BAB I
PENDAHULUAN

1.1 Latar Belakang

Pertumbuhan dan perkembangan jaringan internet telah mengubah kehidupan manusia dalam banyak hal. Pada saat ini, setiap orang dapat terhubung dengan satu sama lain dari mana saja. Begitu pun dengan informasi yang dapat diakses dengan mudah. Namun, seiring dengan semakin meningkatnya perkembangan jaringan tersebut, isu – isu yang berkaitan dengan keamanan jaringan juga semakin beragam. Berdasarkan data (America & Asia, 2020), diketahui bahwa serangan terhadap jaringan mengalami peningkatan dalam lima tahun terakhir. Beberapa serangan tersebut ialah serangan *ransomware*, *malware*, *Denial of Service* (DoS) dan ancaman serangan lain yang semakin berkembang.

Keamanan jaringan menjadi lebih penting dalam pengimplementasian jaringan komputer, terutama pada jaringan yang menjalankan layanan penting atau menyimpan data yang memiliki nilai tinggi. Semakin berkembangnya serangan jaringan yang ada menuntut penelitan mendalam dari berbagai organisasi atau ilmuwan yang berfokus pada pengembangan jaringan. Oleh karena itu, upaya atau langkah-langkah pencegahan diperlukan guna menjaga keamanan jaringan dan memaksimalkan kualitas layanan keamanan jaringan yang disediakan.

Dalam memaksimalkan kualitas layanan keamanan jaringan, dilakukan proses pengumpulan data trafik dan pemantauan data trafik jaringan untuk mendeteksi aktivitas yang terjadi selama koneksi berlangsung (Anggraeni & Andriani, 2021). Pemantauan data trafik jaringan berfungsi untuk mengenali kegiatan yang terjadi selama koneksi berlangsung dan mendeteksi kemungkinan adanya serangan yang dapat mengakibatkan gangguan.

Untuk mendeteksi aktivitas yang terjadi di dalam suatu jaringan, maka diperlukan *Intrusion Detection System* (IDS). *Intrusion Detection System* (IDS) berfungsi mengidentifikasi peristiwa yang terjadi di komputer atau jaringan, serta menganalisanya untuk menentukan apakah peristiwa tersebut bersifat mengganggu atau bersifat normal.

Dalam mendeteksi serangan pada jaringan, IDS membutuhkan metode atau algoritma yang dapat mengenali serangan atau anomali dalam lalu lintas jaringan. Algoritma tersebut berperan dalam mengklasifikasikan antara trafik jaringan yang berbahaya dan trafik jaringan yang normal. Penelitian ini memanfaatkan metode data mining khususnya klasifikasi, yang merupakan proses ekstraksi dan identifikasi informasi dari dataset yang sangat besar. Algoritma yang digunakan dalam proses klasifikasi ini ialah *Decision Tree* C4.5.

Pada penelitian yang dilakukan oleh (Wiyanti, 2019) dalam mendeteksi intrusi jaringan yang ada pada Laboratorium Matematika Universitas Negeri Semarang. Penelitian ini menggunakan algoritma C4.5 yang kemudian diterapkan pada sistem analisa data testing dan memberikan hasil dengan nilai *performance* dan *precision* sebesar 99.09% dengan positif adanya indikasi penyusupan adalah *false.*

Kemudian (Malang & Tree, 2020) melakukan penelitian dengan melakukan deteksi dan mitigasi terhadap serangan DDoS yang ada pada *Software Defined Network* menggunakan algoritma *Decision Tree*. Penelitian ini dilakukan dengan membangun sistem deteksi dan mitigasi serangan DdoS menggunakan algoritma *Decision Tree* yang dibuktikan dengan memberikan skenario pengujian dan memberikan hasil bahwa simulasi serangan dan pengujian yang dibangun dengan model pendeteksian yang ada menunjukkan akurasi sebesar 99,95%.

Penelitian lain dilakukan oleh (Pramana et al., 2021) terkait identifikasi serangan *Denial of Service* (DoS) yang ada pada jaringan dengan menggunakan algoritma C4.5 dan menunjukkan hasil bahwa algoritma C4.5 mampu memberikan ketelitian dan ketepatan yang sangat baik dalam membangun model prediktif dataset NSL – KDD, namun membutuhkan waktu komputasi yang cukup lama.

