Deteksi Serangan DDoS pada Protokol MQTT di IoT Menggunakan Model Semi-supervised DBSCAN - Support Vector Machine

Muhammad Ikhsanudin[1], **Vera Suryani**[2], **Rizka Reza Pahlevi**[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]ikhsanudinmuh@student.telkomuniversity.ac.id, [2]verasuryani@telkomuniversity.ac.id,
[3]rizkarezap@telkomuniversity.ac.id

Abstract

Internet of Things (IoT) is a system of connected objects with sensors, software, control systems and protocols. One of the protocols widely used in IoT is Message Queue Telemetry Transport (MQTT). Considering that users of these IoT devices can control their devices from anywhere makes them susceptible to various types of attacks. Distributed Denial of Service (DDoS) is a common attack vector in the IoT. Among the methods that can be applied for identifying this attack is machine learning. In previous research, DDoS de-tection was accomplished using a singular SVM. The accuracy and f1-score generated by this solitary SVM are still inadequate. This research combines SVM with other machine learning techniques in an effort to enhance SVM's accuracy and f1-score. In this research, semi-supervised DBSCAN and SVM models were utilized. We use three datasets in this research, namely IoTID20, simulation, and CICDDOS2018. The pro-posed model has the ability to detect DDoS attacks with a 99.6% accuracy, 99.6% f1-score, and 0.8% false alarm rate.

Keywords: Internet of Things, MQTT, Semi-supervised model, DBSCAN, SVM