# Feature-Augmented KNN for Injection Detection

## Abstract

Injection attacks such as SQL Injection (SQLi), Cross-Site Scripting (XSS), and Command Injection continue to pose serious threats to the integrity and confidentiality of web applications.

In this study, we propose an advanced application of the k-Nearest Neighbors (KNN) algorithm for identifying webbased injection attacks. The approach combines term frequency-inverse document frequency (TF-IDF) representations with domain-informed statistical and syntactic features designed to capture anomalies in HTTP parameter payloads. Extensive experiments were conducted on multiple public datasets to evaluate both baseline and enhanced models.