**Intrusion Detection Systems Using ML-Based Anomaly Detection.**

**Abstract**

Intrusion detection systems (IDSs) are essential for protecting critical infrastructure (CI), including industrial control systems (ICSs) and SCADA systems, from increasingly advanced cyber-attacks. To enhance IDS performance, this study evaluates six machine learning algorithms: KNeighborsClassifier, RandomForestClassifier, DecisionTreeClassifier, AdaBoostClassifier, GradientBoostingClassifier, and LinearDiscriminantAnalysis. Using original and SMOTE-enhanced datasets, the GradientBoostingClassifier achieved the highest accuracy of 96.08%, outperforming other algorithms in detecting various attack patterns, including zero-day threats. This analysis underscores the effectiveness of Gradient Boosting for securing CI and offers a clear framework for choosing suitable ML models to strengthen cybersecurity defenses.

**Keywords**

Intrusion Detection Systems (IDS); Machine Learning; Critical Infrastructure (CI); Industrial Control Systems (ICS); SCADA Systems; Cybersecurity; Gradient Boosting; SMOTE; Attack Detection; Zero-Day Attacks.