SIMULASI SISTEM DETEKSI SERANGAN TERARAH PADA PROSES TENNESSEE EASTMAN BERBASIS LONG-SHORT TERM MEMORY (LSTM)

Keiza Aurakania Putri

21/481897/TK/53187

Diajukan kepada Departemen Teknik Nuklir dan Teknik Fisika Fakultas Teknik
Universitas Gadjah Mada pada tanggal 20 April 2025
untuk memenuhi sebagian persyaratan untuk memperoleh derajat
Sarjana Program Studi Teknik Fisika

INTISARI

Integrasi *Industrial Control System* (ICS) dengan internet meningkatkan kerentanannya terhadap serangan siber. Upaya perlindungan saat ini hanya terbatas pada analisis lalu lintas jaringan yang acap kali gagal melindungi ICS ketika serangan berhasil menyusupi jaringan dan memanipulasi proses.

Penelitian ini bertujuan untuk mengembangkan sistem deteksi serangan terarah berbasis *Long-Short Term Memory* (LSTM) pada lapisan proses fisik menggunakan data simulasi proses Tennessee Eastman. Pengembangan ini meliputi perancangan arsitektur model, pelatihan dengan variasi konfigurasi *hyperparameter*, serta implementasi model secara daring agar memungkinkan deteksi serangan secara *real-time*. Penelitian ini tidak hanya merancang sistem deteksi, tetapi juga memperluas cakupan analisis dengan mengidentifikasi kerentanan industri proses, khususnya pada proses Tennessee Eastman.

Model dengan performa terbaik diperoleh dengan konfigurasi *hyperparameter batch size* 128, *hidden size* 128, dan *sequence length* 10. Hasil evaluasi menunjukkan rata-rata *recall* dan *precision* model secara berurutan adalah 92,1% dan 94,4%. Sistem deteksi *real-time* berhasil mengidentifikasi baik serangan yang sudah dikenal maupun serangan baru, dengan latensi deteksi sebesar 50 detik untuk serangan yang dikenal dan 140 detik untuk serangan baru.

Kata kunci: Keamanan Siber, Sistem Kontrol Industri, Serangan Terarah, Sistem Deteksi Intrusi, Tennesse Eastman Process

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

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

SIMULATION OF A PHYSICAL PROCESS LAYER INTRUSION DETECTION SYSTEM FOR INDUSTRIAL CONTROL SYSTEMS USING LONG-SHORT TERM MEMORY (LSTM)

Keiza Aurakania Putri

21/481897/TK/53187

Submitted to the Department of Nuclear Engineering and Engineering Physics
Faculty of Engineering Universitas Gadjah Mada on *April 20th, 2025*
in partial fulfillment of the requirement for the Degree of
Bachelor of Engineering in Engineering Physics

ABSTRACT

Integration between Industrial Control Systems (ICS) and the internet increases their vulnerability to cyberattacks. Safeguarding efforts primarily focus on network traffic analysis, which often fails to protect ICS when attacks successfully infiltrate the network and manipulate the processes.

This study aims to develop a targeted attack detection system based on Long Short-Term Memory (LSTM) networks for the physical process layer using simulated Tennessee Eastman Process data. The research includes the design of the model architecture, training with various hyperparameter configurations, and implementing the model in an online setting for real-time attack detection. This work not only develops a real-time attack detection system but also broadens the analysis by identifying vulnerabilities within the process industry, specifically in the Tennessee Eastman Process.

The best-performing model was achieved with a hyperparameter configuration of batch size 128, hidden size 128, and sequence length 10. Evaluation results show an average recall of 92.1% and precision of 94.4%. The real-time detection system effectively identifies both known and novel attacks, with detection latencies of 50 seconds for known attacks and 140 seconds for new attacks.

Keywords: Cybersecurity, Industrial Control System, Targeted Attack, Intrusive Detection System, Tennesse Eastman Process

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

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