhkannya sepenuhnya [1]. DDoS merupakan suatu upaya untuk membuat suatu layanan online tidak berfungsi atau tidak tersedia bagi pengguna dengan mengganggu layanan server, *traffic* penyerang sering menyerupai lalu lintas yang sah dan pola serangan dicampur untuk menyalakan serangan yang nyata. Serangan *Distributed Denial of Service* (DDoS) tidak diragukan lagi masalah yang sangat serius di internet, yang dampaknya telah ditunjukkan dengan baik di komputer literatur jaringan. Tujuan utama dari DDoS adalah gangguan layanan dengan mencoba membatasi akses ke mesin atau layanan, bukan meruntuhkan layanan itu sendiri. jenis serangan ini bertujuan untuk membuat jaringan yang tidak mampu menyediakan layanan normal dengan menargetkan bandwidth jaringan atau konektivitasnya. Serangan ini mencapai tujuannya dengan mengirimkan pada korban aliran paket yang membanjiri jaringan atau kapasitas pemrosesan yang menolak akses ke klien regulernya. Serangan DDoS biasanya berasal dari beberapa mesin yang dioperasikan oleh pengguna ataupun oleh bot, sedangkan serangan DDoS dilakukan oleh satu orang atau satu sistem.

Hasil peneliti Kaspersky mengamati adanya peningkatan besar-besaran dalam jumlah serangan DDoS pada oktober hingga akhir Desember 2021 dimana hasil yang didapatkan yaitu jumlah komparatif serangan DDoS: Q3 dan Q4 2021 serta Q4 2020. Data untuk Q4 2020 diambil 100%.



Gambar 1.1 Hasil Penelitian Kaspersky

(Sumber: Kaspersky.com)

Dibandingkan dengan angka dari kuartal kedua tahun 2021 (Q2 2021), solusi Kaspersky melindungi penggunaanya dari serangan DDoS sekitar 2,5 kali lebih banyak. Dikala yang sama, berbeda dengan pada tahun (Q1 2022) dengan lonjakan serbuan yang dramatis sebab kegiatan hacktivist, jumlah mutlak menyusut pada kuartal 2 tahun ini. Dalam paparan data hasil penelitian Kaspersky dimana serangan DDoS tiap tahunnya meningkat dan ini menjadi suatu masalah yang dihadapi di era teknologi informasi dan ini akan berakibat pada terhambatnya suatu informasi atau data yang diakses oleh user pada suatu server.

Oleh karena itu penting untuk melakukan identifikasi alternatif untuk inspeksi paket jaringan dengan sistem analisis untuk kemudian dapat digunakan dalam melakukan deteksi intrusi dan pelengkap inspeksi paket pada lalu lintas jaringan, dengan alat keamanan *Network Intrusion Detection System* (NIDS)

dengan metode IDS dengan memanfaatkan arsitektur algoritma *Neural Network* yang digunakan secara luas untuk mendeteksi serangan atau aktivitas penyerang pada lalu lintas jaringan. Dengan peningkatan kecepatan jaringan dan jumlah serta jenis serangan dengan tantangan menangkap atau memeriksa setiap paket untuk membandingkanya dengan tanda tangan berbahaya yang ada pada dataset. Tantangan-tantangan ini akan berdampak pada efisiensi *Network Intrusion Detection System* terutama kinerja dan kekuatan tingkat akurasi dalam melakukan identifikasi serangan DDoS pada jaringan komputer.

Bersumber pada paparan diatas penelitian ini menganjurkan mekanisme deteksi terhadap serbuan DDoS. Mekanisme yang akan diajukan yaitu menggunakan arsitektur IDS dengan memanfaatkan Neural Network untuk mendeteksi serangan DDoS. *Neural Network* dipilih karena deteksi penyalahgunaan semua fitur serangan yang diketahui disimpan di dalam dataset menggunakan model yang dikenal dan membandingkan pada data uji dan data latih, untuk memberikan hasil akurasi yang tinggi dalam mendeteksi suatu serangan pada sistem jaringan. IDS berbasis *Neural Network* secara khusus diusulkan untuk mempelajari tipikal karakteristik penggunaan sistem dan mengidentifikasi variasi yang signifikan secara statistic dari perilaku serangan. Dalam pendekatan Neural Network pada Intrusion Detection memperkenalkan data yang mewakili serangan dan aliran normal pada jaringan ke Neural Network untuk menyesuaikan koefisien pada jaringan.

1.2 Rumusan Masalah

Berdasarkan dari uraian latar belakang dapat dirumuskan beberapa permasalahan sebagai berikut:

1. Bagaimana mendeteksi dan melakukan Klasifikasi DDoS pada suatu jaringan dengan berbasis Neural Network dalam membantu IDS dalam mendeteksi serangan.
2. Seberapa besar tingkat akurasi dalam mengklasifikasi atau mendeteksi suatu serangan DDoS menggunakan machine learning berbasis algoritma Neural Network.

1.3 Batasan Masalah

Pada penelitian ini untuk mempersempit pembahasan pada skripsi ini maka dibuat Batasan-batasan masalah sebagai berikut:

1. Penelitian hanya difokuskan pada serangan DDoS saja, tidak untuk jenis serangan lain.
2. Data yang akan digunakan untuk proses training akan diambil dari hasil dataset KDD CUP 99.
3. Pengujian serangan menggunakan Google Collab.
4. Bahasa pemrograman menggunakan Bahasa python.
5. Jenis serangan DDoS.

1.4 Tujuan Penelitian

Adapun beberapa poin tujuan dari penelitian ini adalah sebagai berikut:

1. Memanfaatkan metode IDS berbasis algoritma Neural Network dalam memberikan survey komprehensif dan menjelaskan kumpulan data yang digunakan untuk evaluasi sistem deteksi intrusi dalam penanganan serangan DDoS.
2. Mengetahui tingkat akurasi pada desain IDS yang berbasis algoritma Neural Network dalam mendeteksi serangan DDoS berdasarkan data latih dan data uji, untuk penanganan serangan DDoS dimasa yang akan datang.
3. Meningkatkan keamanan dan membantu IDS dalam melakukan deteksi serangan DDoS.

1.5 Sistematika Penulisan

Sistematika penulisan pada penelitian ini memberikan gambaran dan kerangka yang jelas mengenai pokok bahasan di setiap bab. Berikut sistematika penulisan dan pembahasan pada masing-masing bab:

Bab I Pendahuluan, berisi: latar belakang, rumusan masalah, tujuan penelitian, Batasan masalah, dan sistematika penulisan.

Bab II Landasan Teori, berisi: studi Pustaka yang berisi penjelasan tentang penelitian terkait dan landasan-landasan teori yang berhubungan dengan permasalahan penelitian.

Bab III Metodologi Penelitian, berisi: metodologi penelitian berisi pembahasan tentang rancangan atau prosedur penelitian yang akan di analisis dari awal hingga akhir.

Bab IV Pembahasan, berisi: pembahasan dan uji coba dari hasil setiap rancangan atau prosedur yang telah di analisis sebelumnya untuk dilakukan Analisa hasil uji coba.

Bab V Penutup, berisi: bab terakhir berisi tentang kesimpulan dan saran yang penulis dari hasil uji coba dan pembahasan dalam pene