BAB I
PENDAHULUAN

1. Latar belakang

Serangan *DDoS* adalah salah satu jenis serangan siber yang paling umum dan merugikan. Serangan ini mengakibatkan penurunan kinerja jaringan, yang dapat berdampak pada penggunaan yang lebih rendah, hilangnya data, dan bahkan downtime. Dalam beberapa tahun terakhir, dengan meningkatnya penggunaan *Internet of Things* (*IoT*) di berbagai sektor, serangan terhadap jaringan *IoT* juga semakin meningkat. Serangan *DDoS* pada jaringan *IoT* mengancam keamanan sistem, infrastruktur, dan data. Oleh karena itu, deteksi serangan *LR-DDoS* pada jaringan *SD-IoT* menjadi semakin penting untuk memastikan keamanan jaringan. Meskipun ada beberapa metode deteksi yang ada, metode yang dapat bekerja pada jaringan *SD-IoT* dan memberikan hasil yang akurat masih menjadi tantangan. Dalam penelitian ini, peneliti mengusulkan penggunaan metode *Machine Learning* dengan feature importance *RFC* untuk deteksi serangan *LR-DDoS* pada jaringan *SD-IoT*.

Beberapa penelitian sebelumnya telah dilakukan dalam deteksi serangan *DDoS* pada jaringan *IoT*. Hui , dkk [1] menggunakan metode pembelajaran mesin untuk mendeteksi serangan *DDoS* pada jaringan *IoT* dengan menggunakan algoritma *Naive Bayes*. Namun, penelitian ini memiliki keterbatasan dalam hal deteksi serangan yang lebih kompleks dan akurat. Kemudian, Wu , dkk [2] menggunakan algoritma *k-NN* untuk deteksi serangan *DDoS* pada jaringan *IoT*. Namun, penelitian ini hanya mempertimbangkan faktor latensi sebagai fitur, yang dapat menghasilkan banyak false positive. Penelitian lain yang menggunakan metode pembelajaran mesin adalah penelitian oleh Singh , dkk [3], di mana mereka menggunakan algoritma *decision tree* untuk deteksi serangan *DDoS* pada jaringan *IoT*. Meskipun hasilnya cukup akurat, penelitian ini hanya mempertimbangkan serangan *DDoS* yang spesifik.

Di sisi lain, penelitian oleh Zhang , dkk [4] menggunakan teknik deep learning untuk deteksi serangan *DDoS* pada jaringan *IoT*. Namun, penelitian ini memiliki biaya komputasi yang sangat besar dan memerlukan infrastruktur yang rumit. Kemudian, penelitian oleh Chang , dkk [5] mengusulkan

penggunaan metode pembelajaran mesin dengan algoritma random forest untuk deteksi serangan *DDoS* pada jaringan *IoT*. Namun, penelitian ini hanya mempertimbangkan fitur IP dan port, yang dapat menghasilkan false positive. Penelitian lain yang menggunakan algoritma random forest adalah penelitian oleh Bao , dkk [6], di mana mereka mengusulkan penggunaan metode feature selection untuk meningkatkan akurasi deteksi serangan *DDoS* pada jaringan *IoT*.

Penelitian terdahulu telah dilakukan untuk mengembangkan metode untuk mendeteksi serangan *LrDDoS* pada jaringan *SDN* maupun *SD-IoT* menggunakan Machine Learning. Salah satu penelitian yang dilakukan oleh Mirza dan Fauzi Dwi S S[7] bertujuan untuk mendeteksi *LrDDoS* menggunakan *SVM* yang dikombinasikan dengan *Feature Importance* menggunakan Logistic Regression. Penelitian yang dilakukan oleh Andi Maslan dan Kamaruddin Malik Bin Mohamad[9] menggunakan algoritma *K-Nearest Neighbors* (KNN) untuk klasifikasi deteksi serangan *DDoS* . Penelitian lain yang dilakukan oleh Fauzi Dwi S S dan Wahyuli Dwiki Nanda menggunakan metode Random Forest dengan Logistic Regression Coefficient untuk mendeteksi serangan *LrDDoS* pada jaringan berbasis *SD-IoT*[10].

Dalam penelitian ini, peneliti mengusulkan penggunaan metode pembelajaran mesin dengan feature importance *RFC* untuk deteksi serangan *LR-DDoS* pada jaringan *SD-IoT*. Feature importance *RFC* adalah salah satu Feature Importance untuk machine learning yang populer dan efektif dalam deteksi serangan *DDoS* [7]. Peneliti juga menggunakan teknik *Feature Importance* untuk mengidentifikasi fitur yang paling penting dalam deteksi serangan. Peneliti melakukan eksperimen dengan 8 algoritma pembelajaran mesin yang berbeda, yaitu *SVM* linear, *SVM* RBF, RFC, DTC, MLP, *GNB*, *ADB*, dan KNN. Peneliti menggunakan dataset untuk melatih dan menguji model deteksi peneliti. Dataset yang digunakan berjumlah 204.888 paket yang berisi *TCP SYN* message, transmisi *TCP* yang berulang selain dalam paket normal , dan untuk data normalnya ada 48.509 paket yang diantaranya berisi *HTTP*S, *HTTP*, ICMP, MQTT.

