Attack Detection On Edge IIot Using Ensemble Learning And XAI Model Transparency

Hussain Randika[1], Parman Sukarno[2], Aulia Arif Wardana[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[4]Divisi Digital Service PT Telekomunikasi Indonesia
[1]hrandika@students.telkomuniversity.ac.id,
[2]Psukarno@telkomuniversity.ac.id,[3]auliawardan@telkomuniversity.ac.id,

Abstrak

Industrial Internet of Things (IIoT) telah berkembang pesat, meningkatkan efisiensi produksi dan profitabilitas, sekaligus memperkenalkan tantangan keamanan yang signifikan karena sistem IIoT menjadi lebih rentan terhadap serangan siber. Studi ini menangani tantangan tersebut dengan menerapkan deteksi serangan menggunakan metode ensemble learning dan Explainable Artificial Intelligence (XAI). Model seperti Random Forest, XGBoost, dan LightGBM digunakan bersama SHAP (SHapley Additive Explanations) untuk meningkatkan transparansi model.

Stratified Sampling digunakan untuk mengurangi volume data sambil mempertahankan distribusi fitur, dan seleksi fitur dilakukan menggunakan Random Forest Feature Importance untuk mencapai akurasi dan efisiensi tinggi. Dataset Edge-IIoTset digunakan, dengan preprocessing dan seleksi fitur yang dioptimalkan melalui Random Forest Feature Importance. Pengujian melibatkan dua skenario dengan variasi jumlah fitur dan pembagian data untuk mengevaluasi efektivitas model.

Hasil menunjukkan bahwa model LightGBM mencapai akurasi tertinggi sebesar 97,60%, diikuti oleh XGBoost dengan 96,90%, dan Random Forest dengan 96,51%. Selain itu, SHAP mengidentifikasi fitur-fitur utama yang memengaruhi prediksi, meningkatkan kepercayaan dan pemahaman pengguna. Hasil ini menunjukkan bagaimana kombinasi ensemble learning dan XAI dapat meningkatkan keamanan IIoT secara efektif.

Kata kunci : Explainable AI, Industrial Internet of Things, Feature Selection, Stratified Sampling, Ensemble Learning

Abstract

The Industrial Internet of Things (IIoT) has rapidly developed, improving production efficiency and profitability and introducing significant security challenges as IIoT systems become more vulnerable to cyberattacks. This study addresses these challenges by implementing attack detection using en semble learning methods and Explainable Artificial Intelligence (XAI). Models like Random Forest, XGBoost and LightGBM are employed with SHAP (SHapley Additive Explanations) to improve model transparency. Stratified Sampling reduces data volume while preserving feature distribution, and feature selec tion is performed using Random Forest Feature Importance to achieve high accuracy and efficiency. The Edge-IIoTset dataset is used, with preprocessing and feature selection optimized through Random Forest Feature Importance. Testing involves two sce narios with varying feature counts, and data splits to evaluate effectiveness. Results show that the LightGBM model achieved the highest accuracy 97.60%, followed by XGBoost 96.90% and Random Forest 96.51%. Additionally, SHAP identified key features influencing predictions and improving user trust and understanding. These results demonstrate how well ensemble learning and XAI work together to improve IIoT security.

Keywords : Explainable AI, Industrial Internet of Things, Feature Selection, Stratified Sampling, Ensemble Learning

1. Pendahuluan

1.1 Latar Belakang

IIoT, atau Industrial Internet of Things, telah menjadi bagian penting dalam perkembangan era Industri 4.0, memungkinkan aktivitas industri menjadi lebih otomatis dan saling terhubung. Sebagai salah satu teknologi pendukung IoT, Edge Computing dalam IIoT merupakan konsep yang muncul dari kemajuan pesat IoT [1]. Edge Computing memungkinkan pemrosesan data lebih dekat ke sumbernya, sehingga mengurangi latensi dan