# BAB VI

# PENUTUP

## 6.1 Kesimpulan

Hasil analisis pada BAB IV dan evaluasi pada BAB V memberikan dasar untuk merumuskan kesimpulan sebagai berikut:

1. Penentuan fitur-fitur paling signifikan terhadap prediksi serangan siber menggunakan *Feature Importance* dengan algoritma *Random Forest* telah berhasil diterapkan, dan didapatkan sepuluh fitur paling signifikan dari *dataset* yaitu *url_entropy*, *url_ratio_special*, *url_len*, *content_entropy*, *content_ratio_special*, *lenght*, *content_len*, *url_num_params*, *Method_POST*, *dan url_has_query*. Fitur-fitur ini menjadi dasar utama dalam mengklasifikasikan lalu lintas HTTP menggunakan algoritma *Tree-Based Classifier* tanpa memerlukan proses NLP (*Natural Language Processing*) yang kompleks.
2. Berbeda dengan penelitian oleh [4] yang sangat bergantung pada teknik NLP (*character n-gram*) yang memiliki beban komputasi tinggi, penelitian ini berhasil membuktikan bahwa penggunaan algoritma *Tree-Based Classifier*, yaitu *Decision Tree*, *Random Forest*, GBM, dan *XGBoost*, pada fitur numerik hasil ekstraksi atribut HTTP mampu memberikan performa deteksi yang tetap tinggi namun lebih ringan dan efisien. Pendekatan non-NLP ini menawarkan keunggulan dalam hal efisiensi sumber daya dan interpretabilitas model yang lebih baik, sehingga lebih optimal untuk diimplementasikan pada sistem *Web*

*Application Firewall* (WAF) modern yang membutuhkan deteksi *real-time* tanpa terhambat oleh beban komputasi ekstraksi teks yang rumit.

3. Hasil evaluasi menggunakan *Stratified K-Fold Cross Validation* dan *Hyperparameter Tuning* (*RandomizedSearchCV*) menunjukkan bahwa model *Random Forest* (RF) adalah model yang paling unggul secara keseluruhan dengan nilai *F1-score* mencapai 92,71% dan *Recall* sebesar 94,95% pada *K-Fold* = 7. Meskipun penelitian terdahulu [4] mencapai *accuracy* 99,53% menggunakan SVM, hasil dalam penelitian ini membuktikan bahwa pendekatan *Tree-Based Classifier* hasil *tuning* memberikan performa yang kompetitif. Model RF menunjukkan peningkatan konsisten pada hampir seluruh metrik, sementara model *XGBoost* memberikan kompromi terbaik antara performa *F1-score* mencapai 92% dan efisiensi waktu komputasi yang rendah, hanya 39,45 detik. Selain itu, model *Gradient Boosting Machine* (GBM) juga mengalami peningkatan performa signifikan pasca-*tuning* dengan *F1-score* 92,58%.
4. Berdasarkan analisis mendalam terhadap hasil pengujian, model *Random Forest* (RF) ditetapkan sebagai model dengan efektivitas tertinggi karena mencapai nilai *F1-score* sebesar 92,71% dan *Recall* 94,95%, namun tuntutan sumber daya komputasinya sangat besar dengan waktu eksekusi mencapai 289,76 detik. Meskipun demikian, dalam skenario implementasi dunia nyata pada sistem keamanan *real-time* seperti *Web Application Firewall* (WAF), model *Decision Tree* (DT) justru lebih

direkomendasikan karena menawarkan efisiensi waktu yang luar biasa ekstrem, yakni hanya 2,05 detik atau sekitar 141 kali lebih cepat dibandingkan RF dengan tetap mempertahankan performa metrik yang sangat stabil pada angka *accuracy* sekitar 91,76%. Hal ini menunjukkan adanya *trade-off* strategis di mana penggunaan *Decision Tree* jauh lebih logis untuk lingkungan operasional karena mampu menghilangkan risiko latensi trafik aplikasi web secara signifikan dengan hanya mengorbankan marjin performa sebesar 0,91% dibandingkan model *ensemble* yang jauh lebih berat.

## 6.2 Saran

Berdasarkan keterbatasan dan hasil yang dicapai, terdapat beberapa poin strategis yang disarankan bagi peneliti selanjutnya untuk dieksplorasi lebih lanjut:

1. Mengintegrasikan teknik ekstraksi fitur yang lebih bervariasi untuk menangkap pola serangan *payload* yang terenkripsi agar dapat semakin mendekati atau melampaui performa metode berbasis NLP namun tetap mempertahankan efisiensi komputasi.
2. Melakukan pengujian model pada *dataset* lalu lintas HTTP yang lebih baru dan dinamis untuk memvalidasi ketangguhan model terhadap varian serangan siber *zero-day* yang terus berkembang.
3. Melakukan implementasi model hasil *tuning* ke dalam *environment* server yang sesungguhnya untuk mengukur *latency* dan kecepatan deteksi per unit waktu dalam menangani trafik data yang besar.