BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Internet of Things (IoT) telah membuat kemajuan yang signifikan dalam teknologi komunikasi dan informasi. Oleh karena itu, teknologi tersebut telah digunakan diberbagai industri penting untuk memberikan solusi yang hemat biaya, otomatis, berkelanjutan, dan cerdas [1]. Perangkat IoT memiliki kemampuan untuk berkomunikasi, bekerja sama, memproses, menganalisis dan mengirim data secara mandiri. Penerapan aplikasi dan sistem IoT mulai digunakan secara luas diberbagai bidang, seperti pemantauan kesehatan pribadi dan manajemen industri.

Fenomena ini menarik pihak-pihak yang tertarik untuk melakukan serangan *cyber* terhadap infrastruktur dan aplikasi IoT [2]. *Distributed Denial of Service* (DDoS) adalah salah satu dari berbagai teknik serangan yang digunakan oleh para peretas, yang mengambil keuntungan dari kelemahan dalam sebuah sistem. Salah satu kerentanannya adalah ketika peretas membanjiri sumber daya hingga mengakibatkan kesulitan bagi pengguna untuk mengakses layanan *web service*, serta membuat kinerja jaringan korban menjadi lambat [3]. Keamanan dalam implementasi IoT menjadi krusial untuk melindungi infrastruktur dan aplikasi dari serangan *cyber*.

Distributed Denial of Service (DDoS) merupakan serangan yang ditujukan untuk menggunakan sumber daya jaringan dan *bandwidth* yang tersedia hanya

untuk mencegah akses pengguna asli kejaringan target menjadi terbatas [4]. Salah satu serangan DDoS adalah *SYN Flood*, penyerang akan membanjiri server dengan sejumlah besar paket SYN, memaksanya untuk berulangkali merespon dengan paket SYN ACK. Akibat serangan ini, server tidak dapat menangani permintaan baru, dan sumber dayanya akan terus bertambah [5].

Intrusion Detection System (IDS) dapat digunakan untuk memonitor aliran data jaringan dari penyerang ancaman untuk mengidentifikasi serangan DDoS [6]. Metode baru dalam menerapkan IDS adalah *Deep Learning*, sebuah pendekatan ilmu komputer yang menggunakan teknik statistik untuk memberikan kemampuan pada sistem komputer untuk belajar dari data, salah satu jenis *Deep Learning* yang diterapkan sebagai IDS adalah *Deep Neural Network* (DNN). *Deep Neural Network* adalah jenis *Artificial Neural Network* yang terdiri dari beberapa lapisan yang memisahkan *input* dan *output* [7].

DNN sistem dapat menentukan operasi matematika yang sesuai untuk mengubah *input* menjadi *output*, baik itu berupa hubungan linear atau hubungan non-linear [7]. Kemampuan metode DNN yang mampu mengekstrak pola-pola yang kompleks dan menentukan operasi matematika yang tepat untuk mengubah *input* menjadi *output*, hal ini membuat metode DNN menjadi pilihan yang tepat dalam mendeteksi intrusi terhadap jaringan, termasuk untuk melindungi infrastruktur IoT dari serangan *cyber*. Dengan menggunakan metode DNN sebagai metode deteksi intrusi, perangkat IoT dapat lebih efektif dilindungi dari berbagai ancaman *cyber* yang terus berkembang, memastikan keberlangsungan dan keamanan sistem secara lebih optimal.

Pada penelitian [8], membahas mengenai penerapan *deep learning* dengan metode DNN untuk mendeteksi dan mengklasifikasi serangan DDoS pada jaringan *network*. Penelitian ini mengatakan bahwa penggunaan metode DNN lebih efektif untuk mendeteksi dan mengklasifikasikan serangan DDoS, pada dataset CICDDoS2019 yang di uji memperoleh hasil pengklasifikasian dengan tingkat akurasi sebesar 94,57%. Karena akurasi yang tinggi dalam analisis jaringan, penerapan metode DNN ke dalam sistem deteksi intrusi dan lapisan keamanan jaringan berbasis perangkat lunak seperti IoT merupakan pilihan yang tepat.

