1. Pendahuluan

Latar Belakang

Internet of Things (IoT) adalah sistem objek yang terhubung dengan sensor, perangkat lunak, sistem kontrol dan protokol [14]. Salah satu protokol yang ada di IoT adalah *Message Queue Telemetry Transport* (MQTT), protokol ini banyak digunakan di bidang IoT karena mode berlangganan dan rilisnya, dan telah menjadi standar transmisi data *de facto* [3].Pengguna perangkat IoT ini dapat mengendalikan perangkatnya dari manapun, yang berarti hal ini dapat menyebabkan kerentanan terhadap berbagai macam serangan [9].

Distributed Denial of Service (DDoS) adalah salah satu serangan yang sering terjadi. Serangan ini terjadi ketika banyak klien terus mengirimkan permintaan ke server, yang dapat membuat server terbebani dengan permintaan untuk diproses. Daya tahan baterai perangkat IoT juga dapat terpengaruh oleh serangan ini karena perangkat dapat menyala terus-menerus. Virus botnet unik yang dikenal sebagai Mirai telah muncul dalam beberapa tahun terakhir, yaitu *botnet* yang mampu melakukan serangan DDoS yang telah merusak banyak perangkat IoT [9].

Pendekatan menggunakan *machine learning* merupakan salah satu cara yang paling efektif untuk mendeteksi serangan [9]. Pada penelitian [17] telah dilakukan pendeteksian DDoS pada SDN control plane menggunakan SVM dan menghasilkan akurasi dan *f1-score* yang belum terlalu baik. Penelitian ini mengintegrasikan SVM dengan *machine learning* yang lain dengan tujuan meningkatkan akurasi dan *f1-score* yang dihasilkan. Berdasarkan penelitian sebelumnya [13], DBSCAN telah diuji untuk mendeteksi serangan DDoS pada platform *cloud*. Menurut penelitian ini, DBSCAN dapat dikombinasikan dengan *machine learning* yang lain untuk meningkatkan akurasi. Oleh karena itu, penelitian ini dilakukan untuk menguji apakah integrasi DBSCAN dan SVM dapat mendetek-si serangan DDoS dan seberapa akurat jika DBSCAN diintegrasikan dengan SVM dalam mendeteksi serangan DDoS.

Topik dan Batasannya

Perumusan Masalah :

- Bagaimana mendeteksi serangan DDoS pada protokol MQTT di IoT menggunakan pendekatan *machine learning*?
- Bagaimana model *semi-supervised* DBSCAN dan SVM untuk mendeteksi serangan DDoS pada protokol MQTT di IoT?
- Bagaimana performansi model *semi-supervised* DBSCAN dan SVM yang dibangun dalam mendeteksi serangan DDoS pada data simulasi dan dataset pihak ketiga?

Batasan :

- Menggunakan dataset dari penelitian [16], dataset simulasi yang diperoleh dari simulasi serangan DDoS pada protokol MQTT yang dilakukan mandiri, dan dataset dari penelitian [11].
- Menggunakan model *semi-supervised* DBSCAN dan SVM.
- Deteksi DDoS dilakukan pada dataset, tidak dilakukan secara *real time*.
- Mengukur performansi model menggunakan akurasi, *f1-score*, dan *false alarm rate*.

Tujuan

Tujuan penelitian ini dapat dilihat pada Tabel 1.

Tabel 1. **Keterkaitan antara tujuan, pengujian dan kesimpulan**

No	Tujuan	Pengujian	Kesimpulan
1	Melakukan pendeteksian serangan DDoS pada protokol MQTT menggunakan pendekatan *machine learning*.	Menjalankan pendeteksian serangan DDoS pada protokol MQTT menggunakan pendekatan *machine learning*.	Model *machine learning* yang digunakan pada penelitian ini dapat mendeteksi serangan DDoS dengan baik.
2	Membangun model semi-supervised DBSCAN dan SVM untuk mendeteksi serangan DDoS pada protokol MQTT.	Melakukan penggabungan clustering DBSCAN dan klasifikasi SVM untuk mendeteksi serangan DDoS pada protokol MQTT.	Model gabungan DBSCAN dan SVM yang diajukan dapat mendeteksi serangan DDoS dengan baik.

3	Mengevaluasi performansi model yang dibangun dalam mendeteksi serangan DDoS pada beberapa dataset termasuk dataset hasil simulasi menggunakan *confusion matrix*.	Mengevaluasi kinerja model yang dibangun dalam mendeteksi serangan DDoS pada dataset yang digunakan menggunakan akurasi, f1-score, dan *false alarm rate* dari *confusion matrix*.	Performansi terbaik yang dihasilkan oleh model yang diajukan ialah ketika menggunakan dataset simulasi. Akurasi, f1-score, dan *false alarm rate* terbaik yang didapatkan ialah 99,6%, 99,6%, dan 0,8%.

Organisasi Tulisan

Struktur penelitian ini diuraikan sebagai berikut. Bagian kedua menjelaskan studi terkait. Sistem yang diimplementasikan menjadi topik pembahasan pada bagian tiga pada penelitian ini. Bagian keempat membahas hasil pengujian dan analisisnya. Pada Bagian lima, kesimpulan dan saran untuk penelitian selanjutnya.