Republic of Yemen
Ministry of Higher Education and Scientific Research
Yemeni Academy for Postgraduate Studies

الجمهورية اليمنية
وزارة التعليم العالي والبحث العلمي
الأكاديمية اليمنية للدراسات العليا

Intelligent Intrusion Detection System Based on the Combination of ML and XGBOOST

The rapid advancement of digital technology has significantly transformed the global landscape, leading to increased adoption of technology, particularly the widespread use of the borderless internet that has enhanced seamless communication across organizational and individual boundaries. This technological revolution has bolstered information exchange and impacted the economic and social aspects of daily life. Consequently, data security and information protection have become of paramount importance.

On the other hand, cyber security threats and electronic attacks targeting organizations and individuals incur significant annual costs. Furthermore, data breaches and cyber-attacks often result in the exposure of sensitive information, leading to severe consequences.

Despite the effectiveness of intrusion detection systems, challenges persist in improving accuracy, minimizing false alarms, and detecting advanced cyber intrusions. Addressing these weaknesses is crucial, especially given the rising impact of artificial intelligence (AI)-driven attacks across diverse sectors. This study attempts to developed an intelligent system for detecting cyber-attacks using machine learning, specifically the XGBoost algorithm. Additionally, It proposed a hybrid algorithm by combining filter and wrapper methods (IG, SBS) to select an optimal feature set capable of efficiently identifying various attack patterns. This research utilized the CICIDS2017 dataset, which includes the most modern cyber-attacks.