BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan dari hasil dan analisa penelitian yang telah dilakukan dapat disimpulkan bahwa:

1. Eksperimen penerapan metode *Back Propagation Neural Network (BPNN)* tanpa optimasi *hyperparameter tuning* dilakukan dengan berbagai kombinasi *hyperparameter*, termasuk jumlah neuron pada *hidden layer*, *learning rate*, dan jumlah *epoch*. Hasil eksperimen menunjukkan bahwa performa model tetap berada pada kisaran 96% hingga 97%. Kombinasi dengan 20 neuron pada lapisan tersembunyi, *learning rate* sebesar 0.05, dan 200 *epoch* menghasilkan akurasi, presisi, dan *recall* mencapai 97%, serta *F1-score* mencapai 96%, dengan waktu komputasi yang efisien sekitar 5670.53 detik.
2. Eksperimen penerapan metode *Back Propagation Neural Network (BPNN)* dengan optimasi *hyperparameter tuning* menggunakan *Grid Search* berhasil meningkatkan akurasi hingga 1% dari hasil eksperimen tanpa optimasi. Proses optimasi *hyperparameter* dilakukan dengan mencari kombinasi *dropout rate*, jumlah neuron pada *hidden layer*, dan jumlah *hidden layer* terbaik dengan variasi *learning rate* dan jumlah *epoch*. Hasil eksperimen menunjukkan bahwa kombinasi *learning rate* 0.05, *dropout rate* 0.1, 20 neuron pada lapisan tersembunyi, 2 lapisan tersembunyi, dan 200 *epoch* menghasilkan akurasi, presisi, *recall*, dan *F1-score* mencapai 98%. Meskipun optimasi *hyperparameter* mampu meningkatkan performa model, metode ini memerlukan waktu komputasi yang lebih tinggi.
3. Pengujian *website* deteksi *malware* dengan menggunakan model *neural network* terbaik hasil eksperimen menunjukkan kinerja yang sangat baik dalam mengidentifikasi dan membedakan antara *file malware* dan *benign*. Dalam pengujian menggunakan *real test data*, sistem mampu mencapai akurasi sebesar 96.67%. Eksperimen ini juga menunjukkan bahwa sebagian besar *file malware* dan *benign* berhasil diidentifikasi dengan benar oleh sistem. Dari total 135 *file*

malware, 130 diantaranya berhasil dideteksi dengan akurat, sementara seluruh 15 *file benign* juga berhasil dikenali secara tepat. Hasil ini memberikan indikasi kuat bahwa model *neural network* yang diimplementasikan pada *website* mampu menjalankan tugas deteksi *malware* dengan baik.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan, penulis memberikan saran-saran sebagai berikut:

1. Untuk meningkatkan keandalan dan representatifitas model, dianjurkan untuk memperluas *dataset* dengan mengumpulkan lebih banyak contoh *malware* dan *benign* yang bervariasi untuk meningkatkan kemampuan generalisasi model dalam menghadapi ancaman yang lebih kompleks dan baru.
2. Untuk penelitian lebih lanjut, perlu dilakukan pengujian yang lebih mendalam dengan menggunakan *real test data* yang lebih banyak dan beragam. Hal ini bertujuan untuk menguji kemampuan model dalam berbagai skenario dunia nyata. Selain itu, perlu dilakukan pengujian dengan jenis *malware* yang lebih baru dan kompleks guna memahami sejauh mana model dapat mendeteksi ancaman baru.
3. Eksplorasi lebih lanjut dalam optimasi *hyperparameter* menggunakan teknik lain selain *Grid Search*, seperti *Random Search* atau *Bayesian Optimization*, dapat membantu mencari kombinasi *hyperparameter* yang lebih optimal.
4. Selain *Back Propagation Neural Network*, eksplorasi penggunaan teknik *neural network* lain, seperti *Convolutional Neural Network* (*CNN*) atau *Recurrent Neural Network* (*RNN*), dapat diuji untuk meningkatkan kinerja deteksi.
5. Melibatkan model *ensemble* dengan menggabungkan beberapa model yang berbeda dapat meningkatkan performa deteksi *malware*.