

INTISARI

DETEKSI SERANGAN BERBASIS *AUTO-ENCODER* POHON HIBRID PADA JARINGAN *SUPERVISORY CONTROL AND DATA ACQUISITION*

Oleh

FRESKA ROLANSA
21/485061/SPA/00805

Supervisory Control and Data Acquisition (SCADA) yang dioperasikan pada jaringan internet, membuat SCADA memiliki kerentanan pada saat komunikasi terjadi khususnya komunikasi menggunakan protokol Modbus. Serangan *Man in the middle attack* (MITM) yang dilakukan oleh penyerang pada SCADA dapat menyebabkan bahaya dan kerusakan perangkat. Beberapa model dikembangkan untuk mendeteksi adanya anomali akan tetapi model yang dibangun memiliki kelemahan hanya menentukan serangan atau tidak. Pengembangan model dilakukan dengan pendekatan klasifikasi multi kelas untuk menentukan tipe serangan MITM. Keterbatasan model klasifikasi multi kelas masih memiliki jumlah kesalahan klasifikasi pada kelas minoritas khususnya pada kelas *replay attack* sebanyak 9 dan *read attack* sebanyak 6858 kesalahan.

Untuk mengatasi masalah tersebut, penelitian ini mengembangkan model deteksi serangan berbasis *Auto-Encoder Pohon Hibrid* pada jaringan pada SCADA yang terdiri dari beberapa tahapan yakni preprocessing, resampling dengan hybrid untuk *balancing* data menggunakan kombinasi antara ADASYN oversampling dan ENN undersampling, Autoencoder dengan arsitektur *undercomplete* autoencoder untuk reduksi dimensi fitur beserta pemilihan fitur penting, dan Tree detection yang telah dioptimasi dengan hyperparameter tuning untuk klasifikasi multi kelas serangan MITM.

Berdasarkan hasil eksperimen menggunakan Electra dataset, metode yang diusulkan yakni *A Hybrid Autoencoder-based Tree detection* terbukti dapat mengatasi permasalahan pada penelitian ini. Hasil klasifikasi model multi kelas MITM yang dikembangkan hanya memiliki 15 kesalahan dalam melakukan prediksi pada kelas *read attack* dan hanya 4 kesalahan pada kelas *replay attack*. Model yang diusulkan memiliki performa yang lebih baik dari model lain berdasarkan nilai F1-score yang bernilai 99,89 dan evaluasi terhadap keseimbangan data menggunakan G-means bernilai 99,94.

Kata Kunci : SCADA, *Vulnerability*, MITM, *Auto-Encoder*, Pohon, Hibrid
Electra, *Imbalance*

ABSTRACT

A HYBRID TREE AUTO-ENCODER-BASED ATTACK DETECTION IN A SUPERVISORY CONTROL AND DATA ACQUISITION NETWORK

By

FRESKA ROLANSA
21/485061/SPA/00805

Supervisory Control and Data Acquisition (SCADA), which is operated on the internet, makes SCADA vulnerable during communication, especially communication using the Modbus protocol. Man-in-the-middle (MITM) attacks carried out by attackers on SCADA systems can endanger and damage devices. Several models have been developed to detect anomalies; however, these models can only determine if an attack has occurred. A multi-class classification approach was used to develop a model that can determine the type of MITM attack. However, the multi-class classification model still has a high number of classification errors in the minority class: 9 errors in the replay attack class and 6,858 errors in the read attack class.

To address this issue, this study developed a hybrid autoencoder-based tree detection model for network-based attacks on SCADA, comprising several stages: preprocessing, resampling with hybrid for data balancing using a combination of ADASYN oversampling and ENN undersampling, an autoencoder with an undercomplete autoencoder architecture for feature dimension reduction and selection of important features, and tree detection optimized with hyperparameter tuning for multi-class MITM attack classification.

Based on the results of experiments using the Electra dataset, the proposed method, a hybrid autoencoder-based tree detection, has proven to be able to overcome the problems in this study. The classification results of the multi-class MITM model developed only had 15 errors in predicting the read attack class and only 4 error in the replay attack class. The proposed model performed better than other models based on an F1-score of 99.89 and an evaluation of data balance using G-means of 99.94.

**Keywords : SCADA, Vulnerability, MITM, Auto-Encoder, Tree, Hybrid
Electra, Imbalance**