INTISARI

MODEL BERBASIS *DEEP REINFORCEMENT LEARNING* UNTUK *NETWORK INTRUSION DETECTION SYSTEM*

Oleh

Tities Novaninda Ovari

20/466435/PPA/06001

Network Intrusion Detection System (NIDS) merupakan hal yang esensial dalam menjaga keamanan komunikasi dan informasi yang terjadi pada jaringan internet. Terdapat dua jenis NIDS, yaitu *signature based* NIDS dan *anomaly based* NIDS. *Signature* based NIDS mendeteksi aktivitas mencurigakan berdasarkan *pattern-pattern* yang telah ditentukan sebelumnya. Sedangkan *anomaly based* NIDS, yang akan diteliti pada penelitian ini, mendeteksi aktivitas mencurigakan berdasarkan penyimpangan aktivitas sistem. Dengan *anomaly based* NIDS didapatkan sistem yang dapat mendeteksi *pattern-pattern* baru dari serangan. *Deep Reinforcement Learning* (DRL) merupakan kombinasi antara *Deep Learning* dengan *Reinforcement Learning* (RL). RL memungkinkan agen belajar dari lingkungannya untuk menentukan aksi terbaik berdasarkan *trial* dan *error*. Oleh karena itu, pendekatan DRL memungkinkan dalam mendapatkan *anomaly based* NIDS yang mampu belajar dari lingkungannya sehingga diharapkan dapat tahan terhadap serangan dan memberikan aksi yang tepat.

Algoritma DRL yang akan digunakan pada penelitian ini adalah algoritma *Deep Learning* RNN yang mengaktifkan *Q-Learning* dengan dataset UNSW-NB15. Dengan model pada penelitian ini, akurasi yang didapatkan dalam mendeteksi serangan mencapai 86.19% dengan *False Positive Rate* (FPR) sebesar 20.44%. Hasil ini menunjukkan performa model DRL lebih unggul dibandingkan dengan RNN yang memiliki akurasi sebesar 80.01% dengan FPR sebesar 43.79%, dan LSTM yang memiliki akurasi sebesar 81.13% dengan FPR sebesar 41.48%.

Kata Kunci: NIDS, *Deep Reinforcement Learning*, RNN, Q-*Learning*, UNSW-NB15