# Benchmarking AI-Driven Anomaly Detection: From Tree-Based Ensembles to Graph Neural Networks in IoT and Traditional Systems

**Hamza Talha Gümüş**
Department of Electrical and Electronics Engineering, Kırıkkale University, Kırıkkale, Türkiye

**Aziz Gökhan Alarslan**
Department of Electrical and Electronics Engineering, Kırıkkale University, Kırıkkale, Türkiye

**Hüseyin Aydilek**
Department of Electrical and Electronics Engineering, Kırıkkale University, Kırıkkale, Türkiye

**Mustafa Yasin Erten**
Department of Electrical and Electronics Engineering, Kırıkkale University, Kırıkkale, Türkiye

## Abstract

The rapid expansion of cyber-physical systems and network-based digital infrastructures necessitates the evolution of intrusion detection mechanisms into more flexible, intelligent, and scalable architectures. Traditional signature-based systems prove inadequate against zero-day attacks, high-volume data flows, and the dynamic nature of IoT-based traffic, as they are limited to reacting solely to known threats. Machine learning and deep learning methods transcend these limitations by strengthening anomaly-based detection processes and identifying unknown attacks through the extraction of statistical models of normal behaviour. Predicated on technical trends from the 2020–2025 period, this study presents a comparative analysis of classical and deep learning approaches and introduces a hybrid methodology addressing contemporary challenges such as data imbalance, explainability, real-time performance, and resource efficiency. Models based on LSTM, CNN, Autoencoder, GAN, XGBoost, and Random Forest were evaluated on extensive datasets, and their generalization capacities were tested across IoT, IIoT, and traditional network scenarios. The results indicate that while no single algorithm maintains dominance across every scenario, multi-layered hybrid models demonstrate high accuracy, low false-positive rates, and strong generalization performance. These findings suggest that AI-supported intrusion detection systems will become a fundamental component of future defence architectures, highlighting the critical importance of developing holistic, multi-stage solutions in this domain.

## Keywords

Anomaly Detection, Deep Learning, Intrusion Detection Systems, Machine Learning, Network Traffic Analysis.