

## BAB V PENUTUP

### 5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa optimasi *hyperparameter* menggunakan metode *Random Search* mampu meningkatkan kinerja algoritma *Random Forest* dalam mendeteksi URL *phishing*. Pada tahap awal, model *Random Forest* tanpa optimasi sudah menunjukkan performa yang cukup baik. Model ini mencapai akurasi sebesar 97%, dengan nilai akurasi sebesar 98%, dengan nilai *precision* 98%, *recall* 98%, dan *F1-score* 98%. Kinerja tersebut semakin meningkat setelah diterapkannya metode SMOTE untuk mengatasi masalah ketidakseimbangan data, yang sering menjadi kendala dalam klasifikasi data keamanan seperti *phishing*.

Selanjutnya, dilakukan optimasi *hyperparameter* menggunakan metode *Random Search* dengan berbagai kombinasi *parameter* seperti jumlah pohon (*n\_estimators*), kedalaman maksimum (*max\_depth*), dan kriteria pemisahan (*criterion*). Hasil optimasi menunjukkan peningkatan performa model dengan akurasi naik menjadi 98%. Ini menandakan bahwa pemilihan parameter yang optimal dapat meningkatkan kemampuan model dalam mengenali pola data secara lebih efektif. Peningkatan performa model setelah optimasi menunjukkan bahwa proses tuning *hyperparameter* merupakan langkah penting dalam membangun sistem *machine learning* yang andal, khususnya dalam bidang *cybersecurity*. Deteksi *phishing* yang lebih akurat akan membantu dalam mengurangi risiko serangan siber yang berbasis pada URL *phishing*.

Selain itu, penelitian ini juga menunjukkan bahwa fitur-fitur URL seperti persentase tautan eksternal yang mengarahkan kembali ke *domain* awal, ketidaksesuaian nama *domain* yang sering terjadi, jumlah tanda hubung (-) dalam URL, serta indikasi pengiriman data melalui email merupakan indikator yang relevan dan efektif dalam membedakan URL *phishing* dan *non-phishing*. Dengan demikian, penelitian ini membuktikan bahwa optimasi *hyperparameter*

menggunakan *Random Search* dapat meningkatkan performa *Random Forest* secara signifikan dalam prediksi URL *phishing*. Hasil ini diharapkan dapat menjadi referensi bagi pengembangan sistem deteksi berbasis *machine learning* di bidang keamanan data, sehingga proses identifikasi URL *phishing* dapat dilakukan dengan lebih cepat, efisien, dan akurat.

## 5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, berikut beberapa saran yang dapat dijadikan acuan untuk pengembangan lebih lanjut dan perbaikan di masa mendatang:

1. Implementasi pada Sistem Jaringan Nyata

Penelitian ini masih bersifat simulasi berbasis *dataset*. Untuk pengembangan lebih lanjut, model dapat diintegrasikan secara langsung ke dalam sistem keamanan jaringan seperti *firewall*, *proxy server*, atau *DNS resolver* agar proses deteksi *phishing* dapat dilakukan secara real-time.

2. Kombinasi dengan Teknik Deteksi Lain

Untuk meningkatkan performa sistem secara keseluruhan, model dapat dikombinasikan dengan pendekatan lain seperti analisis konten halaman, analisis sertifikat SSL, atau pemantauan perilaku pengguna, sehingga tidak hanya mendeteksi *phishing* berdasarkan URL, tetapi juga dari konteks penggunaannya.

3. Eksplorasi Algoritma Lain dan Ensemble Learning

Meskipun *Random Forest* terbukti efektif, dapat mengeksplorasi algoritma lain seperti *XGBoost*, *LightGBM*, atau pendekatan *ensemble* yang lebih kompleks agar dapat membandingkan kinerja dan ketahanan model terhadap teknik *phishing* yang semakin canggih.