Chapter 8
Edge Computing in Intelligent IoT

Rajarajeswari S.
Vellore Institute of Technology, Chennai, India

Hema N.
Vellore Institute of Technology, Chennai, India

ABSTRACT

We can perceive, analyse, control, and optimise the conventional physical systems thanks to pervasive IoT applications. Numerous IoT apps have recently had security breaches, which suggests that IoT applications could endanger physical systems. Numerous security issues in IoT applications are mostly caused by two factors: severe resource restrictions and inadequate security architecture. Edge-based security designs for IoT applications are still in their infancy, despite some research efforts in this direction. In addition to providing an in-depth analysis of current edge-based IoT security options, this study seeks to provide inspiration for new edge-based IoT security designs. A significant deal of progress in artificial intelligence (AI) opens up a number of potential avenues for addressing the security challenges in the setting that privacy preservation and security have become essential issues for EC. This chapter addresses issues with edge computing-based internet of things at the computation and security levels.

EDGE INTELLIGENCE

Even though the term edge AI or EI is relatively research, new, and methodology in this area have existed for some time. As indicated before, Microsoft developed an edge-based prototype to support mobile voice command recognition, an AI application, in 2009 to show the advantages of edge computing. Despite the early stages of research, EI still lacks a defined definition. EI is currently referred to as the concept of demonstrating AI algorithms on an device with sensor data / signals) which are formed on the device by the majority of businesses and presses. It is important to highlight that, while this description reflects the current most popular tactic to EI in the real world Ike usage of high end AI chips), it significantly reduces the range of possible solutions. (O.salman et al.,2015) Running computation intensive methods

DOI: 10.4018/978-1-6684-6275-1.ch008

locally, as demonstrated by DNN models, is particularly resource-intensive and necessitates the inclusion of high end processors into the device. Such a mandatory requirement in addition to increase the price of EI but is also unsuited and unfavourable to legacy devices that currently exist and have constrained processing power.

This work states that EI is not limited to only using edge servers or devices to execute AI models. In fact, running DNN models with edge cloud collaboration can decrease end-to-end energy usage and latency when compared to the remote execution method, as shown by a numerous recent research. Because of these useful benefits, it is concluded that such a collaborative hierarchy ought to be incorporated into the creation of effective EI solutions. Additionally, current ideas about EI mostly concentrate on the inference phase (i.e., execution the AI model), assuming that the training of the AI model is carried out in the power cloud data centres because the training phase consumes substantially more number of resources than the inference phase. The vast volume of training data must, however, be transported either from end devices or from the cloud, results in excessive communication costs and worries about data protection (O.salman et al.,2015). As a result, it can be seen that EI does not essentially imply that the DNN model is completely trained or inferred at the edge but instead that it can function in a cloud-edge device synchronization manner via data offloading. EI can be categorized into six stages in accordance with the quantity and path length of data offloading, as displayed in Figure. 1. The following list includes a definition for each degree of emotional intelligence.

Figure 1. Six-level rating for EI