BAB I

PENDAHULUAN

1.1 Latar Belakang

Pesatnya perkembangan teknologi informasi telah memudahkan manusia di banyak sektor penting kehidupan. Pada sektor ekonomi, perkembangan teknologi informasi telah memudahkan manusia dalam perdagangan secara global. Pada sektor pendidikan dan pemerintahan, teknologi informasi telah memudahkan peneliti untuk berkolaborasi serta memudahkan pemerintah untuk menyebarkan informasi secara luas kepada masyarakat. Penggunaan teknologi informasi secara masif ini menghasilkan peningkatan ukuran jaringan dan jumlah data yang mengalir di jaringan dengan pesat [1], seperti data transaksi keuangan, data informasi pribadi dan data penting lainnya. Akan tetapi, seiring perkembangan teknologi informasi, ancaman yang menyertainya juga turut berkembang.

Menurut *National Institute of Standard and Technology* (NIST), intrusi merupakan kejadian, atau rangkaian kejadian dimana seseorang mendapatkan atau mencoba mendapatkan akses ke sistem atau sumber daya sistem tanpa memiliki otoritas untuk melakukannya [2]. Dengan kata lain, intrusi dapat diartikan sebagai percobaan yang dilakukan untuk mengakses sistem secara tidak sah dengan tujuan untuk merusak atau

menyalahgunakannya.

Pada dasarnya, hampir semua sistem jaringan yang ada mempunyai celah keamanan yang mengakibatkan sistem tersebut rentan terhadap intrusi dan penyalahgunaan oleh orang dalam [3]. Walaupun begitu, menemukan dan memperbaiki semua celah keamanan tersebut tidak mudah, dan di sisi lain mengembangkan sistem yang tidak memiliki celah keamanan sama sekali juga merupakan suatu hal yang hampir mustahil untuk dilakukan [3][4]. Oleh karena itu, diperlukan sebuah sistem yang mampu mendeteksi intrusi jaringan secara *real-time* dan memberikan peringatan lebih awal (*early warning*) sehingga pihak berwenang dapat mengatasinya sebelum serangan itu berkembang lebih lanjut. Sistem ini dikenal sebagai *Intrusion Detection System* (IDS).

Sistem deteksi intrusi pertama kali diperkenalkan oleh Jim Anderson pada tahun 1980 [5] yang menggunakan pendekatan statistik untuk mendeteksi intrusi. Jim Anderson menggunakan asumsi awal bahwa suatu aktivitas dapat dikategorikan ke jenis aktivitas tertentu (normal atau serangan) jika aktivitas tersebut memperlihatkan sifat yang sama dengan kelompok aktivitas terntu, yaitu kelompok aktivitas normal dan serangan. Sejak saat itu, berbagai penelitian telah dilakukan untuk pengembangan sistem deteksi intrusi yang lebih baik, efektif, dan efisien.

Salah satu penelitian yang cukup populer yaitu penelitian yang dilakukan oleh *Lincoln Laboratory of MIT* yang melakukan evaluasi terhadap sistem deteksi intrusi menggunakan metode *Receiver Operating Characteristic* (ROC). Akan tetapi, penelitian ini mendapat cukup banyak kritikan, seperti

yang dilakukan oleh John McHugh yang mengkritik metode evaluasi yang digunakan karena metode ROC sendiri memiliki beberapa asumsi dasar yang perlu terpenuhi [6], sedangkan pada penelitian tersebut tidak disebutkan secara jelas apakah asumsi tersebut terpenuhi. Tidak adanya informasi yang jelas mengenai terpenuhinya asumsi ini dapat memberikan hasil evaluasi yang bias [6].

Tak berselang lama setelah penelitian yang dilakukan oleh *Lincoln Laboratory of MIT*, Pada tahun 2001 Dickerson melakukan penelitian mengenai pengembangan sistem deteksi intrusi jaringan menggunakan pendekatan *fuzzy logic* [7]. Pada penelitian ini, metode *Fuzzy C-Means Clustering* digunakan untuk mendeteksi intrusi. Metode ini bekerja cukup baik walaupun dengan *false negative rate*, yaitu proporsi hasil negatif yang salah diprediksi oleh model, yang bernilai cukup tinggi.

