

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam dekade terakhir perkembangan internet dan teknologi informasi berkembang dengan pesat. Pesatnya perkembangan internet dan teknologi informasi membawa kemudahan bagi umat manusia dalam bertukar informasi secara cepat, tepat, dan efisien [1]. Sayangnya perkembangan teknologi informasi yang pesat juga membuka peluang bagi kriminal *hacker* untuk mengeksploitasi teknologi ini [2]. Dalam melakukan aksi eksploitasi ini, *hacker* biasanya menargetkan infrastruktur jaringan organisasi pemerintah maupun non-pemerintah yang menyebabkan kerugian dan kerusakan baik dari segi finansial, data pribadi, dan psikologi. Hal ini memicu meningkatnya kewaspadaan akan ancaman keamanan siber [2].

Minat dan perkembangan dalam teknologi internet dan komunikasi telah menyebabkan keamanan jaringan menjadi bidang penelitian yang sangat penting. Untuk memastikan keamanan jaringan dan semua aset yang terhubung dalam ruang siber, diimplementasikan alat-alat seperti *firewall*, *antivirus*, dan sistem pendeteksi intrusi atau IDS [3]. Salah satu *tools* untuk keamanan jaringan komputer, *network intrusion detection system* (NIDS) adalah mekanisme deteksi serangan yang berfungsi mengawasi terus-menerus lalu lintas jaringan untuk menemukan aktifitas jaringan yang mencurigakan dan berpotensi berbahaya [4][5]. IDS dapat diklasifikasikan menjadi dua kategori: *signature-based* IDS (SIDS) dan *anomaly-based* IDS (AIDS) [3].

Pada dekade terakhir perkembangan dan penggunaan *machine learning* juga ikut ambil dalam perkembangan IDS (*intrusion detection system*) dan *cybersecurity* pada umumnya [6]. *Machine learning* semakin penting dalam hal perkembangan *cybersecurity*. Tujuan utama menerapkan *machine learning* dalam *cybersecurity* adalah untuk membuat proses deteksi malware lebih bisa ditindaklanjuti, terukur

dan efektif daripada pendekatan tradisional, yang membutuhkan campur tangan manusia [7].

Institut Sains dan Bisnis Atma Luhur (ISB Atma Luhur) merupakan salah satu perguruan tinggi yang menjalankan pendidikan tinggi dibidang IT dan bisnis digital di Provinsi Kepulauan Bangka Belitung, memiliki sarana dan prasaran seperti jaringan *Wi-Fi* yang tersebar di lingkungan kampus untuk menunjang proses ajar mengajar baik mahasiswa maupun dosen. Terdapat 2 jenis jaringan komputer yang ada di ISB Atma Luhur, yaitu jaringan *private* kampus ISB Atma Luhur dan jaringan *wifi.id* dimana *access point* nya tersebar di 13 titik di lingkungan ISB Atma Luhur. Layanan internet gratis dari *wifi.id* ini merupakan jaringan internet yang disediakan oleh PT. Telkom Indonesia. Jaringan *wifi.id* ini bersifat publik dan tidak memiliki keamanan *password* sehingga siapapun dapat mengakses jaringan ini. Masalah keamanan jaringan pun timbul mengingat siapapun dapat mengakses jaringan ini sehingga berpotensi terdapat pihak yang tidak bertanggung jawab mencoba melakukan aksi eksploit seperti *reconnaissance* atau *packet sniffing*.

Maka dari itu penulis mengusulkan penelitian yang berjudul “**Penerapan *ML-Based Intrusion Detection System* Untuk Deteksi Serangan Terhadap Keamanan Jaringan di Lingkungan ISB Atma Luhur**”. Pada penelitian ini *machine learning model* yang dibuat menggunakan algoritma klasifikasi *Decision Tree*. Tujuan dari penelitian ini ialah untuk mengembangkan model *machine learning* yang diharapkan mampu mengklasifikasi trafik jaringan normal dan trafik jaringan yang bersifat intrusi. Proses pembelajaran dan uji model *machine learning* akan dilakukan pada *Google Colab* menggunakan *dataset* NSL-KDD dan hasil *capture log* jaringan yang diambil dari jaringan *wi-fi* publik WIFI.ID yang ada di ISB Atma Luhur.

