BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Penelitian ini bertujuan untuk menganalisis penerapan algoritma *Isolation Forest* dan *K-Means* dalam mendeteksi anomali pada trafik jaringan menggunakan dataset CIC-IDS2017, serta mengevaluasi efektivitas kombinasi kedua algoritma tersebut. Berdasarkan hasil pengujian dan analisis, diperoleh beberapa kesimpulan sebagai berikut.

Pertama, algoritma *Isolation Forest* terbukti mampu mendeteksi trafik anomali dengan baik berdasarkan penyimpangan nilai fitur numerik dari distribusi mayoritas data. Hasil pengujian menunjukkan bahwa *Isolation Forest* mendeteksi sekitar 10% data sebagai anomali, yang umumnya memiliki karakteristik berupa *packet size* besar, *duration* panjang, serta nilai bytes_in dan bytes_out yang tinggi. Hal ini menunjukkan bahwa Isolation Forest efektif dalam mengidentifikasi *outlier* individual pada trafik jaringan yang memiliki nilai ekstrem.

Kedua, algoritma *K-Means* mampu mengelompokkan trafik jaringan ke dalam beberapa cluster berdasarkan kemiripan karakteristik fitur. Dari hasil *clustering*, ditemukan bahwa cluster dengan jumlah anggota kecil mengandung data yang memiliki pola trafik tidak lazim, terutama pada volume transfer data. Hasil pengujian menunjukkan bahwa *K-Means* mendeteksi sekitar 8,5% data sebagai indikasi anomali melalui pendekatan *cluster* kecil. Temuan ini menunjukkan bahwa *K-Means* berperan dalam mengungkap struktur distribusi data dan pola komunikasi jaringan yang menyimpang secara kolektif.

Ketiga, kombinasi *Isolation Forest* dan *K-Means* menghasilkan deteksi anomali yang lebih komprehensif dibandingkan penggunaan masing-masing algoritma secara terpisah. Berdasarkan hasil pengujian, pendekatan hybrid mendeteksi sekitar 12% data sebagai anomali, yang merupakan gabungan dari anomali berbasis isolasi nilai ekstrem dan anomali berbasis distribusi *cluster*. Visualisasi menggunakan PCA dua dimensi menunjukkan bahwa data yang

terdeteksi sebagai anomali cenderung terpisah dari kelompok utama trafik normal. Hal ini membuktikan bahwa integrasi kedua algoritma mampu meningkatkan cakupan deteksi anomali pada trafik jaringan.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa penerapan algoritma *Isolation Forest* dan *K-Means*, baik secara individual maupun terintegrasi, dapat digunakan secara efektif untuk mendeteksi anomali pada trafik jaringan. Pendekatan *hybrid* yang diusulkan mampu memberikan deteksi yang lebih adaptif terhadap variasi pola trafik jaringan, sehingga berpotensi mendukung pengembangan sistem deteksi intrusi berbasis *machine learning*.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang dapat dipertimbangkan untuk pengembangan penelitian selanjutnya. Penelitian ini masih berfokus pada analisis deteksi anomali secara deskriptif, sehingga pada penelitian berikutnya disarankan untuk melakukan evaluasi kinerja model secara kuantitatif dengan memanfaatkan label serangan yang tersedia pada dataset CIC-IDS2017. Evaluasi tersebut dapat mencakup pengukuran akurasi, *precision, recall*, dan *F1-score* guna memberikan gambaran yang lebih objektif mengenai performa algoritma dalam mendeteksi trafik anomaly.

Selain itu, penelitian selanjutnya dapat mempertimbangkan penggunaan atau perbandingan deng0,88 cman algoritma deteksi anomali lain, seperti *DBSCAN, One-Class SVM*, maupun *Autoencoder*, untuk mengetahui keunggulan dan keterbatasan pendekatan *hybrid Isolation Forest* dan *K-Means* yang digunakan dalam penelitian ini. Dengan adanya perbandingan tersebut, diharapkan dapat diperoleh model deteksi anomali yang lebih optimal terhadap variasi pola trafik jaringan.

Pengembangan lebih lanjut juga dapat dilakukan dengan menerapkan teknik pemilihan fitur (*feature selection*) atau reduksi dimensi secara lebih mendalam, sehingga model yang dihasilkan tidak hanya akurat, tetapi juga lebih efisien

dalam memproses data berskala besar. Hal ini penting mengingat dataset trafik jaringan umumnya memiliki jumlah fitur dan volume data yang tinggi.

Di samping itu, penelitian selanjutnya disarankan untuk mengimplementasikan model deteksi anomali dalam lingkungan jaringan secara *real-time* guna menguji kinerja algoritma dalam kondisi operasional yang sesungguhnya. Integrasi sistem deteksi anomali dengan perangkat keamanan jaringan seperti *Intrusion Detection System* (IDS) atau *Security Information and Event Management* (SIEM) juga dapat menjadi arah penelitian lanjutan yang relevan, sehingga hasil penelitian tidak hanya bersifat akademis, tetapi juga memiliki nilai praktis dalam mendukung keamanan jaringan.