(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

Khyati Chaudhary, Indira Gandhi Delhi Technical University for Women
Leesha Wadhwa, Indira Gandhi Delhi Technical University for Women

Abstract

Traditional cyber defenses are inadequate for detecting new or previously unidentified attack vectors, since hackers are more sophisticated. The need for advanced systems capable of real-time anomaly detection, irrespective of predefined signatures or criteria, is rising due to the complexity and dynamism of cyber-attacks. Enhancing cyber security systems is now more accessible with AI-based anomaly detection, which use machine learning and deep learning algorithms to autonomously identify atypical system behavior. These AI-driven methodologies provide the advantage of analyzing historical data, facilitating the detection of evolving threats that traditional systems may overlook. This article examines several machine learning methodologies, including supervised, unsupervised, and semi-supervised learning, alongside advanced deep learning models, in relation to cyber security and their use in anomaly detection using artificial intelligence. We examine how these technologies emulate typical user, network, and system behavior to detect fraud, intrusions, and other harmful activities. The essay addresses difficulties related to imbalanced datasets, false positives, model interpretability, and adversarial attacks on AI systems in the context of implementing AI-based anomaly detection. When considering the integration of AI-based models, Security Information and Event Management (SIEM) systems and other contemporary cyber security infrastructures are also evaluated to enhance scalability and real-time responsiveness.

Furthermore, we examine ethical problems like as privacy and surveillance, offering critical insights on achieving a balance between security imperatives and user rights. The paper continues by delineating the potential future of AI-driven anomaly detection in domains such as autonomous threat identification, automated response systems, and the development of proactive and resilient defensive mechanisms via partnership with other cyber security technologies.

Keywords: - Anomaly Detection, Cyber security, Machine Learning, Real-Time Monitoring, Threat Detection.