Deteksi Serangan DoS Pada Jaringan SDN Berbasis P4 Programmable Dataplane menggunakan Machine Learning

Sya Raihan Heggi[1], Parman Sukarno[2], Satria Akbar Mugitama

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]heggiraihan@students.telkomuniversity.ac.id, [2]psukarno@telkomuniversity.ac.id,
[3]satriamugitama@telkomuniversity.ac.id

Abstrak

Pada Tugas Akhir ini mengusulkan penggunaan LSTM-NB, LSTM-NB adalah kombinasi dari dua buat algoritma yaitu Long Short-Term Memory (LSTM) dan Naive Bayes (NB), algoritma ini akan digunakan untuk mendeteksi serangan Denial-of-Service (D0S) pada Programming Protocol-Independent Packet Processor (P4) Language-based Software Defined Network (SDN). Implementasi SDN saat ini semakin populer. Namun, didalam arsitektur SDN ini terdapat aspek yang kritis, salah satunya adalah rentan terhadap serangan DoS yang menyebabkan jaringan kehilangan prinsip CIA Triangle. Saat ini sudah beberapa penelitian yang melakukan pencegahan dari serangan. Namun, ancaman serangan DoS masih ada. Metode yang diusulkan menghasilkan akurasi 88% pada dataset SDN-DL, 98% pada NSL-KDD, dan 96% pada CICIDS2017 dengan nilai FNR 1-2%, selain pengujian menggunakan dataset dilakukan pengujian menggunakan data berdasarkan simulasi Iperf3 dan Hping3. Metode yang diusulkan akan di bandingkan dengan metode *machine-learning* dan *deep-learning* lainnya, berdasarkan evaluasi yang ekstensif, dapat disimpulkan metode yang diusulkan menunjukkan potensi kuat untuk melakukan deteksi serangan DoS di lingkungan SDN.

Kata kunci : Computer Network Security, Intrusion Detection System (IDS), Machine Learning, Deep Learning, Denial of Service (DoS)