

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat telah mendorong berbagai sektor untuk mengadopsi sistem digital, termasuk pada bidang pendidikan. Di lingkungan sekolah dan perguruan tinggi, teknologi jaringan menjadi komponen utama dalam mendukung aktivitas pembelajaran, administrasi, dan komunikasi. Penerapan jaringan komputer, seperti *Local Area Network* (LAN) dan *Wireless LAN* (Wi-Fi), memungkinkan siswa dan tenaga pendidik untuk mengakses berbagai sumber belajar digital, menggunakan sistem manajemen pembelajaran *Learning Management System* (LMS), serta menjalankan kegiatan akademik secara daring dan terintegrasi. Namun, di balik manfaat besar dari teknologi jaringan, terdapat tantangan yang tidak bisa diabaikan, yaitu ancaman terhadap keamanan jaringan. Salah satu serangan siber yang cukup meresahkan institusi pendidikan adalah *Distributed Denial of Service* (DDoS). Serangan DDoS bekerja dengan cara membanjiri jaringan atau server dengan lalu lintas data dari banyak sumber secara bersamaan, hingga sistem menjadi tidak mampu menangani permintaan tersebut. Akibatnya, layanan jaringan seperti akses internet, website sekolah, atau aplikasi pembelajaran daring bisa terganggu bahkan lumpuh total.

Serangan *Distributed Denial of Service* (DDoS) dapat diklasifikasikan menjadi tiga jenis berdasarkan pendekatan dan target serangannya, yaitu serangan berbasis *bandwidth*, berbasis lalu lintas jaringan, dan berbasis aplikasi. Pertama, serangan dengan basis *bandwidth* dilakukan mengirimkan pesan data dalam bentuk

sampah secara massal ke sistem target. Kedua, serangan dengan basis lalu lintas jaringan merupakan bentuk serangan yang paling umum. Serangan ini dilakukan dengan membanjiri jaringan menggunakan sejumlah besar paket TCP, UDP, atau ICMP yang tampaknya sah, tetapi sebenarnya bertujuan untuk menguras kapasitas jaringan atau server. Ketiga, serangan dengan basis aplikasi menasar secara spesifik pada lapisan aplikasi dengan cara mengirimkan permintaan yang tampak legal, seperti akses ke basis data atau layanan web [1]. Serangan DDoS yang pernah terjadi pada instansi pendidikan yaitu Tahun 2016, bahwa serangan tersebut membanjiri *bandwidth* akses, sehingga situs PPDB Online tidak dapat diakses oleh pengguna yang mengakibatkan pendaftaran peserta didik baru tertunda [2].

SMKN 2 Cikarang Barat adalah instansi dibidang pendidikan. SMKN 2 Cikarang Barat memiliki guru sebanyak 91 guru dan peserta didik 1654 siswa, SMKN 2 Cikarang Barat memanfaatkan internet sebagai sarana informasi, komunikasi baik antar guru ataupun sesama siswa. Infrastruktur jaringan SMKN 2 Cikarang Barat menggunakan infrastruktur *wireline* dan *wireless*. Jaringan *wireline* dimanfaatkan untuk sarana pada laboratorium dan jaringan *wireless* yang diterapkan berfungsi untuk kebutuhan dalam belajar mengajar di kelas dan berbagi informasi staff, guru dan kepala sekolah. Dengan infrastruktur jaringan yang telah dibangun, SMKN 2 Cikarang Barat pada dasarnya telah mampu memenuhi kebutuhan sumber daya jaringan bagi seluruh penggunanya, baik untuk kegiatan pembelajaran, administrasi, maupun operasional sekolah. Sistem keamanan jaringan yang diterapkan juga telah mencakup pengelolaan akses terhadap sumber daya jaringan internal, seperti autentikasi pengguna dan pembatasan akses

berdasarkan hak tertentu. Namun demikian, sistem keamanan tersebut masih memiliki keterbatasan dalam hal mitigasi terhadap ancaman eksternal, khususnya serangan siber seperti *Distributed Denial of Service* (DDoS). Infrastruktur yang ada belum sepenuhnya memanfaatkan log dalam menganalisis serangan dari luar jaringan berdasarkan pesan yang terekam pada trafik jaringan, sehingga potensi gangguan terhadap layanan jaringan sekolah masih cukup tinggi. Oleh karena itu, diperlukan suatu pendekatan analisis log sistem jaringan yang mampu mendeteksi dan mengklasifikasikan trafik jaringan normal atau DDoS.

