

ABSTRAK

Keamanan data dan ketersediaan *resource* pada jaringan komputer dari berbagai jenis intrusi, selalu menjadi perhatian banyak pihak, terutama administrator jaringan. Banyaknya jumlah data yang harus diaudit dan perkembangan jenis-jenis intrusi yang terus meningkat menjadi tugas yang tidak mudah bagi administrator. *Data mining* memiliki kemampuan mengekstraksi informasi dari sekumpulan data yang sebelumnya tidak diketahui polanya. Dengan menerapkan konsep dan metode *data mining* pada data aktifitas koneksi jaringan komputer, akan didapatkan informasi dan pola-pola dari data tersebut, sebuah *detection model*. *Detection model* digunakan pada *intrusion detection system* (IDS) sebagai filter untuk menyaring data aktifitas jaringan komputer, yang membedakan antara jenis koneksi normal atau koneksi yang berupa intrusi. Suatu tantangan dalam membangun *detection model* yang memiliki kemampuan deteksi intrusi yang akurat. Pada tugas akhir ini diimplementasikan algoritma *repeated incremental pruning to produce error reduction* (RIPPER) untuk membangun *misuse detection model*. RIPPER merupakan salah satu bentuk *sequence covering algorithm* yang menghasilkan model berupa sekumpulan *rule* (*rule-based classifier*). Penerapan *feature selection* dan *resampling* ditujukan untuk membentuk *training data* yang representatif. Pada tahap analisis dan pengujian, *detection model* yang dihasilkan mampu memberikan nilai akurasi terbaik sebesar 92,91256%. Dan dengan nilai CPE minimum adalah 0,1964, lebih rendah dibanding dengan pemenang KDD Cup 1999 dengan CPE sebesar 0,2331.

Kata Kunci : *intrusion detection system*, *misuse detection model*, RIPPER, *feature selection*, *resampling*.