Abstract—With the increasing popularity of IoT devices, the potential for cyber-attack threats is also rising. These devices can steal valuable information, conduct monitoring activities, or launch ransomware attacks. The cybersecurity community has made considerable progress in developing security tools and methods to protect the users and data within conventional IT systems. One such solution to prevent these threats is the Intrusion Detection System (IDS). Intrusion detection systems powered by artificial intelligence perform outstandingly in detecting attacks. This research uses the XGBoost algorithm to detect attacks on IoT systems, and XAI was applied to the model to improve interpretability and readability. The dataset used is an IoT and IIoT application data collection called Edge-IIoTset. In this research, tests were carried out to compare the performance of XGBoost with Logistic Regression, Decision Tree, and Random Tree. Global and local explanations were created using SHAP to improve the interpretability and readability of the model. This research shows that XGBoost outperforms the other classifiers with an accuracy of 97.5%, precision of 97%, recall of 100%, and an F1 score of 99%.

Kata kunci: iot, xgboost, explainable ai, shap