BAB V

KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan mengenai implementasi algoritma *Recurrent Neural Network* (RNN) untuk mendeteksi pola serangan pada protokol MQTT di lingkungan *Internet of Medical Things* (IoMT), didapatkan kesimpulan sebagai berikut:

1. Implementasi algoritma *Recurrent Neural Network* (RNN) berhasil diterapkan untuk mendeteksi serangan pada protokol MQTT di lingkungan *Internet of Medical Things* (IoMT). Proses implementasi telah mencakup *preprocessing* pada data, *cleaning* data, normalisasi data, pembagian pada dataset menjadi data *training* dan *testing*, serta pelatihan model menggunakan parameter-parameter tertentu seperti jumlah *hidden layers*, *epoch*, dan perubahan yang dilakukan oleh model secara optimal. Hasilnya, RNN dapat memanfaatkan hubungan waktu dalam data untuk mendeteksi pola serangan dengan hasil akurasi yang didapat secara efektif.
2. Kinerja model RNN yang dievaluasi dalam deteksi untuk menemukan hasil akurasi, TPR, F1-*score, Recall*, dan ROC. Model ini diuji dengan berbagai konfigurasi *epoch*, penelitian ini telah menunjukan hasil yang optimal dan imbang pada tahap awal pengujian hasil nilai akurasi mencapai 99.95%, serta *precision*, *recall* dan *F1-score* juga 99,95% hal ini menunjukkan hasil yang konsisten. Evaluasi model pada berbagai jumlah *epoch* (10,50 dan

100) menunjukan stabillitas performa hingga pada pengujian *epoch* 100 model mampu mencapai akurasi hingga 99,99%, Model juga menunjukkan kemampuan diskriminasi yang sangat baik dengan AUC sebesar 1.00, dari semua hasil evaluasi ini menunjukkan bahwa algoritma RNN memiliki kinerja yang cukup baik dalam mendeteksi pola serangan, dengan nilai metrik evaluasi yang mendukung efektivitas model dalam membedakan antara data *benign* dan data serangan.

Kesimpulan hasil akhir pada penelitian ini yaitu menyatakan peneliti telah berhasil mengimplementasikan algoritma *Recurrent Neural Network* (RNN) untuk mendeteksi pola serangan protokol MQTT di lingkungan *Internet of Medical Things* (IoMT) dengan efisien, Implementasi ini tidak hanya meningkatkan keamanan sistem secara optimal. Tatapi model yang dihasilkan pada implementasi ini menunjukkan kinerja yang konsisten dan andal, Pengujian lebih lanjutan mengkonfirmasi bahwa model RNN menunjukkan performa yang unggul dalam mendeteksi hampir semua pola serangan dengan tingkat kesalahan yang kecil.

5.2 SARAN

Penelitian ini telah menunjukkan hasil yang *positif* dalam mendeteksi serangan pada protokol MQTT dalam lingkungan *Internet of Medical Things* (IoMT) dengan menggunakan algoritma *Recurrent Neural Network* (RNN). Namun, terdapa beberapa aspek yang masih perlu diperhatikan lagi. Di antaranya adalah keterbatasan pada pengujian yang dilakukan dalam kondisi *real-time,* ukuran dan berbagai ragam data pada dataset yang digunakan, serta kinerja model ketika

diimplementasikan pada perangkat dengan sumber daya yang sangat terbatas. Oleh karena itu, beberapa saran untuk penelitian selanjutnya adalah sebagai berikut :

1. Menggunaan *Dataset* yang lebih beragam karena *Dataset* yang digunakan dalam penelitian ini memiliki keterbatasan dalam ukuran dan variasi pola serangan. Untuk meningkatkan kemampuan generalisasi model RNN, disarankan agar penelitian di masa depan menggunakan *dataset* yang lebih besar dan mencakup berbagai jenis serangan, seperti kombinasi serangan DDoS atau serangan lain berbasis rekayasa sosial pada protokol MQTT.
2. Efisiensi model RNN pada perangkat IoMT dengan sumber daya terbatas oleh karena itu masih perlu ditingkatkan lagi. Penelitian selanjutnya disarankan untuk lebih memahami arsitektur RNN yang lebih ringan seperti dalam mengkompresi model agar model dapat beroperasi dengan efisien tanpa mengurangi akurasi deteksi.
3. Penelitian selanjutnya dapat mempertimbangkan pengujian model RNN pada lingkungan jaringan IoMT dengan skala yang lebih besar dan kondisi jaringan yang berbeda-beda, seperti pengaruh latensi jaringan, dan gangguan lalu lintas data, guna mengevaluasi ketahanan model terhadap berbagai situasi nyata.

Dengan memperhatikan kekurangan dari saran yang ada, diharapkan penelitian berikutnya bisa memperbaiki sistem keamanan IoMT, agar lebih efektif dalam mendeteksi dan mencegah serangan secara langsung, dengan efisiensi yang lebih baik kedepannya.