BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era digital ini, internet telah menjadi bagian yang sangat penting dalam masyarakat kita dalam berbagai bidang, seperti dalam bidang pemerintahan, bisnis, dan bahkan dalam kehidupan pribadi sehari – hari. Selain itu juga terjadi peningkatan jumlah infrastruktur yang sangat pesat dan mengandalkan jaringan internet, sebagai contoh adalah kontrol lalu lintas udara[1]. Namun, dalam cyberspace ini terdapat banyak serangan yang terjadi, seperti Denial of Service, Distributed Denial of Service (DDOS), Phishing, Email Spamming, Financial Fraud, dan masih banyak lagi jenis serangan yang terjadi. Salah satu serangan yang menjadi ancaman kritis adalah DDoS Attack yang berdampak bagi banyak area dalam kehidupan kita seperti IoT, smart city, rumah sakit, dan komersial[2].

Serangan DDoS semakin mengancam keamanan jaringan dari semua sektor bisnis karena peningkatan kompleksitas, volume, dan frekuensi yang terus menerus[2]. DDoS Attack sendiri adalah serangan dengan metode mengirimkan paket dengan volume besar melalui lalu lintas jaringan dari banyak sistem yang sudah dieksploitasi yang disebut zombie ke target dengan tujuan menghabiskan sumber daya milik target. Dampak dari serangan ini adalah sistem target tidak bisa melayani paket paket yang sebenarnya karena sumber dayanya dihabiskan oleh paket dari serangan DDoS, sehingga server menjadi down yang menyebabkan kerugian finansial atau bahkan hilangnya informasi penting[1].

Berdasarkan FBI's Internet Crime Complaint Centre pada tahun 2009, jumlah kerugian finansial dari serangan dunia maya berjumlah US$559,7 juga. Pada tahun 2011, Symantec mengidentifikasi lebih dari 5,5 miliar serangan, data ini lebih tinggi 81% dari tahun sebelumnya. Selain itu terdapat 403 juta variasi malware dan jumlah serangan web per hari meningkat 36%[2]. Dilansir oleh cloudflare ada 7 serangan DDoS yang terkenal. Pertama "The 2000 Mafiaboy attack". Serangan yang terjadi pada tahun 2000 ini dilakukan oleh anak berusia 15 tahun yang dikenal dengan nama "Mafiaboy", serangan ini menyebabkan website besar seperti CNN, Dell, E-

Trade, eBay, dan Yahoo! Yang menyebabkan kekacauan pada pasar saham dikala itu. Tingkat serangan ini sekitar 1 Gb per detik[2]. Selanjutnya "The 2007 Estonia attack", serangan ini menargetkan negara Estonia. Negara ini adalah pengadopsi awal sistem pemerintahan online yang praktis dan tanpa kertas. Targetnya adalah layanan pemerintahan, lembaga keuangan, dan outlet media. Serangan ini dianggap sebagai tindakan pertama perang dunia maya sehingga menyebabkan terciptanya hukum internasional untuk perang dunia maya. Tingkat serangan ini sekitar 70Gb per detik[2]. Ketiga, pada tahun 2013 terdapat serangan "The 2013 Spamhaus attack". Serangan ini diarahkan ke sebuah organisasi yang membantu memerangi email spam dan aktivitas terkait spam bernama Spamhaus. Akibat serangan ini, lalu lintas ke spam haus mencapai 300 Gbps. Selanjutnya terdapat serangan yang menargetkan GitHub, layanan manajemen kode online populer yang digunakan oleh jutaan pengembang pada tahun 2015. Serangan ini berasal dari China dan secara khusus menargetkan URL dari dua proyek GitHub yang bertujuan menghindari sensor negara China. Kemungkinan serangan ini bertujuan untuk menghapus proyek tersebut. Lalu lintas serangan dibuat dengan menambahkan kode JavaScript ke browser setiap orang yang mengunjungi Baidu. Kode ini menyebabkan browser yang terinfeksi mengirim permintaan HTTP ke halaman GitHub yang ditargetkan. Serangan kelima adalah "The 2016 Dyn attack". Serangan ini menargetkan Dyn, sebuah penyedia DNS utama pada bulan Oktober 2016. Akibat serangan ini terjadi gangguan bagi banyak situs utama, yaitu Airbnb, Netflix, PayPal, Visa, Amazon, The New York Times, Reddit, dan GitHub. Malware yang digunakan pada serangan ini bernama Mirai. Cara kerjanya adalah membuat botnet dari perangkat Internet of Things (IoT) yang disusupi seperti, smart TV, Radio, Kamera, Printer, dan bahkan monitor bayi. Lalu lintas serangan perangkat tersebut diprogram untuk mengirim permintaan ke satu korban. Selanjutnya adalah serangan DDoS yang menargetkan GitHub. Serangan ini mencapai 1,3 Tbps, paket yang dikirimkan dengan kecepatan 126,9 juta per detik. Serangan ini adalah serangan memcached DDoS, jadi tidak ada botnet yang terlibat. Melainkan penyerang memanfaatkan efek amplifikasi dari sistem caching database populer bernama memcached. Penyerang membanjiri server memcached dengan

