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 2, June 2024

MCAD: A Machine Learning Based Cyber Attack Detector using SDN for Healthcare Systems

Akash G[1], Aryadeep M B[2], H Nandeesh[3], Dr. Siddalingesh Bandi[4]
Students, Department of ECE[1,2,3]
Associate Professor, Department of ECE[4]
Global Academy of Technology, Bengaluru, Karnataka, India

Abstract: *The healthcare industry, increasingly reliant on digital technology, has become a prime target for cyberattacks. While traditional security measures address external threats, they often fail to effectively counter a particularly dangerous foe: insider threats. This project proposes MCAD (Machine Learning-based CyberAttack Detector), a groundbreaking approach that leverages the power of machine learning within Software-Defined Networks (SDNs) to bolster healthcare network security.*

Healthcare networks are inherently complex ecosystems, housing a diverse range of medical devices alongside traditional IT infrastructure. This intricate web creates a larger attack surface for malicious insiders with access to critical systems. These insiders can be disgruntled employees or attackers exploiting vulnerabilities in poorly designed systems.

The COVID-19 pandemic further exacerbated this vulnerability as the surge in telehealth services and remote access points opened new avenues for exploitation. The statistics are alarming, with a staggering 92% of healthcare organizations reporting insider-caused security breaches. These breaches not only compromise sensitive patient data but can also disrupt critical healthcare services, potentially jeopardizing patient safety.

MCAD, a Machine Learning-based Cyber Attack Detector, tackles the growing threat of insider attacks in healthcare networks. It employs a multi-pronged approach: collecting both normal and abnormal network traffic to train a real-time machine learning model. This model continuously analyzes network activity, identifying suspicious behavior indicative of insider threats. MCAD seamlessly integrates with SDN controllers for efficient deployment within existing infrastructure, and undergoes rigorous testing with various machine learning algorithms and simulated attacks to ensure optimal protection against evolving cyber threats.

Keywords: healthcare industry.