BAB I
PENDAHULUAN

1.1 Latar Belakang

Semakin tingginya ancaman serangan siber yang dihadapi oleh lembaga atau organisasi di seluruh dunia. *International Business Machines* (IBM) memperlihatkan bahwa selama pandemi Covid-19, serangan siber global naik sebesar 6.000% (Hendra Wicaksana et al., n.d.). Interpol menyebutkan bahwa lanskap kejahatan siber global selama pandemi Covid-19 didominasi oleh beberapa jenis serangan, yaitu *scam* dan *online phising*, *disruptive malware*, *data harvesting malware*, *malicious domain*, dan *misinformation* (Secretariat, 2020). Berbagai penyerangan ancaman siber yang maraknya sering terjadi dikarenakan adanya kecerobohan dan lemahnya sistem keamanan teknologi *online* sehingga menyebabkan dampak yang sangat buruk bagi pemilik akun bahkan *platform* yang terkait akan merasakan dampaknya pula (Sudarmadi & Runturambi, 2019). Berdasarkan publikasi *The Global Cybersecurity Index* (GCI) 2017 yang dirilis oleh *International Telecommunication Union* (ITU), kondisi keamanan siber Indonesia masih termasuk dalam negara dengan kategori keamanan siber yang lemah berada dalam tahap peningkatan optimal (*maturing stage*). Oleh karena itu pencegahan dan deteksi serangan siber menjadi sangat penting dalam menjaga keamanan jaringan dan sistem informasi.

Dinas Komunikasi dan Informatika Kota Palembang sebagai salah satu lembaga pemerintah yang memiliki jaringan komputer dan sistem keamanan informasi yang kompleks sehingga sangat rentan untuk menjadi target serangan siber. Dinas Komunikasi dan Informatika Kota Palembang perlu mengambil tindakan untuk meningkatkan keamanan dan mencegah serangan siber yang dapat mengancam keberlangsungan operasionalnya. Salah satu cara untuk mengatasi hal ini adalah dengan menggunakan teknologi prediksi serangan siber yang dapat memberikan peringatan dini dan membantu dalam mengambil tindakan pencegahan atau *response* terhadap serangan yang terdeteksi.

Algoritma klasifikasi *Random Forest* dapat menjadi solusi untuk memprediksi serangan siber pada periode yang akan datang. Khariwal & Arora mengusulkan deteksi *malware* pada *android* berdasarkan *permission* dengan menggunakan beberapa algoritma *machine learning* seperti SVM, *naive bayes* dan *random forest*. Hasil yang didapat *random forest* memiliki akurasi paling tinggi dalam deteksi malware android berdasarkan *permission* (Yang et al., 2013). Pada studi kasus klasifikasi debitur berdasarkan kualitas kredit menyatakan bahwa klasifikasi *Random Forest* merupakan metode klasifikasi yang memiliki tingkat akurasi paling tinggi untuk klasifikasi kualitas kredit yaitu mencapai 98,16% disusul Naïve Bayes 95,93% (Ignasius et al., n.d.).

Penelitian ini dilakukan dengan tujuan untuk mengimplementasikan algoritma klasifikasi *Random Forest* pada platform RapidMiner untuk memprediksi kategori serangan siber pada Dinas Komunikasi dan Informatika Kota Palembang. Dengan memanfaatkan teknologi prediksi tersebut, diharapkan dapat memberikan

hasil akurasi yang tinggi terhadap jenis serangan yang terjadi sehingga akan memungkinkan pihak yang bertanggung jawab untuk segera mengambil tindakan pencegahan atau response terhadap serangan siber yang terdeteksi.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas, maka penulis dapat menarik kesimpulan bahwa yang menjadi permasalahan adalah sebagai berikut :

1. Bagaimana menerapkan algoritma *Random Forest* dalam memprediksi kategori serangan siber pada *platform RapidMiner*?
2. Bagaimana mendapatkan hasil akurasi yang baik dalam memprediksi kategori serangan siber pada *platform RapidMiner* dengan algoritma *Random Forest*?

1.3 Batasan Masalah

Adapun batasan masalah dari memprediksi kategori serangan siber ini difokuskan pada pencatatan yang berhubungan dengan :

1. Kategori serangan siber.
2. Penerapan Algoritma Klasifikasi *Random Forest*.

1.4 Tujuan Penelitian

Tujuan Penelitian ini adalah :

1. Menerapkan algoritma klasifikasi *Random Forest* pada *platform RapidMiner* untuk memprediksi kategori serangan siber pada *firewall* di Dinas Komunikasi dan Informatika Kota Palembang.
2. Mendapatkan hasil akurasi yang baik dalam memprediksi kategori serangan siber pada *platform RapidMiner* dengan algoritma *Random Forest*.

1.5 Manfaat Penelitian

Dengan dilakukannya penelitian ini diharapkan bisa memberikan manfaat seperti berikut :

1. Dengan menggunakan algoritma klasifikasi *Random Forest*, dapat dilakukan prediksi serangan siber dengan akurasi tinggi sehingga akan memungkinkan pihak yang bertanggung jawab untuk segera mengambil tindakan pencegahan atau *response* terhadap serangan siber yang terdeteksi.
2. Dengan adanya sistem prediksi serangan siber yang efektif, maka dapat mengurangi risiko kerugian yang mungkin terjadi akibat serangan siber seperti hilangnya data, kerusakan sistem, atau gangguan layanan.
3. Memberikan informasi yang mendukung teknis pencegahan dari *server* atau sistem yang menjadi *target* dan identitas dari asal serangan siber.
4. Menjadi referensi bagi lembaga atau organisasi lain yang ingin meningkatkan keamanan jaringan dan sistem informasi. Penelitian ini dapat

menjadi acuan untuk pengembangan sistem prediksi serangan siber pada lembaga atau organisasi lain yang membutuhkan.

5. Meningkatkan kemampuan penulis dalam mengimplementasikan algoritma klasifikasi *Random Forest* pada platform RapidMiner yang dapat berguna untuk penelitian-penelitian lainnya di masa depan.

1.6 Sistematika Penulisan

Agar pembahasan laporan penelitian ini dapat memberikan gambaran sesuai dengan tujuan maka penulisan laporan penelitian ini disusun dengan sistematika sebagai berikut:

BAB I PENDAHULUAN

Bab ini akan menguraikan latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat, lokasi pengumpulan data dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang konsep dasar serta teori-teori yang berkaitan dengan topik penelitian dari sumber pustaka dan referensi yang menjadi landasan dasar dalam perancangan, analisis kebutuhan serta implementasi dan pengujian sistem.

BAB III METODOLOGI PENELITIAN

Bab ini membahas tentang uraian rinci mengenai bahan/data yang akan digunakan sebagai kebutuhan *input* maupun *output*, membahas mengenai kebutuhan *software* dan *hardware*.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi langkah-langkah penelitian yang sudah dilakukan dan dilengkapi dengan pembahasan hasil akurasi dari penerapan Algoritma *Random Forest*.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan tentang keseluruhan dari analisa hasil akurasi serta saran terkait teknis pengamanan *server* atau sistem yang menjadi *target* dan juga identitas pelaku yang melakukan serangan siber pada instansi terkait.