

BAB V

PENUTUP

3.1 KESIMPULAN

Berdasarkan hasil penelitian, maka dapat ditarik kesimpulan sebagai berikut:

1. Model *Convolutional Neural Network* (CNN) yang digunakan dalam penelitian ini terbukti mampu mendeteksi serangan *DDoS* pada jaringan *Internet of Vehicles* (IoV) secara akurat, dengan tingkat akurasi, presisi, *recall*, dan *f1-score* mencapai 100% pada epoch ke-100. Hal ini menunjukkan bahwa model memiliki kemampuan *klasifikasi* yang sangat baik dalam membedakan lalu lintas jaringan normal dan yang mengandung serangan *DDoS*.
2. Teknik *preprocessing*, seperti pembersihan data, penggabungan label, dan ekstraksi fitur menggunakan *Principal Component Analysis* (PCA), berperan penting dalam meningkatkan efisiensi dan efektivitas pelatihan model. PCA membantu menyederhanakan fitur tanpa kehilangan informasi penting, sehingga mempercepat proses pelatihan dan mengurangi risiko overfitting.
3. Peningkatan jumlah *epoch* hingga 100 menghasilkan performa model yang paling stabil dan optimal. Hasil evaluasi menunjukkan bahwa semakin tinggi jumlah *epoch*, maka semakin baik akurasi dan generalisasi model terhadap data uji, dengan nilai loss yang konsisten menurun sepanjang proses pelatihan.

Commented [L1]: Sejajarkan dengan kalimat berikut yg diatas nya

3.2 SARAN

Berikut ini merupakan saran yang diberikan oleh peneliti yang berkaitan dengan topik pembahasan, metodologi penelitian dan proses pelatihan:

1. Penelitian selanjutnya diharapkan dapat menggunakan dataset yang lebih besar dan bervariasi, atau bahkan data real-time dari sistem IoV yang sebenarnya, guna menguji kemampuan generalisasi model terhadap lingkungan nyata yang lebih kompleks.
2. Diperlukan perbandingan performa CNN dengan metode deep learning lainnya seperti LSTM, RNN, ResNet, atau gabungan model (*hybrid*), untuk mengetahui efektivitas relatif dari berbagai arsitektur dalam mendeteksi serangan DDoS secara lebih menyeluruh.
3. Penelitian mendatang dapat memperluas cakupan klasifikasi, tidak hanya terbatas pada deteksi dua kelas (normal dan DDoS), tetapi juga multi-class classification untuk mendeteksi berbagai jenis serangan lain dalam jaringan IoV seperti DoS, Spoofing, dan Brute Force.