Chapter 7
Intrusion Detection on NF-BoT-IoT Dataset Using Artificial Intelligence Techniques

G. Aarthi
B.S. Abdur Rahman Crescent Institute of Science and Technology, India

S. Sharon Priya
B.S. Abdur Rahman Crescent Institute of Science and Technology, India

W. Aisha Banu
B.S. Abdur Rahman Crescent Institute of Science and Technology, India

ABSTRACT

The rapid development of internet of things (IoT) applications has created enormous possibilities, increased our productivity, and made our daily life easier. However, because of resource limitations and processing, IoT networks are open to number of threats. The network instruction detection system (NIDS) aims to provide a variety of methods for identifying the increasingly common cyberattacks (such as distributed denial of service [DDoS], denial of service [DoS], theft, etc.) and to prevent hazardous activities. In order to determine which algorithm is more effective in detecting network threats, multiple public datasets and different artificial intelligence (AI) techniques are evaluated. Some of the learning algorithms like logistic regression, random forest, decision tree, naive bayes, auto-encoder, and artificial neural network were analysed and concluded on the NF-BoT-IoT dataset using various evaluation metrics. In order to train the model for future anomaly detection prediction and analysis, the feature extraction and pre-processing data were then supplied into NIDS as data.

DOI: 10.4018/978-1-6684-8098-4.ch007

INTRODUCTION

The Internet of Things (IoT) is a collection of interconnected IoT nodes that operate autonomously to collect and exchange data with other nodes over an Internet connection. IoT is a widely used technology that is expanding quickly in automated network systems. Security for IoT nodes needs to be decided upon early in the design and implementation process. Even basic gadgets may now connect and share huge volumes of data with other nodes due to the IoT nodes' quick spread. The security of the data must be taken into account because of the vast amount of data being carried across the network. Modern security measures should be used on the network to protect IoT nodes.

Among the most significant security concerns in the IoT are botnet-based attacks like Distributed Denial of Service (DDoS), Denial of Service (DoS), and others (Ge et al., 2019) where attackers infect nodes with malicious code or overload node information and impair performance. Botnet-based assaults are one of the biggest dangers to IoT nodes.

To handle this kind of difficulty, the IoT node should require specialized standards and communication protocols. The Constrained Application Protocol (CoAP), the Advanced Message Queuing Protocol (AMQP), the Message Queue Telemetry Transport (MQTT), and the Extensible Messaging Presence Protocol (XMPP) are just a few of the messaging and communication protocols that are used to ensure reliable and secure data communication between IoT nodes. Because of its low bandwidth requirements, low memory requirements, and low packet loss, MQTT is the most widely used protocol. MQTT is an IoT-focused communications protocol that is an OASIS standard. There are four crucial parts to the publish/subscribe messaging protocol: clients, brokers, topics, and messages. Data exchange between MQTT-Client (IoT nodes) and Broker (Central node). The broker enables IoT nodes to post and subscribe to subjects simultaneously, subject to node capability. MQTT topics are a form of structured, hierarchical addressing, similar to the forward slash (/) delimiter used in file systems. It includes communications, including data collected by various IoT nodes and messages from various networks.

TCP and UDP are the most often utilized transport protocols in the majority of applications. However, depending on the necessity, multiple message distribution functions and compatible standards are required for IoT applications. The majority of Internet of Things (IoT) nodes use the MQTT communication protocol, which runs on top of TCP, to send and receive data between IoT nodes.

The IoT nodes should use quicker and more effective security measures to detect network traffic irregularities. Firewalls, antivirus software, and instruction detection systems (IDSs) are examples of cyber security measures. These techniques defend against both active and passive attacks on the data. Without interfering with the system's operation, a passive attacker just watches and copies data, which typically involves listening in, traffic analysis, etc. IDS is one of the crucial types of detection systems that are used to track abnormalities, in the states of the hardware and the software running in the network, whereas active attackers try to manipulate the content of the data; some of them are DDoS, DoS, etc.

Now, research is concentrated on developing IDSs utilising various supervised and unsupervised learning methods. Machine learning is a sort of AI that can extract data from huge databases. Furthermore, neural networks are the basis of deep learning algorithms, which are a subfield of machine learning. Many cyber security activities, such as botnet identification, network traffic analysis, and instruction detection, involve machine learning and deep learning techniques.