


Chapter 34

Machine Learning Techniques to Mitigate Security Attacks in IoT

Kavi Priya S.

 <https://orcid.org/0000-0002-1292-9728>
Mepco Schlnek Engineering College, India

Vignesh Saravanan K.

Ramco Institute of Technology, Rajapalayam, India

Vijayalakshmi K.

Ramco Institute of Technology, Rajapalayam, India

ABSTRACT

Evolving technologies involve numerous IoT-enabled smart devices that are connected 24-7 to the internet. Existing surveys propose there are 6 billion devices on the internet and it will increase to 20 billion devices within a few years. Energy conservation, capacity, and computational speed plays an essential part in these smart devices, and they are vulnerable to a wide range of security attack challenges. Major concerns still lurk around the IoT ecosystem due to security threats. Major IoT security concerns are Denial of service(DoS), Sensitive Data Exposure, Unauthorized Device Access, etc. The main motivation of this chapter is to brief all the security issues existing in the internet of things (IoT) along with an analysis of the privacy issues. The chapter mainly focuses on the security loopholes arising from the information exchange technologies used in internet of things and discusses IoT security solutions based on machine learning techniques including supervised learning, unsupervised learning, and reinforcement learning.

INTRODUCTION

Today's Internet becomes the connectivity of many smart devices and computers. Any real world object can be attached with a sensor and connected to the network. It paves way for many applications that benefits the users. Some common applications are automation in industry, smart home, patient's effective health monitoring applications etc. Some years back, the devices are connected in a network, which is now getting evolved smarter by the connection of any real-world objects. Clearly it states that Internet of Things(IoT) is a fast-evolving technology. Some statistics on IoT predicts that there will be more than 5 billion IoT devices connected at present. IoT can be any physical device equipped with sensors are connected with a communication channel. Through the connected network the devices can interact with the environment, i.e. collect data from surroundings and send that data for processing. Such devices that interacts with the environment to collect data is called as source node. The data is collected by source node and communicated to the base station or the sink node for processing or storage.

Consequently, an algorithm is the responsible for the data collection or data gathering and routing the data to the base station. All these devices are interconnected to share and exchange the data, that makes the IoT and wireless sensor network open to many challenges in security violations and privacy exploration for the users.

MAIN FOCUS OF THE CHAPTER

In this chapter, provides an idea about the wireless sensor network and IoT, which is an interconnection of the devices controlled through the Human machine interface (HMI). The essential features and use of connected devices or the embedded devices with the network provide a number of uses in many applications. This attractive feature also enables IoT devices connected with the network more prone to security threats and attacks. Depending on the data being communicated over the network, it inhibits an interest over the attackers with a wide range of privacy exploration. Hence providing a secured connected network has to ensure it provides solutions for the various concerns like Privacy of data, data reliability, correct responses from the connected devices, trust-worthy devices and autonomous recovery of the device when compromised. Considering these factors, the IoT requires effective solutions to achieve the above terms.

TECHNOLOGIES CONNECTING VARIOUS IOT DEVICES

The main objective of the Internet of Things is to provide an environment in which the connected devices are able to transfer information without any manual interference. Thus, the exchange of information between two devices is possible under some well-established communication technologies, which are discussed below.

Wireless Sensor Networks (WSN)

Wireless Sensor Networks are comprised of set of independent nodes with limited bandwidth and frequency through which it can communication wirelessly with other nearby devices. In traditional wireless sensor network environment, the sensor node consists of the following parts:

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/machine-learning-techniques-to-mitigate-security-attacks-in-iiot/307476

Related Content

Using Open-Source Software for Business, Urban, and Other Applications of Deep Neural Networks, Machine Learning, and Data Analytics Tools

Richard S. Segall and Vidhya Sankarasubbu (2022). *International Journal of Artificial Intelligence and Machine Learning* (pp. 1-28).

www.irma-international.org/article/using-open-source-software-for-business-urban-and-other-applications-of-deep-neural-networks-machine-learning-and-data-analytics-tools/307905

A Review on Time Series Motif Discovery Techniques and Application to ECG Signal Classification: ECG Signal Classification Using Time Series Motif Discovery Techniques

Ramanujam Elangovan and Padmavathi S. (2019). *International Journal of Artificial Intelligence and Machine Learning* (pp. 39-56).

www.irma-international.org/article/a-review-on-time-series-motif-discovery-techniques-an-application-to-ecg-signal-classification/238127

Power Consumption Prediction of IoT Application Protocols Based on Linear Regression

Sidna Jeddou, Amine Baina, Najid Abdallah and Hassan El Alami (2021). *International Journal of Artificial Intelligence and Machine Learning* (pp. 1-16).

www.irma-international.org/article/power-consumption-prediction-of-iiot-application-protocols-based-on-linear-regression/287585

Autoencoder Based Anomaly Detection for SCADA Networks

Sajid Nazir, Shushma Patel and Dilip Patel (2021). *International Journal of Artificial Intelligence and Machine Learning* (pp. 83-99).

www.irma-international.org/article/autoencoder-based-anomaly-detection-for-scada-networks/277436

Unveiling the Potential: A Comprehensive Exploration of Deep Learning and Transfer Learning Techniques in Bioinformatics

Umesh Kumar Lilhore and Sarita Simaiya (2024). *Applying Machine Learning Techniques to Bioinformatics: Few-Shot and Zero-Shot Methods* (pp. 138-158).

www.irma-international.org/chapter/unveiling-the-potential/342722