BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring dengan bertambahnya pengguna internet, semakin bertambah pula lalu lintas internet. Banyaknya pengguna internet membuat penyedia layanan seperti *website, email,* dan *cloud* perlu melayani jutaan pengguna tiap detiknya. Bersamaan dengan itu tingkat ancaman pada jaringan maupun *server* semakin tinggi [1].

Ancaman pada jaringan komputer dapat disebut dengan *Cyber-Attack* dimana Waxman mendefinisikannya sebagai semua aktifitas yang tidak sah atau tidak diinginkan yang bertujuan untuk mengganggu, mengubah, atau menyerang rahasia seseorang atau mencuri data penting secara diam-diam atau terang-terangan [2].

Mendeteksi *Cyber-Attack* ini menjadi masalah penting pada jaringan komputer. Teknik serangan yang digunakan pun semakin beragam membuat sistem pendeteksian yang telah dibuat sebelumnya kurang efektif. Karenanya dibuat algoritma yang dapat membantu sistem pendeteksian ini dapat mendeteksi serangan lebih efektif dari sebelumnya.

Telah dilakukan riset untuk menggunakan algoritma pada sistem pendeteksi intrusi seperti algoritma: *Decision Tree*[5], *Pattern Matching Algoritm*[3], dan *Naïve Bayes[4]*.

Peneliti pada bidang ini seperti: Vibha Gupta, telah membandingkan algorima-algoritma *Pattern Matching* mana yang paling efektif untuk digunkan sebagai *classifier* deteksi serangan[3]. Ketan Sanjay Desale, telah meneliti perbandingan algoritma *Naïve Bayes, Hoeffding Tree, Accuracy Updated Ensemble,* dan *Accuracy Weighted Ensemble*. Dan didapatkan *Naïve Bayes* dan *Hoeffding Tree* memiliki akurasi dan kecepatan yang lebih tinggi ketimbang *Accuracy Updated Ensmble,* dan *Accuracy Weighted Ensemble*[4].

Pada Tugas Akhir ini, dibentuk sebuah simulasi pendeteksian intrusi yang menggunakan klasifier *Decision Tree, Random Forest,* dan juga *AdaBoost* untuk mendapatkan klasifier mana yang lebih efisien untuk melakukan pendeteksian serangan.

1.2 Tujuan dan Manfaat

1.2.1 Tujuan

Dari latar belakang tersebut, disimpulkan bahwa tujuan dari penelitian tugas akhir ini adalah:

1. Mendapatkan klasifier yang paling efisien untuk mendeteksi serangan.
2. Meningkatkan keamanan didalam jaringan.
3. Menganalisis kinerja dari klasifier yang digunakan.

1.2.2 Manfaat

Diharapkan dari penelitian ini dapat membantu dalam meningkatkan efisiensi waktu dan meningkatkan akurasi pada pendeteksian serangan.

1.3 Rumusan Masalah

1. Klasifier apa yang efektif untuk mendeteksi serangan didalam jaringan?
2. Apa saja yang dapat mempengaruhi kinerja klasifier?
3. Bagaimana menilai performa dari algoritma tersebut?

1.4 Asumsi dan Batasan Masalah

Asumsi dan batasan masalah dibutuhkan agar penetilitan ini tetap fokus pada tujuannya dan tidak membahas masalah diluar dari tujuan utama. Berikut asumsi serta batasan masalah:

1.4.1 Asumsi

1. Klasifier yang efektif adalah *Decision Tree, Random Forest,* dan *AdaBoost.*
2. Kinerja algoritma dipengaruhi oleh beban data yang diberikan pada algoritma tersebut.
3. Penilaian performa dapat dilihat dari akurasi yang diberikan oleh klasifier tersebut.
4. Jumlah fitur yang digunakan berpengaruh terhadap performa klasifier.

1.4.2 Batasan Masalah

1. Klasifier yang digunakan adalah *Decision Tree, Random Forest,* dan *AdaBoost.*
2. Efektivitas dilihat dari waktu yang dibutuhkan algoritma untuk melatih dan menuji dataset yang ada, dan juga akurasi yang didapatkan.
3. Dataset yang digunakan adalah KDDCUP99.
4. Dilakukan dalam simulasi pendeteksian.

1.5 Metode Penelitian

Metode penelitian yang akan diterapkan pada sistem ini sebagai berikut:

1. Studi Literatur

   Studi literatur ini dilakukan untuk mempelajari dan memahami konsep dan teori yang berkaitan dengan algoritma yang akan digunakan, serta simulasi yang akan dilakukan.

2. Perancangan Simulasi

   Perancangan simulasi ini dilakukan dengan cara membuat simulasi pendeteksian menggunakan python didalam laptop.

3. Pengujian dan evaluasi

   Pengujian dan evaluasi akan dilakukan dengan pemantauan pada waktu yang diperlukan algoritma untuk melatih dan menguji, dan juga akurasi yang didapatkan.

4. Penyusunan laporan

   Pada penyusunan laporan akan dijelaskan hasil dari pengujian dan evaluasi dari simulasi yang dibuat.

1.6 Jadwal Pelaksanaan

TABEL 1-1 JADWAL PELAKSANAAN

No	Deskripsi Tahapan	Durasi	Tanggal Selesai	*Milestone*
1	Melakukan studi litelatur	1 minggu	22-Aug-20	Diagram Blok dan spesifikasi *Input-Output*
2	Perancangan	3 minggu	05-Sep-20	List komponen yang akan digunakan
3	Pemograman dan konfigurasi	4 minggu	04-Okt-20	Simulasi deteksi dapat dioperasikan
4	Pengujian dan evaluasi	4 minggu	04-Nov-20	Hasil dari simulasi deteksi yang telah diproses
5	Penyusunan laporan/buku TA	2 minggu	13-Des-20	Buku TA selesai