IJARSCT

ISSN (Online) 2581-9429

IJARSCT

Impact Factor: 7.53

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

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

Volume 4, Issue 3, June 2024

A Novel Deep Learning Approach for IoT Security and Privacy Attack Detection

Aziz Ullah Karimy[1] **and Dr. P Chandrasekhar Reddy**[2]
Department of Electronics and Communication Engineering[1,2]
Jawaharlal Nehru Technological University, Hyderabad, India

Abstract: *The Internet of Things (IoT), often known as the Internet of Objects, is envisioned as a game-changing method of offering a variety of services. IoT is not complete without compact smart devices, which come in a wide variety of uses, sizes, energy capacities, and processing speeds. However, the incorporation of these smart devices into the traditional Internet poses a number of security issues because, in order to accommodate IoT, technologies and communication protocols were not created. Additionally, the commercialization of IoT has raised challenges with personal privacy, the potential of cyberattacks, and organized crime that are related to public security. In this context, significant attempts have been made, largely using conventional cryptographic techniques, to address the security and privacy challenges in IoT networks. The existing approaches, however, are insufficient to cover the complete security spectrum of IoT networks due to the distinctive features of IoT nodes. To deal with various security issues, machine learning (ML) and deep learning (DL) approaches that may embed intelligence in IoT devices and networks can be used. In this work, we offer a powerful model to recognize security concerns using deep learning techniques on the latest datasets, which were made available for undertaking research activities, we may identify privacy-related dangers in the IoT era. Here, we looked at the feature set of the data needed to use the suggested model to identify the various vulnerabilities stated in the given dataset. The classification of binary and multiclass assaults using deep learning techniques is examined in this work.*

Keywords: IoT, IoT threat, Internet of Objects, Security, Privacy, Deep Learning

DOI: 10.48175/568