1. Pendahuluan

Latar Belakang

Saat ini teknologi komunikasi telah berkembang pesat dan manfaatnya telah dirasakan oleh seluruh penduduk dunia dengan hadirnya teknologi yang membantu kegiatan sehari-hari, seperti ketika sedang bekerja atau berada di rumah. Salah satu teknologi yang sering digunakan saat ini adalah *Internet of Things (IoT)*. *IoT* merupakan sistem yang menghubungkan beberapa perangkat untuk mentransfer data melalui jaringan tanpa adanya interaksi dari manusia. Menurut para ahli, selama tahun 2020 ini, penggunaan sistem *IoT* diperkirakan mencapai 31 Triliun Instalasi perangkat *IoT* [1]. Seiring berkembangnya sistem IoT, kebutuhan akan sistem keamanan untuk *IoT* juga meningkat karena walaupun *IoT* menggunakan teknologi yang canggih, namun tidak menutup kemungkinan sistem *IoT* menjadi sasaran dari serangan siber atau *cyberattack*. Serangan pada *IoT* dapat dilakukan dengan berbagai bentuk serangan, yaitu: *Physical Attack, Software Attack, Network Attack, dan Encryption Attack*. Salahsatu tujuan penyerangan pada sistem *IoT* yaitu untuk mencuri data pribadi dan data dari perangkat *IoT* [2].

Cara untuk menanggulangi *cyberattack* adalah dengan *cybersecurity*. *Cybersecurity* diperlukan agar sistem terhindar dari intimidasi dan serangan yang dapat merusak sistem. Hadirnya *cybersecurity* memiliki tujuan untuk melindungi sistem, jaringan, dan program dari *cyberattack* [3]. Salah satu aplikasi *cybersecurity* yang ada saat ini adalah *Intrusion Detection System (IDS). Intrusion Detection System* merupakan *software* atau *hardware* yang sangat penting untuk mencegah akses tak dikenal dan melaporkan serangan tersebut [4]. *Intrusion Detection System* digunakan sebagai pelapis kedua untuk keamanan pada sistem setelah *firewall* sehingga jika *firewall* dapatditembus oleh *cyberattack*, *Intrusion Detection System* dapat menjalankan tugasnya untuk mendeteksi serangan. *Intrusion Detection System* dapat dibangun dengan menggunakan metode *Machine Learning*, salah satunya yaitu *Support Vector Machine (SVM)*. *SVM* merupakan pendekatan *supervised* yang terbukti menghasilkan kinerja yang tinggi untuk menyelesaikan permasalahan klasifikasi sehingga akan cocok dengan *Intrusion Detection System* karena menggunakan sistem klasifikasi dalam mendeteksi serangan.

Topik dan Batasannya

Topik yang dibawakan pada jurnal ini yaitu pembangunan *Intrusion Detectioon System (IDS)* dengan algoritma *Support Vector Machine (SVM)* untuk mengetahui seberapa akurat penggunaan algortima tersebut untuk mendeteksi adanya serangan. Adapun batasan masalah pada jurnal ini yaitu jenis serangan yang akan digunakan pada pengujian ini hanya *ddos* saja.

Tujuan

Tujuan dari penelitian ini adalah sebagai berikut:

1. Membangun *Intrusion Detection System (IDS)* untuk meningkatkan keamanan sistem *Internet of Things (IoT)* dari ancaman serangan.
2. Melakukan analisis akurasi dari *Intrusion Detection System (IDS)* yang dibangun.

Organisasi Tulisan

Organisasi tulisan setelah bagian Pendahuluan yaitu Studi yang berkaitan dengan *Intrusion Detection System* beserta kajian teori mengenai *Internet of Things (IoT), Intrusion Detection System (IDS)*, dan *Support Vector Machine*. Bab 3 dan 4 berturut-turut berisi beberapa tahap yang berlangsung pada sistem dam hasil penguujian beserta analisis kinerja sistem. Bab terakhir merupakan kesimpulan yang dapat diambil dari pengujian.