BAB V

PENUTUP

5.1 KESIMPULAN

Berdasarkan hasil penelitian, implementasi metode Deep Neural Network (DNN) dalam mendeteksi serangan Ransomware pada dataset CIC-MalMem-2022 memberikan hasil yang sangat baik dalam aspek akurasi dan efisiensi pelatihan. Salah satu kunci keberhasilan model ini adalah penerapan teknik early stopping, yang terbukti mampu menghentikan pelatihan secara otomatis pada saat performa terbaik model telah dicapai pada data validasi.

Model DNN dirancang untuk dilatih secara maksimal hingga 100 epoch, namun dengan penggunaan mekanisme early stopping, proses pelatihan tidak bergantung pada jumlah epoch tetap. Sebaliknya, pelatihan dihentikan ketika tidak terjadi peningkatan signifikan selama beberapa iterasi berturut-turut, yang ditentukan melalui parameter patience. Hal ini tidak hanya mencegah overfitting, tetapi juga memastikan bahwa model mengadopsi representasi fitur yang paling optimal dari data tanpa pelatihan berlebih.

Dalam penelitian ini, pendekatan tersebut menghasilkan model klasifikasi yang sangat akurat dan stabil, dengan nilai akurasi 94,27%, presisi 94,30%, recall 94,27%, dan F1-score 94%, menunjukkan bahwa model mampu membedakan antara sampel benign dan Ransomware secara efektif. Hasil ini menunjukkan bahwa dalam pengembangan sistem deteksi malware berbasis deep learning, penggunaan strategi pelatihan yang adaptif dan dinamis seperti

early stopping menjadi sangat krusial, terutama ketika bekerja dengan data berukuran besar dan kompleks.

5.2 SARAN

1. Pemanfaatan Early Stopping untuk Efisiensi Pelatihan

Berdasarkan hasil yang diperoleh, penggunaan early stopping terbukti sangat efektif dalam mengontrol proses pelatihan model deep learning. Oleh karena itu, disarankan bagi peneliti selanjutnya untuk tetap mengandalkan teknik ini ketika bekerja dengan dataset berskala besar, guna menghindari overfitting dan mempersingkat waktu komputasi tanpa mengorbankan performa model.

2. Pengujian Berbasis Dinamis, Bukan Statis

Penelitian ini menunjukkan bahwa pelatihan model tidak memerlukan evaluasi manual terhadap jumlah epoch (misalnya 10, 50, atau 100). Sebagai gantinya, pendekatan berbasis performa dinamis seperti early stopping yang bergantung pada hasil validasi secara langsung jauh lebih efektif. Saran ini penting untuk menghindari pemborosan sumber daya dan memastikan pelatihan berfokus pada hasil terbaik.

3. Eksplorasi Kombinasi Callback Lanjutan

Untuk pengembangan lebih lanjut, disarankan melakukan eksplorasi callback lain dalam proses pelatihan, seperti ReduceLROnPlateau atau ModelCheckpoint, yang dapat dikombinasikan dengan early stopping untuk menyesuaikan laju pembelajaran dan menyimpan bobot terbaik model secara otomatis.

4. Uji Coba Pada Arsitektur Dnn Yang Lebih Dalam

Dengan kontrol pelatihan yang efisien seperti early stopping, peneliti ke depan dapat mencoba arsitektur DNN yang lebih dalam atau lebih kompleks. Hal ini dapat membuka potensi peningkatan kemampuan model dalam mengenali pola serangan yang lebih rumit atau tidak lazim.

5. Replika Pada Jenis Malware Lain

Mengingat penelitian ini fokus pada deteksi Ransomware, saran berikutnya adalah melakukan pendekatan serupa terhadap jenis malware lain seperti trojan atau spyware, menggunakan mekanisme pelatihan otomatis berbasis early stopping, agar diperoleh generalisasi model yang lebih luas dan adaptif terhadap berbagai ancaman.