BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi digital yang pesat dalam beberapa dekade terakhir telah mengubah cara manusia beraktivitas, berkomunikasi, dan mengakses informasi. Salah satu dampak signifikan dari kemajuan ini adalah meningkatnya ketergantungan masyarakat pada perangkat *mobile*, terutama *smartphone*. Penggunaan Android mendominasi di Asia, dengan jumlah pasar sebesar 79% pada Februari 2024 (Sherif, A, 2024). Namun, dominasi Android ini juga membuka celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab, khususnya serangan siber berbasis malware terhadap perangkat Android (Apinento dkk., 2023).

Berdasarkan survei, kejahatan siber di Indonesia tercatat sebesar 1.637.973.022 serangan pada tahun 2022 (Samad, M dkk., 2022). Sebanyak 60% dari total serangan yang terjadi merupakan serangan malware, menunjukkan betapa dominannya ancaman ini dalam lanskap keamanan siber saat ini terutama pada pengguna perangkat *mobile* (Samad, M dkk., 2022). Jumlah serangan yang tinggi ini menandakan bahwa serangan siber berbasis malware masih menjadi salah satu bentuk ancaman serius di dunia maya (Rahul dkk., 2020). Tidak hanya menyebabkan kerusakan teknis pada perangkat, malware juga berpotensi mencuri data pribadi pengguna, menyusup ke dalam sistem perangkat, hingga digunakan sebagai alat pemerasan terhadap pengguna. Situasi ini mendorong pentingnya pengembangan sistem deteksi malware yang tidak hanya akurat, tetapi juga efisien dan dapat diterapkan secara luas (Apinento dkk., 2023).

Pencegahan serangan siber menggunakan malware pada sistem Android merupakan langkah kritis dalam menjaga integritas dan keamanan sistem informasi di era digital (Rahul dkk., 2020). Meski Google Play telah melakukan pengawasan aplikasi, masih diperlukan sistem deteksi malware yang lebih adaptif karena beberapa ancaman tetap berhasil lolos verifikasi. (Lu dkk., 2018). Pendekatan deteksi malware saat ini terbagi ke dalam tiga kategori besar, berbasis tanda tangan (*signature-based*), berbasis perilaku (*behavior-based*), dan berbasis pembelajaran mesin (*machine learning*) (Kouliaridis, V., & Kambourakis, G. 2021). Metode

tradisional seperti *signature-based* mengandalkan pencocokan pola statis dari kode berbahaya, sehingga kurang adaptif terhadap evolusi malware modern yang sering menyamarkan dirinya untuk menghindari deteksi (Lu dkk., 2023), Hal ini menyebabkan para peneliti dan praktisi keamanan siber mulai beralih pada pendekatan yang lebih adaptif, salah satunya dengan menggunakan pendekatan *permission-based* berbasis *machine learning* (ML) (Lu dkk., 2018).

Penelitian terkini menyoroti penggunaan deteksi malware dengan metode pendekatan statis yang mengimplementasikan analisis berbasis ML (Rahul dkk., 2020). Algoritma ML dapat digunakan untuk menganalisis kumpulan data yang besar dari karakteristik ataupun perilaku sistem untuk mengidentifikasi pola-pola halus yang dapat diindikasikan sebagai muatan berbahaya atau malware (Jadhav dkk., 2024). Pada penelitian yang dilakukan oleh (Lu dkk., 2018) menyatakan bahwa data perizinan aplikasi merupakan fitur yang mudah diperoleh dan efektif digunakan sebagai dataset dalam penerapan machine learning untuk deteksi malware (Lu dkk., 2018). Hal ini ditegaskan pada penelitian (Abdullah, T. dkk., 2020) penggunaan *Support Vector Machine* (SVM) sangat efektif untuk mendeteksi malware, karena kemampuannya untuk mengklasifikasikan data yang tidak linier dan berdimensi tinggi. (Lysenko dkk., 2019). Selain itu, SVM bekerja dengan prinsip memaksimalkan jarak antara dua kelas dengan mencari garis pemisah (*hyperplane*) yang memiliki jarak paling jauh dari titik data terdekat di masing-masing kelas. Hal ini membantu mengurangi risiko *overfitting* dan meningkatkan kemampuan model untuk menggeneralisasi data (Nti dkk., 2021). SVM dapat diterapkan dengan berbagai jenis kernel, yang memberikan kemampuan untuk beradaptasi dengan berbagai tipe data (Nti dkk., 2021).

Pada pelaksanaanya, disebutkan pada penelitian (Nti dkk., 2021) bahwa dalam penggunaan SVM dibutuhkan pemilihan fungsi kernel yang paling tepat untuk menyempurnakan penyesuain karakteristik data yang digunakan pada deteksi malware (Nti dkk., 2021). Dengan bantuan *Principal Components Analysis* (PCA) untuk mereduksi dimensi data ektrasi fitur, sehingga kompleksitas komputasi dari SVM dapat diminimalkan secara signifikan dan memungkinkan model SVM untuk lebih memusatkan perhatian pada komponen utama yang benar-benar berkaitan dengan prediksi (Modalavalasa & Makkena, 2020).

