Bab I
Pendahuluan

1.1 Latar Belakang

Internet of Things (IoT) merupakan berbagai perangkat berbeda yang terhubung melalui beberapa *protocol* komunikasi dan sensor yang dapat saling berinteraksi [1]. Seiring dengan pertumbuhan zaman, penggunaan layanan dan aplikasi elektronik telah mendorong kemajuan besar dalam suatu jaringan telekomunikasi [2]. Pada tahun 2022 jumlah koneksi internet yang terhubung melalui jaringan IoT diperkirakan mencapai satu triliun alamat IP ataupun objek [2]. Meningkatnya penggunaan ini dapat menyebabkan masalah keamanan jaringan dan perangkat IoT dapat menjadi target potensial bagi serangan *cyber* berbahaya [3]. Serangan ini dapat merugikan individu maupun organisasi seperti penipuan, pencurian data, bahkan ancaman terhadap keamanan fisik [4]. Meskipun tindakan keamanan jaringan yang sederhana seperti *firewall* mungkin sudah cukup efektif di masa lalu, namun sekarang, dengan semakin kompleksnya serangan *cyber*, tindakan - tindakan tersebut tidak lagi cukup efektif [5]. Sehingga untuk meningkatkan keamanan dalam lingkungan IoT penggunaan *Intrusion Detection System* (IDS) menjadi sangat penting [5]. IDS menjadi perangkat kunci untuk mendeteksi dan memberikan peringatan terhadap aktivitas mencurigakan, melindungi jaringan dan perangkat IoT dari potensi ancaman keamanan yang dapat merugikan.

IDS merupakan sistem yang dapat berupa perangkat keras maupun perangkat lunak yang secara otomatis dapat melakukan pemantauan, mendeteksi aktivitas yang mencurigakan ataupun intrusi, dan memberikan peringatan ke dalam jaringan ataupun computer [6]. Jika terdapat aktivitas yang mencurigakan maupun serangan di dalam jaringan komputer, IDS akan mencatat semua kegiatan - kegiatan tersebut dan memberikan peringatan

kepada *administrator* [7]. Nantinya *administrator* akan melakukan analisis terhadap log yang sudah diberikan oleh IDS untuk mengetahui jenis - jenis serangan yang sudah terjadi dan dapat melakukan perbaikan yang dapat digunakan untuk meningkatkan keamanan jaringan maupun dalam lingkungan IoT [7]. Dalam menghadapi kompleksitas serangan terhadap jaringan dan lingkungan IoT, metode tradisional IDS menghadapi tantangan yang signifikan.

Pola serangan yang semakin berkembang dan jumlah perangkat IoT yang terus bertambah membuat sulitnya mendeteksi ancaman dengan pendekatan konvensional. Oleh karena itu, penerapan teknologi terbaru seperti *Machine Learning* (ML) dalam IDS untuk kasus IoT menjadi krusial. ML memungkinkan sistem untuk belajar dari data secara kontinu, meningkatkan kemampuannya dalam mendeteksi pola serangan baru atau yang lebih canggih. Dengan respons yang lebih cepat dan kemampuan adaptasi terhadap perubahan, integrasi ML dalam IDS menjadi solusi strategis untuk meningkatkan keamanan jaringan dan lingkungan IoT secara menyeluruh.

Terdapat beberapa penelitian terkait ML yang telah diterapkan dalam IDS untuk kasus IoT. Pada tahun 2019 Abhishek dan rekan-rekan telah melakukan penelitian mengenai IDS berbasis ML untuk mengamankan IoT dari serangan *Denial of Service* (DoS) [8]. Algoritma klasifikasi yang digunakan yaitu *Random Forest, AdaBoost, Gradient Boosting*, *Extremely Randomized Trees*, CART, dan MLP. Dari semua algoritma tersebut hasil kinerja terbaik untuk untuk membangun IDS didapatkan dari algoritma CART dan *Gradient Boosting*. Lalu pada tahun 2022, Shatha dan Salameh melakukan penelitian deteksi serangan *network* pada HTTP DATASET CSIC 2010 dengan membandingkan metode ML dengan *Deep Learning* (DL) [9]. Metode ML yang diterapkan yaitu *Decision Tree*, *Random Forest*, *Gradient Boosting*, *Extreme Gradient Boosting*,*AdaBoost*, *Multi Layer Perceptron* MLP, dan *Voting*. Sedangkan untuk metode deep learning yang diterapkan yaitu *Long ShortTerm Memory* (LSTM), *Convolutional Neural Networks* (CNN), dan penggabungan dari LSTM dengan CNN. Hasil penelitian menunjukkan bahwa ketika membandingkan keseluruhan metode, menghasilkan metode dengan

hasil kinerja terbaik diperoleh padametode deep learning LSTM dengan CNN, *accuracy* yang diperoleh sebesar 99%, *precision* sebesar 100%, *recall* sebesar 99%, dan *F1-score* sebesar 99%. Penelitian ini menunjukkan bahwa penggunaan algoritma ini memungkinkan kita untuk mendeteksi banyak serangan dan bertahan dari ancaman eksternalatau internal terhadap jaringan.

