

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian, implementasi sistem, dan pengujian yang telah dilakukan, maka dapat disimpulkan bahwa:

1. Sistem berhasil dirancang dan diimplementasikan dalam bentuk aplikasi web yang dapat menerima input URL secara tunggal. Sistem mampu melakukan ekstraksi fitur otomatis, melakukan klasifikasi menggunakan dua model *machine learning*, dan menampilkan hasilnya dalam bentuk tabel serta grafik.
2. Algoritma *Random Forest* dan *XGBoost* berhasil diterapkan sebagai model klasifikasi terhadap dataset URL yang telah diproses. Keduanya mampu memproses fitur hasil ekstraksi dari URL dan memberikan prediksi kategori (*benign, phishing, malware, defacement*) dengan tingkat akurasi yang tinggi. Proses klasifikasi dilakukan secara *real-time* di dalam sistem web.
3. Berdasarkan hasil evaluasi menggunakan metrik akurasi, *precision*, *recall*, dan *F1-score*, algoritma *XGBoost* menunjukkan performa yang lebih unggul dibandingkan *random forest*. *XGBoost* memperoleh akurasi sebesar 98,7%, sedangkan *random forest* sebesar 96,4%. Hal ini menunjukkan bahwa *XGBoost* lebih tepat digunakan sebagai model utama dalam sistem deteksi *phishing*.

5.2 Saran

Untuk pengembangan sistem di masa mendatang, beberapa saran yang dapat diberikan antara lain:

1. Pembaruan dataset secara berkala, agar model tetap relevan dengan pola dan teknik phishing terbaru yang terus berkembang.
2. Otomatisasi proses retraining, agar sistem dapat melakukan pelatihan ulang model secara otomatis setiap kali data baru ditambahkan, tanpa perlu intervensi manual.
3. Pengayaan fitur dengan menambahkan analisis konten halaman, metadata domain, sertifikat SSL, atau analisis reputasi URL melalui API eksternal, agar sistem lebih kuat dalam mendeteksi *phishing* tingkat lanjut.
4. Peningkatan keamanan aplikasi web, seperti *input validation*, *user session management*, dan integrasi autentikasi dua faktor (2FA), guna mencegah penyalahgunaan sistem.
5. Uji coba pengguna akhir (*user testing*) pada lingkungan nyata seperti institusi pendidikan atau organisasi publik untuk mendapatkan masukan terkait *usability* dan kebutuhan pengguna.

Dengan pengembangan lebih lanjut, sistem ini berpotensi menjadi alat bantu yang lebih komprehensif dan adaptif dalam menghadapi ancaman phishing yang semakin kompleks.