BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Keamanan jaringan komputer sebagai elemen integral dalam suatu sistem informasi memiliki signifikansi yang besar dalam menjaga integritas, validitas data, dan memastikan ketersediaan layanan bagi penggunanya. Pentingnya melindungi sistem dari berbagai serangan *cyber* dan upaya tidak sah, termasuk penyusupan atau pemindaian oleh pihak yang tidak berwenang, menjadi fokus utama. Dalam konteks perlindungan data pribadi di Indonesia, merujuk pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Serta membahas kerangka hukum terkait dengan keamanan *cyber* di Indonesia, termasuk Peraturan Presiden Nomor 53 Tahun 2017 tentang Kebijakan Nasional Keamanan *Cyber*.

Banyak serangan *cyber* terhadap jaringan komputer seringkali baru terdeteksi setelah terjadi kejadian yang mencurigakan dalam jaringan. Administrator seringkali menghadapi tantangan untuk mengidentifikasi permasalahan secara tepat waktu, memerlukan waktu yang cukup lama untuk melakukan audit sistem guna menemukan potensi masalah yang muncul. Untuk mengatasi tantangan ini, diperlukan sistem yang dapat mendeteksi *intruder* atau aktivitas merugikan pada jaringan dengan lebih cepat, memungkinkan respon yang lebih proaktif (Saputro, A 2016).

Serangan *Distributed Denial of Service* (DDoS) telah menjadi ancaman signifikan dalam dunia siber, menyebabkan gangguan besar pada layanan jaringan dan kerugian finansial bagi banyak organisasi. Dengan semakin canggihnya teknik serangan, deteksi dini dan respons cepat terhadap serangan ini menjadi sangat penting. Pemilihan metode yang efektif untuk mendeteksi serangan DDoS adalah kunci untuk mengurangi dampak dan meminimalisir *downtime*. Salah satu pendekatan yang menjanjikan adalah penggunaan algoritma *Machine Learning*, seperti *Random Forest*, yang mampu menganalisis pola lalu lintas jaringan untuk mendeteksi anomali yang mengindikasikan serangan (Harto, M. K., & Basuki, A.

2021). Integrasi sistem deteksi ini dengan layanan pemberitahuan cepat, seperti *Telegram,* memungkinkan tim respons keamanan untuk segera mengambil tindakan mitigasi.

Telegram dirancang untuk memudahkan pengguna bertukar pesan teks, audio, video, gambar, dan stiker dengan keamanan tinggi melalui enkripsi berstandar internasional. Selain itu, Telegram mendukung pengiriman dokumen, musik, dan file zip hingga 1,5 GB, serta berbagi lokasi real-time dan kontak. Pengguna dapat mengakses akun dari beberapa perangkat sekaligus. *Group* chat di *Telegram* dapat menampung hingga 200 orang, dan dapat di-*upgrade* menjadi *Supergroup* dengan kapasitas 5000 orang, dengan *fitur* seperti *Replies*, *Mention*, *Hashtags*, dan *Forwards* yang membuat komunikasi lebih efektif (Shahrul, A., & Wibawa, A. P. 2021). Selain itu, kemampuan untuk membuat "*bot*" yang dapat otomatisasi tugas-tugas tertentu, termasuk pengiriman notifikasi keamanan, menjadikan *Telegram* sebagai alat yang efisien dalam sistem deteksi dan respon terhadap serangan DDoS.

Berbagai metode deteksi serangan DDoS telah diteliti dan diterapkan dalam keamanan jaringan. *Enhanced Evolving Clustering Method* menggunakan pendekatan clustering dinamis untuk mendeteksi anomali, dengan akurasi sekitar 85%. *Adaptive Neuro-Fuzzy Inference System* (ANFIS) menggabungkan jaringan saraf tiruan dan logika fuzzy untuk menangani variabilitas data, mencapai akurasi sekitar 88%. *PCA Neural Network* mengintegrasikan reduksi dimensi dengan klasifikasi, memungkinkan deteksi cepat dengan akurasi 87%. *Fuzzy Logic* memberikan fleksibilitas dalam pengambilan keputusan, dengan akurasi sekitar 82%. Sementara itu, berbagai algoritma *Machine Learning* seperti *K-Nearest Neighbors* (KNN), *Support Vector Machine* (SVM), dan *Decision Trees* menunjukkan performa yang bervariasi, masing-masing dengan akurasi antara 80% hingga 85%.

