

BAB V

PENUTUP

5.1 KESIMPULAN

Berdasarkan penelitian yang telah dilakukan mengenai deteksi serangan *spoofing* pada jaringan *Internet of Medical Things* (IoMT) menggunakan Algoritma *random forest*, dapat disimpulkan beberapa hal sebagai berikut :

1. Algoritma *random forest* berhasil diterapkan untuk mendeteksi serangan *spoofing* pada *Internet of Medical Things* (IoMT) dengan mengklasifikasikan lalu lintas jaringan berdasarkan pola yang diidentifikasi dari dataset.
2. Hasil evaluasi menunjukkan bahwa Algoritma *random forest* memiliki tingkat akurasi yang tinggi yaitu sebesar 99,06%, *precision* sebesar 99,05%, *recall* sebesar 99,06%, dan *F1-Score* sebesar 99,04% dalam mendeteksi serangan *spoofing*, sehingga dapat disimpulkan bahwa algoritma *random forest* sangat efektif dalam mendeteksi serangan *ARP spoofing* pada *Internet of Medical Things* (IoMT).

5.2 SARAN

Penelitian ini telah berhasil mengidentifikasi serangan *ARP spoofing* pada *Internet of Medical Things* (IoMT) menggunakan algoritma *random forest*. Namun, terdapat beberapa keterbatasan yang dapat menjadi peluang untuk pengembangan untuk penelitian selanjutnya. Oleh karena itu, berikut beberapa saran yang diharapkan dapat membantu penelitian selanjutnya agar memperoleh hasil yang lebih baik:

1. Penelitian ini hanya berfokus pada implementasi algoritma *random forest* tanpa membandingkan dengan algoritma lain yang lebih optimal, seperti SVM, *deep learning*, atau C4.5, dan lain-lain.

2. Penelitian ini hanya menyajikan hasil evaluasi tanpa memaparkan mengenai penerapan model dalam praktisi keamanan siber dalam mendeteksi serangan secara *real-time*.