BAB 5
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, sistem deteksi *phishing* berbasis Android berhasil dirancang dan diimplementasikan menggunakan algoritma XGBoost yang dipilih dari perbandingan ketiga algoritma machine learning, yaitu LSTM, Random Forest, dan XGBoost. Aplikasi mampu melakukan deteksi URL *phishing* melalui integrasi model *machine learning* dengan *backend* sehingga pengguna dapat melakukan pemeriksaan URL secara langsung melalui perangkat mobile. Sistem juga dilengkapi dengan mekanisme *whitelist*, *blacklist*, histori pemeriksaan URL, serta fitur *report* URL untuk membantu proses verifikasi dan pembaruan database keamanan secara berkelanjutan.

Hasil pengujian menunjukkan bahwa ketiga algoritma memiliki performa klasifikasi yang sangat baik dalam mendeteksi URL *phishing* dan *legitimate*. Model LSTM memperoleh akurasi sebesar 94,05%, presisi 98,04%, *recall* 89,90%, dan nilai AUC sebesar 0,9790. *Random Forest* memperoleh akurasi sebesar 93,55%, presisi 95,22%, *recall* 91,70%, dan nilai AUC sebesar 0,9820. Sementara itu, XGBoost menunjukkan performa terbaik dengan akurasi sebesar 95,05%, presisi 96,78%, *recall* 93,20%, dan nilai AUC sebesar 0,9902. Selain itu, pengujian menggunakan dataset pribadi pada aplikasi mobile juga menunjukkan bahwa ketiga model mampu bekerja dengan baik pada kondisi implementasi nyata dengan XGBoost yang secara keseluruhan memiliki hasil terbaik. Dari sisi performa layanan, sistem mampu menangani permintaan deteksi *phishing* dari banyak pengguna secara bersamaan pada skenario pengujian 10, 100, 250, dan 500 pengguna dengan *error rate* sebesar 0%, yang menunjukkan bahwa seluruh permintaan dapat diproses tanpa kegagalan layanan. Hasil pengujian juga menunjukkan bahwa peningkatan jumlah pengguna menyebabkan kenaikan *response time*, namun sistem tetap mampu memberikan layanan deteksi *phishing* secara stabil meskipun dengan kenaikan jumlah pengguna bersamaan.

Secara keseluruhan, penelitian ini berhasil menunjukkan bahwa integrasi machine learning pada aplikasi Android dapat digunakan secara efektif untuk mendeteksi *phishing*. Sistem yang dikembangkan tidak hanya mampu memberikan performa klasifikasi yang

tinggi, tetapi juga memiliki performa layanan yang baik sehingga berpotensi menjadi solusi pendukung keamanan digital bagi pengguna perangkat mobile.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang dapat digunakan sebagai pengembangan penelitian pada masa mendatang agar performa dan fitur aplikasi deteksi *phishing* dapat menjadi lebih optimal.

- Penelitian selanjutnya dapat menggunakan dataset dengan jumlah yang lebih besar dan lebih beragam agar model *machine learning* mampu mempelajari pola URL *phishing* yang lebih kompleks dan terbaru
- Penelitian selanjutnya juga dapat melakukan pengujian performa aplikasi pada berbagai jenis perangkat mobile dan kondisi jaringan internet yang berbeda. Pengujian tersebut penting untuk memastikan bahwa aplikasi tetap dapat memberikan performa deteksi yang cepat dan stabil pada berbagai kondisi penggunaan
- Penelitian selanjutnya dapat menambahkan mekanisme pembaruan whitelist dan blacklist secara otomatis sehingga database URL yang digunakan sistem dapat selalu mengikuti perkembangan ancaman *phishing* teerbaru.
- Penelitian selanjutnya dapat menambahkan fitur lainnya seperti peringatan yang lebih rinci sehingga pengguna dapat memahami alasan suatu URL dikategorikan sebagai *phishing*, *suspicious*, atau *legitimate*