Pendeteksian Serangan Distributed Denial of Service Pada Kasus Industrial Internet of Things Menggunakan Algoritma Pembelajaran Mesin

Miharu Idhan Fikriansyah[1], Siti Amatullah Karimah, S.T., M.T.[2], Dr. Farisya Setiadi, S.T., M.T.I.[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]miharufikri@students.telkomuniversity.ac.id, [2]karimahsiti@telkomuniversity.ac.id,
[3]farisyasetiadi@telkomuniversity.ac.id

Abstrak

Internet of Things telah berkembang sangat besar dan cepat selama beberapa tahun terakhir ini. Salah satu bukti perkembangan IoT adalah penggunaan Industrial Internet of Things pada bidang industri. IIoT dapat membantu meningkatkan proses produksi dan keuntungan yang dihasilkan. Namun, IIoT juga memiliki kelemahan pada sisi keamanan. IIoT sangat rentan terkena serangan, utamanya serangan Distributed Denial of Service (DDoS). DDoS dapat menghambat pengiriman data sehingga memperlambat kinerja pada IIoT. Hal ini dapat menyebabkan kerugian yang besar bagi industri itu sendiri. Demi mencegah serangan tersebut maka salah satu caranya adalah dengan melakukan pendeteksian menggunakan pembelajaran mesin. Oleh karena itu, dilakukan penelitian untuk menguji pendeteksian serangan DDoS pada IIoT dengan menggunakan algoritma pembelajaran mesin. Penelitian menggunakan algoritma Random Forest dan Naïve Bayes sebagai model pendeteksian dan diuji menggunakan dataset Edge-IIoTset. Kedua algoritma ini dipilih karena keduanya telah terbukti dapat mendeteksi serangan DDoS pada berbagai jenis jaringan seperti jaringan web, cloud-server, jaringan IoT dan lain-lain. Dalam proses pengujian dilakukan dua skenario yaitu pengujian jumlah fitur yang berbeda dan pengujian menggunakan jumlah pembagian data yang berbeda. Tingkat perfomansi yang dihasilkan dalam pengujian dengan random forest mencapai 100% untuk setiap matriks dan skenario pengujian. Sedangkan untuk tingkat performansi dengan naïve bayes berbeda untuk tiap skenario pengujian. Tingkat performansi terbaik dari naïve bayes adalah dengan jumlah 20 fitur yang dapat mencapai 78.56% untuk accuracy, 79.85% untuk precision, 90.61% untuk recall, dan 84.89% untuk f-1 score. Berdasarkan hasil pengujian metode terbaik yang dapat digunakan untuk melakukan pendeteksian serangan DDoS pada IIoT adalah metode random forest

Kata kunci : industrial internet of things, distributed denial of service, random forest, naïve bayes.

Abstract

Internet Internet of Things has grown very large and fast over the past few years. One proof of the development of IoT is the use of Industrial Internet of Things in the industrial field. IIoT can help improve the production process and the resulting profits. However, IIoT also has a weakness on the security side. IIoT is very vulnerable to attacks, especially Distributed Denial of Service (DDoS) attacks. DDoS can inhibit data transmission and thus slow down the performance of IIoT. This can cause huge losses for the industry itself. In order to prevent these attacks, one way is to detect them using machine learning. Therefore, research is conducted to test the detection of DDoS attacks on IIoT using machine learning algorithms. The research will use Random Forest and Naïve Bayes algorithms as detection models and tested using the Edge-IIoTset dataset. These two algorithms are chosen because both have been proven to detect DDoS attacks on various types of networks such as web networks, cloud-servers, IoT networks and others. In the testing process, two scenarios will be carried out, namely testing a different number of features and testing using a different number of data split. The resulting performance level in testing with random forest reaches 100% for each matrix and test scenario. Meanwhile, the performance level with naïve bayes is different for each test scenario. The best performance level of naïve bayes is with a total of 20 features that can achieve 78.56% for accuracy, 79.85% for precision, 90.61% for recall, and 84.89% for f-1 score. Based on these results, the best method that can be used to detect DDoS attacks on IIoT is the random forest method.

Keywords: industrial internet of things, distributed denial of service, random forest, naïve bayes.

1. Pendahuluan

Latar Belakang

Internet of Things (IoT) adalah perangkat yang terkoneksi pada suatu jaringan yang dapat berkomunikasi antara satu sama lain dan menyediakan data untuk penggunanya melalui internet [1]. IoT saat ini telah berkembang sangat besar dan cepat selama beberapa tahun terakhir. Bahkan, saat ini terdapat 8 milyar perangkat IoT yang telah terkoneksi dan diperkirakan dapat mencapai 41 milyar pada tahun 2027 [1]. Salah satu bidang yang menjadi bidang perkembangan IoT yang besar adalah bidang industri. Penggunaan IoT pada bidang industri ini melahirkan sebuah teknologi baru yang dikenal dengan Industrial Internet of Things (IIoT)