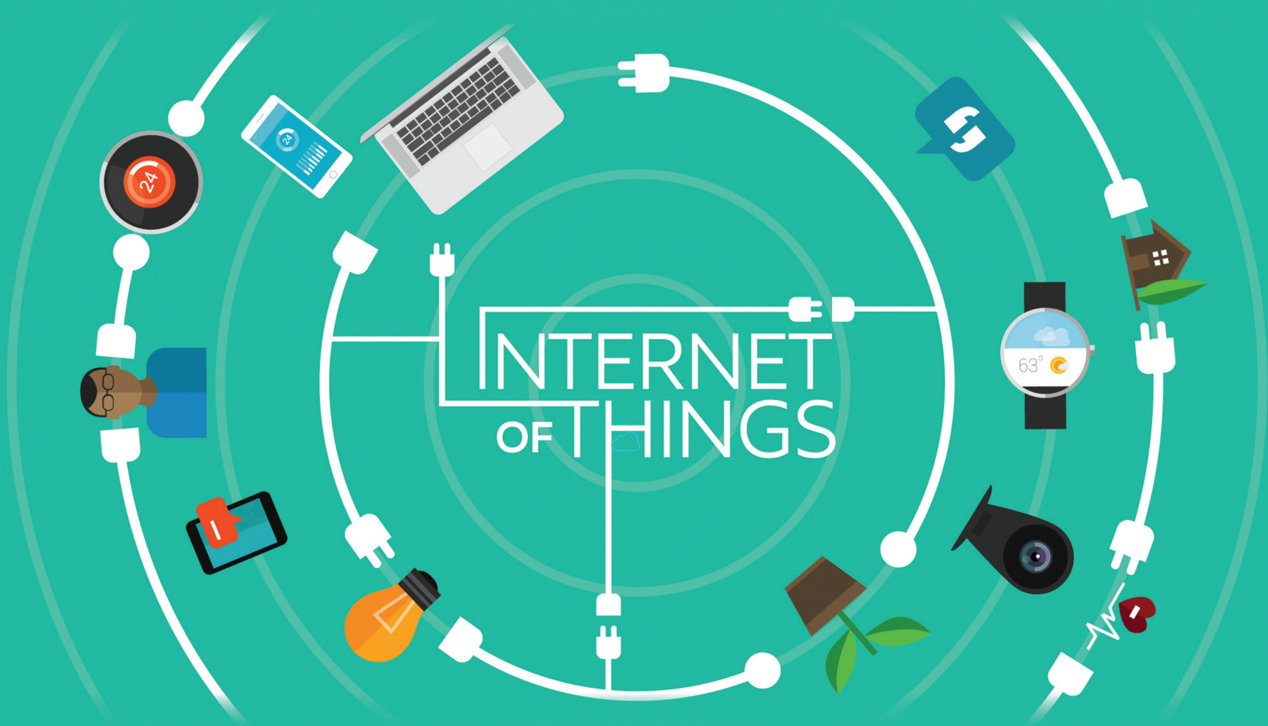
Internet of Things

Principles and Paradigms



Edited by **Rajkumar Buyya & Amir Vahid Dastjerdi**

MORGAN KAUFMANN

Internet of Things

Principles and Paradigms

Page left intentionally blank

Internet of Things

Principles and Paradigms

Edited by

Rajkumar Buyya

Cloud Computing and Distributed Systems (CLOUDS) Laboratory
Department of Computing and Information Systems
The University of Melbourne, Australia
Manjrasoft Pty Ltd, Australia

Amir Vahid Dastjerdi

Cloud Computing and Distributed Systems (CLOUDS) Laboratory
Department of Computing and Information Systems
The University of Melbourne, Australia

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Morgan Kaufmann is an imprint of Elsevier

MK
MORGAN KAUFMANN

Morgan Kaufmann is an imprint of Elsevier
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, USA

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

ISBN: 978-0-12-805395-9

For information on all Morgan Kaufmann publications
visit our website at https://www.elsevier.com/

Publisher: Todd Green
Acquisition Editor: Brian Romer
Editorial Project Manager: Amy Invernizzi
Project Manager: Priya Kumaraguruparan
Designer: Maria Inês Cruz

Typeset by Thomson Digital

Contents

PART III IoT DATA AND KNOWLEDGE MANAGEMENT

PART IV IoT RELIABILITY, SECURITY, AND PRIVACY

Page left intentionally blank

List of Contributors

D. An
Keimyung University, Dalgubeol-daero, Dalseo-gu, Daegu, South Korea

M. Apetroaie-Cristea
Faculty of Engineering and the Environment, University of Southampton, Southampton, United Kingdom

D. Ban
Samsung Electronics, South Korea

B. Bardhi
Department of Information Engineering, Università Politecnica delle Marche, Ancona, Italy

R. Buyya
Cloud Computing and Distributed Systems (CLOUDS) Laboratory, Department of Computing and Information Systems, The University of Melbourne, Australia; Manjrasoft Pty Ltd, Australia

