BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era Industri 4.0, teknologi berkembang pesat, khususnya di bidang Network Security atau keamaan jaringan. Teknologi ini digunakan untuk mengamankan suatu jaringan di perusahaan atau organisasi. Salah satu teknologi Menurut laporan Dari *Tech Crunch* laporan Gertner. yang sering digunakan masyarakat adalah android. Pada Tahun 2017, Gertner melaporkan bahwa penjualan ponsel pintar global meningkat sebesar 9 persen pada kuartal pertama, dengan 380 juta perangkat seluler terjual, dengan Android memimpin pasar dengan 84,1 persen. Menurut laporan Kementerian Komunikasi dan Informatika, jumlah pengguna aktif smartphone di Indonesia melebihi 200 juta orang pada tahun 2024 dan StatCounter melaporkan bahwa jumlah pengguna Android di Indonesia sebesar 91% pada tahun 2018 , sehingga dapat diasumsikan jumlah pengguna Android di Indonesia sekitar 91 juta orang(laporan serangan malware kaspersky). Jumlah pengguna Android meningkat pesat sehingga sistem operasi Android menjadi sasaran serangan malware, sistem operasi yang diserang malware rusak, dan bahkan dengan niat yang lebih jahat, informasi penting dapat dicuri dari sistem dengan bantuan malware. Malware atau malware seperti yang biasa dikenal adalah perangkat lunak yang diprogram untuk menyusup ke sistem operasi dan dapat merusak sistem bahkan mencuri data penting dari perangkat korban. Menurut Lembaga Stnadar Keamanan Menurut konsep Privilege Escalation dalam

keamanan siber Ada banyak jenis malware dan mereka memiliki cara kerja yang berbeda, misalnya serangan malware melalui aplikasi jahat yang menggunakan hak istimewa secara ilegal tanpa izin pengguna dan sistem operasi. Karena kerentanan terhadap serangan malware dan kerentanan yang memengaruhi pengguna Android, diperlukan analisis malware lebih lanjut. Pada Tahun 2019, perusahaan keamanan siber Kaspersky melaporkan 556.486 deteksi malware, dan pada Tahun 2020, Kaspersky juga melaporkan penurunan serangan malware di Indonesia sebesar 31,89% menjadi 378.973. Hal ini menjadikan Indonesia sebagai negara dengan jumlah ancaman malware yang terdeteksi terbanyak di Asia Tenggara dan tertinggi keempat di dunia Analisis statis dilakukan dengan mengekstraksi kode sumber malware dan kemudian memeriksa dan memahami perilaku berbahaya melalui kode sumber, data, dan binari, sehingga proses analisis statis tidak memerlukan malware untuk dijalankan. Analisis statis digunakan untuk mengekstrak fitur dan mengidentifikasi setiap aplikasi menggunakan ApkTool 2.0.3. Berdasarkan data serangan malware dan jumlah pengguna Android yang besar, hal ini menjadi masalah, sehingga penelitian ini menerapkan sistem machine learning untuk menentukan metode klasifikasi yang menjamin akurasi tinggi dalam deteksi dini serangan malware. Beberapa penelitian sebelumnya menggunakan beberapa metode machine learning seperti Naive Bayes, Decision Tree, KNN dan metode lainnya seperti (Wanli Sitorus, Sukarno, and Mandala 2021) yang melakukan penelitian menggunakan beberapa metode machine learning dengan akurasi hingga 95%. Menurut (Wanli Sitorus et al., 2021) Melaporkan bahwa tahun 2018 pengguna

aktif smartphone di Indonesia lebih dari 100 juta orang serta pada tahun yang sama data dari statcounter pengguna android di Indonesia sebanyak 90,85%. Dengan berkembangnya metode pembelajaran mesin untuk klasifikasi, penelitian ini mengadopsi sistem pembelajaran mesin untuk menentukan metode pembelajaran mesin yang memberikan kinerja matriks dalam deteksi dini serangan malware yang lebih baik dari penelitian . Penelitian ini menggunakan metode klasifikasi Support Vector Machine (SVM). Hasil penelitian ini diharapkan dapat membantu pengembang dan pengguna untuk mengunduh aplikasi. Algoritma supervised learning (SVM) adalah algoritma yang digunakan untuk klasifikasi dan regresi dan bekerja dengan mencari hyperplane optimal yang memiliki kemampuan untuk memisahkan dua kelas data dengan margin maksimum. Karakteristik SVM ini memungkinkan mereka menangani data yang sangat besar dan menghasilkan model klasifikasi yang kuat, yang menjadikannya ideal untuk deteksi malware. SVM dapat digunakan untuk mengidentifikasi apakah aktivitas termasuk serangan malware dengan menggunakan data yang telah diproses, seperti fitur penggunaan CPU, memori, dan proses sistem lainnya. Dalam penelitian ini, metode SVM digunakan untuk mengidentifikasi serangan malware menggunakan dataset yang terdiri dari fitur numerik aktivitas sistem. Preprocessing data, normalisasi, ekstraksi fitur, pelatihan model, dan evaluasi performa klasifikasi adalah langkah-langkah yang membentuk proses penelitian. Diharapkan bahwa SVM akan memungkinkan sistem untuk mendeteksi serangan malware dengan lebih akurat dan efektif daripada metode konvensional. Selain itu, penelitian ini bertujuan untuk menentukan seberapa efektif metode SVM dalam mendeteksi malware. Selain itu, penelitian ini

