BAB V

PENUTUP

5.1 KESIMPULAN

Berdasarkan penelitian yang telah dilakukan dalam deteksi *malware* menggunakan metode *Deep Neural Networks Untuk Serangan Spyware*, dapat disimpulkan sebagai berikut:

1. Metode DNN dapat diaplikasikan dalam mendeteksi *malaware* . Pada penelitian ini metode DNN mampu mengenali pola serangan *malware* pada *dataset* yang digunakan.
2. Fitur yang digunakan sebagai pengenalan pola serangan *malware* adalah fitur *Information gain*. Melalui *feature extration information gain* dipilih 15 fitur teratas yang memiliki kontribusi dalam pengenalan pola serangan *malware*.
3. Kinerja metode DNN dalam mendeteksi *malware* dievaluasi dengan menggunakan *confusion matrix* untuk mengetahui nilai *accuracy*, *precission, recall* dan *f1-score*. Deteksi berdasarkan serangan *malware Spyware* mendapatkan *accuracy* 99,99%, *precission* 100%, *recall* 100% dan *f1-score* 100%, serta deteksi serangan *malware Spyware* berdasarkan *category* mendapatkan *accuracy* 88%, *precission 91%*, *recall* 100% dan *f1-score* 95%. Berdasarkan hasil evaluasi menunjukkan bahwa metode DNN mencapai kinerja yang sangat baik, hal tersebut tampak pada nilai *accuracy*, *precission, recall* dan *f1-score* pada berbagai *split data*

5.2 SARAN

Saran pada penelitian ini adalah pada penelitian selanjutnya dalam mendeteksi *malware spyware* menggunakan metode DNN, fitur atau atribut yang digunakan yaitu fitur PCA (*Principal component analyst*) untuk mengetahui tingkat *accuracy*, *precission, recall* dan nilai f1-*score.* Selain itu, pada penelitian selanjutnya dapat menggunakan metode yang berbeda dalam mendeteksi *malware* misalnya dengan menggunakan metode CNN ataupun RNN.