BAB 1

PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan teknologi di era digital saat ini mengalami kemajuan yang cepat. Sehingga pada perkembangan teknologi tersebut khusunya internet dengan segala fungsinya seperti *surfing, browsing, email,* Penyimpanan *cloud* telah menjadi kebutuhan penting bagi berbagai kalangan [1]. Kehadiran internet inilah yang memberikan perubahan yang signifikan bagi kehidupan manusia dalam menjalankan berbagai aktivitas-nya sehari-hari [2]. Salah satu aspek yang menonjol adalah *Internet of Things* (IoT), sebuah teknologi jaringan internet yang tengah berkembang pesat pada saat ini [3]. IoT merupakan sebuah konsep suatu obyek cerdas yang mampu mengirim informasi melalui jaringan tanpa perlunya bantuan manusia. Selain itu, IoT juga memiliki keahlian untuk menghubungkan berbagai objek pintar, memungkinkan interaksi dengan lingkungan sekitar serta perangkat komputasi cerdas lainnya melalui internet [4].

Namun, aspek keamanan pada jaringan IoT ini seringkali menjadi target dalam Serangan Cyber yang mengancam privasi dan keamanan pengguna [5]. Hal ini dikarenakan banyaknya perangkat yang terhubung ke internet dan saling terkoneksi satu sama lain pada jaringan IoT yang kompleks, sehingga membuat jaringan IoT tersebut rentan terhadap serangan cyber [6]. Pelaku kejahatan cyber melakukan

berbagai langkah untuk mengakses sebanyak mungkin informasi dari target, dan salah satu metodenya adalah serangan DDoS [7].

Serangan DDoS merupakan tipe serangan yang terstruktur dan mampu menghentikan kinerja server dengan cara mengalirkan lalu lintas jaringan secara berlebihan, sehingga mengakibatkan jaringan tersebut *down* [8]. Terdapat beberapa varian serangan *Distributive Denial of Service* (DDoS) yang melibatkan berbagai metode, seperti serangan ACK dan SYN *Flood*, *amplifikasi Domain Name Server* (DNS), *amplifikasi Network Time Protocol* (NTP), UDP *fragment*, UDP *Flood*, HTTP *Flood*, ICMP *Flood*, dan serangan DDoS *Zero-Day* [9].

HTTP Flood adalah jenis serangan pada lapisan aplikasi yang memiliki karakteristik yang relatif sederhana, dimana serangan ini menargetkan *server website* dan membanjiri server tersebut dengan permintaan *HTTP* untuk menjatuhkan server tersebut [10]. Sehingga, upaya yang dapat dilakukan dalam pencegahan terjadinya serangan *DDos* dengan cara mengimplementasikan metode *Intrusion Detection System* (IDS) dalam pengamanan jaringan [11].

IDS merupakan suatu sistem yang digunakan untuk mengidentifikasi kehadiran *intruder* pada sebuah sistem dengan memantau lalu lintas jaringan secara langsung [12]. IDS akan memberikan peringatan ketika mendeteksi aktivitas yang dianggap mencurigakan atau tindakan ilegal. Namun, IDS memiliki kekurangan yaitu hanya mendeteksi suatu serangan tanpa melakukan pencegahan dan mengatasi terjadinya serangan [13]. Untuk dapat mendeteksi kapan terjadinya *anomali trafik*, IDS membutuhkan suatu metode. Terdapat beragam pendekatan yang dapat diterapkan, dan

salah satunya adalah menggunakan teknik *deep learninig* [14]. *Deep Learning* sendiri merupakan bagian dari *Neural Network* yang merupakan tipe dari suatu proses *machine learning* dengan arsitektur yang lebih kompleks, melibatkan jumlah layer yang lebih banyak. Hal ini memungkinkan *Deep Learning* untuk menangani permasalahan yang lebih rumit dan memproses data dengan volume yang lebih besar. [15].

Pada penelitian [16] memaparkan metode yang efektif untuk mendeteksi serangan jaringan yaitu menggunakan metode LSTM- RNN untuk mendeteksi serangan pada dataset *NSL-KDD,* sehingga didapatkan hasil mencapai tingkat akurasi yang memuaskan, meskipun masih terdapat peluang untuk meningkatkan performa lebih lanjut.

Kemudian Pada penelitian [17], diuraikan sebuah pola untuk mendeteksi serangan SSH dan FTP *brute-force* yang menggunakan pendekatan *Machine Learning* dengan menerapkan algoritma LSTM. Penelitian ini memanfaatkan dataset *CIC-IDS-2017*. Setelah dilakukan pengujian, ditemukan bahwa pendeteksian serangan *Brute-force* mencapai akurasi tertinggi dengan penerapan fungsi aktivasi TANH (*tangen hiperbolik*) dan menggunakan fungsi optimasi *categorical crossentropy*, yang menghasilkan tingkat akurasi sebesar 99,88%.

Dan pada penelitian [18], dibahas tentang penerapan pendekatan *Deep Learning* untuk mendeteksi serangan *SSH-Brute Force* pada dataset *CIC-IDS 2018*. Hasil eksperimen menunjukkan bahwa *Convolutional Neural Network* (CNN) menunjukkan kinerja lebih unggul dibandingkan dengan metode *Deep Learning* lainnya, yaitu *Naïve Bayes, Logistic Regression, Decision Tree, k-Nearest Neighbor*, dan *Support Vector*

Machine. CNN mencapai akurasi sebesar 94,3%, tingkat presisi sebesar 92,5%, tingkat *recall* sebesar 97,8%, dan *F1-score* sebesar 91,8% dalam mengidentifikasi serangan SSH-Brute Force.

