BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Internet of things atau biasa dikenal dengan IoT merupakan sebuah konsep dimana sebuah objek dapat melakukan transfer data melalui jaringan tanpa perlu adanya interaksi dengan manusia. Dengan berkembangnya teknologi *internet of things* dalam waktu dekat akan menjadi hal yang biasa digunakan pada masa yang akan mendatang nanti [1]. Perkembangan *internet of things* (IoT) banyak diartikan dengan istilah *smart* diintegrasikan dengan infrastruktur yang sudah ada dan bersifat konvensional, seperti *smart city, smart health, smart transportation,* dan *smart home* [2].

Hadirnya *internet of things* memberikan kemudahan dan mempercepat proses interaksi antar manusia dengan objek, *internet of things* dapat di aplikasikan dalam berbagai bidang diantaranya bidang kesehatan, industri, otomotif dan lainnya [3]. Penerapan *internet of things* (IoT) dalam kehidupan sehari-hari misalnya sebuah *remote control* yang dapat memberitahukan kepada pemiliknya via pesan singkat mengenai pemakaian ac dirumahnya yang belum dimatikan saat pemiliknya sedang berpergian keluar rumah, contoh lainnya yaitu jika dirumah terjadi kebocoran gas maka pemilik rumah akan mendapatkan peringatan melalui pesan secara otomatis [4].

Namun dengan segala kemudahan yang diberikan oleh *internet of things* (IoT) seringkali mendapatkan serangan dikarenakan banyaknya perangkat yang terhubung pada jaringan internet dan saling terkoneksi antar satu sama lain sehingga membuat jaringan rentan terhadap serangan *cyber* seperti *phising*, *malware*, dan serangan *Distributed Denial-of-Service* (DDoS), serangan tersebut dapat merusak perangkat IoT, mengakses data pribadi yang tersimpan pada perangkat, dan bahkan dapat memanfaatkan kelemahan keamanan dari perangkat sehingga dapat mengakses ke jaringan yang lain [5].

Distributed Denial-Of-Service (DDoS) merupakan serangan yang mampu melumpuhkan *server* dengan membanjiri lalu lintas jaringan yang mengakibatkan jaringan menjadi *down* [6]. Salah satu jenis serangan *Distributed Denial-of-Service* (DDoS) adalah *UDP Flood*, *UDP Flood* dapat menyebabkan sebuah komputer *server* menjadi *eror* akibat dari banyaknya paket yang diterima oleh komputer *server*. *UDP Flood* akan melakukan pengiriman karakter yang akan menguji jaringan sehingga akan terjadi aliran data yang tidak diperlukan pada jaringan korban [7].

Untuk melakukan deteksi terhadap serangan *Distributed Denial-Of-Service* (DDoS) yang terjadi dapat menggunakan sebuah sistem yaitu *Intrusion Detection System* (IDS) yang berfungsi untuk melakukan pengamatan kegiatan yang mencurigakan pada jaringan [8]. Metode yang baru dalam mengkombinasikan IDS untuk melakukan deteksi yaitu menggunakan pendekatan *deep learning*, metode pembelajaran mesin yang menggabungkan jaringan saraf tiruan dengan

meniru cara kerja otak manusia serta algoritma yang digunakan terinspirasi dari struktur otak manusia [9] [10].

Pada penelitian [11] membahas tentang pengembangan sistem deteksi serangan pada *cloud computing* dimana *cloud computing* juga rentan terhadap serangan *Distributed Denial-Of-Service* (DDoS), penelitian menggunakan dataset KDDCup 99 dan menggunakan metode *Deep Learning* yaitu *Recurrent Neural Network* (RNN) dengan hasil akurasi 94,12%. RNN menjadi akurasi terbaik dibanding metode lainnya.

Selanjutnya pada penelitian [12] membahas tentang serangan *malware* dengan menggunakan *recurrent neural network* dan menggunakan data *malware* dan *non-malware* sebanyak 215 menghasilkan akurasi sebesar 86% dan *f1 score* sebesar 85%.

