

Behavior-Based Cyber Threat Detection Using Machine Learning

Amit Singla, IT Head & HOD, Department of Computer Science, Seth G.L. Bihani S.D. P.G. College, Sri Ganganagar

Abstract

The rapid growth of digital networks, cloud-based services, and connected devices has significantly increased the complexity and frequency of cyber threats. Traditional security mechanisms that primarily rely on predefined signatures and rules may struggle to identify sophisticated, previously unseen, or rapidly evolving attacks. Behaviour-based cyber threat detection offers an alternative approach by identifying abnormal patterns in user, network, and system activities. This paper explores the application of Machine Learning (ML) techniques for detecting cyber threats through behavioural analysis. The study focuses on how machine learning models can learn normal patterns of activity and identify deviations that may indicate malicious behaviour, unauthorized access, data breaches, or other security incidents. Various approaches, including supervised, unsupervised, and anomaly-detection techniques, are examined with respect to their effectiveness in identifying abnormal activities. The paper also discusses important challenges such as false-positive rates, imbalanced datasets, feature selection, model interpretability, data privacy, and the ability to detect emerging threats. A conceptual framework for integrating behavioural analytics with machine learning is proposed to support continuous and adaptive cyber threat monitoring. The study highlights that combining behavioural indicators with intelligent analytical techniques can strengthen threat detection capabilities and improve the responsiveness of cybersecurity systems. The findings provide a foundation for developing adaptive security solutions capable of addressing increasingly dynamic and complex cyber threats.

Keywords: Cybersecurity, Machine Learning, Behaviour-Based Detection, Cyber Threat Detection, Anomaly Detection, Intrusion Detection, Behavioural Analytics, Network Security.

