Abstrak— Dengan semakin populernya perangkat IoT, potensi ancaman serangan siber juga meningkat. Perangkat ini dapat mencuri informasi berharga, melakukan aktivitas pemantauan, atau meluncurkan serangan ransomware. Komunitas keamanan siber telah membuat kemajuan besar dalam mengembangkan alat dan metode keamanan untuk melindungi pengguna dan data dalam sistem TI konvensional. Salah satu solusi untuk mencegah ancaman ini adalah Sistem Deteksi Intrusi (IDS). Sistem deteksi intrusi yang didukung oleh kecerdasan buatan memiliki kinerja luar biasa dalam mendeteksi serangan. Penelitian ini menggunakan algoritma XGBoost untuk mendeteksi serangan pada sistem IoT, dan XAI diterapkan pada model untuk meningkatkan interpretabilitas dan keterbacaan. Kumpulan data yang digunakan adalah kumpulan data aplikasi IoT dan IIoT yang disebut Edge-IIoTset. Dalam penelitian ini, pengujian dilakukan untuk membandingkan kinerja XGBoost dengan Regresi Logistik, Pohon Keputusan, dan Pohon Acak. Penjelasan global dan lokal dibuat menggunakan SHAP untuk meningkatkan interpretabilitas dan keterbacaan model. Penelitian ini menunjukkan bahwa XGBoost mengungguli pengklasifikasi lain dengan akurasi 97,5%, presisi 97%, recall 100%, dan skor F1 99%.

Kata kunci: iot, xgboost, explainable ai, shap