ABSTRAK

Nama : *Raihan Putra Kurniawan*

Program Studi : *Teknik Informatika*

Judul : *RANCANG BANGUN SISTEM DETEKSI SERANGAN DISTRIBUTED DENIAL OF SERVICE BERBASIS MACHINE LEARNING*

Serangan *Distributed Denial of Service* (DDoS) merupakan ancaman serius dalam keamanan jaringan, terutama pada lingkungan *Software Defined Networking* (SDN). Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem deteksi serangan DDoS berbasis machine learning yang efektif. Sistem ini menggunakan berbagai algoritma machine learning, termasuk Random Forest, Naïve Bayes, dan Neural Networks, untuk mendeteksi pola lalu lintas jaringan yang mencurigakan. Pengujian dilakukan melalui dua metode: pertama, menggunakan aplikasi Streamlit yang menyediakan antarmuka visual, dan kedua, melalui simulasi menggunakan *Ryu Controller* dan *Mininet* untuk evaluasi dalam kondisi jaringan nyata. Hasil pengujian menunjukkan bahwa metode pertama dengan Streamlit menghasilkan akurasi yang baik dalam mendeteksi serangan *DDoS.* Namun, metode kedua menggunakan Ryu dan Mininet menghasilkan banyak *false positive*, menunjukkan adanya tantangan dalam penerapan model di lingkungan jaringan yang lebih kompleks. Pengembangan lebih lanjut diperlukan untuk mengatasi masalah ini, termasuk perbaikan pada pemilihan fitur, pengelolaan kompleksitas model, dan peningkatan representasi dataset. Sistem ini memiliki potensi signifikan dalam meningkatkan keamanan jaringan melalui deteksi dini terhadap serangan DDoS dengan penyesuaian yang tepat.

Kata Kunci: DDoS, Deteksi, Machine Learning, SDN, Streamlit, Ryu, Mininet, False Positive

ABSTRACT

Name : *Raihan Putra Kurniawan*

Study Program : *Teknik Informatika*

Title : *DESIGN AND DEVELOPMENT OF A MACHINE LEARNING-BASED DISTRIBUTED DENIAL OF SERVICE ATTACK DETECTION SYSTEM*

Distributed Denial of Service (DDoS) attacks are a serious threat to network security, particularly in Software Defined Networking (SDN) environments. This research aims to design and implement an effective DDoS attack detection system based on machine learning. The system utilizes various machine learning algorithms, including Random Forest, Naïve Bayes, and Neural Networks, to detect suspicious network traffic patterns. Testing was conducted using two methods: first, through the Streamlit application, which provides a visual interface, and second, through simulations using the Ryu Controller and Mininet for evaluation in a more realistic network environment. The testing results show that the first method, using Streamlit, achieved good accuracy in detecting DDoS attacks. However, the second method, using Ryu and Mininet, resulted in many false positives, indicating challenges in applying the model in more complex network environments. Further development is needed to address these issues, including improvements in feature selection, model complexity management, and dataset representation. With the appropriate adjustments, this system holds significant potential for enhancing network security through early detection of DDoS attacks.

Keywords: *DDoS, Detection, Machine Learning, SDN, Streamlit, Ryu, Mininet, False Positive*