# ABSTRAK

Dalam era perkembangan teknologi yang pesat saat ini, inovasi-inovasi baru terus bermunculan, termasuk di bidang jaringan komputer melalui perangkat server. Server berfungsi untuk menyimpan informasi dan data dalam suatu jaringan. Server berperan penting dalam melayani *client* atau *workstation* yang terhubung ke jaringan dan berfungsi sebagai inti dari sistem komunikasi jaringan yang menyediakan layanan (server) kepada pengguna. Server menyimpan banyak aktivitas *log* yang mencatat berbagai tindakan dan kejadian dalam sistem komputer. Namun, pengelola *log* aktivitas server yang besar seringkali dilakukan secara manual, sehingga memerlukan penguatan keamanan teknologi informasi dan otomatisasi dalam analisis *log*. Ini membantu perusahaan menghadapi ancaman keamanan dengan lebih efektif dan melindungi integritas data di server.

Solusi yang diusulkan dalam proyek ini memanfaatkan server berbasis Linux sebagai alternatif untuk mengurangi pengeluaran yang seharusnya digunakan untuk lisensi perangkat lunak. Server Linux dikenal karena fleksibilitasnya yang tinggi yang memungkinkan penyesuaian sesuai dengan persyaratan khusus perusahaan. Selanjutnnya, proyek ini juga mengadopsi solusi ELK *Stack* (Elasticsearch, Logstash, Kibana) yang memberikan kelebihan dalam hal kemudahan aksebilitas. Di samping itu, ELK *Stack* memampukan pengguna untuk melakukan pencarian, analisis, dan visualisasi data secara instansi.

Selama pelaksanaan proyek ini, kami melaksanakan pengawasan pada jaringan switch selama 24 jam. Hasil pemantauan menunjukkan bahwa ada sejumlah 6325 paket yang tiba selama periode tersebut. Data ini dapat direpresentasikan secara visual melalui grafik batang (*bar chart*) dan grafik garis (*line chart*). Untuk mencapai tujuan prediksi jumlah paket yang akan tiba pada waktu berikutnya, menggunakan metode *Support Vector Regression* (SVR) dan *Random Forest Regression* (RFR) untuk mencapainya. Dalam kesimpulannya, penelitian ini dapat dilakukan dengan berbagai rentang waktu, dan hasil prediksi digunakan untuk mengidentifikasi apakah terjadi peningkatan yang signifikan dalam jumlah paket yang tiba.

**Kata kunci**: Elasticsearch, Logstash, dan Kibana