PEMBANGUNAN MODEL DETEKSI SERANGAN *DENIAL OF SERVICE* PADA PROSES TENNESSEE EASTMAN BERBASIS *LIGHT GRADIENT BOOSTING MACHINE*

Natha Triforestcetta
21/474199/TK/52300

Diajukan kepada Departemen Teknik Nuklir dan Teknik Fisika Fakultas Teknik
Universitas Gadjah Mada pada tanggal 9 April 2025
untuk memenuhi sebagian persyaratan untuk memperoleh derajat
Sarjana Program Studi Teknik Fisika

INTISARI

Industrial Control System (ICS) merupakan teknologi yang penting dalam mengontrol dan memastikan stabilitas operasi dalam proses industri. Salah satu komponen ICS adalah *Supervisory Control and Data Acquisition* (SCADA), yang memungkinkan pemantauan dan pengendalian secara *real-time*. Namun, keterbukaan jaringan pada sistem SCADA membuat ICS rentan terhadap serangan siber, khususnya pada serangan *Denial of Service* (DoS), yang dapat mengganggu ketersediaan data dan memengaruhi proses produksi. Meskipun banyak sistem deteksi berfokus pada analisis jaringan, masih sedikit yang mempertimbangkan dampak serangan DoS terhadap variabel proses, yang mengganggu hasil produksi. Sistem *Intrusion Detection System* (IDS) konvensional seringkali bergantung pada aturan tetap, yang tidak dapat mendeteksi *zero-day attack*. Sebagai solusi, penggunaan *machine learning* dapat mengenali pola anomali tanpa bergantung pada aturan tetap. Selain itu, sistem pendeteksian serangan yang berjalan secara *real-time* akan membantu menjaga kelangsungan proses. Oleh karena itu, diperlukan sistem deteksi serangan DoS menggunakan *machine learning* dan implementasinya secara *real-time*.

Pada penelitian ini, program deteksi serangan DoS dibangun menggunakan algoritma *Light Gradient Boosting Machine* (LGBM). Data yang digunakan merupakan simulasi dari proses Tennessee Eastman. Data disegmentasi berdasarkan variasi ukuran jendela. Hasil segmentasi kemudian dilakukan ekstraksi fitur *time series*, analisis, dan seleksi fitur. Model deteksi serangan DoS dibangun dan diimplementasikan secara *real-time,* serta divisualisasikan dengan Kibana.

Hasil penelitian menunjukkan model LGBM memiliki kinerja terbaik pada ukuran jendela 50 dengan *overlap* 20, dengan *recall* dan *f1-score* sebesar 0,98 dan 0,89. Kebutuhan *real-time* dipenuhi oleh model yang memiliki rata-rata waktu deteksi selama 0,533 detik.

Kata kunci: deteksi serangan, *Denial of Service*, *Light Gradient Boosting Machine*, *real-time*

Pembimbing Utama : Dr.-Ing. Awang N. I. Wardana, S.T., M.T., M.Sc., IPM.

Pembimbing Pendamping : Dr. Ir. Eng. Dwi Joko Suroso, S.T., M.Eng.,IPP.

BUILDING DETECTION MODEL DENIAL OF SERVICE ATTACK ON TENNESSEE EASTMAN PROCESS BASED ON LIGHT GRADIENT BOOSTING MACHINE

Natha Triforestcetta

21/474199/TK/52300

Submitted to the Department of Nuclear Engineering and Engineering Physics
Faculty of Engineering Universitas Gadjah Mada on April 9, 2025
in partial fulfillment of the requirement for the Degree of
Bachelor of Engineering in Engineering Physics

ABSTRACT

Industrial Control System (ICS) is an important technology in controlling and ensuring operation stability in industrial processes. One component of ICS is Supervisory Control and Data Acquisition (SCADA), which enables real-time monitoring and control. However, the openness of the network in SCADA systems makes ICS vulnerable to cyberattacks, especially Denial of Service (DoS) attacks, which can disrupt data availability and affect production processes. While many detection systems focus on network analysis, few consider the impact of DoS attacks on process variables that disrupt production output. Conventional Intrusion Detection Systems (IDS) often rely on fixed rules that cannot detect zero-day attacks. The use of machine learning can recognize anomalous patterns without relying on fixed rules. In addition, an attack detection system that runs in real-time will help maintain process continuity. Therefore, a DoS attack detection system that uses machine learning and is implemented in real time is needed.

In this research, the DoS attack detection program is built using the Light Gradient Boosting Machine (LGBM) algorithm. The data used is a simulation of the Tennessee Eastman process, segmented based on window size variations. The segmentation results are then subjected to time series feature extraction, analysis, and feature selection. The DoS attack detection model is built and implemented in real-time and visualized with Kibana.

The results show that the LGBM model has the best performance at window size 50 with overlap 20. With recall and f1-score of 0.98 and 0.89. Real-time requirements are met by the model which has an average detection time of 0.533 seconds.

Keywords: attack detection, Denial of Service, Light Gradient Boosting Machine, real time

Supervisor : Dr.-Ing. Awang N. I. Wardana, S.T., M.T., M.Sc.,IPM.

Co-supervisor : Dr. Ir. Eng. Dwi Joko Suroso, S.T., M.Eng.,IPP.