

BAB I PENDAHULUAN

I.1 Latar Belakang

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% dari total populasi atau sekitar 204,7 juta pengguna. Angka tersebut naik sebanyak 1% dibandingkan dengan data pengguna internet pada tahun 2021. 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*. Lalu lintas jaringan *inbound* merupakan data jaringan masuk atau unduh yang dilakukan oleh pengguna internet. Sedangkan lalu lintas jaringan *outbound* merupakan data jaringan keluar atau unggah yang dilakukan oleh pengguna internet.

Pada lalu lintas jaringan *inbound* dan *outbound*, akan menampilkan tren data normal dan tidak normal atau 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. Aktivitas yang menyebabkan adanya anomali pada lalu lintas jaringan bukan hanya karena masalah jaringan saja, tetapi dapat juga dikarenakan oleh adanya kerusakan pada sistem layanan internet atau bahkan adanya serangan kejahatan *cyber*.

Lalu lintas jaringan yang anomali ditunjukkan pada perubahan secara tiba-tiba pada grafik *multi router traffic grapher* (MRTG) yang awalnya konsisten normal pada pergerakannya, tiba-tiba menjadi naik volumenya yang berarti terjadi sesuatu yang tidak biasa sehingga menimbulkan kecurigaan adanya gangguan yang terjadi. *Multi router traffic grapher* (MRTG) merupakan suatu aplikasi yang digunakan untuk memantau grafik volume penggunaan pada lalu lintas jaringan. Penggunaan internet yang semakin banyak akan menimbulkan data lalu lintas jaringan yang semakin tinggi frekuensinya yang dapat menyebabkan semakin sulit dalam monitoring lalu lintas jaringan dan sulit untuk mengetahui penyebab adanya data anomali karena aktifitas anomali dapat berkamufase dengan mudah bersamaan dengan data lainnya. Untuk menghindari hal tersebut maka perlu mendeteksi anomali pada lalu lintas jaringan *inbound* dan *outbound* supaya dapat mengetahui

penyebab adanya data anomali tersebut sehingga dapat melakukan perbaikan layanan untuk memperkecil kemungkinan terjadinya anomali.

Salah satu organisasi yang melakukan monitoring lalu lintas jaringan di Indonesia adalah PT XYZ. PT XYZ merupakan perusahaan yang berfokus pada bidang jasa layanan teknologi informasi dan komunikasi (TIK) dan jaringan telekomunikasi di Indonesia. Salah satu misi PT XYZ adalah mengorkestrasi ekosistem digital untuk memberikan pengalaman digital pelanggan terbaik. Berkaitan dengan misi tersebut, PT XYZ terus melakukan memperbaiki kinerja menjadi lebih baik. Salah satu hal yang harus dilakukan adalah mencegah terjadinya serangan kejahatan *cyber* dengan menggunakan *intrusion detection system* (IDS) melalui deteksi anomali. Hal tersebut dilakukan untuk menjaga aktivitas jaringan tetap normal dan aman dengan meminimalisir adanya anomali sehingga perusahaan dapat memberikan pengalaman digital pelanggan terbaik tanpa ada gangguan. IDS merupakan sistem deteksi gangguan lalu lintas jaringan yang dapat mencegah terjadinya serangan kejahatan *cyber* (Said Elsayed dkk., 2020). Untuk mendeteksi anomali pada lalu lintas jaringan internal dapat menggunakan IDS. Perusahaan mengalami kendala yaitu belum bisa mendeteksi setiap anomali pada lalu lintas jaringan internal dikarenakan belum ada sistem IDS yang melakukan deteksi anomali dan memiliki dataset yang *time-series*.

Berdasarkan permasalahan tersebut, maka dilakukan penelitian untuk mengembangkan model sebagai solusi yang dapat mendeteksi anomali pada lalu lintas jaringan internal data *inbound* dan *outbound* perusahaan. Data *inbound* dan *outbound* perusahaan merupakan data yang memiliki ukuran besar, *time-series*, dan berupa data sekuen, sehingga peneliti tidak dapat membangun model menggunakan *machine learning* karena faktor tersebut. Salah satu model yang dapat digunakan untuk mendeteksi anomali pada lalu lintas jaringan internal data *inbound* dan *outbound* yaitu model *deep learning* karena proses yang dilakukan lebih mendalam daripada *machine learning*. *Deep learning* mampu menyelesaikan masalah dengan tingkat akurasi lebih baik yang tidak dapat dikerjakan dengan menggunakan metode sebelumnya yaitu *machine learning* (Gulli dkk., t.t.). Eka Setya Wijaya, Abdul Syukur, dan Romi Satria Wahono menggunakan *deep learning* untuk mendeteksi anomali lalu lintas jaringan. Penelitian tersebut menghasilkan model yang dapat

mendeteksi adanya anomali lalu lintas jaringan dengan tingkat akurasi di atas 99%. Berdasarkan hal tersebut, model *deep learning* (DL) diharapkan dapat memecahkan masalah yang sedang dihadapi oleh peneliti.

