BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era modern saat ini, teknologi informasi telah menjadi bagian penting dalam kehidupan sehari-hari, baik dalam bidang bisnis, pemerintahan, pendidikan, maupun layanan publik lainnya. Namun, seiring dengan meningkatnya penggunaan teknologi, ancaman terhadap keamanan cyber juga semakin berkembang. Serangan cyber merupakan upaya yang dilakukan untuk merusak, memanipulasi, atau mencuri informasi dari sistem komputer atau jaringan digital. Serangan ini dapat dilakukan melalui berbagai cara, mulai dari penyebaran virus komputer, malware, phishing, hingga serangan jaringan yang lebih kompleks [1]. Serangan tersebut tidak hanya menyerang individu, tetapi juga organisasi besar dan infrastruktur penting. Dampak dari serangan ini sangat merugikan, seperti kehilangan data, gangguan layanan, hingga kerugian finansial yang signifikan. Salah satu teknologi yang dapat digunakan untuk menghadapi ancaman ini adalah Machine Learning (ML). ML adalah cabang dari Artificial Intelligence (AI) yang memungkinkan sistem untuk belajar secara otomatis dari data, tanpa perlu diprogram ulang secara eksplisit. ML dikembangkan dengan landasan berbagai disiplin ilmu seperti statistika, matematika, dan data mining, sehingga mesin dapat menganalisis dan mempelajari data untuk mengambil keputusan secara mandiri [2].

Dengan kemajuan teknologi informasi dan internet, para pelaku serangan cyber kini dapat melakukan aksinya dengan lebih mudah, efisien, dan hemat biaya. Serangan ini terutama menargetkan industri dan instansi pemerintah yang menyimpan data penting sehingga menimbulkan kekhawatiran dan risiko kehilangan data pribadi maupun aset digital. Selain sebagai alat politik, serangan cyber juga digunakan dalam konteks ekonomi untuk mengganggu kestabilan pihak tertentu [3]. Dalam menghadapi tantangan tersebut, kemampuan machine learning untuk mempelajari data baru dan beradaptasi dengan perubahan situasi sangat bermanfaat. Teknologi ini memungkinkan deteksi dini terhadap serangan cyber, serta membantu organisasi dalam menganalisis dan mengurangi risiko serangan secara lebih efektif.

Penelitian ini menggunakan algoritma random forest, salah satu metode dalam machine learning yang termasuk dalam kelompok ensemble learning. Random forest merupakan gabungan dari beberapa decision tree (pohon keputusan), dimana hasil klasifikasi akhir ditentukan melalui proses voting mayoritas dari seluruh pohon yang terbentuk [4]. Berdasarkan masalah tersebut, maka penelitian ini penting dilakukan untuk menerapkan machine learning yang dapat menganalisis kejahatan cyber, khususnya menggunakan algoritma random forest sebagai upaya menghadapi peringatan serangan digital yang semakin meningkat.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, rumusan masalah dari penelitian ini adalah “Bagaimana menerapkan *machine learning* untuk

menganalisis kejahatan *cyber* di tengah serangan digital menggunakan algoritma *random forest*?".

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah menerapkan *machine learning* untuk menganalisis kejahatan *cyber* di tengah serangan digital menggunakan algoritma *random forest.*

1.4 Batasan Masalah

Batasan masalah dibuat agar memberikan pemahaman yang terarah dan sesuai dengan yang diharapkan. Agar pembahasan ini tidak menyimpang dari pokok perumusan masalah yang ada, maka dibuat batasan masalah yaitu:

1. Hanya berfokus terhadap serangan *cyber* yang bisa diketahui lewat membaca pola-pola jaringan yang dianggap tidak normal sehingga sistem membaca itu sebagai suatu anomaly dan tidak berfokus pada serangan lainnya.
2. Metode dan algoritma penelitian ini hanya sebatas analisis sehingga semua *output* yang dihasilkan merupakan *output* yang kompleks lewat perhitungan dan analisis sistem yang sudah dirancang.
3. Membutuhkan data serangan yang sudah pernah terjadi sebelumnya untuk dibuat sebagai awal pengenalan *machine learning* mendeteksi serangan *cyber*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut:

1. Peningkatan Keamanan *Cyber*

   Penelitian ini dapat membantu organisasi atau perusahaan untuk meningkatkan kemampuan mereka dalam mendeteksi dan merespons ancaman *cyber* secara lebih cepat dan efektif, sehingga mampu melindungi aset digital dari serangan yang merugikan.

2. Pengurangan Kerugian Finansial

   Dengan mampu menganalisis serangan *cyber* secara efektif, perusahaan dapat mengurangi risiko kerugian finansial yang sering kali terjadi akibat pencurian data, peretasan sistem, atau gangguan operasional.

3. Efisiensi Operasional

   Model *machine learning* yang diterapkan secara otomatis dapat mengurangi ketergantungan pada pemantauan manual oleh tim keamanan, sehingga meningkatkan efisiensi operasional dan alokasi sumber daya.

4. Kontribusi pada Pengembangan Teknologi Keamanan

   Kontribusi pada Pengembangan Teknologi Keamanan Penelitian ini dapat memberikan kontribusi pada pengembangan teknologi baru di bidang

keamanan *cyber*, khususnya dalam penggunaan *machine learning*, yang bisa dimanfaatkan oleh industri keamanan di masa depan.

5. Pengetahuan Akademis

   Hasil penelitian ini juga akan memperkaya pengetahuan akademis di bidang *machine learning* dan keamanan *cyber* memberikan wawasan bagi penelitian lebih lanjut tentang aplikasi teknologi ini dalam menghadapi ancaman *cyber* yang terus berkembang.

6. Perbaikan Sistem Deteksi

   Penelitian ini memungkinkan evaluasi dan pengembangan algoritma *machine learning* yang lebih baik untuk deteksi serangan, sehingga bisa menciptakan sistem deteksi yang lebih akurat dan responsif.

1.6 Sistematika Penulisan

Sistematika penulisan digunakan untuk menggambarkan alur penulisan tugas akhir ini agar lebih mudah dipahami. Sistematika penulisan tugas akhir adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian dan juga sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang *state of the art* perbandingan penelitian terdahulu dengan penelitian yang akan dilakukan, landasan teori.

BAB III ANALISIS DAN PERANCANGAN

Bab ini berisi tentnag analisis dan perancangan sistem, peran pengguna serta perangkat pendukung.

BAB IV IMPLEMENTASI SISTEM

Bab ini berisikan metode yang digunakan dalam penelitian juga terdapat analisis dan peran sistem, peran pengguna dan perangkat pendukung serta perancangan sistem.

BAB V PENGUJIAN DAN ANALISIS HASIL

Bab ini membahas tentang pengujian sistem, analisis serta hasil dari sistem yang telah di bangun.

BAB VI PENUTUP

Bab ini berisikan kesimpulan yang diperoleh dari hasil pengembangan sistem serta saran terhadap sistem untuk perkembangan selanjutnya.