Dari berbagai metode tersebut, *Random Forest* menonjol dengan akurasi deteksi sekitar 90% dan waktu deteksi rata-rata 0,3 detik, menjadikannya pilihan yang efisien dan andal untuk mendeteksi serangan DDoS secara *real-time*. Menurut penelitian oleh Harto, M. K., & Basuki, A. (2021) dalam "Deteksi Serangan DDoS Menggunakan Algoritma *Random Forest*", algoritma ini tidak hanya menunjukkan tingkat akurasi yang lebih tinggi dibandingkan metode lain, tetapi juga

menunjukkan kecepatan deteksi yang superior, yang esensial dalam menghadapi serangan *cyber* yang cepat berkembang.

Penelitian ini bertujuan untuk mengoptimalkan keamanan jaringan dengan menerapkan model *Random Forest*. *Random Forest* merupakan algoritma *Machine Learning* yang efektif dalam mendeteksi aktivitas mencurigakan atau potensial serangan *cyber* pada server. Pendekatan ini memanfaatkan kemampuan *Random Forest* dalam menangani kompleksitas dan ketidakpastian dari lalu lintas jaringan dengan mempertimbangkan berbagai variabel yang bersifat ambigu dan kontinu secara efisien.

Namun, optimasi keamanan jaringan tidak hanya terbatas pada deteksi serangan. Respon yang cepat terhadap serangan juga menjadi kunci dalam menjaga keamanan jaringan. Oleh karena itu, penggunaan media pemberitahuan seperti *Telegram* untuk memberikan notifikasi secara cepat menjadi suatu kebutuhan. Pemberitahuan yang cepat memungkinkan administrator jaringan untuk segera merespon dan mengatasi serangan sebelum menyebabkan dampak yang lebih besar.

Berdasarkan latar belakang ini, penelitian diharapkan dapat memberikan kontribusi positif terhadap pengembangan sistem keamanan jaringan menciptakan keamanan jaringan yang aman dan terlindungi. Oleh karena itu, penelitian ini berfokus pada perancangan model deteksi serangan DDoS menggunakan algoritma *Random Forest*, dilengkapi dengan sistem pemberitahuan melalui *Telegram*, untuk meningkatkan keamanan jaringan sehingga peneliti memilih judul **"Perancangan Model Deteksi DDoS Menggunakan Algoritma Random Forest dengan Pemberitahuan Cepat Melalui Telegram"**.

1.2 Rumusan Masalah Penelitian

1. Bagaimana rancangan model deteksi *Distributed Denial of Service* (DDoS) menggunakan algoritma *Random Forest* dalam konteks keamanan jaringan?
2. Bagaimana performa model model deteksi *Distributed Denial of Service* (DDoS) menggunakan algoritma *Random Forest* dalam konteks keamanan jaringan?

3. Bagaimana integrasi pemberitahuan cepat melalui *platform Telegram* terhadap serangan *Distributed Denial of Service* (DDoS) yang terdeteksi?
4. Bagaimana performa integrasi pemberitahuan cepat melalui *platform Telegram* terhadap serangan *Distributed Denial of Service* (DDoS) yang terdeteksi?

1.3 Tujuan Penelitian

1. Untuk mengetahui rancangan model deteksi *Distributed Denial of Service* (DDoS) berbasis algoritma *Random Forest*
2. Untuk mengevaluasi dan menganalisis performa model deteksi *Distributed Denial of Service* (DDoS) menggunakan algoritma *Random Forest* dalam konteks keamanan jaringan.
3. Untuk menerapkan integrasi pemberitahuan cepat melalui platform Telegram terhadap serangan *Distributed Denial of Service* (DDoS) yang terdeteksi.
4. Untuk mengetahui performa pemberitahuan cepat melalui *Telegram* terhadap serangan *Distributed Denial of Service* (DDoS) yang terdeteksi.