Deep learning merupakan metode yang dapat digunakan pada data yang tidak terstruktur. Hal tersebut sesuai dengan data yang digunakan oleh peneliti yaitu berupa data tidak terstruktur. ANN merupakan bagian dari *deep learning* yang cara bekerjanya dirancang seperti cara saraf otak manusia bekerja, sehingga komputer dapat mempelajari data abstrak dan permasalahan yang tidak didefinisikan dengan baik kemudian memberikan keputusan yang paling baik (Hurwitz & Kirsch, 2018). ANN memiliki beberapa metode seperti *convolutional neural network* (CNN) dan *recurrent neural network* (RNN). Dua metode tersebut merupakan metode yang banyak digunakan. CNN dan RNN sendiri merupakan metode tingkat lanjut dari *neural network* yang ada pada *deep learning*. CNN memiliki cara kerja yang terinspirasi dari konsep klasik sel sederhana dan sel kompleks pada visual ilmu saraf. Namun CNN tidak memiliki hubungan antar saraf pada layer yang sama pada model, alur data *input* serta data *output* yang menyebabkan sulit untuk memproses data yang saling terkait atau mirip pada CNN. Sedangkan RNN dapat memproses input berdasarkan urutan dengan menggunakan status memori sehingga dapat diterapkan untuk pengenalan suara atau pengenalan tulisan karena pada RNN data input saling terkait satu sama lain. Dengan menggunakan RNN yang memiliki tingkat lebih tinggi dari CNN, dapat menyelesaikan permasalahan tersebut untuk memproses data sekuensial (Wei, Chu, Sun, Xu, Deng, Chen, Wei & Lei, 2019).

Fathu Rahman melakukan penelitian untuk deteksi anomali data jaringan menggunakan *long short-term memory* (LSTM) yang merupakan salah satu modifikasi RNN yang populer digunakan. Penelitian tersebut berhasil menghasilkan model yang dapat mendeteksi adanya anomali pada dataset yang diteliti. Dengan menggunakan LSTM dapat menyimpan inputan dalam jangka waktu lama sehingga dapat membaca, menulis, dan menghapus informasi dari memori lebih baik. Berdasarkan hal tersebut peneliti menggunakan algoritma LSTM untuk mendeteksi anomali lalu lintas jaringan internal pada data *inbound* dan *outbound*. Dengan menggunakan LSTM dapat memproses data sekuen yang panjang, harapannya LSTM dapat menghasilkan model yang memiliki akurasi tinggi dan hasil yang baik terhadap deteksi anomali lalu lintas jaringan internal data *inbound* dan *outbound*.

I.2 Perumusan Masalah

Berdasarkan latar belakang, rumusan masalah yang mendasari penelitian ini adalah:

- a. Bagaimana rancangan deteksi anomali lalu lintas jaringan internal *inbound* dan *outbound*?
- b. Bagaimana proses untuk mendeteksi anomali lalu lintas jaringan internal *inbound* dan *outbound*?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

- a. Menganalisis rancangan deteksi anomali lalu lintas jaringan internal *inbound* dan *outbound* untuk mendukung *quality control* perusahaan.
- b. Menganalisis proses untuk mendeteksi anomali lalu lintas jaringan internal *inbound* dan *outbound*.

I.4 Batasan Penelitian

Penelitian ini dibatasi dengan fokus pada:

- a. Deteksi anomali menggunakan data lalu lintas jaringan internal bulan Januari hingga November tahun 2022 yang diberikan oleh PT XYZ.
- b. Deteksi anomali menggunakan data lalu lintas jaringan internal dengan id 2, 7, 12, 13, 19, 23, 28, 70

I.5 Manfaat Penelitian

Manfaat penelitian ini adalah:

- a. Bagi perusahaan, penelitian ini bermanfaat dalam mendeteksi anomali lalu lintas jaringan pada data internal *inbound* dan *outbound* dengan menggunakan model *deep learning*, sehingga dapat mendeteksi anomali lalu lintas jaringan data internal untuk mendukung *quality control* perusahaan dan meningkatkan kinerja menjadi lebih baik lagi.
- b. Bagi peneliti lain yang fokus dalam bidang *machine learning* dan *deep learning*, penelitian ini diharapkan dapat bermanfaat dalam memberikan wawasan dalam mendeteksi anomali lalu lintas jaringan internal *inbound* dan *outbound* menggunakan algoritma LSTM sehingga dapat memberikan solusi peningkatan efisiensi kinerja.

I.6 Sistematika Penulisan

Pada penelitian ini dibagi menjadi beberapa bab dari pokok pembahasan, secara umum dapat dijelaskan sebagai berikut.

BAB I PENDAHULUAN

Bab ini menjelaskan uraian konteks permasalahan dan latar belakang, perumusan masalah, tujuan penelitian, batasan penelitian, dan sistematika dari penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan mengenai literatur terkait yang digunakan dan penelitian terdahulu yang berkaitan sebagai referensi dasar pengerjaan penelitian.

BAB III METODOLOGI PENELITIAN

Tahapan penelitian dijelaskan secara garis besar pada bab ini yang terdiri dari kerangka pemecahan masalah dalam penelitian, sistematika penyelesaian masalah, pengumpulan data, pengolahan data, dan metode evaluasi.

BAB IV ANALISIS DAN PERANCANGAN

Bab ini berisi analisis dan perancangan proses penelitian yang akan dilakukan berdasarkan penjelasan pada bab sebelumnya.

BAB V IMPLEMENTASI HASIL ANALISIS

Bab ini berisi penjelasan implementasi dan hasil analisis dari perancangan yang dijelaskan pada bab sebelumnya serta tahap evaluasi hasil analisis.

BAB VI KESIMPULAN DAN SARAN

Bab ini berisi jawaban atas pertanyaan penelitian yang disajikan pada pendahuluan serta menyajikan saran untuk penelitian selanjutnya.