IMPLEMENTASI MACHINE LEARNING UNTUK DETEKSI SERANGAN DDOS PADA ARSITEKTUR KOMUNIKASI SISTEM *SMART HYDROPONIC* FIK UPNVJ

RAHMAN ILYAS AL KAHFI

ABSTRAK

Integrasi teknologi *Internet of Things* (IoT) pada sistem pertanian modern membawa efisiensi tinggi, salah satunya sistem IoT *Smart Hydroponic* FIK UPNVJ. Namun, ketergantungan pada konektivitas jaringan membuka celah kerentanan terhadap serangan *Distributed Denial of Service* (DDoS) yang dapat melumpuhkan *server* serta menggagalkan transmisi data sensor dan aktuator. Penelitian ini bertujuan mengimplementasikan pendekatan *supervised learning* menggunakan tiga algoritma machine learning, serta menganalisis efektivitas performa deteksinya dalam memitigasi serangan DDoS pada arsitektur komunikasi WebSocket dan REST API. Metode penelitian meliputi perekaman lalu lintas data mentah menggunakan Tshark, pra-filtrasi paket port 8000, serta ekstraksi fitur aliran menggunakan CICFlowMeter menjadi empat kelas target (*BENIGN*, *HTTP_FLOOD*, *TCP_SYN_FLOOD*, dan *WS_FLOOD*). Hasil penelitian menunjukkan algoritma Support Vector Machine (SVM) dan Random Forest memberikan performa paling optimal. SVM mencapai kinerja tertinggi dengan *Accuracy* 98,56%, *Precision* 98,67%, *Recall* 98,48%, dan *F1-Score* 98,57%, kemudian disusul *Random Forest* dengan *Accuracy* 98,29%, *Precision* 98,48%, *Recall* 98,09%, dan *F1-Score* 98,25%. Sebaliknya, algoritma *Decision Tree* mencatat kinerja terendah dengan *Accuracy* 96,50%, *Precision* 96,97%, *Recall* 95,88%, dan *F1-Score* 96,31%. Ketiga model mencatatkan klasifikasi mutlak 100% pada kelas serangan *TCP_SYN_FLOOD*.

Kata Kunci : DDoS, IoT, *Machine Learning, Smart Hydroponic*, *Supervised Learning*.

MACHINE LEARNING IMPLEMENTATION FOR DDOS ATTACK DETECTION IN THE COMMUNICATION ARCHITECTURE OF THE FIK UPNVJ SMART HYDROPONIC SYSTEM

RAHMAN ILYAS AL KAHFI

ABSTRACT

The integration of Internet of Things (IoT) technology into modern agricultural systems delivers high efficiency, as demonstrated by the IoT Smart Hydroponic system at FIK UPNVJ. However, a heavy reliance on network connectivity exposes vulnerabilities to Distributed Denial of Service (DDoS) attacks, which can paralyze servers and disrupt data transmission between sensors and actuators. This study aims to implement a supervised learning approach using three machine learning algorithms and analyze their detection effectiveness in mitigating DDoS attacks across WebSocket and REST API communication architectures. The methodology encompasses raw network traffic recording via Tshark, pre-filtering packets on port 8000, and flow feature extraction using CICFlowMeter into four target classes (BENIGN, HTTP_FLOOD, TCP_SYN_FLOOD, and WS_FLOOD). The results indicate that the Support Vector Machine (SVM) and Random Forest algorithms achieved optimal performance. SVM demonstrated the highest performance, with Accuracy of 98.56%, Precision of 98.67%, Recall of 98.48%, and F1-Score of 98.57%, closely followed by Random Forest with Accuracy of 98.29%, Precision of 98.48%, Recall of 98.09%, and F1-Score of 98.25%. Conversely, the Decision Tree algorithm recorded the lowest performance, achieving Accuracy of 96.50%, Precision of 96.97%, Recall of 95.88%, and F1-Score of 96.31%. Notably, all three models achieved a perfect 100% classification performance for the TCP_SYN_FLOOD attack class.

Keywords: DDoS, IoT, *Machine Learning, Smart Hydroponic*, *Supervised Learning*.