

# Preface

## Overview

The Internet of Things (IoT) is a dynamic global network infrastructure of self-configuring physical objects, embedded with connectivity protocols to enable collection and exchange of data and communication with other smart objects. The objects, or *things* in the network, react autonomously to events, without requiring man-machine intervention in real time. The IoT vision revolves around increased machine-to-machine communication, built on the cloud computing paradigm and networks of data-gathering sensors. This is now the vision of the *Internet of the future* that has the potential to revolutionize pervasive computing and its applications.

The IoT is transforming our lives, e.g., through the use of intelligent wearables, living in self-governing smart cities and driving autonomous cars in the *Internet of Vehicles* on smart roads. It is also transforming the business sector where the growth potential is explosive, as billions of smart interconnected units are already generating more than \$1 trillion in revenue. According to analysts, the market for intelligent systems will reach nearly four billion connected devices by 2016, representing more than \$2 trillion in revenue. Experts predict that there will be anywhere from 20 to 50 billion connected objects by 2020.

As perhaps the biggest of the latest technology trends, IoT is going to give us the most disruption, driving profound changes in many dimensions of our lives, as well as the most opportunity over the next few years. However, success of the IoT vision is highly dependent on the system architectures, network capabilities, communication protocols, and ubiquitous computing technologies to support effective and reliable physical and cyber interconnections. The IoT environment is heterogeneous where devices are supplied by a variety of vendors that follow different communication protocols and utilize diverse technologies. In this case, achieving interoperability can be highly complex, as data formats and encryptions also vary. Since seamless connectivity and interoperability are prerequisites in a multi-

network heterogeneous distributed environment such as the IoT, achieving reliable and resilient connectivity has already become a challenge. Besides, as *objects* are becoming more and more intelligent, device connectivity is also beginning to impact on regulatory compliance.

With this background, there is an urgent need for properly integrated solutions taking into account data and device security, signaling and device detection, device and data management, communication protocols and platforms, network bandwidth and topology, seamless connectivity and interoperability, and worldwide regulations and legal compliance. A major challenge that the IoT ecosystem must also overcome is the risks resulting from legal issues and performance problems caused by the mass deployment of inefficient, insecure, and/or defective IoT devices which may lead to further serious problems.

In this context, this book, *Connectivity Frameworks for Smart Devices: The Internet of Things from a Distributed Computing Perspective*, aims to capture the state of the art on the current advances in the connectivity of diverse devices. Majority of the contributions focus on the communication, security, privacy, access control, and authentication aspects of the device connectivity in distributed environments. Twenty-seven researchers and practitioners of international repute have presented latest research developments, frameworks and methodologies, current trends, state-of-the-art reports, case studies, and suggestions for further understanding, development, and enhancement of the IoT vision.

## Objectives

The aim of this volume is to present and discuss the state of the art in terms of frameworks and methodologies for connecting diverse *things* in relation to the IoT vision. The objectives include:

- Capturing the state-of-the-art research and practice relating to the IoT and distributed environments
- Discussing developments with respect to connectivity of heterogeneous smart and sensory devices
- Analyzing the relevant theoretical frameworks, practical approaches, and methodologies for machine-to-machine communication
- Discussing the latest advances, current trends, and future directions in the subject areas relating to the IoT
- In general, advancing the understanding of the emerging new methodologies relevant to the Internet of Things vision

## Organization

There are 14 chapters in *Connectivity Frameworks for Smart Devices: The Internet of Things from a Distributed Computing Perspective*. These are organized in three parts, as follows:

- **Part I: *Device Connectivity in the Internet of Things*.** This section has a focus on device connectivity within the IoT. There are four chapters. In the first two chapters, the emphasis is on security aspects of interconnections. The third contribution discusses machine-to-machine connectivity presenting an agent-based framework relevant to the IoT environment. The fourth contribution discusses vehicle-to-vehicle connectivity, presenting evolution of VANET in relation to the Internet of Vehicles.
- **Part II: *Architecture and Frameworks for the Internet of Things*.** This part of the book comprises six chapters that focus on frameworks and methodologies. The first chapter presents a resource-based architecture for IoT, whereas the second contribution presents integration approaches for the IoT environment. The next chapter proposes a resource management framework for corporate device clouds. The fourth contribution suggests a novel solution for interoperable data management in multi-clouds. The next contribution has a focus on the performance optimization of intelligent home networks, and the final contribution in this section presents a fuzzy cognitive map extend technology roadmap with respect to network neutrality in the IoT environment.
- **Part III: *Security Mechanisms for the Internet of Things*.** There are four chapters in this section that focus on security of connectivity mechanisms. The first two chapters present data security, privacy, access control, and authentication mechanisms with respect to the interconnection of varied devices in the distributed IoT environment. The third contribution presents a security perspective in relation to developing smart sustainable cities. The final chapter addresses generic security challenges within the IoT environment.

## Target Audiences

This volume is a reference text aimed at supporting a number of potential audiences, including the following:

- *Communication engineers and network security specialists* who wish to adopt the newer approaches to ensure the security of data and devices for seamless connectivity
- *Students and lecturers* who have an interest in further enhancing the knowledge of technologies, mechanisms, and frameworks relevant to the IoT environment from a distributed computing perspective

- *Researchers* in this field who require up-to-date knowledge of the current practices, mechanisms, and frameworks relevant to the IoT vision, to further enhance the connectivity between heterogeneous devices

Derby, UK  
Potchefstroom, South Africa

Zaigham Mahmood

Connectivity Frameworks for Smart Devices  
The Internet of Things from a Distributed Computing  
Perspective

Mahmood, Z. (Ed.)

2016, XIX, 356 p. 98 illus., 57 illus. in color., Hardcover

ISBN: 978-3-319-33122-5