BAB V

PENUTUP

5.1 KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan maka dapat disimpulkan bahwa:

1. Pengenalan pola serangan *UDP Flood* pada jaringan IoT berhasil di identifikasi menggunakan pendekatan *deep learning*, dimana teknik *deep learning* mampu mempelajari pola-pola serangan sehingga dapat mengenali antara serangan berbahaya dan serangan normal.
2. Penerapan metode *Recurrent Neural Network* (RNN) dalam mendeteksi serangan *UDP Flood* mampu dan berhasil dalam melakukan deteksi, dengan menghasilkan tingkat *accuracy*, *precision*, *recall* dan *f1-score* yang sangat baik. Hal ini menggambarkan bahwa keunggulan dari metode RNN dalam mengenali serangan pada jaringan IoT yang kompleks.
3. Hasil pengujian menggunakan tiga parameter *epoch* (iterasi) diantaranya 10, 50, dan 100, pada *epoch* 100 memiliki nilai performa yang sangat baik dengan nilai *accuracy* mencapai 98%, *precision* 99%, *recall* 99%, dan *f1-score* 99% dimana model *Recurrent Neural Network* (RNN) dapat melakukan pengenalan pola-pola serangan dengan sangat baik.

5.2 SARAN

Berdasarkan penelitian yang telah dilakukan serta hasil penelitian yang telah disimpulakan, adapun saran untuk peneliti selanjutnya yaitu:

1. Diharapkan kepada peneliti berikutnya menggunakan jumlah *dataset* yang lebih banyak lagi.
2. Pada proses pengujian sebaiknya dapat menggunakan *split data* (pembagian data), penggunaan parameter *epoch* (iterasi), dan *batch size* yang lebih beragam sehingga dapat dilakukan komparasi hasil.
3. Untuk peneliti selanjutnya dapat menggunakan deteksi serangan menggunakan metode *deep learning* selain *Recurrent Neural Network* (RNN) diantaranya *Convolutional Neural Network* (CNN), *Long Short Term Memory* (LSTM), *Artificial Neural Network* (ANN) dan metode-metode lainnya sehingga dapat melihat nilai performa yang terbaik.