BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Dalam era teknologi yang semakin berkembang pesat saat ini, komputer digunakan untuk memudahkan pekerjaan manusia [1]. Pada pengoperasiannya terdapat software yang berjalan diatas sistem operasi, dan sangat berperan penting dalam melakukan tugas yang dikerjakan oleh pengguna dalam menyelesaikan tugasnya [2]. Namun tidak semua *software* dapat membantu pekerjaan manusia, adapun *software* yang melakukan perusakan atau tindak kejahatan yaitu *malicious software* atau *malware* [3].

Malware merupakan sistem yang di rancang untuk menghancurkan sistem dan program komputer karena dapat menginfeksi sistem komputer, menghapus file data, dan mencuri informasi berharga [4]. Jenis *malware* bermacam-macam seperti *virus*, *worm*, *trojan*, dan *spyware* [5]. *Trojan horse* merupakan salah satu jenis *malware* yang dimasukkan kedalam sebuah sistem dan bekerja menyalin informasi tanpa izin pengguna [6]. Penyerang menggunakan *trojan* untuk menyebarkan *virus* atau jenis *malware* lainnya ke dalam sistem tanpa sepengetahuan pengguna [7]. Jenis *trojan horse* yang di masukan seperti *backdoor*, yang digunakan oleh penyerang untuk mengontrol dan mengakses komputer [8]. Di sisi lain, virus *trojan horse* juga dapat menyebabkan mesin asli terpengaruh oleh virus ganas lainnya [9]. Deteksi serangan *malware trojan horse* pada program jaringan komputer dapat di lakukan dengan metode *Deep learning* (DL) [10].

DL merupakan salah satu cabang dari *machine learning*. DL dirancang untuk terus menganalisa data seperti pada otak manusia dalam mengambil keputusan [11]. Agar kemampuan DL semakin mumpuni maka DL menggunakan algoritma *artifical neural network* (ANN), yang terinspirasi dari jaringan biologis otak manusia [12]. Salah satu metode yang saat ini tren untuk mendeteksi *malware* adalah DL [13]. Beberapa metode DL yaitu *multilayer perceptron* (MLP), *convolutional neural network* (CNN), *recurrent neural network* (RNN), dan *deep neural networks* (DNN) [14]. Metode DL yang memiliki potensi untuk di terapkan dalam deteksi *malware* yaitu DNN, karena dapat mencapai akurasi tinggi dalam pengenalan pola [15].

Pada penelitian sebelumnya [16] melakukan deteksi *malware* android menggunakan teknik *machine learning* didapatkan hasil 139 panggilan sistem dari 3048 aplikasi (1795 jinak dan 1253 *malware*) serta memiliki akurasi sebesar 99%. Pada penelitian selanjutnya [17] untuk mendeteksi *malware* statis menggunakan DNN pada *portable executable* menunjukkan bahwa dalam situasi yang melibatkan data terstruktur, penggunaan *neural networks* masih bisa lebih efisien dibandingkan dengan *decision tree*. Hal yang sama juga di tunjukkan pada penelitian deteksi *malware android* menggunakan metode DNN di dapatkan hasil akurasi 99,38%, tingkat presisi 99,32% dan nilai sensitifitas 99,39% dari hasil tersebut menunjukkan bahwa metode yang di gunakan sangat efektif [18]. Metode DNN selain di gunakan untuk deteksi *malware* juga dapat digunakan pada objek lainnya, Pada penelitian yang menggunakan data diagnosis penyakit kelapa sawit dari Dinas Perkebunan Provinsi Jambi [19] menunjukkan hasil cukup baik dengan

nilai akurasi tertinggi 0,88. Selain itu penelitian menggunakan metode DNN dengan dataset *stroke prediction* [20] mendapatkan hasil akurasi 0,96, f1-*score* sebesar 0,9611 dan AUC sebesar 0,81.

Penelitian menggenai deteksi malware *trojan horse* menggunakan metode DL terutama metode *deep neural networks* dapat dilakukan [21]. Oleh karena itu, pada penelitian ini mengusulkan penelitian DETEKSI *MALWARE TROJAN HORSE* MENGGUNAKAN METODE *DEEP NEURAL NETWORKS*.

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang maka rumusan masalah pada penelitian ini :

1. Bagaimana menerapkan metode DNN untuk deteksi *malware trojan horse* ?
2. Bagaimana memilih fitur atau atribut yang digunakan untuk mengenal pola *malware trojan horse*?
3. Bagaimana kinerja dari deteksi *malware trojan horse* menggunakan metode 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*
3. Pengujian kinerja dilakukan dengan mengunakan nilai akurasi, nilai presisi, nilai *recall* dan F1-*score*

1.4 TUJUAN DAN MANFAAT PENELITIAN

1.4.1 TUJUAN

Adapun tujuan yang ingin dicapai pada penelitian ini adalah :

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

1.4.2 MANFAAT

Adapun manfaat yang diperoleh dalam penelitian ini adalah :

1. Memberikan informasi hasil deteksi *malware trojan horse* menggunakan metode DNN

2. Memberikan informasi tingkat keakurasian metode DNN dalam mendeteksi *malware trojan horse*

3. Penelitian ini diharapkan mampu memberikan informasi, wawasan dan pengetahuan mengenai deteksi *malware trojan horse* 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 trojan horse* 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 trojan horse* 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.