Penelitian ini bertujuan untuk menganalisis pengembangan model deteksi malware dengan memanfaatkan algoritma SVM yang diimplementasikan melalui berbagai konfigurasi kernel. Penggunaan model SVM pada penelitian ini didasarkan pada kemampuannya dalam melakukan klasifikasi data berlabel secara efisien, khususnya pada daftar panjang perizinan aplikasi (Abdullah, T. dkk., 2020). Dalam penelitian ini, konfigurasi fungsi kernel akan menggunakan metrik *accuracy*, *precision*, *recall*, dan *F1-score*, yang digunakan untuk mengukur tingkat ketepatan, kelengkapan, dan keseimbangan kinerja model dalam mengidentifikasi malware (Hemalatha dkk., 2021).

1.2 Rumusan Masalah Penelitian

Berdasarkan latar belakang yang telah dipaparkan masalah yang akan diteliti adalah:

1. Bagaimana pengembangan model deteksi malware menggunakan algoritma *Support Vector Machine* (SVM) dalam mendeteksi malware dengan pendekatan *permission-based*?
2. Bagaimana pengaruh pemilihan jenis fungsi kernel terhadap kinerja deteksi malware menggunakan algoritma SVM dalam mendeteksi malware dengan pendekatan *permission-based*?

1.3 Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah di atas, berikut adalah tujuan dari penelitian ini:

1. Melakukan pengujian kinerja model deteksi malware menggunakan algoritma *Support Vector Machine* (SVM) dengan pendekatan *permission-based.*
2. Melakukan pengujian dan menganalisis pengaruh jenis fungsi kernel terhadap performa model deteksi malware yang diterapkan pada algoritma SVM dengan pendakatan *permission-based*.

1.4 Batasan Penelitian

Berdasarkan latar belakang dan rumusan masalah di atas, berikut adalah batasan dari penilitian ini:

1. Penelitian ini hanya menggunakan fitur izin aplikasi (*permission*) sebagai parameter untuk deteksi malware.
2. Dataset yang digunakan berasal dari sumber publik yang telah tersedia dan mencakup aplikasi jinak dan berbahaya
3. Algoritma yang digunakan dalam penelitian ini terbatas pada *Support Vector Machine* (SVM), tanpa melakukan perbandingan langsung dengan algoritma *Machine Learning* (ML) lainnya.
4. Jenis fungsi kernel yang diuji pada model SVM terbatas pada *kernel linear*, *polynomial*, *radial basis function* (RBF), dan *sigmoid*.
5. Evaluasi performa model didasarkan pada metrik *accuracy*, *precission*, *recall*, dan *F1-score*.

1.5 Manfaat Penelitian

Berdasarkan latar belakang dan rumusan masalah di atas, berikut adalah batasan dari penilitian ini:

1. Memberikan kontribusi keilmuan dalam penerapan algoritma *Support Vector Machine* (SVM) untuk deteksi malware berbasis izin aplikasi Android.
2. Menjadi referensi akademik terkait pengaruh pemilihan fungsi *kernel* terhadap performa klasifikasi pada algoritma SVM.
3. Memberikan gambaran teknis mengenai pengembangan sistem deteksi malware yang efisien dan ringan menggunakan pendekatan *permission-based detection*.
4. Mendorong penerapan sistem keamanan berbasis *Macihne Learning* (ML) yang dapat diimplementasikan pada perangkat dengan sumber daya terbatas.
5. Menjadi dasar pengembangan lebih lanjut untuk sistem deteksi *malware* yang adaptif terhadap varian *malware* baru.

1.6 Sistematika Penulisan

Untuk memberikan kemudahan dalam memahami keseluruhan isi pembahasan skripsi ini, akan dijelaskan mengenai struktur penulisan atau sistematika yang digunakan. Struktur organisasi skripsi ini mencakup beberapa aspek sebagai berikut.

BAB I PENDAHULUAN

Bab I pendahuluan berfungsi sebagai pengantar yang menyajikan latar belakang penelitian, menjelaskan motivasi di balik pelaksanaan penelitian tersebut. Di dalam bagian ini, juga disampaikan rumusan permasalahan yang diangkat serta tujuan penelitian yang mencerminkan harapan terhadap hasil yang ingin dicapai. Selain itu, bagian ini juga menguraikan manfaat penelitian yang diharapkan dapat diperoleh dari pelaksanaan penelitian ini.

BAB II KAJIAN PUSTAKA

Bab II Kajian Pustaka menyajikan *state of the art* atau penelitian terbaru yang relevan dengan penelitian ini. Selain itu, bab ini juga menguraikan teori-teori yang mendasari pelaksanaan penelitian ini.

BAB III METODE PENELITIAN

Bab ini menyajikan penjelasan mengenai pendekatan metode yang diterapkan, termasuk desain penelitian, langkah-langkah penelitian yang diambil, serta informasi mengenai partisipan dan alat serta bahan yang digunakan dalam penelitian.

BAB IV TEMUAN DAN PEMBAHASAN

Temuan dan pembahasan menyajikan hasil dari penelitian yang dilaksanakan berdasarkan diagram alur desain penelitian guna menjawab pertanyaan yang telah dirumuskan.

BAB V SIMPULAN, IMPLIKASI DAN REKOMENDASI

Bab ini menyajikan kesimpulan, implikasi, dan saran berdasarkan hasil penelitian. Konten bab ini memberikan gambaran singkat mengenai hasil yang diperoleh dari penelitian yang telah dilaksanakan.