ABSTRACT

In the rapidly evolving era of technology, new innovations continue to emerge, including in the field of computer networking through server devices. Servers function to store information and data within a network. They play a crucial role in serving clients or workstations connected to the network and serve as the core of the network communication system that provides services to users. Servers store a multitude of log activities that record various actions and events within a computer system. However, managing the logs of such extensive server activities is often done manually, necessitating the strengthening of information technology security and log analysis automation. This helps companies more effectively address security threats and safeguard data integrity on the server.

The proposed solution in this project utilizes Linux-based servers as an alternative to reduce expenses that would otherwise be allocated for software licensing. Linux servers are renowned for their high flexibility, allowing customization to meet specific company requirements. Furthermore, this project also adopts the ELK Stack solution (Elasticsearch, Logstash, Kibana), which offers advantages in terms of ease of accessibility. Additionally, ELK Stack enables users to perform real-time data search, analysis, and visualization.

During the implementation of this project, we conducted network switch monitoring for 24 hours. The monitoring results indicated that there were a total of 6325 packets arriving during that period. This data can be visually represented through bar charts and line charts. To achieve the goal of predicting the number of packets that will arrive in the next time frame, we employed the Support Vector Regression (SVR) and Random Forest Regression (RFR) methods. In conclusion, this research can be conducted across various time ranges, and the prediction results are used to identify whether there is a significant increase in the number of incoming packets.

Keywords: Elasticsearch, Logstash, Kibana