Review of Adaptive Deep Learning Approaches for Intrusion Detection in IoT Network

Pooja Khare[1] and Akash Singh[2]

Research Scholar, Babulal Tarabai Institute of Research and Technology, Sagar, India[1]

Assistant Professor, Computer science & Engineering, Babulal Tarabai Institute of Research and Technology, Sagar[2]

poojakhare1523@gmail.com and akashst133@gmail.com

Abstract: *As the Internet of Things (IoT) ecosystem continues to expand, the security of IoT networks becomes an increasingly critical concern. The vast and interconnected nature of IoT devices introduces unique challenges for intrusion detection systems (IDS) to safeguard against potential threats. Traditional intrusion detection methods often fall short in addressing the dynamic and evolving nature of attacks in IoT environments. This paper explores the efficacy of adaptive deep learning approaches for intrusion detection in IoT networks, aiming to enhance the resilience and responsiveness of security mechanisms.*

The proposed adaptive deep learning model leverages the power of neural networks to automatically learn and adapt to emerging threats. The model is designed to dynamically adjust its parameters based on the evolving characteristics of the network and the attack landscape. The adaptive nature of the deep learning approach enables it to continuously improve its detection capabilities without requiring explicit retraining, making it well-suited for the dynamic nature of IoT environments.

The study begins with an overview of the unique challenges posed by IoT networks, including the heterogeneity of devices, resource constraints, and the need for real-time threat detection. Subsequently, a comprehensive review of existing intrusion detection techniques in IoT is presented, highlighting their limitations and the motivation for adopting adaptive deep learning methodologies..

Keywords: Intrusion Detection Systems (IDS), Adaptive Deep Learning Models, IoT Network Security, Anomaly Detection Techniques, Cyber Threat Mitigation