IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 1, July 2024

Cyber Threat Hunters : Machine Learning Survey for Security

Swarangi P. Saraikar, Shivani A. Dhomase, Dr. Sharmila S. More
MIT ACSC Alandi(D), Pune, Maharashtra
swarangiprashantsaraikar@mitacsc.edu.in, shivanianildhomase@mitacsc.edu.in, ssmore@mitacsc.ac.in

Abstract: *Machine learning (ML) has become available across various sectors, revolutionizing fields like healthcare, finance, and cybersecurity. It is not affected by its large potential, ML models are susceptible to diverse security threats. This survey delves into the intricate landscape of ML security, providing a comprehensive overview of the current state-of-the-art. We begin by outlining various attack vectors, including data poisoning, adversarial attacks, and model inversion, which can compromise the integrity and functionality of ML systems. Subsequently, we explore established and emerging defence mechanisms designed to mitigate these vulnerabilities. The survey further analyses the challenges and limitations are making more difficult for the development of strong and secure ML models. Finally, we discuss promising research directions and open problems that warrant further investigation to ensure the secure and trustworthy deployment of ML in security-critical applications.*

Keywords: Machine Learning, Security, Adversarial Attacks, Data Poisoning, Model Inversion, Defence Mechanisms, Security Challenges

DOI: 10.48175/568