BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Dalam era digital yang dihubungkan melalui internet, telah terjadi perubahan signifikan yang dimana cara informasinya disebarkan, dikelola, dan diakses. Meskipun memberikan banyak kemudahan yang diiringi dengan semakin meningkatnya ancaman keamanan, yang terutama dari serangan *malware*. Selain ancaman keamanan yang ditimbulkan oleh *malware*, terdapat juga sistem keamanan telah dikembangkan untuk melindungi komputer, jaringan, dan data dari serangan atau akses yang tidak sah serta penggunaan alat, kebijakan, konsep keamanan yang bertujuan untuk melindungi aset organisasi dan pengguna, dikenalsebagai *cyber security*. Dibeberapa dekade terakhir, telah terjadi taktik pengintaian di ranah digital yang mengalami peningkatan signifikan, salah satunya melalui eksploitasi menggunakan *malware* pada perangkat target [1]. Di Indonesia menjadi salah satu negara dengan tingkat serangan *malware* tertinggi di kawasan Asia Pasifik [2]. *Malware* yang merupakan istilah untuk program atau perangkat lunak yang dirancang untuk merusak atau menyusup ke dalam sistem komputer. Mereka dianggap berbahaya karena tujuan pembuatannya, salah satu contoh adalah *virus ransomware* dengan tujuan khusus untuk mengeksploitasi kerentanan dalam program [3].

Dalam bidang teknologi, *malware* sering menyebabkan gangguan pada sistem dengan mencuri data sensitif atau memberikan akses tanpa izin ke sistem[4]. Karena jumlah *malware* terus meningkat, dibutuhkan metode yang efisien untuk

mengidentifikasinya. Salah satu cara untuk mendeteksi *virus ransomware* adalah dengan menggunakan *deep learning neural network* [5]. Metode ini mampu mendeteksi *malware* dengan akurat, dan teknologi pembelajaran mendalam seperti *deep learning* dapat memberikan hasil yang lebih baik, bahkan dengan penambahan jumlah data. *Deep learning neural network* memiliki beberapa keuntungan [6], seperti karakteristik yang universal yang memungkinkan implementasinya hampir di semua ranah aplikasi. Kelebihan lainnya adalah kekuatan dalam menghadapi variasi data yang sesuai secara alami dengan fakta yang sebenarnya. Hal ini membuat *deep learning* menjadi metode yang sangat *robust*, dengan salah satu aspek menariknya yaitu kemampuannya untuk belajar secara otomatis tanpa memerlukan desain fitur yang dibuat secara manual untuk mengidentifikasi dan memahami pola dalam data.

Beberapa penelitian sebelumnya [7], [8], [9] yang mengusulkan deteksi *malware* menggunakan metode *deep neural network*, pada penelitian [7] Deteksi *Malware* Statis Menggunakan *Deep neural networks* pada *portable executable*, penelitian ini menunjukkan bahwa penggunaan jaringan saraf dalam deteksi *malware* statis efektif dan berpotensi untuk peningkatan eksperimen analisis statis dapat menjadi alat yang efektif dalam klasifikasi *malware*, dan lebih efisien.

Penelitian [8] Mendeteksi *Malware* dengan metode *ensemble* berbasis *deep neural network*. dengan hasil MalNet adalah metode deteksi *malware* baru yang menggabungkan *CNN* dan *LSTM*, dengan akurasi tinggi (99,88%) dan tingkat kesalahan deteksi rendah (0,1%). Selain itu, *MalNet* berhasil mengklasifikasikan *malware* dengan akurasi 99,36%. Ini juga efektif dalam mengklasifikasikan

malware dan meningkatkan efisiensi deteksi dibandingkan dengan metode lain pada dataset *malware* Microsoft.

