

**ANALISIS KERENTANAN LAPISAN *EDGE* IIOT TERHADAP
SERANGAN DOS PADA SISTEM KOMUNIKASI PLC BERBASIS MQTT**
HILMI DZAKIANA MAULIDIA
21/473269/TK/52150

Diajukan kepada Departemen Teknik Nuklir dan Teknik Fisika Fakultas Teknik
Universitas Gadjah Mada pada tanggal 7 Maret 2025
untuk memenuhi sebagian persyaratan untuk memperoleh derajat
Sarjana Program Studi Teknik Fisika

INTISARI

Permintaan terhadap implementasi *Industrial Internet of Things* (IIoT) semakin bertambah di dunia industri. Salah satu elemen penting dalam IIoT adalah lapisan *Edge*, yang menghubungkan *Local Area Network* (LAN) dan *Wide Area Network* (WAN). Meskipun memberikan banyak keuntungan, integrasi ini juga membawa risiko keamanan. Hal ini disebabkan karena lapisan *Edge* yang terbuka terhadap koneksi eksternal akan rentan terhadap serangan siber. Oleh karena itu, penelitian ini bertujuan untuk mensimulasikan serangan *Denial of Service* (DoS) pada lapisan *Edge* dan menganalisis dampaknya terhadap performa komunikasi sistem.

Penelitian ini menyimulasikan serangan DoS jenis *SYN flood* menggunakan modul Hping3 yang ditujukan pada lapisan *Edge* dari integrasi komunikasi IIoT antara *Programmable Logic Controller* (PLC) dan *Virtual Private Server* (VPS). Protokol komunikasi yang digunakan adalah OPC-UA dan MQTT, dengan Node-RED sebagai *platform* lapisan *Edge* yang menghubungkan kedua perangkat. Analisis dilakukan terhadap tiga metrik kinerja jaringan, yaitu RTT OPC-UA, *delay* antar *publish* MQTT, dan *throughput* jaringan, menggunakan metode *Two-Way MANOVA* untuk mengevaluasi pengaruh *payload* dan *interval*.

Hasil analisis MANOVA menunjukkan bahwa perubahan *payload* tidak signifikan, dengan nilai uji p Wilk's Lambda sebesar 0,230. Sebaliknya, perubahan *interval* signifikan terhadap ketiga metrik, dengan nilai p Wilk's Lambda sebesar 0,000. Berdasarkan uji *eigenvalue* terhadap *interval*, *throughput* memiliki *eigenvalue* tertinggi sebesar 115,594 dengan proporsi variasi sebesar 0,991, yang menunjukkan bahwa *throughput* jaringan adalah metrik yang paling terpengaruh.

Kata kunci: *Denial of Service*, Lapisan *Edge*, OPC-UA, MQTT

Pembimbing Utama : Dr.-Ing. Ir. Awang Noor Indra Wardana, S.T., M.T.,
M.Sc., IPM.

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



VULNERABILITY ANALYSIS OF EDGE LAYER IIOT AGAINST DOS ATTACKS ON MQTT-BASED PLC COMMUNICATION SYSTEMS

HILMI DZAKIANA MAULIDIA

21/473269/TK/52150

Submitted to the Departement of Nuclear Engineering and Engineering Physics
Faculty of Engineering Universitas Gadjah Mada on March 7, 2025
in partial fulfillment of the requirement for the Degree of
Bachelor of Engineering in Engineering Physics

ABSTRACT

The demand for Industrial Internet of Things (IIoT) implementation is increasingly growing in the industrial sector. One of the critical elements in IIoT is the Edge layer, which connects the Local Area Network (LAN) and Wide Area Network (WAN). Although it offers numerous advantages, this integration also introduces security risks. This is because the Edge layer, being open to external connections, becomes vulnerable to cyberattacks. Therefore, this research aims to simulate Denial of Service (DoS) attacks on the Edge layer and analyze their impact on the communication performance of the system.

This research simulates a SYN flood DoS attack using the Hping3 module, targeting the Edge layer of the IIoT communication integration between a Programmable Logic Controller (PLC) and a Virtual Private Server (VPS). The communication protocols used are OPC-UA and MQTT, with Node-RED serving as the Edge layer platform connecting the two devices. The analysis focuses on three network performance metrics: OPC-UA RTT, MQTT inter-publish delay, and network throughput, using the Two-Way MANOVA method to evaluate the influence of payload and interval.

The MANOVA analysis results indicate that changes in payload have no significant effect, with a Wilk's Lambda p-value of 0.230. In contrast, changes in interval significantly affect all three matrices, with a Wilk's Lambda p-value of 0.000. Based on the eigenvalue test for the interval, throughput has the highest eigenvalue of 115.594, with a variation proportion of 0.991, indicating that network throughput is the most affected.

Keywords: Denial of Service, Edge Layer, OPC-UA, MQTT

Supervisor : Dr.-Ing. Ir. Awang Noor Indra Wardana, S.T., M.T., M.Sc., IPM.

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

