BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pengujian terhadap lima algoritma *Machine Learning*, yaitu *Random Forest, K-Nearest Neighbors (KNN), Support Vector Machine (SVM), Naïve Bayes,* dan *Logistic Regression*, dapat disimpulkan bahwa algoritma Random Forest dengan optimasi *GridSearchCV* memberikan performa terbaik dalam mendeteksi anomali dan serangan pada jaringan komputer, baik dalam skenario klasifikasi biner maupun multi-kelas.

Model *Random Forest* memperoleh akurasi tertinggi, yaitu 99,1% (klasifikasi biner) dan 94,2% (multi-kelas) pada dataset *NSL-KDD*, serta 95,5% (biner) dan 91,7% (multi-kelas) pada dataset *UNSW-NB15*. Selain akurasi, Random Forest juga mencatat nilai *F1-score* tertinggi dan paling stabil, terutama pada kelas-kelas minoritas, menunjukkan kemampuannya yang unggul dalam menangani data tidak seimbang dan mendeteksi berbagai jenis serangan secara konsisten.

Model *K-Nearest Neighbors (KNN)* menunjukkan performa kompetitif, terutama pada dataset NSL-KDD, dengan akurasi hingga *97,8%* dan nilai F1-score yang cukup baik. Namun, model ini mengalami penurunan performa pada klasifikasi multi-kelas di dataset *UNSW-NB15*. Sementara itu, algoritma seperti *Naïve Bayes* dan *Logistic Regression* tidak mampu menangani distribusi kelas yang tidak seimbang secara efektif, dengan penurunan F1-score yang signifikan pada beberapa kelas serangan.

Secara keseluruhan, penelitian ini menyimpulkan bahwa *Random Forest* dengan tuning parameter menggunakan *GridSearchCV* adalah model yang paling efektif, stabil, dan adaptif untuk digunakan dalam sistem deteksi anomali jaringan berbasis Machine Learning, terutama dalam konteks lingkungan nyata yang menghadirkan variasi serangan dan distribusi data yang kompleks.

5.2 Saran

Penelitian selanjutnya disarankan untuk mencoba algoritma lain yang lebih kompleks, seperti algoritma *deep learning* (misalnya *Artificial Neural Network, Convolutional Neural Network,* atau *Recurrent Neural Network*) yang memiliki kemampuan lebih baik dalam mengenali pola data yang kompleks. Selain itu, dapat pula dieksplorasi penggunaan teknik ensemble seperti *XGBoost* atau *LightGBM* yang sering menunjukkan performa tinggi dalam klasifikasi. Dengan mencoba berbagai pendekatan tersebut, diharapkan hasil deteksi serangan dapat menjadi lebih akurat dan kokoh terhadap berbagai jenis ancaman pada jaringan