

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil penelitian yang dijelaskan pada bab 4, dapat ditarik kesimpulan sebagai berikut:

- a. *Data set* KDD Cup 1999 merupakan data transaksi yang dapat melalui proses data *mining* menggunakan teknik *sequential pattern*. *Rules* yang dihasilkan dari proses *data mining* dapat diterapkan kedalam model arsitektur Snort IDS.
- b. Algoritma CM-SPADE membutuhkan waktu proses yang lebih kecil dalam melakukan proses *data mining* jika dibandingkan dengan algoritma SPADE.
- c. Penerapan teknik data *mining* CM-SPADE pada data KDD Cup 1999 memiliki tingkat akurasi sebesar 97,976%.
- d. Performa algoritma CM-SPADE dapat dikategorikan sebagai performa yang bagus, karena mampu mendapatkan akurasi sebesar 97,976%. Hal ini jika dibandingkan dengan algoritma *data mining* sebelumnya yang telah digunakan dalam merancang IDS. Yaitu algoritma sarang semut (ANTIDS) yang mampu mendapatkan akurasi 99,97%, kombinasi algoritma SVM dan sarang semut (CSVAC) yang mampu mendapatkan akurasi 94,86 %, dan kombinasi algoritma SVM dengan K-Means yang mampu mendapatkan akurasi 93.33%.

5.2. Saran

Dalam pelaksanaan penelitian, penulis menyadari bahwa banyak kekurangan di dalam penelitian ini. Oleh karena itu, penulis menyampaikan beberapa saran agar penelitian yang akan dilakukan mengenai pembahasan yang serupa dengan penelitian ini dapat menjadi lebih baik. Beberapa saran penulis untuk penelitian selanjutnya, antara lain sebagai berikut :

- a. Proses *preprocessing* membutuhkan tahapan yang banyak dan cukup lama. Hal ini disebabkan SPMF yang hanya mampu menerima data

masuk dengan syarat yang spesifik. Untuk selanjutnya disarankan untuk menggunakan alat lain sehingga proses *preprocessing* menjadi lebih pendek.

- b. Pada proses *preprocessing* penulis menggunakan berbagai macam tahapan seperti *discretize*, *feature selection* dan sebagainya. Untuk selanjutnya disarankan untuk memodifikasi tahapan tersebut untuk mencari perbandingannya, apakah bisa lebih baik atau tidak. Contohnya menggunakan tahapan *feature selection* menggunakan teknik selain *correlation attribute*.
- c. Pada algoritma CM-SPADE, algoritma hanya mampu menampilkan model yang mendeskripsikan label data tipe koneksi normal. Hal ini menyebabkan jenis serangan hanya dikelompokkan menjadi satu yaitu DOS. Untuk selanjutnya bisa mencoba teknik *sequential pattern* yang lain yang mampu menampilkan model yang mendeskripsikan label data tipe serangan secara mendetail.
- d. Pada penelitian ini penulis menggunakan data KDD Cup 1999 sebagai data *training* maupun data *testing*. Untuk selanjutnya bisa dicoba menggunakan data jaringan yang lain, untuk mengetahui perbandingan model yang dihasilkan.