1.2 Rumusan Masalah

Berdasarkan pemaparan latar belakang yang telah dibahas sebelumnya, maka timbul rumusan masalah yang ingin dipecahkan dalam penelitian ini. Rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana model *ML-Based IDS* ini mampu mengklasifikasi trafik jaringan normal dan trafik jaringan berpotensi serangan menggunakan algoritma *decision tree* ?
2. Bagaimana evaluasi performa dan akurasi dari model *ML-Based IDS machine learning* menggunakan algoritma *decision tree* ?

1.3 Batasan Masalah

Batasan masalah ditentukan untuk membantu menentukan ruang lingkup percobaan yang akan dilakukan serta keterbatasan penelitian atau batasan-batasan tertentu yang ada dalam penelitian. Berdasarkan cakupan dan kebutuhan yang terbatas, maka batasan-batasan dalam penelitian ini ialah sebagai berikut:

1. Pada penelitian ini dilakukan pengembangan model *ML-Based IDS* menggunakan klasifikasi *decision tree*,
2. Pengembangan model *ML-Based IDS* dilakukan pada *Google Colab* menggunakan bahasa pemrograman *Python*,
3. *Dataset* yang digunakan untuk proses *training* dan *testing* model *machine learning* adalah *dataset* NSL-KDD serta uji deteksi menggunakan data yang diambil dari hasil *capture log* jaringan *wi-fi* publik WIFI.ID yang ada di ISB Atma Luhur,
4. Evaluasi performa model *machine learning* yang diukur berupa nilai *accuracy*, nilai *precesion*, dan nilai *recall*.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Berdasarkan latar belakang masalah yang telah dipaparkan maka tujuan yang ingin dicapai dalam penelitian ini ialah sebagai berikut:

1. Mengembangkan model *machine learning* yang mampu mendeteksi intrusi pada jaringan menggunakan klasifikasi *decision tree*.
2. Penerapan model *ML-Based IDS* untuk mendeteksi serangan pada jaringan menggunakan data uji yang ditangkap dari jaringan *wi-fi* publik *wifi.id* yang ada di ISB Atma Luhur.

3. Mengukur hasil kinerja performa, akurasi, dan *recall* dari model *ML-Based IDS* yang telah dibangun.

1.4.2 Manfaat Penelitian

Manfaat yang diharapkan dari hasil penelitian *ML-Based IDS* ini ialah diharapkan menghasilkan model *machine learning ML-Based IDS* yang mampu mendeteksi intrusi yang terjadi pada jaringan internet atau jaringan lokal komputer.

1.5 Sistematika Penulisan

Pada penulisan dan penyusunan laporan skripsi ini digunakan sistematika penulisan yang terstruktur secara sistematis sehingga keseluruhan isi laporan dapat mudah dipahami. Sistematika penulisan laporan skripsi ini terdiri dari 5 bagian yaitu sebagai berikut:

BAB I PENDAHULUAN

Pada Bab I Pendahuluan memaparkan tentang latar belakang permasalahan yang diambil, rumusan masalah yang hendak dipecahkan, tujuan dan manfaat yang diharapkan dari penelitian ini, batasan-batasan masalah yang telah ditentukan, dan sistematika penulisan laporan.

BAB 2 LANDASAN TEORI

Pada Bab 2 Landasan Teori memaparkan pembahasan mengenai konsep dasar teori yang terkait dengan topik penelitian yang dilakukan. Dengan memaparkan landasan teori, penelitian ini akan dapat memanfaatkan pengetahuan dan teori-teori yang sudah teruji sebelumnya.

BAB 3 METODOLOGI PENELITIAN

Pada Bab 3 Metodologi Penelitian ini akan dibahas mengenai metodologi atau pendekatan yang digunakan secara terstruktur untuk mencapai tujuan penelitian ini dari awal hingga akhir penelitian.

BAB 4 PEMBAHASAN

Pada Bab 4 Pembahasan akan menguraikan secara mendetail tentang sistem yang sedang dikembangkan, perancangan algoritma, serta hasil implementasi algoritma pada model yang telah dibuat berdasarkan data yang telah dikumpulkan sebelumnya.

BAB V PENUTUP

Pada Bab V Penutup dipaparkan isi hasil kesimpulan secara keseluruhan dari penelitian yang telah dilakukan serta saran-saran yang dapat dilakukan untuk pengembangan penelitian terkait kedepannya.

