BAB V
KESIMPULAN DAN SARAN

Pada bab ini akan diuraikan beberapa kesimpulan yang dapat diambil dari pembahasan sebelumnya dan saran mengenai masalah yang bisa dibahas sebagai kelanjutan dari penelitian ini.

5.1 Kesimpulan

Berdasarkan hasil penelitian dan analisis yang telah dilakukan, dapat disimpulkan bahwa metode *Transformer* yang dioptimasi dengan *transfer learning* mampu secara efektif mengklasifikasikan jenis serangan siber yang terjadi pada server, khususnya serangan SQL *Injection* dan DDoS. Proses klasifikasi dilakukan dengan memanfaatkan model *pretrained* seperti BERT dan RoBERTa, yang mampu menangkap pola-pola kontekstual dalam data log sekuensial. Untuk mendukung proses pelatihan, data serangan siber diproses melalui tahapan data *preprocessing*, termasuk pembersihan data, tokenisasi, *encoding*, dan normalisasi, agar sesuai dengan format input model berbasis *Transformer*. Tahapan ini memastikan bahwa data *log* yang awalnya tidak terstruktur dapat diolah secara efisien oleh arsitektur model *Transformer*. Klasifikasi jenis serangan siber seperti Normal, SQL *Injection*, dan DDoS dapat dilakukan secara efektif dengan menggunakan metode *Transformer*, khususnya model BERT dan RoBERTa. Model ini mampu mengenali pola dalam log aktivitas HTTP dan membedakan antara jenis serangan dengan tingkat akurasi yang tinggi, mencapai 0.90 pada data uji.

Selain itu, penelitian ini juga menunjukkan bahwa penerapan metode *transfer learning*, khususnya pendekatan ULMFiT, mampu mengoptimalkan performa model *Transformer*. Dengan memanfaatkan pengetahuan awal dari model bahasa umum dan melakukan *fine-tuning* pada data serangan spesifik, model menjadi lebih akurat dan stabil dalam proses klasifikasi. Setelah dioptimasi, akurasi model meningkat hingga 0.97, yang menunjukkan bahwa *transfer learning* sangat efektif dalam menangani keterbatasan data minoritas seperti pada kasus serangan

DDoS. Evaluasi performa menggunakan metrik akurasi, *precision*, *recall*, f1-*score*, dan *confusion matrix* menunjukkan peningkatan signifikan dalam kemampuan model mengenali jenis serangan yang sebelumnya sulit terdeteksi. Dengan demikian, kombinasi antara metode *Transformer* dan *transfer learning* terbukti menjadi solusi yang andal dan efisien untuk membangun sistem deteksi serangan siber yang cerdas dan adaptif.

5.2 Saran

Berdasarkan hasil perancangan dan pengujian yang telah dilakukan dalam penelitian ini, dapat diberikan beberapa saran untuk penelitian selanjutnya.

1. Penggunaan dataset yang lebih besar dan beragam agar model lebih tangguh terhadap berbagai jenis serangan.
2. Menerapkan teknik penanganan data tidak seimbang seperti *oversampling*, *undersampling*, atau *class weight adjustment* untuk meningkatkan deteksi kelas minoritas.
3. Mengeksplorasi model *transformer* lain seperti *XLNet*, *ELECTRA*, atau *LLaMA* untuk membandingkan performa lebih lanjut.
4. Mengintegrasikan pendekatan semi-*supervised learning* atau *unsupervised anomaly detection* untuk deteksi serangan baru yang belum dilabeli.
5. Mengembangkan sistem klasifikasi ini dalam bentuk aplikasi atau sistem monitoring *real-time* untuk implementasi langsung di lingkungan produksi.