BAB I

PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Keamanan informasi merupakan suatu hal penting dalam era digital yang mengintegrasikan semua aspek ke dalam internet. Beberapa aspek yang harus dijaga dalam sebuah informasi yaitu Confidentiality, Integrity, Avaibility, Authentication, Authorization dan Non Repudation untuk memastikan bahwa informasi tersebut tidak terserang oleh pelaku kejahatan internet [1]. Suatu informasi dapat dipastikan aman sangatlah sulit dikarenakan banyaknya penjahat internet yang berusaha untuk menyerang suatu system [2]. Analisa dinamis dari sebuah trafik di dalam internet diperlukan untuk mengetahui ancaman serangan malware dengan memerhatikan perilakunya di dalam jaringan internet [3]. Data trafik internet yang berjumlah banyak membuat proses analisa dinamis secara manual sulit untuk dilakukan, sehingga perlu adanya sebuah algoritma Machine Learning yang dapat memeriksa banyak trafik sekaligus.. yang dapat memeriksa banyak trafik sekaligus.

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 [5].

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 [6]. 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. 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 algoritme 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.

Saat ini, dengan peningkatan jumlah malware yang di hasilkan , 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 di program 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.

Deep Neural Network adalah sebuah Artificial Neural Network dengan beberapa lapisan antara lapisan input dan output, Deep Neural Network sudah menjadi alternatif pembelajaran Machine Learning karena kemajuan yang signifikan dalam algoritma pelatihan [9]. Deep Neural Network dapat menemukan manipulasi matematis yang benar untuk mengubah input menjadi output, apakah itu hubungan linear atau hubungan non-linear. Jaringan bergerak melalui lapisanlapisan yang menghitung probabilitas setiap keluaran.

Pada tugas akhir ini akan dilakukan perancangan sebuah algoritma Deep Neural Network menggunakan tool Python yang dilakukan pada sistem operasi windows dengan menggunakan dataset yang didapatkan dari Keggle, kemudian akan dibandingkan dengan dataset lain untuk mengklarifikasi akurasi dari rancangan Deep Neural Network untuk membandingan sebuah file terinfeksi Malware atau tidak. Dari permasalahan diatas maka penliti tertarik merancang sistem pendeteksi serangan malware yang berjudul "SISTEM DETEKSI MALWARE DENGAN DEEP NEURAL NETWORK UNTUK SERANGAN SPYWARE".

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang maka rumusan masalah pada penelitian ini :

1. Bagaimana menerapkan proses deep neural network dalam system identifikasi malware jenis spyware
2. Bagaimana Mendaptkan hasil accuracy yang tinggi dalam sistem pendeteksian malware jenis spyware berbasis DNN ?

1.3 BATASAN MASALAH

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

1. *Dataset* yang di gunakan adalah CIC-MalMem-2022
2. *Tools* yang di gunakan adalah *google colaboratory* dengan Bahasa pemograman *phyton* Pengujian kinerja dilakukan dengan mengunakan nilai akurasi, nilai presisi, nilai *recall* dan F1-*score*

3. Mengklasifikasikan menggunakan fitur seleksi *Univariate* dengan algoritma *Deep Nueral Network.*.

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. Menerapkan metode DNN untuk mendeteksi *malware jenis spyware*.
2. Menentukan fitur atau atribut yang di gunakan sebagai pola *malware jenis spyware.*
3. Mengukur kinerja dari metode DNN dalam mendeteksi *malware jenis spyware*.

1.4.2 Manfaat Penelitian

Adapun manfaat yang diperoleh dalam penelitian ini adalah :

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

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 DNN

BAB IV : ANALISIS DAN HASIL

Pada bab ini mengenai analisa berisikan tentang pembahasan mengenai Analisa metode DNN terhadap deteksi *malware* berserta tingkat akurasi nya.

BAB V : PENUNTUP

Dalam bab ini akan di jelaskan mengenai kesimpulan dari hasil penelitian yang telah di lakukan dan saran terhadap penelitian kedepan nya.