Pada penelitian ini mengusulkan menggunakan algoritma LSTM untuk mendeteksi serangan *HTTP Flood* pada jaringan IoT. Algoritma LSTM adalah salah satu varian arsitektur dari algoritma RNN yang sering diterapkan dalam konteks masalah yang terkait dengan *deep learning* [19]. Algoritma ini terbukti sangat efektif untuk tugas-tugas seperti klasifikasi, pemrosesan, dan prediksi berdasarkan data *time series*, terutama ketika ada ketidakpastian terkait durasi antar peristiwa penting dalam rangkaian waktu [20]. LSTM memiliki cell state, yang berfungsi sebagai mekanisme penyimpanan informasi baik dalam jangka waktu yang panjang maupun singkat. Metode ini juga melibatkan blok memori yang menentukan nilai mana yang akan dianggap sebagai keluaran yang relevan berdasarkan pada masukan yang diberikan. Keunggulan utama dari LSTM terletak pada kemampuannya untuk mengelola informasi jangka panjang, menjadikannya lebih efektif dalam menangani ketergantungan temporal yang kompleks dalam data time series atau urutan peristiwa. [21].

Berdasarkan berbagai penjelasan dari penelitian yang telah dipaparkan, peneliti mengusulkan untuk melakukan penelitian tentang Deteksi Serangan *HTTP Flood* pada Jaringan IoT dengan menggunakan *Long Short-Term Memory Network* (LSTM). Tujuan utama dari penerapan metode LSTM ini adalah untuk mencapai hasil deteksi serangan *HTTP Flood* yang optimal. Kualitas hasil deteksi ini akan tergantung pada

tingkat akurasi algoritma, di mana peneliti berharap dapat menghasilkan metode yang memberikan tingkat kesalahan yang rendah.

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang tersebut, rumusan masalah yang dapat diformulasikan pada penelitian ini adalah:

1. Bagaimana menentukan fitur yang relevan untuk mendeteksi serangan DDoS *HTTP Flood*?
2. Bagaimana mendeteksi serangan *HTTP Flood* menggunakan metode LSTM?
3. Bagaimana Kinerja LSTM dalam mendeteksi serangan *HTTP Flood*?

1.3 BATASAN MASALAH

Berikut merupakan beberapa batasan masalah yang dapat diuraikan pada penelitian ini, antara lain:

1. Algoritma yang digunakan hanya berfokus untuk mendeteksi serangan *HTTP Flood.*
2. Menggunakan dataset *CIC-IOT_Dataset2023.*
3. Menggunakan *tools Google Colaboratory* dengan bahasa pemograman *Phyton.*
4. Tidak membahas bagaimana cara mencegah serangan *HTTP Flood* pada jaringan *Interner of Things* (IoT).

1.4 TUJUAN DAN MANFAAT PENELITIAN

1.4.1 Tujuan Penelitian

Tujuan dari penelitian ini, yaitu antara lain:

1. Menerapkan LSTM untuk mendeteksi serangan DDoS HTTP *Flood* pada jaringan IoT.
2. Melakukan seleksi fitur berbasis *SelectKBest* untuk mengidentifikasi fitur-fitur penting dalam proses deteksi serangan *HTTP Flood*.
3. Mengukur hasil kinerja dari LSTM dalam mendeteksi serangan *HTTP Flood*.

1.4.2 Manfaat Penelitian

Untuk manfaat dari penulisan penelitian ini, yaitu :

1. Sebagai referensi untuk membangun IDS yang lebih baik kedepannya dalam mendeteksi serangan DDoS *HTTP Flood*.
2. Memperoleh kinerja optimal terbaik pada proses deteksi menggunakan algoritma *Long Short Term Memory (LSTM).*
3. Sebagai acuan atau referensi untuk peneliti lainnya yang ingin melakukan penelitian mengenai serangan *DDoS HTTP Flood.*

1.5 SISTEMATIKA PENULISAN

Sistematika penulisan penelitian tugas akhir dapat disusun sebagai berikut:

BAB I : PENDAHULUAN

Bab ini menguraikan tentang latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan juga tatacara penulisam penelitian.

BAB II : TINJAUAN PUSTAKA

Bab ini memberikan penjelasan konsep dasar mengenai *LSTM, DDoS HTTP Flood*, dan teori-teori terkait lainnya yang berkaitan dengan penelitian ini.

BAB III : METODOLOGI

Bab ini mencakup tentang pengumpulan data, prosedur penelitian, dan metode analisis yang terdiri dari pendekatan penyelesaian masalah. Informasi ini bertujuan sebagai pendukung dalam pelaksanaan penelitian.

BAB IV : HASIL DAN ANALISIS

Bab ini memaparkan proses penelitian seperti penginputan data, analisis data, normalisasi data, testing dataset, validasi hasil data training dan data testing, alat

dan bahan yang akan digunakan pada peoses penelitian, serta hasil akhir dari penelitian tersebut.

BAB V : PENUTUP

Bab ini memuat rangkuman kesimpulan dari hasil penelitian serta saran yang membangun untuk penelitian yang akan dating.