1.4 Batasan Penelitian

1. Penelitian ini dibatasi pada serangan *Distributed Denial of Service* (DDoS) yang hanya berfokus pada jenis serangan volumetrik.
2. Batas Lingkup penelitian akan terbatas pada perancangan model *Random Forest* sebagai metode deteksi serangan *Distributed Denial of Service* (DDoS).
3. Penelitian ini hanya berfokus pada pengembangan model tanpa mengintegrasikannya ke dalam jaringan nyata.
4. Sistem pemberitahuan cepat akan dibatasi pada penggunaan *platform* komunikasi *Telegram*.
5. Penelitian ini hanya berfokus pada deteksi, tanpa melanjutkan ke tahap tindakan selanjutnya.

1.5 Manfaat Penelitian

Adapun manfaat yang ingin dicapai dari penelitian ini baik secara teoritis maupun praktis, sebagai berikut:

1.5.1 Manfaat Teoritis

Penelitian ini diharapkan memberikan kontribusi teoritis dengan mengembangkan model deteksi serangan yang lebih cerdas melalui integrasi algortima *Random Forest* dan pemberitahuan cepat melalui *Telegram*. Dengan mengeksplorasi dan memahami teori algortima *Random Forest* dalam konteks keamanan jaringan, penelitian ini membuka ruang bagi pengembangan teori respon cepat terhadap serangan, berpotensi menjadi dasar untuk teori-teori deteksi serangan terbaru dan kerangka kerja konseptual untuk optimasi keamanan jaringan.

1.5.2 Manfaat Praktis

1. Peningkatan Keefektifan Deteksi Serangan

   Sistem yang dihasilkan akan meningkatkan efektivitas dalam mendeteksi serangan jaringan, terutama yang kompleks, melalui integrasi algortima *Random Forest* dan pemberitahuan cepat melalui *Telegram*. Hal ini dapat mengurangi risiko serangan yang tidak terdeteksi dan memastikan respon yang tepat waktu.

2. *Respons* Cepat dan Efisien

   Implementasi pemberitahuan cepat melalui *Telegram* akan memberikan manfaat langsung dalam respons cepat dan efisien terhadap serangan. Administrator jaringan dapat segera mengambil tindakan preventif atau responsif, mengurangi potensi kerugian dan dampak serangan

3. Keamanan Jaringan yang Lebih Optimal

   Hasil penelitian ini diharapkan memberikan manfaat praktis dalam mencapai keamanan jaringan yang lebih optimal. Dengan adanya sistem yang lebih cerdas dan responsif dapat meningkatkan tingkat perlindungan terhadap serangan yang dapat merugikan.

1.6 Struktur Organisasi Skripsi

Struktur organisasi skripsi ini berfungsi sebagai panduan bagi penulis untuk menyusun skripsi dengan lebih teratur. Oleh karena itu, penulis menyusun struktur organisasi skripsi yang mencakup urutan penulisan dari Bab I hingga Bab terakhir sebagai berikut.

BAB I Pendahuluan, meliputi Latar Belakang Penelitian, Rumusan Masalah, Tujuan Penelitian, Manfaat Penelitian, dan Stuktur Organisasi Skripsi.

BAB II Kajian Pustaka, berisi teori-teori yang menjadi landasan dalam penyusunan skripsi ini sesuai dengan bidang yang dikaji, serta penelitian terdahulu yang relevan.

BAB III Metode Penelitian, berisi Metode Penelitian, Model *Machine Learning*, dan Metode Evaluasi.

BAB IV Temuan dan Pembahasan, membahas mengenai hasil yang diperoleh setelah melakukan penelitian yang berkaitan dengan masalah penelitian.

BAB V Simpulan, Implikasi, dan Rekomendasi, berisi penafsiran dan pemaknaan peneliti terhadap hasil analisis temuan penelitian.