CHAPTER 5

Machine and Deep Learning Approaches for IoT Networks

Hina Kirn, Ayesha Altaf, Muhammad Anwar, and Marina Md-Arshad

5.1 INTRODUCTION

The term "Internet of Things" (IoT) refers to a network of interconnected computing devices that can exchange data and coordinate their efforts to carry out certain activities. IoT encompasses a wide range of networks and applications, including those for use in the home and workplace, as well as in industry, medicine, and the air. To evaluate the data or defend the data and network against assaults, researchers, data scientists, and Artificial Intelligence (AI) professionals employ a wide variety of methods. IoT and the integration of AI into it are two of the most promising and rapidly expanding fields of study and practice today and in the future. Machine learning, a subfield of AI, is concerned with the use of computational and statistical methods to discover previously unsuspected relationships in large amounts of data. Deep learning is a type of machine learning that employs Artificial Neural Networks (ANNs) to analyse and extract more nuanced features and patterns from data. This scenario can be seen in Figure 5.1.

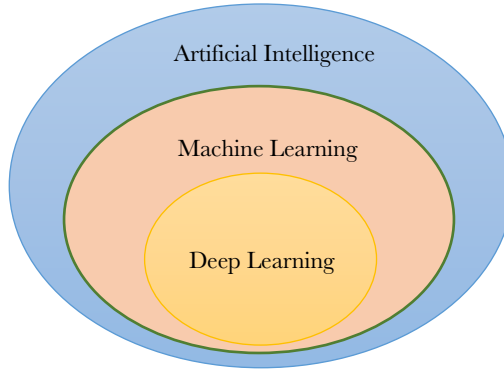

Figure 5.1 AI vs ML vs DL

In this chapter, we will go over the applications of machine learning and deep learning to analyse IoT network data to spot trends and potential threats. We look at how AI has had a wide-ranging effect on enhancing the IoT and what it means for the end user. We discuss several machines and deep learning categories and algorithms in different areas of IoT. The machine and deep learning algorithms deployed in the IoT networks, smart grids, cyber security, smart transportation systems, smart cities, and healthcare are studied.

To set the stage for the rest of the chapter, Section 5.2 presents previous research that has addressed similar topics. The chapter advances with the study's findings and discussion in Section 5.3, and finally, the chapter concludes in Section 5.4.

5.2 RELATED WORKS

The private and public spheres can both benefit from implementing IoT initiatives. With the use of IoT, consumers may monitor their lost pets, home security systems, and appliance upkeep routines. The IoT enables consumers to do things like reserve a table at a popular restaurant, keep tabs on their fitness and health and get discounts at nearby stores simply

by-passing past. Organizations can utilize IoT for predictive maintenance of equipment, inventory management, customer spending tracking and feedback collection, and inventory management.

5.2.1 IoT Security

Hussain et al. (2020) used machine and deep learning to integrate intelligence in IoT devices and networks. The study examines the dangers to IoT networks, potential methods of attack, and the remedies discovered thus far.

A methodology for effectively detecting security and privacy-related vulnerabilities in an IoT context by using several machine learning and deep learning approaches. Data features needed by the proposed model to detect the various risks included in the provided dataset are investigated. The Recurrent Neural Network (RNN) model surpassed its competitors in both binaries with an accuracy of 99.4% and multiclass threat detection with an accuracy of 96.2% (Janardhana et al., 2021).

Ferrag et al. (2021) analyzed the flaws in federated learning-based privacy and security solutions that might be used by malicious actors using three distinct deep learning methods convolutional neural networks, deep neural networks, and recurrent neural networks. Centralized and federated learning for each deep learning model is compared on three traffic-related IoT datasets namely MQTTset, TON IoT, and Bot-IoT. These results demonstrate the superior performance of federated deep learning algorithms over traditional, centralized machine learning methods (non-federated learning) when it comes to protecting the privacy of data collected by IoT devices and preventing intrusions.

Meanwhile, Nascita et al. (2022) evaluated the performance of cutting-edge deep learning-based traffic classifiers in identifying and categorizing IoT attacks. This study identifies distinct types of attacks and isolates them from legitimate network traffic. The efficiency of our "early" (i.e., "predictive") machine learning classifiers to that of more conventional