ABSTRAK

Kompleksitas serangan siber yang semakin meningkat dalam arsitektur *Internet of Things* (IoT) memerlukan *Intrusion Detection System* (IDS) yang tidak hanya akurat dalam mendeteksi ancaman, tetapi juga mampu menjaga privasi data pengguna. Pendekatan IDS konvensional yang berbasis arsitektur terpusat dianggap tidak efektif karena rentan terhadap titik kegagalan tunggal dan berisiko menyebabkan kebocoran data. Untuk mengatasi hal ini, *Federated Learning* (FL) muncul sebagai solusi inovatif yang memungkinkan pelatihan model secara kolaboratif di antara perangkat tanpa perlu mengirimkan data mentah ke server pusat. Namun, efektivitas FL sangat dipengaruhi oleh pilihan metode agregasi, yang memengaruhi konvergensi model, akurasi deteksi, dan ketahanan sistem, terutama saat menangani data dengan karakteristik tidak independen dan tidak identik terdistribusi (*non*-IID). Beberapa peneliti telah membahas metode agregasi dalam FL terkait data *non*-IID, tetapi tanpa mengevaluasi secara eksplisit pengaruh kekuatan regularisasi pada FedProx di bawah kondisi distribusi data *non*-IID. Tesis ini mengusulkan pengembangan Sistem Deteksi Intrusi Kolaboratif berbasis FL menggunakan dua metode agregasi, FedAvg dan FedProx, untuk mengevaluasi kinerja deteksi serangan pada dataset CICIoT2023. Eksperimen dilakukan pada skenario data IID dan *non*-IID menggunakan model *Deep Neural Network* (DNN) dan teknik seleksi fitur berdasarkan nilai Feature Importance Gain dari XGBoost. Hasil menunjukkan bahwa pada data IID, kombinasi FedAvg dan seleksi fitur memberikan akurasi tertinggi sebesar 97,76%. Sementara itu, pada data *non*-IID, kombinasi FedProx (μ = 1.0) dan seleksi fitur mencapai akurasi terbaik sebesar 96,92%.

Kata Kunci: *Internet of Things, CIDS, Federated Learning, Deep Learning, CICIoT2023*