R.N. Calheiros
Cloud Computing and Distributed Systems (CLOUDS) Laboratory, Department of Computing and Information Systems, The University of Melbourne, Australia

V. Chellappan
Department of Computer Science and Engineering, Indian Institute of Technology Madras, Chennai, India

A. Claudi
ADB Broadband S.p.A., Viale Sarca, Milano, Italy

S.J. Cox
Faculty of Engineering and the Environment, University of Southampton, Southampton, United Kingdom

A.V. Dastjerdi
Cloud Computing and Distributed Systems (CLOUDS) Laboratory, Department of Computing and Information Systems, The University of Melbourne, Australia

C. Georgoulis
Athens Information Technology, Marousi, Greece

S.K. Ghosh
Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India

H. Gupta
Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India

S. Han
Samsung Electronics, South Korea

E. Heo
Samsung Electronics, South Korea

S. Hosseinzadeh
Department of Information Technology, University of Turku, Finland

S. Hyrynsalmi
Department of Information Technology, University of Turku, Finland

S.J. Johnston
Faculty of Engineering and the Environment, University of Southampton, Southampton, United Kingdom

S. Karunasekera
Department of Computing and Information Systems, The University of Melbourne, Australia

N. Kefalakis
Athens Information Technology, Marousi, Greece

F. Khodadadi
Cloud Computing and Distributed Systems (CLOUDS) Laboratory, Department of Computing and Information Systems, The University of Melbourne, Australia

J. Krishnamurthy
School of Computer Science, McGill University, Montreal, Quebec, Canada

C. Leckie
Department of Computing and Information Systems, The University of Melbourne, Australia

V. Leppänen
Department of Information Technology, University of Turku, Finland

K. Li
Department of Computer Science, State University of New York, NY, United States of America

X. Liu
Cloud Computing and Distributed Systems (CLOUDS) Laboratory, Department of Computing and Information Systems, The University of Melbourne, Australia

M. Maheswaran
School of Computer Science, McGill University, Montreal, Quebec, Canada

S. Majumdar
Department of Systems and Computer Engineering, Carleton University, Ottawa, Canada

S. Misra
Ericsson Canada, Montreal, Quebec, Canada

M. Moshtaghi
Department of Computing and Information Systems, The University of Melbourne, Australia

M. Noack
Communication Systems Group CSG, Department of Informatics IFI, University of Zurich, Zürich, Switzerland

C.E. Palau
Distributed Real-Time Systems Research Group, Escuela Tecnica Superior de Ingenieros de Telecomunicación at the Universitat Politecnica de Valencia, Spain

S. Petris
Athens Information Technology, Marousi, Greece

J.V. Pradilla
Escuela Técnica Superior de Ingenieros de Telecomunicación at the Universitat Politècnica de Valencia, Spain

S. Sarkar
Department of CSIS, Birla Institute of Technology and Science Pilani, K.K.Birla Goa Campus, Goa, India

C. Schmitt
Communication Systems Group CSG, Department of Informatics IFI, University of Zurich, Zürich, Switzerland

M. Scott
Faculty of Engineering and the Environment, University of Southampton, Southampton, United Kingdom

K.M. Sivalingam
Department of Computer Science and Engineering, Indian Institute of Technology Madras, Chennai, India

J. Soldatos
Athens Information Technology, Marousi, Greece

L. Spalazzi
Department of Information Engineering, Università Politecnica delle Marche, Ancona, Italy

B. Stiller
Communication Systems Group CSG, Department of Informatics IFI, University of Zurich, Zürich, Switzerland

G. Taccari
Par-Tec S.p.A., Milano, Italy

L. Taccari
Department of Information Engineering, Università Politecnica delle Marche, Ancona, Italy

W. Wu
Department of Computer Science, Sun Yat-sen University, Guangzhou, China

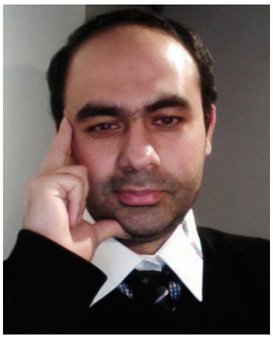
Z. Yang
Department of Computer Science, Sun Yat-sen University, Guangzhou, China

