BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil evaluasi model, algoritma *Random Forest* menunjukkan performa terbaik dalam mendeteksi website phishing dibandingkan dengan *Support Vector Machine* (SVM) dan *Naive Bayes*. Hal ini ditunjukkan dari jumlah kesalahan klasifikasi yang paling sedikit, yaitu 70 false negative dan 73 *false positive*. Sementara itu, model SVM mencatatkan 101 false negative dan 134 *false positive*. Sedangkan model *Naive Bayes* memiliki jumlah kesalahan terbesar dengan 376 *false negative* dan 126 *false positive*.

Dari segi metrik evaluasi, *Random Forest* unggul di semua aspek dengan *accuracy*, *precision*, *recall*, dan *F1-score* sebesar 96%. Selanjutnya model SVM menempati posisi kedua dengan *accuracy* 93%, *precision* 92%, *recall* 94%, dan F1-score 93%. Sedangkan Naive Bayes memperoleh hasil paling rendah dengan *accuracy* 85%, *precision* 91%, *recall* 78%, dan F1-score 84%. Berdasarkan hasil tersebut, dapat disimpulkan bahwa algoritma *Random Forest* merupakan metode paling efektif yang digunakan dalam penelitian ini untuk mendeteksi *website phishing* berdasarkan URL.

5.2 Saran

Penelitian selanjutnya disarankan untuk mengeksplorasi algoritma lain seperti *XGBoost*, *Gradient Boosting*, atau pendekatan *deep learning* yang berpotensi memberikan performa lebih baik dalam mendeteksi *phishing*. Selain itu, penggunaan *dataset* yang lebih besar, beragam, dan terkini dapat meningkatkan kemampuan generalisasi model terhadap berbagai pola serangan *phishing* yang semakin kompleks dan dinamis.