Router menjadi salah satu perangkat penting dalam manajemen lalu lintas jaringan. Router tidak hanya berfungsi sebagai pengatur jalur data, tetapi juga menyimpan log aktivitas jaringan yang mencatat semua kejadian di dalam jaringan, termasuk akses pengguna, permintaan koneksi, dan anomali trafik. Log ini dapat dijadikan sumber data penting dalam proses pemantauan dan analisis keamanan jaringan. Salah satu ancaman yang dapat diidentifikasi melalui analisis log adalah serangan *Distributed Denial of Service* (DDoS). DDoS dapat menyebabkan gangguan serius, dimulai dari lambatnya koneksi internet, tidak tersedianya layanan pembelajaran online, hingga lumpuhnya seluruh sistem jaringan. Di sinilah peran log router menjadi sangat penting. Dengan menganalisis pola trafik yang tidak wajar dari log router, administrator jaringan dapat mendeteksi indikasi awal dari serangan DDoS sebelum dampaknya meluas. Namun, proses analisis log secara manual membutuhkan waktu dan ketelitian yang tinggi. Oleh karena itu, diperlukan pendekatan berbasis data mining atau *machine learning* untuk melakukan otomatisasi proses tersebut. Salah satunya adalah dengan menerapkan algoritma

Decision Tree, yang mampu mengklasifikasikan pola-pola serangan berdasarkan data historis dari log jaringan.

Dalam penelitian ini, peneliti menggunakan banyak penelitian sebelumnya yang telah menjadi peneliti dari studi ini untuk menyelesaikan masalah dalam studi ini, adapun penelitian-penelitian tersebut adalah berjudul Identifikasi Serangan *Denial Of Service (Dos)* Di Jaringan Dengan Algoritma *Decision Tree C4.5* dengan kesimpulan yaitu algoritma C4.5 menggunakan dataset training mendapatkan akurasi dalam melakukan prediksi serangan *DoS* mencapai $\geq 99,8 \%$ dibandingkan menggunakan dataset testing yang akurasinya $90,68 \%$ [3]. Penelitian selanjutnya berjudul implementasi algoritma c.45 untuk klasifikasi deteksi serangan pada protokol jaringan dengan hasil yaitu sebanyak 125543 data terdapat deteksi *worm trojan* yaitu sebanyak 28 paket data. Hasil analisis klasifikasi data jaringan dengan menggunakan menggunakan algoritma C.45 didapatkan nilai akurasi yaitu $93,62 \%$ [4]. Penelitian selanjutnya berjudul Klasifikasi Serangan Jaringan Menggunakan Metode *Decision Tree* Berbasis Website dengan hasil implementasi metode *decision tree* berjalan sesuai dengan fungsinya, file terklasifikasi adanya serangan atau tidak ada serangan dari DDoS dan aplikasi ini berhasil melakukan validasi hasil deteksi *Intrusion Detection System (IDS)* apakah benar atau salah [5].

Berdasarkan penelitian-penelitian terdahulu, peneliti akan menerapkan algoritma *Decision Tree* dalam analisis log sistem router di SMKN 2 Cikarang Barat, penelitian ini bertujuan untuk mendeteksi serangan DDoS secara lebih cepat, akurat, dan efisien. Pendekatan ini diharapkan dapat membantu pihak sekolah

dalam mengidentifikasi ancaman jaringan secara dini, serta mendukung pengambilan keputusan yang lebih tepat dalam pengelolaan sistem keamanan jaringan atau *firewall* pada Router. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan efektivitas deteksi serangan siber serta memaksimalkan pemanfaatan log sistem sebagai sumber data strategis dalam perlindungan infrastruktur jaringan sekolah. Berdasarkan latar belakang tersebut peneliti membuat penelitian yang berjudul **“PENERAPAN ALGORITMA *DECISION TREE* DALAM ANALISIS LOG SISTEM ROUTER UNTUK PENGKLASIFIKASIAN SERANGAN DDoS”**

1.2 Identifikasi Masalah

Berdasarkan latar belakang diatas, peneliti dapat menyimpulkan identifikasi masalah sebagai berikut,

