BAB V

KESIMPULAN

5.1 KESIMPULAN

Penelitian ini telah disadari oleh penulis bahwa masih ada beberapa kekurangan yang menjadi saran atau masukan untuk pengembangan penelitian ini adalah sebagai berikut :

1. Dari hasil pengujian model *DNN* menggunakan data serangan jaringan menggunakan dataset *Obfuscated-MalMem*2022 yang disediakan oleh *UNIVERSITY OF NEW BRUNSWICK* terdiri dari 58.596 data dengan 57 atribut (fitur),
2. Model *DNN* yang dirancang terbukti efektif dalam mendeteksi dan mengklasifikasikan serangan jaringan yang disebabkan oleh jenis *malware* tertentu, seperti *ransomware*.
3. Pada pengujian dengan klasifikasi *class benign* dan *malware*, model *DNN* berhasil mencapai tingkat akurasi, *presisi*, *recall*, dan *f1-score* sebesar 100%. Hal ini menunjukkan keefektifan model dalam mengklasifikasikan kedua kelas tersebut, selanjutnya dilakukan pengujian dengan *Category* (*malware ransomware*), model awal memberikan tingkat klasifikasi sebesar 72%. Untuk meningkatkan kinerja model, dilakukan peningkatan menggunakan teknik *Principal Component Analysis* (PCA) dengan variasi jumlah fitur (15, 25, dan 35). Hasil terbaik diperoleh menggunakan 15 dan 25 fitur, dengan mencapai akurasi sebesar 82%.

Ini menunjukkan bahwa penggunaan *PCA* berhasil meningkatkan kemampuan model dalam mengklasifikasikan kategori *malware*.

5.2 SARAN

Penelitian ini telah disadari oleh penulis bahwa masih ada beberapa kekurangan yang menjadi saran atau masukan untuk pengembangan penelitian ini adalah sebagai berikut :

1. Perlu dilakukan analisis lebih lanjut untuk meningkatkan akurasi model. Eksplorasi parameter-model dan *fine-tuning* dapat menjadi fokus untuk mencapai performa yang lebih baik.
2. Diperlukan penerapan teknik ekstraksi fitur atau seleksi fitur lainnya untuk meningkatkan model. Metode lain dapat dieksplorasi untuk memperoleh representasi fitur yang lebih optimal.