Cybersecurity Threat Detection Using Machine Learning

Abstract: This study presents machine learning approaches for real-time cybersecurity threat detection. We develop anomaly detection systems using unsupervised learning and graph neural networks for network traffic analysis. Our system identifies zero-day attacks with 94%% accuracy.

Introduction

Cyber threats are evolving rapidly, requiring intelligent defense systems. Traditional signature-based detection fails against novel attacks. Machine learning enables adaptive threat detection by learning patterns from network behavior.

Methodology

We employed autoencoders for anomaly detection and graph neural networks for analyzing network topology. The system processes packet-level data in real-time, flagging suspicious activities. Transfer learning enables rapid adaptation to new attack vectors.