Chapter 6
Network Intrusion Detection and Prevention Systems for Attacks in IoT Systems

Vetrivelan Pandu
VIT Chennai, India

Jagannath Mohan
VIT Chennai, India

T. S. Pradeep Kumar
VIT Chennai, India

ABSTRACT

Internet of things (IoT) has transformed greatly the improved way of business through machine-to-machine (M2M) communications. This vast network and its associated technologies have opened the doors to an increasing number of security threats which are dangerous to IoT and 5G wireless networks. The first part of this chapter presents instruction detection system (IDS) which detect the various attacks in 6LoWPAN layer. An IDS is to detect and analyze both inbound and outbound network traffic for abnormal activities. An IPS complements an IDS configuration by proactively inspecting a system's incoming traffic to weed out malicious requests. A typical IPS configuration uses web application firewalls and traffic filtering solutions to secure applications. An IPS prevents attacks by dropping malicious packets, blocking offending IPs and alerting security personnel to potential threats. Machine learning (ML)-based instruction detection and prevention system (IDPS) is proposed and implemented in Contiki simulation environment.

DOI: 10.4018/978-1-5225-8241-0.ch006

INTRODUCTION

Internet of Things (IoT) is a smart system which associates everything to the web to exchange data with concurred conventions. Intrusion Detection System (IDS) is utilized to screen the activity specifically hub and system. It can go about as a second line of protection which can guard the system from interlopers. Interruption is an undesirable or noxious movement which is destructive to sensor hubs. IDS recognizes the system parcels and decide if they are gatecrashers or authentic clients. There are three segments of IDS: Monitoring, Analysis and identification, Alarm (Shanzhi et al., 2014). The checking module screens the system's traffics, examples and assets. Examination and Detection is a center part of IDS which distinguishes the interruptions as indicated by determined calculation. Caution module raised an alert if the interruption is identified.

Background

IoT is a quickly developing advancement that will significantly change the manner in which people live. It tends to be thought of as the following enormous advance in Internet innovation (Tejas et al., 2017). The changing working condition related to the Internet of Things speaks to impressive effect to the attack surface and risk condition of the Internet and Internet associated frameworks (Jun et al., 2014).

Data science is an interdisciplinary field about procedures and frameworks to extricate learning or experiences from information in different structures, either organized or unstructured, which is a continuation of a portion of the information investigation fields, for example, measurements, machine learning, information mining and learning revelation, and prescient examination (Khan et al., 2016).

As constrained remote detecting and activating gadgets are logically incorporated with the Internet interchanges foundation, the significance of recognizing and managing attacks against its security and strength shows up as a principal necessity. This coordination is turning into a reality, because of an institutionalized correspondences stack being intended for the IoT, enabled by conventions, for example, the 6LoWPAN adjustment layer, RPL (IPv6 Routing Protocol for Low Power and Lossy Networks), and the Constrained Application Protocol (CoAP). Other protocols could also be considered at the application layer, such as MQTT (Message Queuing Telemetry Transport) (B. Andrew et al., 2014), but our focus in CoAP is motivated by its support of low-energy wireless local communication environments, machine-to-machine (M2M) communications between constrained sensors and actuators and other external Internet devices, and its direct compatibility with HTTP.