Pada penelitian [9] Deteksi *malware* pada platform android menggunakan *Deep Neural Network*, bahwa studi ini menghasilkan model deteksi ancaman mobile yang lebih akurat daripada model sebelumnya, dengan akurasi tinggi untuk model statis dan dinamis. Model statis memiliki akurasi 92,94% dan modeldinamis memiliki akurasi 94,22% dengan F1-Score 90,08. Aplikasi yang gagal mendeteksi tanda tangan sebelumnya dapat ditemukan. Maka dari uraian permasalahan diatas akan dilakukan penelitian yang membahas tentang Deteksi *malware ransomware* menggunakan *deeep neural network.*

Berdasarkan beberapa ulasan diatas *Malware ransomware* adalah jenis perangkat lunak berbahaya yang secara khusus dirancang untuk merusak atau menyusup ke dalam sistem komputer tanpa terdeteksi oleh program keamanan yang ada. *Ransomware* memiliki tujuan khusus, yaitu mengenkripsi atau mengunci data yang ada di dalam sistem, kemudian menuntut pembayaran tebusan dari pemilik data untuk mendapatkan kunci dekripsi atau pemulihan akses.

Oleh karena itu, penelitian ini akan melakukan pendeteksian *malware* menggunakan metode *deep neural network* (DNN) untuk serangan ransomware. dengan beberapa evaluasi kinerja seperti *Accuracy, true positive rate, false positive rate,dan precision atau predictive value*.

1.2 RUMUSAN MASALAH

Berdasarkan uraian latar belakang, maka rumusan masalah pada penelitian ini yaitu:

1. Bagaimana pola dari *malware ransomware*?
2. Bagaimana mendeteksi *malware ransomware* menggunakan *deep neural network?*
3. Bagaimana mengukur performa akurasi deteksi *malware ransomware*?

1.3 BATASAN MASALAH

Untuk menghindari pembahasan yang meluas pada penelitian ini, maka penulis memberikan pembatasan masalah yaitu:

1. Data yang digunakan merupakan data dari *UNIVERSITY OF NEW BRUNSWICK*, yaitu dataset *CIC Obfuscated-MalMem*2022 yang memiliki 58597 data,
2. Penelitian ini berfokus pada penerapan *Deep neural network* yang dimana untuk meningkatkan kinerja atau memberikan solusi yang lebih baik dalam mendeteksi *malware ransomware*.
3. Penelitian ini menggunakan serangan yang berjenis *ransomware*.
4. Penelitian ini menggunakan evaluasi kinerja deteksi yang meliputi *precision, recall, f1-score, Accuracy*.
5. Penelitian ini menggunakan *tools google colab*.

1.4 TUJUAN PENELITAN

Adapun tujuan dari penelitian ini adalah

1. Menentukan pola atau fitur *Malware Ransomware.*
2. Merancang sistem *deteksi Malware Ransomware menggunakan Deep Neural Network.*
3. Mengukur kinerja dari deteksi *Malware Ransomware* menggunakan *Deep*

Neural Network.

1.5 MANFAAT PENELITIAN

Adapun manfaat dari penelitian ini adalah:

1. Penelitian ini dapat melacak *malware rasnsomware*, dan mencegah serangan *ransomware* dengan lebih baik.
2. Dengan mendeteksi *ransomware*, mampu mengurangi waktu yang lama.
3. Penelitian ini dapat sebagai sumber referensi bagi peneliti lain yang membahas mengenai serangan *malware* terutama serangan *Ransomware*

1.6 SISTEMATIKA PENULISAN

Sebagai panduan dalam penyusunan laporan penelitian ini, maka sistematika penulisan meliputi:

BAB I : PENDAHULUAN

Pada bab pendahuluan ini berisi tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian dan sistematika penulisan laporan penelitian.

BAB II : LANDASAN TEORI

Pada bab landasan teori ini berisi tentang teori-teori relevan yang dikutip dari beberapa para ahli dan penelitian yang sejenis, di manateori yang di jelaskan tentang gambaran umum mengenai mendeteksi serangan *Ransomware* menggunakan metode *Deep Neural Network.*

BAB III : METODOLOGI PENELITIAN

Pada bab metodologi penelitian ini, berisi tentang langkah-langkah yang harus diambil untuk menyelesaikan masalah yang dibahas serta

menjelaskan gambaran umum metode yang digunakan.

BAB IV : ANALISIS DAN PEMBAHASAN

Pada bab analisis dan pembahasan ini berisi mengenai analisis dan pembahasan terkait deteksi serangan *Malware Ransomware* menggunakan metode *Deep Neural Network*.

BAB V : PENUTUP

Pada bab penutup ini berisikan tentang kesimpulan penelitian yang telah dilakukan dan memuat saran bagi peneliti selanjutnya.