

Abstrak

Semakin berkembangnya teknologi informasi secara tidak langsung membuat semakin banyak jenis intrusi yang membahayakan keamanan dari suatu jaringan komputer atau sistem informasi. Untuk mendeteksi adanya intrusi tersebut maka dibutuhkan sebuah sistem yang disebut dengan *Intrusion Detection System (IDS)*. Banyak metode yang bisa dilakukan untuk membangun IDS. Salah satunya adalah teknik data mining untuk menghasilkan *detection model* yang bisa membedakan antara jenis koneksi normal atau intrusi. Pada tugas akhir ini, diimplementasikan sebuah algoritma *hybrid* yang menggunakan dua algoritma learning, yaitu *Eager Learning* dan *Lazy Learning*. Untuk *Eager Learning* digunakan algoritma RIPPER sedangkan untuk *Lazy Learning* digunakan algoritma Nearest Neighbour (K-NN). Sesuai dengan namanya, *Eager Learning* lebih banyak menginvestasikan waktu untuk fase *learning*, sedangkan *Lazy Learning* lebih banyak meluangkan waktu dalam fase klasifikasi. Penerapan feature selection dan resampling pada *training data* digunakan untuk membentuk *training data* yang lebih representatif. Pengujian dilakukan dengan beberapa skenario untuk mengetahui nilai akurasi, precision, recall, dan f-measure dari *detection model* yang dihasilkan. Pada tahap analisis dan pengujian, *detection model* yang dihasilkan mampu memberikan nilai akurasi terbaik sebesar 92.3220% dengan menggunakan *testing data*.

Kata kunci: intrusion detection system, algoritma hybrid, klasifikasi, ripper, nearest neighbour.