Selanjutnya pada penelitian [7], yang membahas ketidak pastian dalam menemukan jenis serangan dan meningkatkan kompleksitas serangan *cyber*, IDS memerlukan integritas DNN untuk memprediksi serangan pada *Network Intrusion Detection System* (N-IDS). Setelah melakukan uji coba pada dataset KDDCup-‘99’ dengan hasil *accuracy*, *precision*, *recall*, dan *f1-score* yang dibandingkan antar algoritma, didapat hasil bahwa DNN dengan 3 layer mengungguli dari semua algoritma *machine learning* yang lain. Hal ini dikarenakan kemampuan DNN untuk mengekstrak data dan fitur dengan abstraksi yang lebih tinggi dan non-linear menambah keunggulan dibandingan dengan algoritma lainnya.

Berdasarkan penjelasan diatas, penulis akan membahas bagaimana menerapkan *Deep Learning* dengan metode *Deep Neural Network* (DNN) untuk mendeteksi salah satu serangan *Distributed Denial of Service* (DDoS) yaitu *SYN Flood* pada jaringan IoT khususnya seranga *SYN Flood*.

1.2 RUMUSAN MASALAH

Berikut merupakan rumusan masalah pada penelitian ini:

1. Bagaimana menerapkan metode *Deep Neural Network* (DNN) untuk mendeteksi serangan *SYN Flood*?
2. Bagaimana mengetahui akurasi atau kinerja dari metode *Deep Neural Network* (DNN)?
3. Bagaimana mengetahui kelebihan dan kekurangan penerapan metode *Deep Neural Network* (DNN) dalam mendeteksi serangan *cyber*?

1.3 BATASAN MASALAH

Agar penelitian ini berjalan dengan baik, maka dibuatlah beberapa batasan penelitian sebagai berikut:

1. Dataset yang digunakan pada penelitian ini adalah CICIoT 2023
2. *Tools* yang digunakan dalam penelitian ini adalah *Google Colab*.
3. Metode yang digunakan untuk mendeteksi serangan *SYN Flood* adalah *Deep Neural Network* (DNN).
4. Pengujian tidak dilakukan pada lalu lintas jaringan *real-time*.
5. Tidak membahas tentang langkah pencegahan serangan tersebut.

1.4 TUJUAN DAN MANFAAT PENELITIAN

1.4.2 Tujuan Penelitian

Adapun tujuan penelitian adalah sebagai berikut:

1. Menerapkan IDS dengan menggunakan metode *Deep Neural Network* (DNN) pada jaringan IoT.
2. Mengulas kinerja metode DNN dalam mendeteksi serangan DDoS *SYN Flood*.
3. Mengetahui kelebihan dan kekurangan dari penerepan metode *Deep Neural Network* (DNN).

1.4.2 Manfaat Penelitian

Adapun manfaat penelitian adalah sebagai berikut:

1. Mampu membedakan antara data normal dan serangan pada protokol *SYN Flood*.
2. Dapat mengetahui efektivitas dari metode *Deep Neural Network* (DNN) dalam mendeteksi serangan DDoS *SYN Flood* pada jaringan IoT.
3. Sebagai sumber referensi bagi peneliti lain yang membahas mengenai serangan DDoS terutama serangan *SYN Flood*.

1.5 SISTEMATIKA PENULISAN

Dalam penelitian ini, untuk mendeskripsikan susunan bab-bab penelitian adalah sebagai berikut:

BAB I : PENDAHULUAN

Pada bab ini, berisi latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian serta sistematika penulisan mengenai pendekatan *Deep Neural Network* (DNN) dalam mendeteksi serangan DDoS *SYN Flood* pada jaringan *Internet of Things* (IoT).

BAB II : LANDASAN TEORI

Pada bab ini, berisi landasan teori yang diambil dari beberapa sumber penelitian, serta tinjauan literatur mengenai masalah penelitian yang berkaitan dengan penerapan metode *Deep Neural Network* (DNN) dalam mendeteksi serangan DDoS *SYN Flood* pada jaringan *Internet of Things* (IoT).

BAB III : METODOLOGI PENELITIAN

Pada bab ini, akan dijelaskan secara terperinci dan bertahap mengenai langkah-langkah yang diperlukan untuk membuat kerangka kerja dalam menyelesaikan penelitian tugas akhir ini.

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini, berisi hasil pengujian yang telah dilakukan, dimana data yang telah di uji akan dianalisis menggunakan metode yang digunakan dan hasilnya akan divalidasi.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini, berisi kesimpulan dan saran yang didapat dari hasil penelitian yang telah dilakukan.