BAB I

PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Perkembangan teknologi informasi yang pesat membawa banyak manfaat bagi berbagai sektor kehidupan, mulai dari pendidikan, bisnis, hingga pemerintahan. Namun di sisi lain, kemajuan teknologi juga menimbulkan berbagai ancaman keamanan siber. Salah satu ancaman yang paling umum dan berbahaya adalah *malware* atau *malicious software*, yaitu perangkat lunak yang dirancang untuk merusak, mengganggu, mencuri, atau bahkan mengambil alih sistem komputer korban [1].

Salah satu jenis *malware* yang paling sering digunakan dalam serangan siber adalah *Trojan Horse*. *Trojan* bekerja dengan menyamar sebagai perangkat lunak yang sah untuk mengecoh pengguna, sehingga pengguna secara tidak sadar memberikan akses kepada penyerang ke dalam sistem mereka. Menurut laporan, *Trojan* merupakan jenis *malware* paling dominan, dengan lebih dari 60% dari total *malware* baru yang terdeteksi setiap tahunnya tergolong dalam kategori ini. *Trojan* dapat menyebabkan berbagai kerusakan, mulai dari pencurian data pribadi hingga pengambilalihan kendali sistem secara penuh [2].

Seiring meningkatnya kompleksitas dan jumlah serangan *Trojan*, pendekatan konvensional dalam deteksi *malware* seperti *signature-based detection* menjadi kurang efektif. Metode ini sangat bergantung pada pembaruan basis data tanda tangan *malware* dan tidak mampu mengenali varian baru yang belum dikenali

sebelumnya. Oleh karena itu, dibutuhkan pendekatan baru yang lebih adaptif dan cerdas.

Dalam beberapa tahun terakhir, *deep learning*, khususnya *Convolutional Neural Network* (CNN), telah menunjukkan kinerja yang menjanjikan dalam berbagai bidang, termasuk pengenalan pola dan klasifikasi citra. CNN memiliki kemampuan untuk mengekstraksi fitur penting dari data mentah secara otomatis, sehingga sangat cocok untuk digunakan dalam mendeteksi pola-pola mencurigakan dari *file* yang terinfeksi *malware*.

Berbagai penelitian telah mendukung efektivitas pendekatan ini. Misalnya, Mahmut Tomak dkk**.** menggunakan metode CNN untuk mendeteksi *malware* Android pada *dataset* AMD dan mencapai akurasi 96,94%. Penelitian oleh Shoupu Lu dkk**.** menunjukkan bahwa CNN dapat digunakan untuk mendeteksi *Trojan* dengan tingkat akurasi hingga 99%. Sementara itu, Didih Rizki Chandranegara dkk. mengklasifikasikan *malware* berbasis citra menggunakan CNN dan memperoleh akurasi sebesar 94,8%. Hasil-hasil tersebut menunjukkan bahwa CNN memiliki potensi besar untuk diterapkan dalam deteksi *malware*.

Namun, sebagian besar penelitian sebelumnya masih terbatas pada jenis *malware* Android atau pendekatan berbasis data non-*Trojan*. Oleh karena itu, dibutuhkan penelitian lebih lanjut yang secara khusus fokus pada deteksi *malware* jenis *Trojan Horse*, terutama dengan pendekatan berbasis citra menggunakan CNN. Dataset CIC-Malmem-2022, yang menyediakan data serangan berbasis memori dunia nyata, digunakan dalam penelitian ini karena mencakup jenis *Trojan* yang relevan dan representatif.

Penelitian sebelumnya menunjukkan bahwa *malware* dapat direpresentasikan dalam bentuk citra (*image-based malware detection*), yang kemudian dianalisis menggunakan CNN untuk mendeteksi anomali atau pola serangan [3].

Malware adalah perangkat lunak berbahaya yang mengacu pada program yang secara sengaja mengeksploitasi kerentanan dalam sistem komputasi untuk tujuan yang berbahaya [4]. Dengan komputer dan Internet yang sudah menjadi bagian penting dalam kehidupan sehari-hari, *malware* merupakan ancaman serius bagi keamanan setiap pengguna komputer. *Malware* terus memfasilitasi serangan *cyber*, dimana sebagai penyerang, *malware* tetap menjadi salah satu alat utama kampanye mereka. Oleh karena itu, Untuk melawan penjahat *cyber*, penting bagi para pembela untuk memahami perilaku *malware*, seperti pola penyebaran atau rekrutmen keanggotaan, ukuran *botnet*, dan distribusi *bot* [4].

