BAB 5
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pengujian terhadap lima algoritma *Machine Learning*, yaitu *Isolation Forest*, *Neural Network*, *Random Forest*, *Support Vector Machine (SVM)*, dan *XGBoost*, dapat disimpulkan bahwa:

1. Berdasarkan penelitian, didapatkan algoritma yang paling efektif mendeteksi *phishing* dan *non-phishing*, yaitu *Neural Network*, yang mampu memprediksi URL benar *non-phishing* sebanyak 534, dan mampu mengidentifikasi URL *phishing* dengan benar sebanyak 532. Dengan masing-masing nilai *Training* Akurasi 97%, Presisi 96%, *Recall* 98%, dan AUC 97%. Validasi Akurasi 92%, Presisi 92%, *Recall* 92%, AUC 92%. Uji Akurasi 93%, Presisi 93%, *Recall* 93%, dan AUC 93%.
2. Sistem pendeteksi URL *phishing* berbasis web berhasil dirancang dan diimplementasikan menggunakan model *Neural Network* yang dilatih pada data URL *phishing* dan legitimate. Dengan memanfaatkan TF-IDF vectorizer dan framework Flask, sistem ini memungkinkan pengguna untuk memeriksa URL secara langsung melalui antarmuka web. Hasil prediksi ditampilkan secara langsung dan disertai penjelasan, sehingga sistem ini dapat membantu pengguna dalam mengidentifikasi dan mencegah ancaman *phishing* secara praktis.

5.2 Saran

Berdasarkan hasil penelitian dan analisis yang telah dilakukan, penulis menyadari bahwa penelitian ini masih memiliki beberapa keterbatasan. Oleh karena itu, agar penelitian di masa yang akan datang dapat dikembangkan lebih lanjut dan memberikan dampak yang lebih luas, berikut beberapa saran yang dapat menjadi bahan pertimbangan bagi peneliti selanjutnya:

1. Penelitian selanjutnya disarankan untuk menggunakan data URL *phishing* dan *non-phishing* yang diambil secara *real-time* dari aplikasi

WhatsApp atau layanan monitoring *phishing* terkini. Hal ini dapat meningkatkan relevansi dan efektivitas model dalam menghadapi pola serangan yang terus berkembang.

2. Sistem yang dikembangkan dalam penelitian ini masih difokuskan pada pengguna *WhatsApp*. Penelitian ke depan dapat mengembangkan sistem serupa untuk mendeteksi *phishing* pada *platform* media sosial lainnya seperti Instagram, Facebook, atau Telegram, sehingga cakupan perlindungannya menjadi lebih luas.
3. Pengembangan lebih lanjut dapat mencakup integrasi dengan chatbot atau sistem notifikasi otomatis (misalnya melalui Telegram atau *WhatsApp* API), yang memberikan peringatan secara langsung kepada pengguna ketika mereka menerima atau mengklik *link* mencurigakan.
4. Antarmuka aplikasi dapat terus disempurnakan agar lebih interaktif dan responsif. Selain itu, implementasi sistem di server hosting yang stabil (bukan hanya via Ngrok) akan membuat layanan ini lebih dapat diakses secara luas dan berkelanjutan.