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 3, June 2024

Machine Learning Based IoT Intrusion Detection System

Dr. Srinivas Kanakala
Department of CSE
VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India
srinivaskanakala@gmail.com

Abstract: *Today, the use of IoT devices has increased rapidly. Every home network has at least one IoT device. These devices communicate over the Internet through various additional Networking protocols, one of the main protocols is* ***The MQTT Protocol****. This protocol is one of the hot layers for attacks on IoT devices. Various unauthorized devices or authorized devices with malicious intent try to connect to the network and compromise the devices. Hence, it's very important to detect the Intruder in our network. For the detection of Intruders, we use the* ***IDS (Intrusion Detection system)****. This system should be trained to identify the MQTT attacks and get them to the notice of the Network Administrator. We'll be using ML techniques to train the IDS in identifying the attacks. We'll be using datasets that include unidirectional data flow, bidirectional data flow, and packet-based data flow information. Thus, through this project, an IDS with enough Accuracy in detecting the attacks will be developed. To train our IDS, we will be using MQTT-IoT-IDS2020 Dataset. We will be training our IDS with this dataset and will be analyzing the above dataset with our networking knowledge and will be making respective alterations in the dataset according to the attacks to improve the accuracy.*

Keywords: MQTT Protocol