Berbagai kategori pendekatan deteksi telah diusulkan, termasuk *Signature Based*, yang membutuhkan aturan buatan tangan sendiri untuk bendapatkan data yang relevan agar bisa melakukan deteksi, dan *Machine Learning*, yang secara otomatis memberikan alasan tentang data *Malware* dan *Benignware* agar sesuai dengan parameter model deteksi [5]. Sampai saat ini, komputer industri keamanan lebih memilih menggunakan metode *Signature Based* karena dilihat dari tingkat *Low False Positive Rates* yang dapat dicapai oleh metode tersebut [6]. Namun, dalam beberapa tahun terakhir, *Machine Learning* berhasil mencapai deteksi tingkat tinggi pada tingkat *Low False Positive Rates* tanpa beban generasi tangan manusia yang diperlukan dengan metode manual.

Seleksi Fitur merupakan suatu proses untuk mengurangi dimensi atribut. Pengurangan dimensi tersebut dilakukan untuk mendapatkan atribut-atribut yang relevan dan tidak berlebihan sehingga dapat mempercepat proses klasifikasi dan dapat meningkatkan akurasi dari algoritma klasifikasi [7]. Pada penelitian ini mengusulkan sebuah pendekatan berbasis pembelajaran mesin yang efektif untuk *Android Malware* Deteksi menggunakan algoritma genetika evolusioner untuk pemilihan fitur diskriminatif [8]. Hasil eksperimen memvalidasi itu Algoritma genetik memberikan bantuan *subset* fitur yang paling optimal pengurangan dimensi fitur menjadi kurang dari setengah aslinya set fitur. Akurasi klasifikasi lebih dari 94% adalah pemilihan fitur postingan yang dipertahankan untuk berbasis pembelajaran mesin pengklasifikasi, saat mengerjakan dimensi fitur yang jauh berkurang, dengan demikian, berdampak positif pada kompleksitas komputasi pengklasifikasi belajar [8].

Saat ini, dengan peningkatan jumlah *malware* yang dihasilkan, kebutuhan untuk metode yang lebih otomatis dan cerdas untuk belajar, beradaptasi, dan menangkap *malware* sangat penting, sejumlah solusi mutakhir ditawarkan para perusahaan keamanan untuk mencegah serangan *malware* berbahaya. Yang terbaru adalah kapabilitas *Machine Learning* untuk menangkal *Malware* secara *real-time*. *Machine Learning* sendiri adalah sebuah cabang aplikasi dari kecerdasan buatan yang fokus pada pengembangan sebuah sistem yang mampu belajar "sendiri" tanpa harus berulang kali diprogram oleh manusia. Salah satu arsitektur kerja dari *Machine Learning* adalah *Artificial Neural Network*, yang merupakan sistem

komputasi yang diilhami oleh jaringan saraf biologis yang memiliki struktur seperti otak hewan, sedangkan *Deep Neural Network* memiliki struktur yang lebih rumit.

Dengan mempertimbangkan hal tersebut, penelitian ini bertujuan untuk membangun sistem deteksi serangan *malware* jenis *Trojan Horse* menggunakan metode CNN, yang diharapkan dapat meningkatkan akurasi deteksi dan kemampuan sistem dalam mengenali serangan baru yang sebelumnya tidak diketahui. Pendekatan ini tidak hanya menawarkan solusi yang lebih adaptif, tetapi juga dapat diintegrasikan ke dalam sistem keamanan siber modern sebagai lapisan pertahanan tambahan. Dari permasalahan di atas maka peneliti tertarik merancang sistem pendeteksi serangan *malware* yang berjudul "**Sistem Deteksi Serangan *Malware* Jenis *Trojan Horse* dengan Menggunakan Metode CNN**" .

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang maka rumusan masalah pada penelitian ini :

1. Bagaimana cara merepresentasikan data *malware* jenis *Trojan Horse* agar dapat diolah oleh metode *Convolutional Neural Network* (CNN)?
2. Bagaimana merancang dan mengimplementasikan arsitektur CNN yang efektif untuk mendeteksi serangan *malware* jenis *Trojan Horse*?
3. Seberapa akurat metode CNN dalam mendeteksi serangan *malware* jenis *Trojan Horse* dibandingkan dengan metode deteksi konvensional?
4. Apa saja kelebihan dan kekurangan penggunaan CNN dalam sistem deteksi *malware* jenis *Trojan Horse*?

