BAB I
PENDAHULUAN

1.1 Latar Belakang

Kejahatan siber atau *cyber crime* merupakan suatu dampak negatif dari perkembangan internet. Hal tersebut terjadi karena kejahatan siber menggunakan internet dalam tindak kejahatannya (Rahmawati, 2017). Akibat dari banyaknya jumlah pengguna internet, menyebabkan kejahatan siber tidak dapat dicegah atau bahkan dihentikan. Maka dari itu, hampir setiap tahunnya dibeberapa negara, seperti China, Jepang, UK, USA, dan Indonesia selalu mengalami kejahatan siber. Salah satu jenis kejahatan siber adalah serangan siber atau *cyber attack*. Serangan siber adalah kejahatan di dunia maya yang menargetkan sistem informasi komputer, infrastruktur, jaringan komputer, serta sistem keamanan komputer. Serangan tersebut bertujuan untuk mengganggu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersedian informasi (*availability*) (Subagyo, 2018). Salah satu serangan yang sering terjadi dan menjadi tren saat ini adalah dengan memanfatkan celah kemanan pada jaringan komputer. Oleh karena itu, sistem keamanan jaringan harus mampu mendeteksi adanya serangan agar data atau informasi tidak dapat diambil oleh pihak yang tidak bertanggung jawab. Salah satu sistem atau alat yang dapat mendeteksi adanya serangan adalah *Intrusion Detection System* (IDS).

Intrusion Detection System (IDS) dalam penerapannya akan mendeteksi intrusi-intrusi, pemindaian, penyerangan atau penyusupan dan berbagai ancaman pada lalu lintas jaringan. Dalam prosesnya terjadi pengklasifikasian aktivitas jaringan yang sedang berlangsung ke dalam model yang sudah dibangun sistem ke dalam *library*, sehingga bisa dikategorikan sebagai aktifitas normal atau serangan (Chakraborty, 2017). Ketika serangan terdeteksi maka IDS akan membuat *log* serangan yang terjadi. *Log* tersebut nantinya akan dianalisa oleh administrator keamanan jaringan menggunakan mekanisme pertahanan yang disebut *Security Event Management* (SEM). SEM berfungsi menyediakan informasi secara *real time* dari aplikasi, sistem *host*, dan semua jaringan serta perangkat keamanan, berupa *log* dan *alert*. Sehingga, setiap peristiwa keamanan yang dihasilkan di seluruh infrastruktur akan diperiksa, dibandingkan, dan segera diberitahukan (Carr, 2005).

Oleh karena itu, diperlukan metode di dalam *data mining* yang dapat mengetahui fitur-fitur apa saja yang berpengaruh pada pendeteksian serangan, sehingga administrator keamanan jaringan dapat lebih mudah dalam menganalisa SEM.

Salah satu metode yang dapat digunakan untuk mengetahui fitur-fitur apa saja yang berpengaruh dalam mendeteksi serangan adalah dengan menggunakan metode seleksi fitur. Seleksi fitur merupakan salah satu praproses dalam *data mining* yang berfungsi untuk menentukan fitur-fitur yang signifikan di dalam *dataset* yang sesuai untuk permasalahan yang akan diselesaikan (Mutaqien, 2016). Menurut Parimala dkk. (2017) implementasi seleksi fitur sangat berpengaruh karena dapat meningkatkan hasil akurasi dari 99.25% menjadi 99.6%.

Oleh karena itu, pada penelitian ini dilakukan proses data mining dengan menerapkan *ranking importance* untuk metode seleksi fitur serta algoritma klasifikasi *Decision Tree* untuk penghitungan akurasi.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan maka penulis menidentifikasi masalah sebaai berikut:

1. Apa saja fitur-fitur yang berpengaruh dalam mendeteksi serangan?
2. Bagaimana performa *Decision Tree* dalam melakukan klasifikasi serangan setelah dilakukan seleksi fitur?

1.3 Ruang Lingkup

Agar mendapatkan hasil yang optimal dalam penulisan ini, maka penulis membatasi ruang lingkup pembahasan sebagai berikut:

1. Algoritma yang digunakan untuk klasifikasi adalah *Decision Tree*.
2. Metode yang digunakan untuk seleksi fitur adalah *ranking importance*.
3. Data yang digunakan adalah data *log Intusion Detection System* (IDS).
4. Aplikasi *Intusion Detection System* (IDS) yang digunakan adalah Suricata.
5. Kelas yang digunakan dalam menentukan *ranking importance* adalah 10 kelas.

1.4 Tujuan Penelitian

Penelitian ini memiliki tujuan menerapkan *ranking importance* untuk menentukan fitur-fitur yang berpengaruh dalam mendeteksi serangan.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah untuk memudahkan administrator jaringan dalam menganalisa serangan dilihat dari fitur-fitur yang berpengaruh, guna meningkatkan keamanan jaringan.

1.6 Luaran yang Diharapkan

Luaran yang diharapkan dari penelitian ini adalah dapat mengetahui urutan terpenting dari suatu fitur sehingga dapat mengetahui fitur-fitur yang berpengaruh dalam mendeteksi suatu serangan.

1.7 Sistematika Penulisan

Untuk memberikan gambaran yang terperinci terhadap penelitian ini, maka sistematika penulisan ini dibagi menjadi 5 (lima) bab yang tiap nan memiliki sub bab. Berikut ini adalah sistematika penulisan dari penelitian ini:

BAB I PENDAHULUAN

Pada bab ini menjelaskan secara singkat dan jelas mengenai latar belakang permasalahan, rumusan masalah, ruang lingkup, tujuan penelitian, manfaat penelitian, luaran yang diharapkan, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini menjelaskan beberapa uraian teori-teori yang meliputi definisi konsep dan sumber studi yang relevan untuk dijadikan bahan acuan dalam penulisan dan pengembangan aplikasi.

BAB III METODOLOGI PENELITIAN

Pada bab ini menjelaskan beberapa metode penelitian yang digunakan oleh penulis dalam mengambil sumber data.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini menjelaskan implementasi sistem aplikasi dan hasil pengujian, serta dilakukan analisis terhadap hasil pengujian yang dilakukan dalam penelitian ini.

BAB V PENUTUP

Pada bab ini menjelaskan kesimpulan dan saran dari hasil dan pembahasan yang terdapat pada bab 4 (empat) yang sudah dilakukan yang dilakukan sebagai acuan agar sistem dapat lebih dikembangkan pada penelitian selanjutnya.

DAFTAR PUSTAKA