1. Router Mikrotik telah mencatat log sistem, tetapi analisis DDoS manual terhadap log tersebut tidak efisien, karena membutuhkan waktu yang lama untuk menganalisis satu persatu serta kurang akurat.
2. Belum diterapkannya metode cerdas yang mampu mendeteksi dan mengklasifikasikan serangan DDoS secara akurat.
3. Belum terdapat evaluasi sistematis terhadap kinerja algoritma *Decision Tree* dalam membedakan lalu lintas jaringan normal dan serangan DDoS

1.3 Rumusan Masalah

Berdasarkan latar belakang diatas, penulis menyimpulkan rumusan masalah sebagai berikut, "Bagaimana menganalisis log sistem pada router menggunakan bantuan *machine learning* untuk membedakan aktivitas jaringan normal dan pola

serangan DDoS menggunakan algoritma *Decision Tree*, guna mendeteksi serangan secara efektif dan membantu administrator jaringan dalam mengoptimalkan konfigurasi *firewall*.

1.4 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah:

1. Berfokus pada jaringan di SMKN 2 Cikarang Barat yang menggunakan router Mikrotik CCR1016-12G sebagai perangkat utama.
2. Data yang digunakan untuk analisis hanya berasal dari log sistem router dalam waktu 1 Bulan.
3. Hanya menggunakan algoritma *Decision Tree* untuk analisis dan klasifikasi serangan DDoS.
4. Penelitian dilakukan pada lingkungan jaringan SMKN 2 Cikarang Barat terfokus pada ISP Metrosolusindo.

1.5 Tujuan Penelitian

Adapun tujuan dalam melakukan penelitian ini sebagai berikut,

1. Membantu mendeteksi serangan DDoS secara real-time dengan menganalisis log jaringan dari router Mikrotik.
2. Membedakan antara aktivitas jaringan yang normal dengan pola serangan DDoS menggunakan algoritma *Decision Tree*.
3. Meningkatkan akurasi dalam mendeteksi serangan DDoS dibandingkan dengan metode manual.
4. Kontribusi dalam bidang keamanan jaringan, khususnya dalam penerapan algoritma *Decision Tree*.

1.6 Manfaat Penelitian

Adapun manfaat yang didapat dalam melakukan penelitian ini sebagai berikut,

1. Klasifikasi log jaringan membantu memastikan bahwa layanan jaringan tetap stabil dan dapat diakses oleh pengguna, baik siswa, guru, maupun staf administrasi.
2. Memberikan wawasan tentang pola serangan DDoS yang sering terjadi, sehingga sekolah dapat mengembangkan strategi keamanan yang lebih baik.
3. Menjadi acuan untuk mengevaluasi efektivitas algoritma Decision Tree dalam klasifikasi trafik jaringan antara aktivitas normal dan serangan.

1.7 Sistematika Penulisan

Sistematika penulisan tugas akhir ini terdiri dari lima bab. Dalam proses penulisan tugas akhir, terdapat beberapa tahapan yang ditempuh untuk menyelesaikan permasalahan yang ada. Rincian masing-masing bab adalah sebagai berikut,

Bab I Pendahuluan

Pada bab ini membahas latar belakang, identifikasi masalah, rumusan masalah, tujuan dan manfaat, batasan masalah dan sistematika penulisan.

Bab II Tinjauan Pustaka

Pada bab ini berisi tinjauan pustaka, mengurai materi yang mendukung judul, dan terdapat enam rangkuman penelitian terdahulu.

Bab III Metodologi Penelitian

Pada bab ini membahas tentang gambaran umum objek penelitian, penguraian kerangka penelitian, penguraian cara kerja algoritma *Decision Tree* dalam mengklasifikasikan serangan DDoS, uraian metode pengumpulan data log sistem dari router Mikrotik, alur penelitian, penerapan algoritma *Decision Tree*, dan metode evaluasi yang digunakan.

Bab IV Hasil dan Pembahasan

Pada bab ini memaparkan hasil evaluasi performa algoritma *Decision Tree* dan hasil dari olah data log Mikrotik dengan output klasifikasi jaringan normal/serangan DDOS.

Bab V Kesimpulan dan Saran

Berisi kesimpulan dari hasil penelitian dan saran untuk pengembangan keamanan jaringan serta penelitian lanjutan.