1.3 BATASAN MASALAH

Untuk menghidari pembahasan yang sangat luas, maka peneliti melakukan pembatasan pada pembahasan masalah :

1. Jenis *malware* yang diteliti dibatasi hanya pada *Trojan Horse*, tidak mencakup jenis *malware* lain seperti *worm*, *ransomware*, *spyware*, atau *virus*.
2. Data *malware* yang digunakan berupa yang telah *dataset* tersedia secara publik atau hasil konversi *file malware* ke dalam bentuk citra (*image-based*) agar dapat diproses oleh metode CNN.
3. Model deteksi dikembangkan menggunakan metode *Convolutional Neural Network* (CNN) tanpa menggabungkan metode lain seperti RNN, SVM, atau *Random Fores*.
4. Penelitian difokuskan pada proses klasifikasi antara *file malware* (*Trojan*) dan *non-malware* (*benign*), bukan pada deteksi secara *real-time* atau pencegahan serangan langsung.
5. Evaluasi sistem dilakukan berdasarkan metrik klasifikasi standar, seperti akurasi, *precision*, *recall*, dan *F1-score*, tanpa membahas aspek performa sistem dalam kondisi dunia nyata seperti integrasi dengan antivirus atau sistem operasi.

1.4 TUJUAN PENELITIAN DAN MANFAAT PENELITIAN

Adapun tujuan dan manfaat dari penelitian yang dibuat oleh peneliti adalah dapat memberikan peningkatan kondisi yang ada pada saat ini, Adapun antara lain sebsgai berikut:

1.4.1 Tujuan Penelitian

Adapun tujuan yang ingin dicapai pada penelitian ini adalah :

1. Untuk membangun sistem deteksi *malware* jenis *Trojan Horse* dengan memanfaatkan metode *Convolutional Neural Network* (CNN) berbasis data citra.
2. Untuk menganalisis dan menguji kinerja model CNN dalam mengklasifikasikan *file* sebagai *malware* (*Trojan*) atau non-*malware*.
3. Untuk mengevaluasi akurasi dan efektivitas metode CNN dalam mendeteksi *Trojan Horse* dibandingkan dengan pendekatan deteksi tradisional.
4. Untuk menyediakan solusi berbasis kecerdasan buatan yang dapat dikembangkan lebih lanjut dalam sistem keamanan siber modern.

1.4.2 Manfaat Penelitian

Adapun manfaat yang diperoleh dalam penelitian ini adalah :

1. Memberikan informasi hasil deteksi *Trojan Horse* menggunakan metode CNN
2. Memberikan informasi tingkat keakurasian dari proses deteksi dalam klasifikasi *malware jenis Trojan Horse*.
3. Penelitian ini diharapkan mampu memberikan informasi, wawasan dan pengetahuan mengenai sistem deteksi dalam klasifikasi *malware jenis Trojan Horse* menggunakan metode CNN

1.5 SISTEMATIKA PENULISAN

Sistematika dari penulisan ini guna memberikan gambaran secara umum mengenai keseluruhan bab yang saling berhubungan satu sama lainnya dan sesuai dengan ruang lingkup judul, sistematika penulisan ini antara lain sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini dibahas tentang latar belakang masalah, perumusan masalah, pembatasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II : LANDASAN TEORI

Pada bab ini peneliti membuat landasan teoritis yang mendasari pembahasan secara khusus berisi definisi-definisi yang mendasari penelitian yang didapatkan dengan melakukan studi pustaka sebagai

dalam melakukan deteksi *malware* termasuk penelitian yang telah di lakukan sebelumnya.

BAB III : METODOLOGI PENELITIAN

Pada bab ini berisi mengenai metode penelitian yang digunakan dan meliputi semua tahapan dalam metode CNN.

BAB IV : ANALISIS DAN HASIL

Pada bab ini mengenai analisa berisikan tentang pembahasan mengenai analisa metode CNN terhadap deteksi *malware* berserta tingkat akurasinya.

BAB V : PENUTUP

Dalam bab ini akan dijelaskan mengenai kesimpulan dari hasil penelitian yang telah dilakukan dan saran terhadap penelitian ke depannya.