PERANCANGAN SISTEM PENDETEKSIAN THREAT BERBASIS DEEP LEARNING UNTUK INTRUSION DETECTION SYSTEM

ABSTRAK

Abstrak- *Intrusion Detection System* (IDS) adalah konsep pengenalan suatu objek maupun suatu kejadian pada sistem yang berfungsi untuk pengenalan *threat*. *Threat* adalah kegiatan atau kejadian yang berpotensi mengganggu *confidentiality, integrity* dan *availability* pada sistem. IDS memiliki dua pendekatan dasar untuk pengawasan dan pengenalan *threat* yaitu *knowledge-based* dan *behavior-based*. Pendekatan Dasar pada IDS memiliki permasalahan pada akurasi dan adaptif. Berdasarkan permasalahan tersebut, dilakukan sebuah penelitian yang bertujuan untuk meningkatkan akurasi pendeteksian *threat* dan membangun sistem pendeteksian *threat* yang adaptif. Penelitian yang dilakukan menggunakan pendekatan *convolutional neural network* (CNN) dan menggunakan dataset CTU- 13. Penelitian ini melakukan *data preprocessing,* pembuatan model, pelatihan model, pengujian model dan evaluasi ketika melakukan simulasi pendeteksian *threat*. Hasil penelitian dibandingkan dengan penelitian lainnya yang menggunakan dataset CTU- 13. Penelitian pembanding menggunakan pendekatan *knowledge-based* dan menggunakan *rule* dalam menerjemahkan botnet ke sistem. Penelitian ini menunjukkan meningkatkannya akurasi sebesar 8% dalam pengenalan *threat* yang dikenali dibandingkan penelitian pembanding. Penelitian ini juga memperlihatkan adaptivitas model dalam pengenalan *threat* yang berbeda tetapi masih memiliki karakteristik yang sama, hasil dari pengenalan *threat* yang berbeda yaitu mendapatkan akurasi sebesar 0,94 dan nilai adaptif dari sistem pendeteksian yaitu sebesar 0,63 yang didapat berdasarkan cara penghitungan nilai adaptif yang diusulkan. Hasil tersebut dikategorikan sangat adaptif berdasarkan perbedaan karakteristik *threat* yang terlibat.

Kata kunci: Adaptif, *Intrusion Detection System, deep learning, threat, convolution neural network*

DEEP LEARNING-BASED THREAT DETECTION SYSTEM DESIGN FOR INTRUSION DETECTION SYSTEM

ABSTRACT

Abstract- Intrusion Detection System (IDS) is the concept of recognizing an object or an event on the system that functions for threat recognition. Threats are activities or events that compromise the confidentiality, integrity and availability of the system. IDS has two basic approaches to surveillance and threat recognition, namely knowledge-based and behavior-based. The Basic Approach to IDS has problems with accuracy and adaptability. Based on these problems, a study was conducted that aims to improve the accuracy of threat detection and build an adaptive threat detection system. The research was conducted using a convolutional neural network (CNN) approach and using the CTU-13 dataset. This research performs data preprocessing, model creation, model training, model testing and evaluation when performing threat detection simulations. The results of the study were compared with other studies using the CTU-13 dataset. Comparative research uses a knowledge-based approach and uses rules in translating the botnet to the system. This study demonstrated an 8% increase in accuracy in the recognition of known threats compared to a comparison study. This research is also based on the adaptation model in recognizing different threats but still having the same characteristics, the results of the introduction of different threats are getting an accuracy of 0.94 and the adaptive value of the detection system is 0.63 which is obtained by the proposed adaptive value method. The results are grouped based on the different characteristics of the threats involved.

Keywords: Adaptive, Intrusion Detection System, deep learning, threats, convolution neural network.