

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

ABSTRACT

DEEP REINFORCEMENT LEARNING BASED MODEL FOR NETWORK INTRUSION DETECTION SYSTEM

By

Titites Novaninda Ovari

20/466435/PPA/06001

Network Intrusion Detection System (NIDS) is essential in maintaining the security of communication and information that occurs on the internet network. There are two types of NIDS, namely signature based NIDS and anomaly based NIDS. Signature based NIDS detects suspicious activity based on predetermined patterns. On the other hand, anomaly based NIDS, which will be researched in this study, detects suspicious activity based on deviations in system activity so that a system can detect new patterns of attack. Deep Reinforcement Learning (DRL) is a combination of Deep Learning and Reinforcement Learning (RL). RL allows agent to learn from their environment to determine the best course of action based on trial and error. Therefore, the DRL approach makes it possible to obtain anomaly based NIDS that is able to learn from its environment so that it is expected to be able to withstand attacks and provide appropriate action.

The DRL algorithm that will be used in this research is the Deep Learning RNN algorithm that activates Q-Learning with the UNSW-NB15 dataset. Using the model in this research, the accuracy obtained in detecting attacks reaches 86.19% with a False Positive Rate (FPR) of 20.44%. These results indicate that DRL model performance is better compared to RNN which has an accuracy of 80.01% with a FPR of 43.79% and LSTM which has an accuracy of 81.13% with FPR of 41.48%.

Keywords: NIDS, Deep Reinforcement Learning, RNN, Q-Learning, UNSW-NB15