Y. Yoon
Hongik University, Wausan-ro, Mapo-gu, Seoul, South Korea

Page left intentionally blank

About the Editors

Rajkumar Buyya is a Fellow of IEEE, Professor of Computer Science and Software Engineering, and Director of the Cloud Computing and Distributed Systems (CLOUDS) laboratory at the University of Melbourne, Australia. He is also serving as the founding CEO of Manjrasoft, a spin-off company of the University, commercializing its innovations in Cloud Computing. He has authored over 500 publications and 6 textbooks including "Mastering Cloud Computing" published by McGraw Hill, China Machine Press, and Morgan Kaufmann for Indian, Chinese, and international markets respectively. He is currently serving as the Co-Editor-in-Chief of *Journal of Software: Practice and Experience*. For further information, please visit www.buyya.com



Amir Vahid Dastjerdi is a research fellow with the Cloud Computing and Distributed Systems (CLOUDS) laboratory at the University of Melbourne, Australia. He received his PhD in Computer Science from the University of Melbourne and his areas of interest include Internet of Things, Big Data, and Cloud Computing.

Page left intentionally blank

Preface

The Internet of Things (IoT) paradigm promises to make "things" including consumer electronic devices or home appliances, such as medical devices, fridge, cameras, and sensors, part of the Internet environment. This paradigm opens the doors to new innovations that will build novel type of interactions among things and humans, and enables the realization of smart cities, infrastructures, and services for enhancing the quality of life and utilization of resources.

IoT as an emerging paradigm supports integration, transfer, and analytics of data generated by smart devices (eg, sensors). IoT envisions a new world of connected devices and humans in which the quality of life is enhanced because management of city and its infrastructure is less cumbersome, health services are conveniently accessible, and disaster recovery is more efficient. Based on bottom-up analysis for IoT applications, McKinsey estimates that the IoT will have a potential economic impact of \$11 trillion per year by 2025—which would be equivalent to about 11% of the world economy. They also expect that one trillion IoT devices will be deployed by 2025. In majority of the IoT domains such as infrastructure management and healthcare, the major role of IoT is the delivery of highly complex knowledge-based and action-oriented applications in real-time.

To realize the full potential of the IoT paradigm, it is necessary to address several challenges and develop suitable conceptual and technological solutions for tackling them. These include development of scalable architecture, moving from closed systems to open systems, dealing with privacy and ethical issues involved in data sensing; storage, processing, and actions; designing interaction protocols; autonomic management; communication protocol; smart objects and service discovery; programming framework; resource management; data and network management; power and energy management; and governance.

The primary purpose of this book is to capture the state-of-the-art in IoT, its applications, architectures, and technologies that address the abovementioned challenges. The book also aims to identify potential research directions and technologies that will facilitate insight generation in various domains from science, industry, business, and consumer applications. We expect the book to serve as a reference for systems architects, practitioners, developers, researchers, and graduate-level students.

ORGANIZATION OF THE BOOK

This book contains chapters authored by several leading experts in the field of IoT. The book is presented in a coordinated and integrated manner starting with the fundamentals, and followed by the technologies that implement them. The content of the book is organized into five parts:

1. IoT Ecosystem Concepts and Architectures
2. IoT Enablers and Solutions
3. IoT Data and Knowledge Management
4. IoT Reliability, Security, and Privacy
5. IoT Applications

Part I presents an overview of IoT and its related concepts and evolution through time. It throws light upon different IoT architectures and their components and discusses emerging paradigms such as

Fog computing. In addition, the essential element of a cloud computing infrastructure for IoT services is discussed and a novel framework for collaborative computing between IoT devices and cloud is presented.

Part II is dedicated to platforms and solutions supporting development and deployment of IoT applications. It covers embedded systems programming languages as they play an important role in the development of IoT. Moreover, this part provides an elaborate introduction to message passing mechanisms such as RPC, REST, and CoAP that are indispensable for distributed programming in IoT. Furthermore, techniques for resource sharing and partitioning to enable multitenancy are explored. Three basic virtualization techniques for embedded systems are considered: full virtualization, paravirtualization (as instances of hardware-level virtualization), and containers (as instances of operating-system-level virtualization). Besides, it introduces an architecture which utilizes both cloud and virtualization for effective deployment of Cyber Physical Systems.

Part III focuses on data and knowledge management which have always been an integral part of IoT applications. It explains how stream processing toolkits offer scalable and reliable solutions to handle a large volume of data in motion and how they can be utilized in IoT environments. Furthermore, this part introduces a framework for distributed data analysis (machine learning mechanism) based on the core idea of Fog computing to use local resources to reduce the overhead of centralized data collection and processing. It will explain how this can be achieved by learning local models of the data at the nodes, which are then aggregated to construct a global model at a central node.