Penelitian ini memberikan kontribusi dalam deteksi serangan *LR-DDoS*

pada jaringan *SD-IoT* dengan mengusulkan penggunaan algoritma pembelajaran mesin dengan algoritma *RFC* dan teknik *Feature Importance* untuk identifikasi fitur yang paling penting dalam deteksi serangan. Selain itu, peneliti melakukan eksperimen dengan 8 algoritma pembelajaran mesin yang berbeda untuk membandingkan kinerja model deteksi peneliti. Hasilnya menunjukkan bahwa model yang diusulkan memiliki akurasi yang lebih tinggi dan lebih efektif dalam deteksi serangan *LR-DDoS* pada jaringan *SD-IoT* dibandingkan dengan metode yang ada. Penelitian ini dapat membantu meningkatkan keamanan jaringan *SD-IoT* dan memberikan pandangan baru dalam penggunaan metode pembelajaran mesin dalam deteksi serangan *DDoS* pada jaringan *IoT*.

2. Rumusan masalah

Rumusan masalah dari penelitian ini diuraikan sebagai berikut:

1. Bagaimana membangun sistem deteksi serangan *LrDDoS* menggunakan *Machine Learning* dengan *Feature Random Forest Classifier* ?
2. Bagaimana efektifitas proses deteksi menggunakan metode *Machine Learning* dengan algoritma *Support Vector Machine* (SVM) dengan Kernel *Liniear* dan *Radial Basis Function* (RBF), Random Forest (RFC), *Desicion Tree* (DTC), *Multi-Layer Perceptron* (MLP), *Gaussian Naïve Bayes* (*GNB*), *AdaBoost Classifier* (*ADB*), *K-Nearest Neighbor* (KNN) dinilai dari *Accuracy*, *Precision*, *Recall*, F1-*Score*, dan *classificasion-loss*?

3. Tujuan penelitian

a. Menganalisis karakteristik serangan *LrDDoS* pada jaringan *SD-IoT* dan menyediakan informasi yang diperlukan untuk mengembangkan metode deteksi yang efektif.

b. Membangun model deteksi serangan *LrDDoS* pada jaringan *SD-IoT* menggunakan *Machine Learning* dengan metode *Feature Importance* dan metode *Random Forest Classifier* yang efektif dan akurat.

c. Membandingkan performa dari beberapa algoritma *Machine Learning* dalam mendeteksi serangan *LrDDoS* pada jaringan *SD-IoT* dan menemukan

algoritma yang paling efektif dan akurat.

d. Mengukur performa model deteksi yang dibangun dalam mendeteksi serangan *LrDDoS* pada jaringan *SD-IoT* menggunakan metode *Feature Importance* dan metode *Random Forest Classifier*.

e. Memberikan kontribusi pada pengembangan teknologi deteksi serangan cyber pada jaringan *SD-IoT* dan meningkatkan keamanan jaringan *SD-IoT* dari serangan *LrDDoS* .

4. Batasan penelitian

a. Penelitian ini hanya difokuskan pada deteksi serangan *LrDDoS* pada jaringan *SD-IoT*, dan tidak membahas jenis serangan cyber lainnya.

b. Data yang digunakan dalam penelitian ini berasal dari simulasi yang dibuat di laboratorium, sehingga hasilnya mungkin tidak sepenuhnya merepresentasikan kondisi di lapangan.

c. Algoritma *Machine Learning* yang digunakan terbatas pada SVM, RBF, RFC, DTC, MLP, *GNB*, *ADB*, dan KNN, sehingga ada kemungkinan ada algoritma lain yang lebih efektif dalam mendeteksi serangan *LrDDoS* pada jaringan *SD-IoT*.

d. Penelitian ini hanya difokuskan pada penggunaan metode *Feature Importance* pada algoritma *RFC* untuk menentukan fitur yang paling penting dalam mendeteksi serangan *LrDDoS* , sehingga tidak membahas metode Feature Selection yang lain.

e. Menggunakan *Mininet-IoT* untuk emulasi jaringan *SD-IoT*.

f. Menggunakan *RYU* sebagai *Controller* pada jaringan *SD-IoT*.

g. Dataset yang digunakan adalah data primer.

h. Model serangan menggunakan protokol *CoAP*.

i. Paket rate yang digunakan untuk serangan Low-Rate adalah 50, 100 dan 200.