Bab I

Pendahuluan

1.1 Latar Belakang

Dengan pesatnya perkembangan internet, malware telah menjadi salah satu ancaman utama di dunia cyber saat ini. Malware dapat berupa perangkat lunak berbahaya, pencurian data dan informasi, serta spionase. Menurut definisi Kaspersky Labs (2017), malware adalah program komputer yang dirancang untuk menginfeksi komputer pengguna dan menimbulkan kerusakan di dalamnya dengan berbagai cara.

Perlindungan dari malware pada sistem komputer adalah tugas keamanan cyber yang penting bagi pengguna karena satu serangan saja dapat mengakibatkan kerusakan yang cukup besar. Saat ini, metode populer dalam mendeteksi malware menggunakan teknik klasifikasi statis dan dinamis yang berdasarkan algoritma yang mempelajari signature based dari malware, seperti yang dijelaskan oleh Chumachenko (2017).

Namun, terdapat banyak pro dan kontra mengenai metode statis dan dinamis. Kelebihan teknik analisis statik adalah malware tidak dijalankan, sehingga mengurangi risiko terinfeksi malware. Meskipun begitu, metode ini memiliki keterbatasan, seperti tidak dapat mendeteksi jenis malware baru. Saat ini, penulis malware sering menggunakan teknik yang membuat proses analisis malware statik semakin sulit, seperti menggunakan packer untuk melakukan modifikasi kode secara otomatis. Di sisi lain, analisis dinamis lebih efisien dan tidak memerlukan executable untuk dibongkar atau didekripsi. Namun, metode ini memakan waktu dan sumber daya yang banyak, seperti yang dijelaskan oleh Nataraj, Karthikeyan, Jacob and Manjunath (2011).

Penelitian lainnya, seperti yang dilakukan oleh Oh, Go and Lee (2017), menggunakan deteksi malware berbasis signature-based dengan mengidentifikasi ciri-ciri malware yang berada di database. Namun, metode ini tidak sepenuhnya optimal ketika terjadi serangan zero-day, dan banyak malware yang tidak terdeteksi.

Pada tahun Vyas, Luo, McFarland and Justice (2017). melakukan penelitian dengan menginvestigasi fitur statis untuk mengusulkan sistem deteksi malware jaringan waktu nyata. Fitur-fitur tersebut diekstraksi dari header

dan bagian file PE dan dikelompokkan menjadi empat kategori: metadata file, file pengepakan, DLL yang diimpor, dan fungsi yang diimpor. Fitur-fitur ini kemudian digunakan untuk melatih beberapa mesin pengklasifikasi pembelajaran.

Penelitian lainnya, seperti yang dilakukan oleh Rezaei, Manavi and Hamzeh (2021) menggunakan teknik deteksi malware berbasis Pe-Probe (Pe file) yang berdasarkan 9 fitur dari pe header dengan tingkat akurasi 95,5% menggunakan Random Forest.

Dari permasalahan itu, penelitian ini berfokus pada pengembangan deteksi dan klasifikasi akurasi malware berbasis feature-feature yang terdapat dalam pe-probe (pe file), dengan membuat sebuah prototype untuk deteksi malware dengan menggunakan machine learning untuk mendeteksi dan mengklasifikasikan akurasi dari PE-Probe (pe file). Diharapkan penelitian ini dapat menjadi metode optimal dalam mendeteksi malware.

1.2 Latar belakang di atas, rumusan masalah tugas akhir ini adalah sebagai berikut:

1. Bagaimana cara algoritma machine learning dapat mengklasifikasikan malware ?

2. Bagaimana cara mengembangkan *prototype* untuk mendeteksi dan kalsifikasi malware berdasarkan studi algoritma klasifikasi yang telah dilakukan?

3. Bagaimana cara algoritma machine learning dapat mendeteksi malware berdasarkan fitur fitur pe-probe?

1.3 Tujuan

1. Melakukan studi algoritma untuk meningkatkan akurasi klasifikasi malware.

2. Melakukan analisis dan membuat pengembangan deteksi malware menggunakan machine learning berbasis *PE-Probe(Pe-File.*

3. membuat validasi deteksi malware pada prototype

1.4 Batasan Masalah

Berikut adalah ruang lingkup yang ada pada penulisan tugas akhir ini :

1. Sistem yang dibuat hanya untuk membandingkan machine learning yang terbaik untuk mendeteksi malware yang terdapat dalam pe-probe.

2. Klasifikasi dan deteksi malware hanya berbasis dataset yang sudah dipelajari oleh machine learning.

3. Pengujian deteksi malware hanya bisa menggunakan jenis file berbentuk .exe, dll.

4. sistem yang dibuat tidak untuk mendeteksi jenis family malware

1.5 Hipotesis

1. Algoritma deteksi malware menghasilkan akurasi yang tinggi dan akurat

2. Metode yang diusulkan menjadi metode yang lebih baik dalam mendeteksi malware

1.6 Sistematika Penulisan

Tugas Akhir ini disusun dengan sistematika penulisan sebagai berikut :

- **BAB I Pendahuluan**. Bab ini membahas mengenai latar belakang, rumusan masalah, dan tujuan pengerjaan Tugas Akhir ini.

- **Bab II Kajian Pustaka**. Bab ini membahas fakta dan teori yang berkaitan dengan perancangan sistem untuk mendirikan landasan berfikir. Dengan menggunakan fakta dan teori yang dikemukakan pada bab ini penulis menganalisis kebutuhan akan rancangan arsitektur sistem yang dibangun.

- **BAB III Metodologi dan Desain Sistem**. Bab ini menjelaskan metode penelitian, rancangan sistem dan metode pengujian yang dilakukan dalam penelitian.

- **BAB IV Hasil dan Pembahasan**. Bab ini menjelaskan hasil uji dan analisa hasil uji dari yang telah dilakukan sesuai teori dan metode yang digunakan

- **BAB IV Hasil dan Pembahasan**. Bab ini menjelaskan Kesimpulan dan saran dari keseluruhan penelitian ini