Abstrak

Penggunaan internet yang terus meningkat memerlukan sistem deteksi serangan yang handal agar penyusup atau *cracker* yang hendak melakukan *cyberattacks* dapat terdeteksi dengan cepat. Mitigasi dan pertahanan dari ancaman serangan *cyber* menjadi sangat penting mengingat masyarakat sudah mulai ketergantungan pada teknologi internet yang bisa mengancam setiap saat. Ketika sejumlah besar paket datang, maka perlu dideteksi apakah paket tersebut paket data normal atau paket data serangan. *Intrusion Detection System* (IDS) dapat digunakan untuk mendeteksi setiap serangan pada jaringan atau sistem informasi. Deteksi anomali adalah jenis IDS yang mendeteksi serangan anomali pada jaringan berdasarkan probabilitas statistik.

Pada penelitian ini deteksi serangan dilakukan dengan menggunakan metode *Knowledge Discovery in Databases* (KDD) berbasis *machine learning* untuk menganalisis serangan berdasarkan 2 (dua) sumber dataset yaitu UNSW-NB15 dan CICIDS2017. Algoritma J48, naïve bayes dan AdaBoostM1 digunakan untuk melakukan klasifikasi serangan. Pemrosesan data menggunakan tools WEKA.

Seleksi jumlah atribut dilakukan menggunakan metode CFs-*Greedystepwise* untuk memilih atribut yang sangat berpengaruh terhadap pendeteksian serangan untuk efisiensi. Hasil pengujian menunjukkan algoritma J48 menghasilkan akurasi tertinggi sebesar 99.839%.

Keyword : *Data mining, Intrusion Detection System, Cyberattacks,* Algoritma *Machine Learning,* WEKA.