Di sisi lain, jaringan WiFi di Jurusan Teknik Informatika Universitas Malikussaleh merupakan representasi dari lingkungan jaringan yang kompleks dan seringkali menjadi target serangan jaringan. Melakukan klasifikasi terhadap lalu lintas jaringan WiFi ini penting untuk mendeteksi dan mencegah serangan jaringan yang berpotensi mengganggu operasional dan integritas data.

Keberadaan jaringan WiFi yang luas dan kompleks di Jurusan Teknik Informatika membuatnya menjadi objek yang menarik untuk diteliti. Penelitian ini

dapat memberikan wawasan mendalam mengenai potensi risiko keamanan yang mungkin terjadi dan solusi pencegahannya. Dengan demikian, penelitian ini diharapkan dapat meningkatkan kesadaran dan kewaspadaan terhadap keamanan jaringan WiFi di jurusan ini, serta memberikan rekomendasi strategis dalam memperkuat keamanan jaringan.

Berdasarkan latar belakang diatas, maka pada penelitian ini akan dilakukan proses monitoring jaringan untuk mengetahui penggunaan internet melalui data jaringan yang terjadi di prodi Teknik Informatika Universitas Malikussaleh. Yang kemudian akan dilakukan klasifikasi terhadap serangan yang ada pada data yang diujikan dengan menggunakan algoritma *Decision Tree* C4.5, sehingga penulis tertarik untuk mengangkatnya sebagai Tugas Akhir dengan judul **"Implementasi Algoritma *Decision Tree* C4.5 Untuk Klasifikasi Deteksi Serangan Pada Protokol Jaringan"**

1.2 Rumusan Masalah

Dalam konteks ini, rumusan masalah penelitian ini adalah :

1. Bagaimana proses pengimplemetasian algoritma *Decision Tree* C4.5 untuk klasifikasi deteksi serangan pada protokol jaringan?
2. Sejauh mana keefektifan algoritma *Decision Tree* C4.5 dalam mendeteksi serangan pada protokol jaringan dapat diukur?

1.3 Batasan Masalah

Dalam mengembangkan skripsi ini, penelitian akan dibatasi pada beberapa aspek tertentu untuk menjaga fokus dan keterukuran hasil. Adapun batasan masalah yang menjadi cakupan penelitian ini adalah:

1. Penelitian ini akan dilakukan pada Ruang Gedung Teknik Informatika Universitas Malikussaleh.
2. Fokus penelitian akan terbatas pada deteksi serangan yang umum terjadi pada protokol jaringan seperti *Distributed Denial of Service* (DDoS) berbasis ICMP *Flood* , *Port Scan* dan *Brute Force.*
3. Penelitian ini hanya akan menggunakan algoritma *Decision Tree* C4.5 sebagai

metode klasifikasi untuk mendeteksi serangan pada protokol jaringan.

4. Atribut yang digunakan pada penelitian ini ialah *source, length, protocol,* dan *destination.*
5. Output dari penelitian ini ialah sistem klasifikasi *Decision Tree* C4.5 yang menampilkan hasil klasifikasi dan pohon keputusan yang di *embed* melalui WEKA.

1.4 Tujuan Penelitian

Berikut merupakan tujuan dari perancangan penelitian yang berdasarkan uraian masalah di atas:

1. Mengimplementasikan algoritma *Decision Tree* C4.5 untuk klasifikasi deteksi serangan pada protokol jaringan.
2. Mengevaluasi kinerja model *Decision Tree* C4.5 dalam mendeteksi serangan pada protokol jaringan.

1.5 Manfaat Penelitian

Manfaat yang akan di dapatkan dari penelitian ini antara lain :

1. Menambah pengetahuan dan wawasan mengenai pengklasifikasian deteksi serangan jaringan yang ada pada protokol jaringan serta dapat digunakan sebagai panduan untuk langkah selanjutnya dalam mengimplementasikan algoritma *Decision Tree* C4.5 untuk deteksi serangan yang ada.
2. Mengetahui tingkat efisiensi deteksi serangan jaringan yang ada pada protokol jaringan dengan menggunakan algoritma *Decision Tree* C4.5.