permintaan palsu sehingga dapat memperkuat serangan mereka dengan kekuatan sekitar 50.000 kali. Terakhir, serangan terbesar yang pernah tercatat terjadi pada tahun 2020 yang menargetkan pelanggan AWS. Puncak lalu lintas masuk yang terjadi pada serangan ini mencapai 2,3 Tbps. Namun AWS tidak mengungkap pelanggan mana yang menjadi target serangan tersebut. Penyerang menggunakan server web Connection-less Lightweight Directory Access Protocol (CLDAP) yang dibajak. Protokol ini adalah protokol untuk direktori pengguna, alternatif untuk LDAP[3]. Ketujuh serangan diatas merupakan sebuah ancaman tingkat internasional, yang memiliki dampak sangat besar pada korban tersebut. Namun pada tingkat nasional sendiri, berdasarkan informasi dari cnnindonesia.com di Indonesia pada 25 Juni 2020 terjadi serangan DDoS yang menargetkan website DPR RI. Akibat serangan ini, website dpr.go.id tidak dapat diakses[4].

Setelah melihat berbagai serangan yang terjadi baik pada tingkat nasional maupun internasional serta dampak yang diakibatkan oleh serangan DDoS, maka perlu mengembangkan sistem pendeteksian serangan DDoS dengan memanfaatkan machine learning. Karena serangan DDoS ini tidak mudah untuk dideteksi maka diperlukan machine learning yang dapat mengintegrasikan statistik dan ilmu komputer untuk membangun algoritma yang lebih efisien ketika diterapkan pada data yang relevan. Machine learning adalah algoritma komputasi yang ditingkatkan dari pengalaman secara otomatis. Sehingga dapat membuat keputusan tanpa diprogram secara khusus untuk melakukannya[5]. Pada penelitian ini, metode yang digunakan adalah Decision Tree karena merupakan metode yang efektif untuk melakukan klasifikasi. Selain itu metode ini juga mudah digunakan, bebas dari nilai ambigu, dan bahkan kuat dihadapkan pada nilai nilai yang hilang[6]. Decision Tree sendiri merupakan salah satu algoritma klasifikasi yang dipelajari secara langsung membangun model dari kumpulan data yang telah diklasifikasi sebelumnya. Setiap data ditentukan oleh nilai atribut. Klasifikasi dilihat dari pemetaan sekumpulan atribut ke kelas atribut tertentu. Algoritma ini mengklasifikasikan data yang diberikan menggunakan nilai atributnya[7].

1.2 Rumusan Masalah

Berdasarkan latar belakang maka dapat dirumuskan bagaimana performa klasifikasi serangan *distributed denial of service* menggunakan algoritma *decision tree*?

1.3 Batasan Masalah

Untuk mempersempit pembahasan pada skripsi ini, maka dibuat batasan – batasan sebagai berikut:

a. Dataset yang digunakan adalah NSL_KDD.
b. Algoritma *machine learning* yang digunakan adalah *decision Tree* untuk melakukan klasifikasi serangan *DDoS*.
c. Metrik evaluasi menggunakan akurasi, presisi, recall, dan f1 score.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam skripsi ini adalah dapat membuat model yang paling efektif dalam melakukan klasifikasi serangan *DDoS*.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat dalam klasifikasi serangan *DDoS*, di antaranya:

a. Penelitian ini diharapkan bisa bermanfaat untuk mengembangan klasifikasi serangan *DDoS*.
b. Penelitian ini diharapkan dapat menemukan algoritma yang tepat dan akurat dalam melakukan klasifikasi serangan *DDoS*.