

# Feature selection and DDoS Detection using Relief and Decision Tree

---

## **Abstract:**

importance of detecting a DDoS attack lies in the fact that it can disrupt the availability and performance of online services, leading to financial losses, reputational damage, and legal liabilities. Detecting and mitigating such attacks is crucial to ensure uninterrupted operation, protect user data, and maintain customer satisfaction. Early detection can minimize the impact and prevent recurrence.

This project aims to detect DDoS (Distributed Denial of Service) attack using minimum number of relative features. Specifically, the Relief algorithm is used for feature selection and Decision Tree for DDoS detection.

The Relief algorithm can effectively be identifying relevant features according the type of class of the dataset. The selected features are then used as input to the Decision Tree classifier to detect DDoS attacks. To evaluate the performance of our approach, we conduct experiments for a public available dataset consists of 225745 instances of network traffic using accuracy measure. The results show that our method can effectively detect DDoS attacks with 99.8% accuracy using only three features and a low false positive rate