Pada penelitian ini menggunakan *Deep Learning* metode *Recurrent Neural Network, Recurrent Neural Network* (RNN) memiliki akurasi yang tinggi, serta permodelan yang kuat untuk melakukan deteksi serta kinerja dari metode ini lebih unggul [13]. *Recurrent Neural Network* (RNN) memiliki kelebihan yaitu dapat melakukan proses data secara berulang-ulang membentuk *time series*, setiap keluaran atau *output* dari *hidden layer* akan mengalami perulangan sehingga menghasilkan *output* yang akurat [14]. Maka dari uraian permasalahan diatas akan dilakukan penelitian tentang Deteksi Serangan DDoS *UDP Flood* pada jaringan IoT menggunakan *Recurrent Neural Network*.

1.2 RUMUSAN MASALAH

Berdasarkan uraian yang telah dijelaskan pada latar belakang, maka rumusan masalah pada penelitian ini adalah:

1. Bagaimana mengenali pola serangan *UDP Flood* pada jaringan IoT?
2. Bagaimana menerapkan metode *Recurrent Neural Network* pada deteksi serangan *UDP Flood*?
3. Bagaimana nilai performa pada deteksi serangan *UDP Flood* menggunakan metode *Recurrent Neural Network*?

1.3 BATASAN MASALAH

Adapun agar penelitian ini lebih terarah maka penulis menetapkan batasan masalah pada penelitian ini:

1. *Dataset* yang digunakan pada penelitian ini adalah CICIoT2023
2. *Tools* yang digunakan dalam penelitian ini adalah Google Colab
3. Pengujian performa yang digunakan pada penelitian ini menggunakan *confusion matrix*
4. Jenis serangan yang di deteksi adalah serangan *UDP Flood* pada jaringan IoT

1.4 TUJUAN DAN MANFAAT PENELITIAN

1.4.1 Tujuan Penelitian

Adapun tujuan dari dilakukan penelitian ini adalah sebagai berikut:

1. Untuk mengenali pola serangan *UDP Flood* pada jaringan IoT
2. Menerapkan metode *Recurrent Neural Network* (RNN) untuk mendeteksi serangan *UDP Flood*

3. Mengukur kinerja dari sistem deteksi serangan *UDP Flood* menggunakan *Recurrent Neural Network* (RNN)

1.4.2 Manfaat Penelitian

Adapun manfaat dari dilakukan penelitian ini sebagai berikut:

1. Dapat mengetahui pola serangan *UDP Flood* dengan menggunakan algoritma *Deep Learning* yaitu *Recurrent Neural Network* (RNN)
2. Mengetahui nilai performa dari metode *Recurrent Neural Network* (RNN) dalam mendeteksi serangan *UDP Flood* pada jaringan IoT
3. Menambah pengetahuan penulis mengenai deteksi serangan jaringan IoT menggunakan *Recurrent Neural Network* (RNN)

1.5 SISTEMATIKA PENULISAN

Berikut penyajian sistematika penulisan dari penelitian ini agar mempermudah dalam memahami penulisan laporan:

BAB I : PENDAHULUAN

Pada bab ini memuat tentang uraian latar belakang permasalahan, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, dan juga sistematika penulisan pada laporan.

BAB II : LANDASAN TEORI

Pada bab ini berisikan mengenai kajian-kajian dan konsep umum mengenai IoT, *Deep Learning*, Serangan Jaringan, dan lain-lain sebagai pendukung proses penelitian yang bersumber dari jurnal, buku dan sumber lainnya.

BAB III : METODOLOGI PENELITIAN

Pada bab ini berisikan pembahasan tentang kerangka kerja penelitian, pengumpulan data, rancangan eksperimen, dan alat bantu yang digunakan dalam penelitian.

BAB IV : DETEKSI SERANGAN DAN PENGUJIAN

Pada bab ini dilakukan pengujian menggunakan *tools* Google Colab terhadap serangan *UDP Flood* menggunakan metode *Deep Learning*, dan melakukan perhitungan performa dari metode yang digunakan.

BAB V : PENUTUP

Pada bab ini berisikan kesimpulan dan saran dari penelitian yang telah dijalankan.