

ABSTRAK

Saat ini penggunaan internet sudah menjadi kebutuhan dalam kegiatan sehari-hari. Berdasarkan laporan DataReportal, pengguna internet di Indonesia pada Januari 2022 ada sebanyak 73,7%. Data tersebut menunjukkan bahwa seiring berkembangnya era digital, pengguna internet juga akan terus bertambah. Setiap aktivitas penggunaan internet akan terekam dalam suatu lalu lintas jaringan *inbound* dan *outbound*. Pada lalu lintas jaringan *inbound* dan *outbound*, akan menampilkan tren data normal. Namun dapat juga muncul data yang diluar tren yang disebut sebagai data anomali. Lalu lintas jaringan anomali tersebut dapat terjadi karena adanya peningkatan yang signifikan dalam volume data lalu lintas jaringan. Salah satunya dapat diakibatkan masalah jaringan ataupun serangan *cyber*. Anomali pada data lalu lintas jaringan *inbound* dan *outbound* juga terjadi pada data lalu lintas jaringan PT XYZ yang merupakan perusahaan yang berfokus pada bidang jasa layanan teknologi informasi dan komunikasi (TIK) dan jaringan telekomunikasi di Indonesia. Untuk mencegah terjadinya data anomali, dapat menggunakan *intrusion detection system* (IDS) melalui deteksi anomali dengan algoritma yang dapat memproses data sekuen dan data skala besar. Hal tersebut dilakukan untuk menjaga aktivitas jaringan tetap normal dan aman. Algoritma yang digunakan dalam penelitian ini adalah *Long Short-Term Memory* (LSTM). Penelitian ini menggunakan metodologi CRISP-DM sebagai sistematika penyelesaian masalah. Terdapat beberapa tahapan yang diterapkan yaitu *business understanding*, *data understanding*, *data preparation*, *modelling*, dan evaluasi. Analisis dan perancangan yang dilakukan dalam penelitian ini berlandaskan pada *business rules* perusahaan PT XYZ untuk menyesuaikan peraturan dan kebutuhan perusahaan. Pengujian model dan evaluasi model dilakukan berdasarkan parameter yang ditentukan menghasilkan model yang dapat mendeteksi anomali.

Kata kunci: deteksi anomali, *deep learning*, *long short-term memory* (*lstm*)