ABSTRACT

Currently, the use of the internet has become a necessity in daily activities. Based on a DataReportal report, internet users in Indonesia in January 2022 were 73.7%. The data shows that as the digital era develops, internet users will also continue to grow. Every internet usage activity will be recorded in inbound and outbound network traffic. On the inbound and outbound networks data, traffic will display the normal trend data. However, data that is out of trend data can also appear which is referred to as anomalous data. Such anomalous network traffic can occur due to a significant increase in the volume of network traffic data. One of them can be caused by network problems or cyber-attacks. Anomalies in inbound and outbound network traffic data also occur in PT XYZ is a company that focuses on information and communication technology (ICT) services and telecommunications networks in Indonesia. To prevent anomalous data from occurring in traffic networks, you can use an intrusion detection system (IDS) through anomaly detection with an algorithm that can process sequence data and large-scale data. This is enough to keep network activity normal and safe. The algorithm used in this research is Long Short-Term Memory (LSTM). This study uses the CRISP-DM methodology as a systematic problem solution. There are several stages that are implemented, like business understanding, data understanding, data preparation, modeling, and evaluation. The analysis and design carried out in this study are based on PT XYZ company business rules to adjust to company regulations and needs. Model testing and model evaluation are carried out based on the specified parameters to produce a model that can detect anomalies.

Keywords: anomaly detection, deep learning, long short-term memory (lstm)