

## BAB V PENUTUP

### 5.1 Kesimpulan

Berdasarkan hasil penelitian, implementasi, dan pengujian yang telah dilakukan, maka dapat ditarik beberapa kesimpulan sebagai berikut:

Metode *machine learning*, secara spesifik menggunakan algoritma XGBoost, dapat digunakan secara efektif untuk mendeteksi *link phishing* melalui ekstraksi fitur leksikal dan statistik dari struktur URL tanpa perlu membuka isi halaman *website*. Sistem memproses karakteristik tautan—dengan fitur *Shannon Entropy* (tingkat keacakan karakter) sebagai indikator pendeteksi paling dominan—untuk membedakan URL berbahaya dan aman. Berdasarkan hasil pengujian pada dataset ekosistem platform X, model ini terbukti andal dengan mencapai tingkat akurasi sebesar 82,50% dan telah berhasil diimplementasikan ke dalam purwarupa aplikasi "Unmask" sebagai sistem perlindungan pengguna secara *real-time*.

### 5.2 Saran

Meskipun penelitian ini telah mencapai tujuannya, terdapat beberapa saran untuk pengembangan lebih lanjut guna meningkatkan keandalan sistem:

1. Pengembangan Dataset: Penelitian selanjutnya disarankan untuk menambah volume dan variasi dataset secara periodik guna mengikuti evolusi teknik pengaburan URL yang terus berkembang di media sosial.
2. Integrasi Konten: Disarankan untuk mengintegrasikan analisis gambar atau video (*Image/Video Processing*) bersamaan dengan analisis URL guna memberikan deteksi yang lebih komprehensif terhadap konten dewasa yang dijadikan umpan.
3. Ekspansi Platform: Sistem ini dapat dikembangkan lebih lanjut agar mampu mendeteksi tautan berbahaya di platform media sosial lain yang juga memiliki tingkat kerentanan serupa terhadap penyebaran konten ilegal.

4. Optimasi Hyperparameter: Melakukan eksperimen lebih mendalam pada tahap *tuning hyperparameter* algoritma XGBoost untuk mencapai skor evaluasi yang lebih tinggi lagi seiring dengan penambahan fitur-fitur baru.

