

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

Muhammad Ikhsanudin¹, Vera Suryani², Rizka Reza Pahlevi³

^{1,2,3}Fakultas Informatika, Universitas Telkom, Bandung

¹ikhsanudinmuh@student.telkomuniversity.ac.id, ²verasuryani@telkomuniversity.ac.id,

³rizkarezap@telkomuniversity.ac.id

Abstrak

Internet of Things (IoT) adalah sistem objek yang terhubung dengan sensor, perangkat lunak, sistem kontrol, dan protokol. Salah satu protokol yang banyak digunakan dalam IoT adalah *Message Queue TelemetryTransport (MQTT)*. Mengingat pengguna perangkat IoT ini dapat mengontrol perangkatnya dari mana saja membuat mereka rentan terhadap berbagai jenis serangan. *Distributed Denial of Service (DDoS)* adalah vektor serangan umum di IoT. Diantara metode yang dapat diterapkan untuk mengidentifikasi serangan ini adalah machine learning. Dalam penelitian sebelumnya, deteksi DDoS dilakukan dengan menggunakan *single SVM*. Akurasi dan f1-score yang dihasilkan oleh *single SVM* ini masih kurang memadai. Penelitian ini menggabungkan SVM dengan *machine learning* lainnya dalam upaya meningkatkan akurasi dan f1-score dari SVM. Dalam penelitian ini, model *semi-supervised DBSCAN* dan SVM digunakan. Kami menggunakan tiga dataset pada penelitian ini, yaitu *IoTID20*, simulasi, dan *CICDDOS2018*. Model yang diusulkan memiliki kemampuan untuk mendeteksi serangan DDoS dengan akurasi 99,6%, f1-score 99,6%, dan *false alarm rate* 0,8%.

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