Perbandingan Kinerja Algoritma dalam Klasifikasi Serangan DDoS Berdasarkan Data *CIC IoMT Dataset*

Fikri Azhari

ABSTRAK

Dengan semakin luasnya penerapan *Internet of Things* (IoT) di berbagai sektor, termasuk sektor medis dengan *teknologi Internet of Medical Things* (IoMT), serangan *Distributed Denial of Service* (DDoS) menjadi ancaman serius bagi keberlangsungan sistem. Penelitian ini membandingkan empat algoritma *machine learning Random Forest*, *LightGBM*, *Naïve Bayes*, dan *K-Nearest Neighbors* (KNN) untuk mendeteksi serangan DDoS pada IoMT. Evaluasi dilakukan berdasarkan akurasi dan waktu komputasi yang berjalan secara paralel (GPU) menggunakan pendekatan *Weighted Sum Method*. Hasil menunjukkan bahwa *Random Forest* memiliki performa terbaik dengan skor 0.971578, diikuti oleh *Naïve Bayes* dengan skor 0.961235. Meskipun KNN memiliki akurasi tinggi, algoritma ini kurang efisien secara waktu, sedangkan *LightGBM* menunjukkan performa terendah dalam hal akurasi dan efisiensi. Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan sistem deteksi ancaman siber yang cepat dan akurat pada lingkungan IoMT.

Kata Kunci : *Internet of Things* (IoT), *Internet of Medical Things* (IoMT), *Distributed Denial of Service* (DDoS), *Machine Learning*, Deteksi Serangan.

Comparison of Algorithm Performance in DDoS Attack Classification Based on the CIC IoMT Dataset

Fikri Azhari

ABSTRACT

With the widespread application of the Internet of Things (IoT) in various sectors, including the medical sector with Internet of Medical Things (IoMT) technology, Distributed Denial of Service (DDoS) attacks are a serious threat to the sustainability of the system. This research compares four machine learning algorithms Random Forest, LightGBM, Naïve Bayes, and K-Nearest Neighbors (KNN) to detect DDoS attacks on IoMT. The evaluation is based on accuracy and computation time running in parallel (GPU) using the Weighted Sum Method approach. The results show that Random Forest has the best performance with a score of 0.971578, followed by Naïve Bayes with a score of 0.961235. Although KNN has high accuracy, it is less time efficient, while LightGBM shows the lowest performance in terms of accuracy and efficiency. This research is expected to contribute to the development of a fast and accurate cyber threat detection system in the IoMT environment.

Keywords : *Internet of Things (IoT), Internet of Medical Things (IoMT), Distributed Denial of Service (DDoS), Machine Learning, Attack Detection.*