INTISARI

ANALISIS KINERJA KLASIFIKASI SERANGAN DDOS PADA SOFTWARE DEFINED NETWORK MENGGUNAKAN ALGORITMA SUPPORT VECTOR MACHINE, RANDOM FOREST, DAN EXTREME GRADIENT BOOSTING DENGAN MEMANFAATKAN SFLOW PROTOCOL

Oleh

Nadhir Fachrul Rozam

20/466425/PPA/05991

Software Defined Network (SDN) merupakan paradigma baru dalam jaringan komputer. Teknologi SDN dengan kontrol terpusat menjadikannya lebih rentan terhadap serangan *Distributed Denial of Service (DDOS).* Ketika jaringan SDN mendapatkan serangan DDOS, baik pada *Control Plane* dan *Data Plane* akan mengalami kekurangan sumber daya. Hal tersebut apabila tidak dideteksi lebih awal dapat mengakibatkan jaringan SDN gagal bekerja. Memanfaatkan kemampuan sFlow Protocol untuk melakukan *capture traffic flow* secara *realtime*, data yang dihasilkan dari sFlow disimpan pada Prometheus untuk selanjutnya dapat dilakukan klasifikasi serangan DDOS.

Terdapat tiga algoritma yang digunakan yaitu Support Vector Machine (SVM), Random Forest dan Extreme Gradient Boosting (XGBoost). Dataset diambil dari Prometheus sebagai *timeseries database* yang dapat mengambil data dari sFlow Collector. Terdapat 4 dataset yang digunakan. Dataset 1 dan 2 dengan jumlah data 6109, masing-masing terbagi dalam 2 kelas dan 3 kelas. Dataset 3 dan 4 dengan jumlah data 400488 masing-masing terbagi dalam 2 dan 3 kelas. Pengujian dilakukan dengan melakukan perhitungan *accuracy, precision, recall, F1-score* menggunakan *test set* dari dataset dan data *realtime traffic*.

Berdasarkan skenario pengujian yang dilakukan, Dataset 4 dengan 3 kelas mendapatkan hasil paling optimal untuk setiap algoritma. Menggunakan Dataset 4 untuk masing-masing *accuracy, precision, recall* dan *F1-score* algoritma XGBoost mendapatkan 99,84%, 99,86%, 99,87% dan 99.86%, Random Forest mendapatkan 99.81%, 99.83%, 99.85% dan 99.84%, dan SVM mendapatkan 99.48%, 99.52%, 99.56% dan 99.54%. Sementara selisih pengujian *realtime traffic* dengan dataset test paling tinggi 0,40%. Hasil tersebut menjadikan ketiga algoritma memiliki kinerja optimal dengan Dataset 4 dan juga terbukti konsisten untuk diterapkan sebagai langkah awal mengatasi serangan DDOS.

Kata Kunci: Software Defined Network, sFlow, Distributed Denial of Service, Support Vector Machine, Random Forest dan Extreme Gradient Boosting.

ABSTRACT

CLASSIFICATION PERFORMANCE ANALYSIS ON SOFTWARE-DEFINED NETWORK DDOS ATTACK USING SUPPORT VECTOR MACHINE, RANDOM FOREST, AND EXTREME GRADIENT BOOSTING ALGORITHMS WITH UTILIZING THE SFLOW PROTOCOL

By

Nadhir Fachrul Rozam

20/466425/PPA/05991

Software Defined Network (SDN) is a new paradigm in computer networking. SDN technology with centralized control makes it more vulnerable to Distributed Denial of Service (DDOS) attacks. When a Software Defined Network overwhelms by DDOS attack, both Control Plane and Data Plane will lack resources. If this is not detected early, it can cause the SDN network to fail to work. Utilizing the ability of the sFlow Protocol to capture traffic flow in real time, the data generated from sFlow is stored in Prometheus for further classification of DDOS attacks.

There are three algorithms used, namely Support Vector Machine (SVM), Random Forest and Extreme Gradient Boosting (XGBoost). The dataset is taken from Prometheus as a time series database that can retrieve data from the sFlow Collector. There are 4 datasets used. Datasets 1 and 2 with a total of 6109 data, each divided into 2 classes and 3 classes. Datasets 3 and 4 with a total data of 400488 are divided into 2 and 3 classes, respectively. The test is carried out by calculating accuracy, precision, recall, F1-score using a test set from the dataset and realtime traffic data.

Based on the results of the test scenario, Dataset 4 with 3 classes has the most optimal results for each algorithm. Using Dataset 4 for accuracy, precision, recall and F1-score, XGBoost algorithm got 99.84%, 99.86%, 99.87% and 99.86%, Random Forest got 99.81%, 99.83%, 99.85% and 99.84%, and SVM got 99.48% , 99.52%, 99.56% and 99.54% respectively. Meanwhile, the highest difference between the realtime traffic test and the dataset test is 0.40%. These results make the three algorithms have optimal performance with Dataset 4 and are proven consistent to be applied as a first step to overcome DDOS attacks.

Keywords: Software Defined Network, sFlow, Distributed Denial of Service, Support Vector Machine, Random Forest dan Extreme Gradient Boosting.