INTISARI

PENDETEKSIAN SERANGAN DDoS PADA *SOFTWARE-DEFINED NETWORK* MENGGUNAKAN ALGORITMA *RANDOM FOREST* DENGAN MEMANFAATKAN PROTOKOL SFLOW

Software-Defined Network merupakan paradigma baru dalam jaringan komputer, yaitu dengan memisahkan antara C*ontrol Plane* dan *Data Plane*. Namun hal tersebut juga dapat menjadi kerentanan tersendiri apabila antara *Control Plane (controller)* dan *Data Plane (switch)* tidak dapat saling terhubung. Serangan jaringan yang bisa dilakukan agar komunikasi antara *controller* dan *switch* dapat digagalkan yaitu *Distributed Denial of Service (*DDoS*).*

Sebagai langkah awal mengatasi serangan tersebut, pada proyek akhir ini diterapkan *Machine Learning* dengan menggunakan Algoritma Klasifikasi *Random Forest* untuk membuat sistem deteksi intrusi. Pada *Machine Learning* tersebut dilakakukan *train dataset* berupa trafik normal (*benign traffic*) dan trafik serangan DDoS (*attack traffic*). *Dataset* yang dipilih sebagai *data training* yaitu CSE-CIC-IDS2018 yang memiliki data karakteristik trafik serangan DDoS maupun trafik normal (*benign traffic*) lebih relevan untuk digunakan sekarang. Dengan memanfaatkan sFlow yang dapat melakukan monitor *flow* trafik secara *realtime*, *machine learning* yang telah dilakukan *training* diterapkan untuk melakukan klasifikasi trafik pada saat itu apakah terdapat serangan DDoS atau tidak.

Kata Kunci: *Software-Defined Network, DDoS, Machine Learning, Random Forest, SFlow.*

ABSTRACT

DDOS ATTACK DETECTION IN SOFTWARE-DEFINED NETWORK USING RANDOM FOREST ALGORITHM WITH UTILIZING SFLOW PROTOCOL

Software-Defined Network is a new paradigm in computer networks by separating Control Plane and Data Plane. But this can also be a vulnerability when the Control Plane (Controller) and Data Plane (Switch) not connected each other. Network attack that can disconnect the controller and switch connection is Distributed Denial of Service (DDoS).

As a first step to overcome this attack, Machine Learning is applied by using the Random Forest Classification Algorithm to create an intrusion detection system. The machine learning is trained with benign traffic data and DDoS attacks data. The dataset that is used as training data is CSE-CIC-IDS2018 which has more relevant traffic characteristic data on DDoS attacks and benign traffic for use today. By utilizing sFlow, which can monitor real-time traffic flow, machine learning used to classify traffic whether is a DDoS attack or not.

Keywords: software-defined network, DDoS, machine learning, random forest, sflow.