(ISSN: 2393-8048)

International Seminar on September 16th, 2024
"Exploring the Frontiers of Interdisciplinary Research (ICEFIR-2024)"
Organized By: Nagpal Charitable Trust, Sri Ganganagar
Venue: Maharaja Agrasen Vidya Mandir School, Sri Ganganagar

# AI-Based Anomaly Detection in Cybersecurity Systems

Leesha Wadhwa, Indira Gandhi Delhi Technical University for Women

## Abstract

The rapid growth of digital infrastructure, cloud computing, Internet of Things (IoT) devices, and interconnected networks has significantly increased the complexity and frequency of cybersecurity threats. Conventional security mechanisms that rely primarily on predefined rules and known attack signatures often struggle to identify emerging, sophisticated, and previously unknown threats. Artificial Intelligence (AI)-based anomaly detection provides a promising approach by employing machine learning and intelligent data analysis techniques to identify deviations from normal system behavior. These systems can analyze large volumes of network traffic, user activities, system logs, and endpoint data to detect suspicious patterns and potential security incidents in real time. Supervised, unsupervised, and deep learning algorithms can be utilized to recognize anomalous behavior and improve the detection of zero-day attacks, insider threats, malware, and network intrusions. Furthermore, adaptive AI models can continuously learn from changing environments, enabling cybersecurity systems to respond more effectively to evolving attack strategies. However, the implementation of AI-based anomaly detection presents challenges, including high false-positive rates, imbalanced datasets, adversarial attacks, data privacy concerns, computational requirements, and the interpretability of complex models. This paper examines the role of AI in anomaly detection for cybersecurity systems, focusing on its methodologies, applications, benefits, and limitations. It also discusses emerging trends and the importance of explainable, adaptive, and robust AI solutions for developing reliable cybersecurity frameworks capable of protecting modern digital environments.

**Keywords: Artificial Intelligence, Anomaly Detection, Cybersecurity, Machine Learning, Deep Learning, Network Intrusion Detection, Zero-Day Attacks, Threat Detection.**

(ISSN: 2393-8048)