

Anomaly Detection in Cybersecurity Using Random Forest

Mr. Ashish Modi¹ and Mr. Kunj Navadiya²

Asst. Prof, Department of Computer and Information Science¹

Student, Department of Computer and Information Science²

Nagindas Khandwala College, Mumbai, Maharashtra, India

Abstract: *Cybersecurity threats are increasing at an alarming rate, making effective detection methods more important than ever. Traditional security systems often struggle to keep up with evolving threats, which is where machine learning comes into play. Random Forest (RF), a powerful ensemble learning technique, has proven to be highly effective for anomaly detection. This paper explores how RF can be applied to cybersecurity, highlighting its strengths, practical implementation, and how it compares to other approaches. Our findings, using the UNSW-NB15 dataset, show that RF can identify malicious activities, particularly DoS and Backdoor attacks, with impressive accuracy while keeping false positives low. Additionally, we compare RF with deep learning-based techniques and discuss future improvements for real-time cybersecurity applications.*

Keywords: Cybersecurity, Anomaly Detection, Machine Learning, Random Forest, Network Security.