juga akan memberikan kontribusi terhadap pengembangan sistem keamanan informasi yang lebih tahan terhadap ancaman siber yang terus meningkat.

1.2 Identifikasi Masalah

Algoritma SVM telah banyak digunakan dalam deteksi malware, tetapi masih ada beberapa masalah saat menggunakannya anatara lain:

1. *Malware* dapat merusak sistem operasi
2. *Malware* dapat menurunkan kinerja sistem
3. Serangan mlaware masih meningkat setiap tahun
4. *False negative* dalam deteksi malware masih sangat tinggi sehingga kesalahan deteksi masih sangat tinggi.

1.3 Batasan Masalah

Batasan pendeteksian serangan malware menggunakan metode Support Vector Machine (SVM) adalah Fokus menggunakan SVM untuk mendeteksi serangan *malware* di OS Windows. Fitur yang digunakan dalam deteksi malware terbatas pada opcode dan urutan byte,dan Dataset yang digunakan dalam penelitian dikumpulkan dan diberi label dengan benar sebelumnya

1.4 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan di atas dan identifikasi masalah, maka rumusan masalah pendeteksian serangan malware menggunakan metode Support Vector Machine (SVM) adalah sebagai berikut:

1. Bagaimana Cara Mendeteksi Serangan *Malaware* Menggunakan Algoritma SVM?
2. Bagaimana Melakukan pemilihan fitur dalam mendeteksi serangan malware?
3. Baagaimana perfomance atau kinerja dari algoritma SVM?

1.5 Tujuan Penelitian

Tujuan penelitian ini adalah sebagai berikut

1. Untuk mendeteksi serangan malware menggunakan algoritma SVM
2. Untuk melakukan pemilihan fitur dalam mendeteksi serangan malware.
3. Untuk mengetahui perfomance atau kinerja dari algoritma SVM

1.6 Manfaat Penelitian

Manfaat penelitian ini sangat jelas tercantum dan di gambarkan dalam uraian latar belakang penelitian ini. Secara umum manfaat penelitian ini terbagi menjadi 2 yaitu sebagai berikut:

1.6.1 Secara Teoritis

Secara teoritis, mendeteksi serangan malware menggunakan metode Support Vector Machine (SVM) memiliki keuntungan sebagai berikut:

1. Dukungan dan validasi teori SVM sebagai algoritma klasifikasi yang efektif. Dalam teori pembelajaran mesin, SVM telah terbukti sebagai algoritma klasifikasi yang efektif dan efisien untuk memecahkan masalah klasifikasi.

Dengan penelitian yang menunjukkan keefektifan SVM dalam mendeteksi serangan *malware*.

2. Mengembangkan dan memperluas teori pembelajaran mesin untuk mendeteksi serangan *malware*. Hasil penelitian dapat membantu dalam pengembangan dan pengembangan teori pembelajaran mesin untuk mendeteksi serangan malware, termasuk fitur yang berguna dan teknik untuk menangani masalah ketidakseimbangan data.

1.6.2 Secara Praktis

Dalam praktis mendeteksi serangan malware menggunakan metode Support Vector Machine (SVM) memiliki keuntungan sebagai berikut:

1. Tingkatkan keamanan sistem dari serangan malware langsung. Dengan sistem deteksi malware yang kuat dan akurat, dapat mendeteksi dan mencegah serangan malware pada sistem operasi Windows, meningkatkan keamanan sistem dari serangan malware.
2. Mengurangi kerugian dari serangan malware langsung. Serangan malware dapat menyebabkan kerusakan sistem, kehilangan data, dan biaya pemulihan sistem. Sistem deteksi malware yang efektif dan akurat dapat mengurangi kerugian akibat serangan malware


UPB
Universitas Putera Batam