INTISARI

Deteksi serangan *Distributed Denial of Service* menggunakan komparasi metode *LightGBM, XGBoost* dan *CatBoost*

DDoS adalah salah satu ancaman utama terhadap keamanan internet karena pola serangannya semakin sulit untuk dideteksi. Hal tersebut dikarenakan trafik serangannya sangat mirip dengan trafik normal pada umumnya di sebagian besar kasus. Banyaknya jenis serangan DDoS melalui berbagai port pun juga menambah kesulitan dalam membedakan antara trafik serangan atau trafik asli.

Sudah ada banyak penelitian yang menyelidiki efek dari penggunaan algoritma klasifikasi untuk mendeteksi dan mencegah serangan DDoS. Namun, penelitian yang ada memiliki banyak kendala termasuk pencapaian tingkat kinerja dari sistem deteksi, keterlambatan deteksi, serta kemampuan untuk menangani dengan dataset dengan ukuran yang sangat besar. Metode – metode Gradient Boost Decision Tree (GBDT) merupakan metode yang dapat dilakukan untuk mempercepat proses klasifikasi pada dataset yang berukuran besar. Pada paper ini dipilih metode LightGBM, XGBoost, dan CatBoost untuk melakukan klasifikasi. Ketiga Algoritma ini akan melakukan pelatihan dengan menggunakan dataset dari CICIDS, kemudian hasilnya akan dibandingkan satu sama lain pada CPU dan GPU untuk mengetahui algoritma mana yang paling baik untuk mengklasifikasi trafik DDoS pada Intrusion Detection System (IDS).

Hasil penelitian menunjukkan bahwa ketiga meode menghasilkan model pendeteksian dengan akurasi lebih dari 95%, dan pelatihan menggunakan GPU lebih cepat daripada pelatihan menggunakan CPU.

Oleh

Nendra Haryo Wijayandanu

16/394097/PA/17188

Kata Kunci: ***Distributed Denial of Service, Machine Learning, Gradient Boosting Decision Tree, LightGBM, XGBoost, CatBoost.***

ABSTRACT

Distributed Denial of Service Attack Detection Using Comparison of LightGBM, XGBoost, and CatBoost Methods

DDoS is one of the main threats to internet security as its attack patterns are increasingly difficult to detect. This is because the attack traffic is very similar to normal traffic in most cases. The wide variety of DDoS attacks via multiple ports also adds to the difficulty in distinguishing between attack traffic or genuine traffic.

There have been many studies investigating the effects of using classification algorithms to detect and prevent DDoS attacks. However, existing research has many constraints including attaining performance levels of detection systems, detection delays, and the ability to deal with datasets of very large sizes. Gradient Boost Decision Tree (GBDT) methods are methods that can be used to speed up the classification process on large datasets. In this paper, the LightGBM, XGBoost, and CatBoost methods are selected to perform classification. These three algorithms will conduct training using the dataset from CICIDS, then the results will be compared with each other on the CPU and GPU to find out which algorithm is best for classifying DDoS traffic on the Intrusion Detection System (IDS).

The results showed that the three methods produced a detection model with an accuracy of more than 95%, and training using the GPU was faster than training using the CPU.

By
Nendra Haryo Wijayandanu
16/394097/PA/17188

Keywords: ***Distributed Denial of Service, Machine Learning, Gradient Boosting Decision Tree, LightGBM, XGBoost, CatBoost***