BAB VI
PENUTUP

Bab ini akan menutup penelitian dengan memberikan kesimpulan dari penelitian yang telah dilakukan serta memberikan saran untuk penelitian deteksi *email phishing* kedepannya. Berikut merupakan bab 6 pada penelitian ini.

6.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan, maka dapat disimpulkan bahwa:

1. Perancangan model *machine learning* untuk deteksi kejahatan siber dilakukan menggunakan dua metode yaitu NLP dan regresi. Model dengan metode NLP seperti *email phishing*, email spam, dan Twitter spam dirancang menggunakan algoritma LSTM. Sedangkan, kejahatan siber lainnya seperti *web phishing* dan Facebook spam menggunakan algoritma *random forest* untuk melakukan klasifikasi.
2. Perolehan model *machine learning* dilakukan untuk mendapatkan model terbaik dari hasil rancangan yang sudah dibuat. Proses ini dilakukan dengan menerapkan berbagai metode optimasi, seperti Cross-Validation pada metode NLP dan GridSearchCV pada metode regresi, guna meningkatkan performa model yang dihasilkan. Melalui penerapan metode tersebut, diperoleh model deteksi untuk email phishing, email spam, Twitter spam, web phishing, dan Facebook spam dengan tingkat akurasi berturut-turut sebesar 99,70%, 99,06%, 89,05%, 94,18%, dan 95,83%.

6.2 Saran

Berdasarkan penelitian yang telah dilakukan, terdapat beberapa saran yang dapat diberikan dalam penelitian selanjutnya terkait deteksi *email phishing* agar penelitian selanjutnya dapat menghasilkan kinerja terbaik dan dapat menyelesaikan permasalahan yang muncul akibat dari *email phishing*. Berikut merupakan saran yang dapat diberikan untuk penelitian selanjutnya:

1. Penelitian selanjutnya diharapkan untuk memperkaya model dengan menambahkan jumlah training dataset sehingga model dapat bekerja lebih baik.
2. Penelitian selanjutnya lebih baik menambahkan beberapa elemen tambahan pada email yang dideteksi seperti *header email* yang memberikan informasi terkait pengirim, *subject*, dan *attachment*.