Hybrid Deep Learning untuk Deteksi Serangan Botnet di Jaringan IoT menggunakan CNN-GRU

Edward Billy Hadipuspito[1], Vera Suryani[2]

[1,2]Fakultas Informatika, Universitas Telkom, Bandung
[1]edwardbilly@student.telkomuniversity.ac.id, [2]verasuryani@telkomuniversity.ac.id

Abstrak

Pertumbuhan cepat Internet of Things juga memperkenalkan risiko keamanan dan serangan, terutama untuk perangkat IoT komersial, yang sering menjadi target para penjahat cyber. Untuk mengatasi tantangan keamanan ini, kami mengusulkan model pembelajaran mendalam hibrida Convolutional Neural Network-Gated Recurrent Unit (CNN-GRU) untuk mendeteksi anomali pada sembilan perangkat IoT komersial. Model CNN-GRU ini memanfaatkan kekuatan dari CNN dan GRU. CNN terkenal dengan kemampuannya untuk mengekstrak fitur spasial dari data, membuatnya ideal untuk mengidentifikasi pola dalam data perangkat IoT. Di sisi lain, GRU sangat baik dalam menangkap karakteristik temporal, memungkinkan mereka untuk memahami urutan dan waktu dari titik data. Model ini dilatih dan dievaluasi menggunakan dataset N-BaIoT, kumpulan lalu lintas jaringan yang komprehensif dari sembilan perangkat IoT komersial yang berbeda. Model ini mencapai hasil F1-score yang luar biasa dalam membedakan lalu lintas serangan botnet Bashlite dan normal. Namun, untuk beberapa jenis serangan, model ini menghadapi tantangan. Kami juga membandingkan kinerja dengan model CNN-LSTM, pendekatan pembelajaran mendalam yang populer lainnya. Perbandingan ini didasarkan pada akurasi dan waktu pelatihan. Hasilnya menunjukkan bahwa CNN-GRU melampaui kinerja CNN-LSTM untuk sebagian besar model perangkat, mencapai akurasi tertinggi sebesar 85,04%. Yang patut dicatat, model ini juga mencapai waktu pelatihan yang lebih rendah pada semua perangkat, dengan perbedaan terbesar adalah 82,04 detik. Penelitian ini menyoroti efisiensi model pembelajaran mendalam hibrida seperti CNN-GRU dalam meningkatkan keamanan perangkat IoT komersial dengan efektif mendeteksi anomali.

Kata kunci : internet of things, botnet, deep learning, convolutional neural network, gated recurrent unit.

Abstract

The rapid growth of Internet of Things also introduces security risks and attacks particularly for commercial IoT devices, which are often targeted by cybercriminals. To address these security challenges, we propose a Convolutional Neural Network-Gated Recurrent Unit (CNN-GRU) hybrid deep learning model to detect anomalies in nine commercial IoT devices. This CNN-GRU model leverages the strengths of both CNN and GRU. CNNs are renowned for their ability to extract spatial features from data, making them ideal for identifying patterns in IoT device data. On the other hand, GRUs are excellent at capturing temporal characteristics, allowing them to understand the sequence and timing of data points. The model was trained and evaluated using the N-BaIoT dataset, a comprehensive collection of network traffic from nine different commercial IoT devices. It achieved exceptional F1- score results on differentiating normal and Bashlite botnet attack traffic. However, for certain types of attacks, the model is challenged. We also compared the performance with the CNN-LSTM model, another popular deep learning approach. The comparison was based on accuracy and training times. The results revealed that CNN-GRU surpassed the performance of CNN-LSTM for most device models, achieving the highest accuracy of 85.04%. Notably, it also achieved lower training times on all devices, with the largest difference being 82.04 second. This research highlights the efficiency of hybrid deep learning models like CNN-GRU in enhancing the security of commercial IoT devices by effectively detecting anomalies.

Keywords: internet of things, botnet, deep learning, convolutional neural network, gated recurrent unit.

1. Introduction

The Internet of Things or IoT has grown quickly over the past several years. IoT is a network of small autonomous devices that can communicate and interact without requiring a huge amount of human intervention and limitless possibilities [14]. As a result of the rapid growth, security risks and attacks are increasing. Research