Pada tahun 2022 Khan dkk, telah mengembangkan IDS untuk mengatasi ancaman keamanan dan privasi di jaringan komputer dan jaringan IoT [10]. Sistem ini bertujuan untuk mencegah kerahasiaan data, integritas, dan kerusakan ketersediaan jika terjadi kegagalan pencegahan IDS. Selanjutnya pada tahun 2023, Jonathan dkk melakukan penelitian mengenai IDS pada Bot-IoT Dataset membandingkan tiga algoritma ML yaitu *K-Nearest Neighbors*, *Random Forest, Gaussian Naıve Bayes* [11]. Penelitian ini menghasilkan algoritma KNN adalah algoritma terbaik dalam melakukan IDS pada lingkungan IoTini dengan hasil *precision* 96%, *recall* 99% dan *accuracy* 97%. Evaluasi dan perbandingan terhadap metode-metode ML yang digunakan dalam penelitian-penelitian tersebut, hasilnya menunjukkan bahwa algoritma ML dapat digunakan untuk mengidentifikasi serangan yang tidak diketahui sebelumnya dengan tingkat akurasi yang tinggi.

Teknik konvensional terbukti kurang efektif dalam menghadapi serangan tingkat lanjut, mendorong perlunya teknik pembelajaran mendalam tingkat lanjut untuk deteksi intrusi otomatis dan identifikasi perilaku abnormal jaringan. Untuk mengatasi tantangan ini, penggunaan teknik augmentasi data menjadi krusial guna memperoleh dataset yang lebih akurat dan handal dalam melatih model ML dan DL. Keunggulan DL terlihat karena mampu mempelajari data tanpa label dan berlabel secara diawasi maupun tidak diawasi, membuatnya cocok untuk sistem deteksi intrusi. Meskipun banyak metode Deep Learning, seperti CNN, LSTM, dan RNN, telah dikembangkan untuk deteksi intrusi pada IoT, penelitian yang memadai untuk membandingkan kinerja ketiganya masih terbatas. Oleh karena itu, penelitian ini bertujuan untuk mengisi kesenjangan analisis dengan membandingkan efektivitas ketiga metode tersebut dalam mendeteksi intrusi pada sistem IoT. Dengan demikian, diharapkan penelitian ini dapat memberikan pemahaman yang lebih mendalam

untuk memilih metode yang paling efektif dan mendukung pengembangan IDS yang lebih tangguh dalam melindungi lingkungan IoT.

1.2 Rumusan Masalah dan Batasannya

Berdasarkan latar belakang yang telah diuraikan diatas, maka rumusan masalahnya adalah sebagai berikut :

1. Bagaimana perbandingan kinerja dari *Convolutional Neural Networks* (CNN), *Long ShortTerm Memory* (LSTM), dan *Recurrent Neural Networks* (RNN) untuk mendeteksi intrusi pada lingkungan *Internet of Things* (IoT)?
2. Bagaimana hasil evaluasi dari ketiga metode tersebut?

Adapun batasan masalah pada penelitian ini adalah sebagai berikut :

1. Data yang digunakan pada penelitian ini yaitu The UNSW-NB15 dataset
2. Metode yang digunakan yaitu *Convolutional Neural Networks* (CNN), *Long ShortTerm Memory* (LSTM), dan *Recurrent Neural Networks* (RNN) untuk mendeteksi intrusi pada lingkungan *Internet of Things* (IoT)?
3. Matriks evaluasi yang digunakan yaitu *Loss, Accuracy, Val-Los, Val-Accuracy, Precision, Recall, F1-score*

1.3 Tujuan

Berdasarkan rumusan dan batasan yang telah dipaparkan, maka tujuan dari penelitian ini yaitu:

1. Implementasi proses model algoritma *Convolutional Neural Networks* (CNN), *Long Short-Term Memory* (LSTM), dan*Recurrent Neural Networks* (RNN) untuk mendeteksi intrusi pada lingkungan *Internetof Things* (IoT).

2. Mengevaluasi performa CNN, LSTM, dan RNN menggunakan dataset The UNSW-NB15 dengan matriks evaluasi untuk menentukan metode yang paling efektif dalam mendeteksi intrusi pada lingkungan IoT.