BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring dengan pesatnya perkembangan teknologi informasi, ancaman terhadap keamanan sistem informasi juga semakin meningkat. Tren serangan siber menunjukkan peningkatan signifikan, dengan laporan dari Check Point Research yang mengungkapkan bahwa serangan siber global meningkat sebesar 30% pada tahun 2024, dengan rata-rata 1.636 serangan per organisasi setiap minggunya [1]. Selain itu, IBM mencatat bahwa biaya rata-rata akibat pelanggaran data mencapai USD 4,88 juta [2]. Salah satu ancaman utama dalam dunia maya adalah malware, yaitu perangkat lunak berbahaya yang dirancang untuk merusak atau mengakses sistem tanpa izin.

Dengan meluasnya penggunaan teknologi seperti Internet of Things (IoT), komputasi awan, dan perangkat mobile, permukaan serangan menjadi semakin besar dan kompleks, meningkatkan peluang bagi penyerang siber [3]. Seiring dengan kerentanan yang meningkat, berbagai jenis malware seperti virus, worm, dan trojan semakin sering ditemukan, masing-masing dengan cara kerja yang unik.

Berbagai jenis malware mencakup virus, yang mampu mereplikasi dirinya sendiri dan menyebar ke file atau program lain; worm, yang menyebar melalui jaringan tanpa interaksi pengguna; serta trojan, yang menyamar sebagai perangkat lunak yang sah untuk mengecoh pengguna agar menginstalnya. Selain itu, terdapat ransomware yang mengenkripsi data korban dan menuntut tebusan untuk pemulihannya; spyware yang mencuri informasi pribadi; adware yang menampilkan iklan tidak diinginkan; serta rootkit yang memberikan akses tingkat tinggi kepada penyerang [3].

Dengan semakin canggihnya teknik yang digunakan oleh penyerang dan semakin terintegrasinya teknologi dalam kehidupan sehari-hari, ancaman malware terus berkembang dan menjadi tantangan besar bagi keamanan siber. Menurut laporan keamanan siber terbaru, jumlah serangan malware terus meningkat setiap tahun [1]. Malware tidak hanya menyerang individu, tetapi juga organisasi besar, termasuk institusi keuangan, perusahaan teknologi, dan pemerintahan. Dampak dari serangan malware dapat sangat merugikan, baik dari segi finansial, kehilangan data,

hingga kerugian reputasi [4].

Oleh karena itu, deteksi malware menggunakan teknologi canggih seperti *Deep Neural Networks* (DNN) menjadi semakin penting untuk mengidentifikasi pola perilaku malware dengan lebih efektif dan akurat. Pendekatan ini diharapkan dapat meningkatkan kemampuan sistem dalam mendeteksi ancaman yang terus berkembang, serta memberikan analisis yang lebih komprehensif terhadap potensi serangan yang kompleks.

Pada tahun 2024, dua penelitian penting dalam deteksi malware menggunakan pendekatan berbeda menunjukkan hasil yang signifikan. Penelitian oleh Supriyanto et al. yang berjudul *"Deteksi Malware Menggunakan Algoritma K-Nearest Neighbor dan Seleksi Fitur"* memanfaatkan algoritma kNN dengan teknik seleksi fitur *Information Gain* dan *PCA*, dan berhasil mencapai akurasi dan F1-Score tertinggi sebesar 96,9% [5]. Sementara itu, Edwin Lesmana Tjiong dalam penelitiannya yang berjudul *"Pendeteksi Malware Javascript Menggunakan Fitur Semantik Program"* menggunakan pohon sintaksis abstrak (AST) serta fitur *N-Gram* dan 28 fitur statis baru untuk mendeteksi malware pada file Javascript, dan berhasil mencapai F1-score sebesar 99% [6]. Jika dibandingkan dengan metode DNN dalam klasifikasi deteksi malware, DNN sering kali menawarkan performa yang lebih baik dalam menangani data besar dan kompleks dengan akurasi tinggi, meskipun memerlukan sumber daya komputasi yang lebih besar [7].

Tradisionalnya, deteksi malware dilakukan menggunakan metode berbasis tanda tangan (*signature-based*), yang mengidentifikasi malware berdasarkan pola atau tanda tangan unik yang telah diketahui dalam database antivirus [9]. Meskipun efektif untuk mendeteksi malware yang sudah dikenal, metode ini memiliki keterbatasan signifikan dalam menghadapi malware baru atau varian yang belum dikenali (*zero-day malware*) karena tidak memiliki tanda tangan yang dapat dibandingkan [10]. Selain itu, teknik *obfuscation* dan *polymorphism* yang digunakan oleh penyerang untuk mengubah tanda tangan malware mereka semakin memperumit proses deteksi.

Dengan mempertimbangkan kekurangan metode tradisional serta meningkatnya kompleksitas serangan siber, pendekatan berbasis *Deep Learning*

seperti DNN menawarkan solusi yang lebih adaptif dan tangguh dalam menghadapi dinamika ancaman malware. Kemampuan DNN dalam mengekstraksi fitur secara otomatis dan mengenali pola kompleks menjadikannya teknologi yang relevan dan potensial dalam mendeteksi malware secara lebih akurat dan efisien.

1.2 Rumusan Masalah

Untuk menjaga fokus penelitian dan memastikan kesesuaiannya dengan tujuan yang telah ditetapkan, rumusan masalah dalam penelitian ini dirumuskan dalam pertanyaan-pertanyaan berikut:

a. Bagaimana implementasi Deep Neural Network (DNN) dalam mendeteksi dan mengklasifikasikan malware?
b. Bagaimana Deep Neural Network (DNN) dapat mendeteksi varian baru atau *zero-day* malware?
c. Sejauh mana DNN dapat beradaptasi untuk mendeteksi evolusi malware yang tidak terdeteksi?

1.3 Tujuan Penelitian

Tujuan penelitian untuk klasifikasi deteksi malware menggunakan metode Deep Neural Network (DNN) adalah sebagai berikut:

a. Menguji dan mengevaluasi efektivitas model Deep Neural Network (DNN) dalam mendeteksi varian malware baru atau *zero-day*.
b. Menguji performa model DNN dalam mendeteksi malware dengan metode *static Heuristic-based Detection*.
c. Mengukur kemampuan model DNN dalam mendeteksi pola-pola yang tidak terdeteksi, guna meningkatkan responsivitas sistem informasi terhadap ancaman siber.

1.4 Batasan Masalah

Untuk melakukan penelitian yang ingin dicapai sesuai dari tujuan dan target penelitian maka perlu adanya batasan masalah sebagai standar penelitian yang akan dilakukan;

a. Fokus pada pengembangan dan evaluasi model deteksi malware menggunakan metode Deep Neural Network (DNN), tanpa mencakup implementasi sistem deteksi penuh secara menyeluruh.
b. Penggunaan dataset malware yang tersedia secara publik (data sekunder) dan berasal dari sumber terpercaya, dengan kriteria ukuran yang memungkinkan pengolahan efisien, seperti jumlah sampel yang memadai dan fitur-fitur yang relevan untuk pelatihan model.
c. Evaluasi performa model dilakukan berdasarkan metrik standar dalam deteksi malware, seperti akurasi, presisi, recall, dan F1-score.
d. Analisis dibatasi pada file executable pada sistem operasi windows.
e. Pengembangan model dilakukan menggunakan perangkat lunak dan platform komputasi umum yang tersedia secara luas, seperti Python dan TensorFlow.
f. Penelitian ini tidak membahas aspek hukum, etika, atau privasi yang berkaitan dengan penggunaan teknologi deteksi malware.