1. Pendahuluan

1.1 Latar Belakang

Jaringan komputer merupakan hal yang kompleks dan sulit untuk dikelola. Hal ini terjadi karena banyaknya perangkat yang digunakan pada jaringan [5]. Selain itu, perangkat pada jaringan tradisional memiliki desain, perangkat lunak, dan perangkat keras yang terkait dengan satu vendor. Setiap vendor memiliki desain dan perangkat yang berbeda [17]. Untuk mengatasi kompleksitas tersebut, diusulkan teknik Software Defined Network (SDN) [5]. SDN memiliki karakteristik yang berbeda jika dibandingkan dengan jaringan tradisional yaitu pemisahan control plane dan data plane dari perangkat jaringan [5, 17]. SDN menerapkan konsep sentralisasi pada arsitektur jaringannya seperti jaringan tradisional. Namun, itu membuat jaringan arsitektur SDN rentan terhadap serangan cyber [9]. Ada tiga jenis serangan yang menargetkan jaringan SDN. Ini adalah serangan penipuan, serangan intrusi, dan serangan perusakan berbahaya [13]. Salah satu serangan terhadap jaringan SDN adalah Denial of Services; kerentanan ini disebabkan oleh arsitektur SDN [11].

Denial of Services atau biasa dikenal dengan DoS adalah kejahatan dunia maya dengan metode pengiriman paket secara berlebihan dan bertujuan untuk mengeksploitasi sumber daya jaringan [8]. Pemisahan bidang kontrol dan data menyebabkan serangan DoS di SDN [11]. Penyerang memanfaatkan control plane dan data plane [15], sehingga akan mengganggu flow rule decision dan juga dapat mengakibatkan terjadinya bottleneck pada jaringan. Ini bisa berbahaya jika ada kegagalan pada komponen jaringan [4]. Ada dua jenis serangan DoS, yaitu serangan volumetrik seperti ICMP-Flood, UDP-Flood, dan TCP-SYN Flood, dan serangan *application layer* [4, 16, 18], untuk mencegah serangan DoS dapat dibuatnya *Intrusion Detection System* (IDS) [20], IDS nantinya dapat berbasiskan *anomaly-based* dan *signature-based*. Namun kedua metode ini memiliki kekurangan jika diterapkan secara tradisional [21], terkait dengan kemampuan adaptasi dan skenario yang berbeda, oleh karena itu masalah ini dapat diselesaikan dengan menerapkan Machine-Learning . Pada tugas akhir ini diusulkan LSTM-NB, kombinasi dari algoritma Long Short-Term Memory (LSTM) dan Naive Bayes (NB), untuk memecahkan masalah ini.

Tabel 1. Akurasi beberapa metode

Asal Paper	Akurasi dan Metode	Dataset Digunakan
Musumeci et al. [9]	SVM (97%), KNN (97%), **RandomForest(98%)**	Dataset Pribadi
Tang et al. [17]	**GRU-RNN (89%)**, RNN (44.39%), DNN (75.9%), NBtree (82.2%), dan SVM (69.52%)	NSL-KDD dan CICIDS2017
Ahuja et al [2]	CNN (98%), LSTM(95%), **CNN-LSTM (99%)**, SVC-SOM (95%), dan SAE-MLP (99%)	SDN-DL

Selain itu dilakukan pula evaluasi dengan membandingkan performansi dari sistem yang diusulkan dengan algoritma lainnya, diantaranya dapat dilihat pada tabel 1, untuk dataset yang digunakan untuk evaluasi akan menggunakan dataset SDN-DL[1], CICIDS2017, dan NSL-KDD[2]. selain evaluasi tersebut akan dilakukan evaluasi menggunakan data yang berasal dari simulasi menggunakan Hping3 dan Iperf3 pada simulasi P4-Mininet.

1.2 Topik dan Batasannya

Rumusan masalah yang menjadi dasar dari tugas akhir ini, karena saat ini IDS tradisional dan penggunaan IDS berbasiskan *Shallow Learning* masih memiliki keterbatasan, keterbatasan ini baik dari sisi akurasi dan kedinamisan model (tidak perlu *retrain* model berkali-kali). Sehingga permasalahan tersebut akan diselesaikan dengan menggunakan *Deep Learning*, yaitu dengan metode LSTM yang dikombinasikan dengan Naive Bayes (BA). Untuk pengerjaan tugas akhir ini akan menggunakan NSL-KDD, CICIDS 2017 [17] dan SDN-DL [10] ketiga dataset ini digunakan untuk melakukan perhitungan performansi, selanjutnya nanti akan diterapkan pada simulasi menggunakan Mininet dengan Dataplane P4.

1.3 Tujuan

Tujuan dari penelitian ini adalah untuk meningkatkan keamanan jaringan dari serangan DoS, hal ini dicapai dengan menggunakan Algoritma LSTM-NB, selain itu dibuat juga simulasi jaringan menggunakan P4-Mininet. Keterkaitan antara tujuan, pengujian, dan kesimpulan dapat dilihat pada Tabel 2

Tabel 2. Keterkaitan antara tujuan, pengujian dan kesimpulan

No	Tujuan	Pengujian	Kesimpulan
1	Meningkatkan Keamanan Jaringan SDN dari Serangan DoS menggunakan Algoritma LSTM-NB	Algoritma LSTM-NB dapat melakukan deteksi serangan DoS, evaluasi yang dilakukan akan menggunakan dataset yang sudah disediakan yaitu NSL-KDD, CICIDS2017, dan SDN-DL	Algoritma LSTM-NB memiliki akurasi 98% pada Dataset NSL-KDD dengan nilai FNR 1.5%, 96% pada Dataset CICIDS2017 dengan nilai FNR 2.3%, dan pada dataset SDN-DL memiliki akurasi 89% dengan nilai FNR 13%
2	Melakukan Simulasi Menggunakan P4-Mininet	Algoritma LSTM-NB dapat melakukan deteksi pada jaringan SDN yang dibangun dengan menggunakan P4-Mininet	Sistem dapat melakukan deteksi ketika dilakukan simulasi dengan data yang dibuat menggunakan Iperf3 dan Hping3, untuk metode yang digunakan dapat menyiapkan data terlebih dahulu atau dapat membuat sistem \textit{realtime} untuk melakukan klasifikasi paket yang masuk

[1] https://data.mendeley.com/datasets/jxpfjc64kr/1
[2] http://www.di.uniba.it/ andresini/datasets.html

1.4 Organisasi Tulisan

Pada jurnal tugas akhir ini akan memiliki organisasi tulisan sebagai berikut. Bab 1 akan membahas mengenai pendahuluan yang akan berisi latar belakang, topik dan batasan, tujuan dan organisasi tulisan dari jurnal tugas akhir. Bab 2 akan membahas mengenai dasar atau kajian teori yang mendukung pengerjaan dan penulisan tugas akhir. Bab 3 akan menjelaskan mengenai sistem yang akan dibangun, rencana evaluasi, dan metode evaluasi yang akan digunakan. Bab 4 akan berisi hasil evaluasi yang sudah dilakukan dan menjelaskan apa yang menjadi tujuan dari penelitian ini. Di akhir jurnal ini akan terdapat Bab 5 dimana didalamnya akan berisi kesimpulan dari kegiatan penelitian yang dilakukan.