1. Pendahuluan

Latar Belakang

Keamanan siber adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, dan teknologi yang dapat digunakan untuk melindungi lingkungan dunia maya dan organisasi serta aset pengguna[1]. Organisasi menggunakan berbagai strategi untuk melindungi sistem komputer dari serangan keamanan siber, termasuk memasang firewall dan perangkat lunak *anti-virus*, menerapkan protokol autentikasi pengguna, mengenkripsi data sensitif, dan melatih karyawan dalam praktik keamanan terbaik. Intrusion Detection System (IDS) adalah perangkat atau aplikasi perangkat lunak yang memonitor jaringan atau sistem untuk aktivitas berbahaya atau pelanggaran[2].

IDS dirancang untuk mendeteksi dan merespons *cyber attacks* secara *real-time*, mengingatkan personel keamanan akan potensi pelanggaran keamanan dan membantu mencegah atau mengurangi kerusakan yang disebabkan oleh serangan. Tetapi banyak IDS masih mengalami tingkat alarm palsu yang tinggi, menghasilkan banyak peringatan pada situasi yang tidak mengancam, yang menimbulkan beban bagi analis keamanan dan dapat menyebabkan serangan yang sangat berbahaya diabaikan[3].

Machine Learning (ML) membuat sistem untuk belajar dan meningkatkan kemampuan otomatis sistem berdasarkan pengalaman tanpa diprogram secara eksplisit. Implementasi algoritma ML pada IDS dapat meningkatkan performa sistem menjadi lebih akurat dalam mendeteksi serangan dengan jumlah data yang besar dalam waktu yang lebih singkat[4]. ML memiliki potensi untuk menyediakan kapabilitas keamanan siber yang dinamis, adaptif, *context-aware*, dan kolaboratif antara manusia dan mesin. Oleh karena itu metode *Incremental Learning* dapat digunakan untuk meningkatkan kinerja IDS.

Incremental Learning menggunakan ML untuk terus belajar dan beradaptasi dengan ancaman dan serangan baru, menjadikannya lebih efektif dari waktu ke waktu. Sistem mampu menganalisis lalu lintas jaringan dan mengidentifikasi pola yang mengindikasikan adanya serangan, lalu mengambil tindakan yang tepat untuk memblokir atau mengurangi serangan tersebut [5].

Topik dan Batasannya

Topik yang dibawakan pada jurnal ini membahas pembangunan *Intrusion Detection System* (IDS) menggunakan metode *Incremental Learning* untuk mengetahui seberapa akurat penggunaan metode tersebut untuk mendeteksi adanya serangan. Adapun batasan masalah pada penelitian ini adalah dataset yang digunakan adalah UAV Intrusion Detection Dataset.

Tujuan

Tujuan dari penelitian ini adalah sebagai berikut:

1. Melakukan analisis *Intrusion Detection System* menggunakan metode *Incremental Learning*
2. Melakukan implementasi metode *Incremental Learning* pada *Intrusion Detection System*
3. Mengetahui bagaimana *Incremental Learning* dapat bekerja pada *Intrusion Detection System*

Organisasi Tulisan

Penjelasan mengenai organisasi tulisan seperti pada bab 2 berisi pembahasan mengenai studi literatur dan rancangan sistem yang berkaitan dengan penelitian. Bab 3 berisi pembahasan mengenai hasil hasil eksperimen yang dilakukan pada penelitian. Pada bab 4 membahas rangkuman hasil evaluasi pada penelitian berupa kesimpulan dan saran.