Pada tahun 2019, Xianwei Gao mengembangkan sistem deteksi intrusi dengan pendekatan *machine learning*. Xianwei menggunakan metode *ensemble* adaptif dengan beberapa *classifier*, seperti *Decision Tree*, *Deep Neural Network*, *K-Nearest Neighbor* (KNN), dan beberapa *classifier* lain [8] dengan dataset pelatihan yang bernama NSL-KDD. Dengan menggunakan pendekatan ini, metode *ensemble* adaptif yang dikembangkan berhasil memperoleh akurasi 85,2%.

Disamping pendekatan *machine learning* klasik, metode deteksi intrusi jaringan dengan model berbasis *deep learning* juga menunjukkan hasil yang cukup menjanjikan. Pada tahun 2017, Chuanlong Yin menggunakan

pendekatan *deep learning* dengan model *Recurrent Neural Network* (RNN) untuk melakukan deteksi intrusi [9]. Berdasarkan hasil yang diperoleh, diketahui bahwa model RNN yang dikonstruksi menunjukkan performa yang lebih baik dibandingkan model *machine learning* tradisional seperti *random forest* dan *naive bayes classifier* [9]. Model RNN menawarkan akurasi yang tinggi dengan *false positive rate* yang rendah.

Pada tahun 2020, Wooyeon dkk. menggunakan model *Convolutional Neural Network* (CNN) mendeteksi intrusi. [10]. Pada penelitiannya, Wooyeon dkk. diajukan 3 teknik *preprocessing* data, yaitu *direct conversion*, *weighted conversion* dan *compressed conversion* [10]. Ketiga teknik *preprocessing* ini digunakan untuk mengonversi data pada dataset NSL-KDD menjadi data gambar untuk diolah menggunakan model *Convolutional Neural Network* (CNN). Dengan menggunakan teknik ini, model CNN berhasil mencapai akurasi sebesar 88,2%. Penelitian ini menunjukkan keunggulan model berbasis *deep learning* untuk masalah deteksi intrusi.

Berdasarkan penelitian mengenai sistem deteksi intrusi yang telah dilakukan sebelumnya, diketahui model berbasis *neural network* banyak diterapkan untuk masalah deteksi intrusi jaringan dan bahkan memiliki performa yang lebih baik dibandingkan dengan model *machine learning* klasik. Oleh karena itu, pada penelitian ini Penulis akan mengkaji penerapan model *deep learning Deep Neural Network* (DNN) untuk sistem deteksi intrusi jaringan. Pada penelitian ini, model DNN akan digunakan untuk melakukan klasifikasi data dengan kelas biner (BENIGN dan ATTACK) sehingga dapat

digunakan untuk deteksi intrusi.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, masalah yang dibahas pada penelitian ini adalah:

1. Bagaimana arsitektur dan *hyperparameter* dari model *Deep Neural Network* (DNN) yang diterapkan pada sistem deteksi intrusi jaringan?
2. Bagaimana performa dari model *Deep Neural Network* (DNN) yang diterapkan pada sistem deteksi intrusi jaringan berdasarkan metrik evaluasi *accuracy*, *precision*, dan *recall*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dipaparkan, penelitian ini memiliki tujuan yang ingin dicapai, yaitu:

1. Memperoleh arsitektur dan *hyperparameter* model *Deep Neural Network* (DNN) yang diterapkan pada sistem deteksi intrusi jaringan.
2. Mengetahui performa model *Deep Neural Network* (DNN) yang diterapkan pada sistem deteksi intrusi jaringan berdasarkan metrik evaluasi *accuracy*, *precision*, dan *recall*.

1.4 Sistematika Penulisan

Skripsi ini terdiri dari lima bab. Pada Bab I, dimuat latar belakang, perumusan masalah, tujuan penulisan dan sistematika penulisan. Kemudian pada Bab II dibahas tentang konsep dasar yang menjadi landasan untuk penelitian ini. Bab III berisi informasi sumber data yang digunakan, dan tahapan yang dilakukan dalam penelitian. Pada Bab IV, terdapat pembahasan mengenai implementasi *Deep Neural Network* (DNN) untuk sistem deteksi intrusi, serta evaluasi dari hasil deteksi model yang diperoleh. Terakhir untuk Bab V memuat kesimpulan dari penelitian yang telah dilaksanakan dan saran untuk penelitian berikutnya.