Part IV presents an argument for developing a governance framework for tackling the data confidentiality, data integrity, and operation control issues faced by IoT. It outlines the organizational, structural, regulatory, and legal issues that are commonly encountered in the IoT environment. In addition, it provides a detailed overview of the security challenges related to the deployment of smart objects. Security protocols at the network, transport, and application layers are discussed, together with lightweight cryptographic algorithms to be used instead of conventional and demanding ones, in terms of computational resources. Many of IoT applications are business critical, and require the underlying technology to be dependable, that is, it must deliver its service even in the presence of failures. Therefore, this part discusses the notion of reliability and recovery oriented systems in general and then explains why this is important for an IoT-based system. A range of failure scenarios and reliability challenges are narrated and tackled by failure-prevention and fault-tolerance approaches to make an IoT-based system robust.

Part V introduces a number of applications that have been made feasible by the emergence of IoT. Best practices for architecting IoT applications are covered, describing how to harness the power of cutting-edge technologies for designing and building a weather station with over 10 sensors using a variety of electronic interfaces connected to an embedded system gateway running Linux. This part also introduces Internet of Vehicles (IoV) and its applications. It starts by presenting the background, concept, and network architecture of IoV, and then analyzes the characteristics of IoV and correspondingly new challenges in IoV research and development. Finally, this part discusses the role of IoT in enabling efficient management of smart facilities and presents architecture for a cloud-based platform for managing smart facilities and the underlying middleware services. Techniques for effective management of resources in sensor networks and in parallel systems performing data analytics on data collected on a facility are discussed.

Acknowledgments

First and foremost, we are grateful to all the contributing authors for their time, effort, and understanding during the preparation of the book.

Raj would like to thank his family members, especially his wife, Smrithi and daughters, Soumya and Radha Buyya, for their love, understanding, and support during the preparation of the book. Amir would like to thank his wife Elly and daughter Diana.

Finally, we would like to thank the staff at Morgan Kauffman, particularly, Amy Invernizzi, Priya Kumaraguruparan, Brian Romer, and Todd Green. They were wonderful to work with.

Rajkumar Buyya
The University of Melbourne and Manjrasoft Pty Ltd, Australia

Amir Vahid Dastjerdi
The University of Melbourne, Australia

Page left intentionally blank

PART

IoT ECOSYSTEM CONCEPTS AND ARCHITECTURES

I

Page left intentionally blank

CHAPTER

INTERNET OF THINGS: AN OVERVIEW

1

F. Khodadadi*, A.V. Dastjerdi*, R. Buyya*,**

Cloud Computing and Distributed Systems (CLOUDS) Laboratory, Department of Computing and Information Systems, The University of Melbourne, Australia;Manjrasoft Pty Ltd, Australia*

1.1 INTRODUCTION

After four decades from the advent of Internet by ARPANET [1], the term "Internet" refers to the vast category of applications and protocols built on top of sophisticated and interconnected computer networks, serving billions of users around the world in 24/7 fashion. Indeed, we are at the beginning of an emerging era where ubiquitous communication and connectivity is neither a dream nor a challenge anymore. Subsequently, the focus has shifted toward a seamless integration of people and devices to converge the physical realm with human-made virtual environments, creating the so- called Internet of Things (IoT) utopia.

A closer look at this phenomenon reveals two important pillars of IoT: "Internet" and "Things" that require more clarification. Although it seems that every object capable of connecting to the Internet will fall into the "Things" category, this notation is used to encompass a more generic set of entities, including smart devices, sensors, human beings, and any other object that is aware of its context and is able to communicate with other entities, making it accessible at any time, anywhere. This implies that objects are required to be accessible without any time or place restrictions.

Ubiquitous connectivity is a crucial requirement of IoT, and, to fulfill it, applications need to support a diverse set of devices and communication protocols, from tiny sensors capable of sensing and reporting a desired factor, to powerful back-end servers that are utilized for data analysis and knowledge extraction. This also requires integration of mobile devices, edge devices like routers and smart hubs, and humans in the loop as controllers.

Initially, Radio-Frequency Identification (RFID) used to be the dominant technology behind IoT development, but with further technological achievements, wireless sensor networks (WSN) and Bluetooth-enabled devices augmented the mainstream adoption of the IoT trend. These technologies and IoT applications have been extensively surveyed previously [2–5], however, less attention has been given to unique characteristics and requirements of IoT, such as scalability, heterogeneity support, total integration, and real-time query processing. To underscore these required advances, this chapter lists IoT challenges and promising approaches by considering recent research and advances made in the IoT ecosystem, as shown in Fig. 1.1. In addition, it discusses emerging solutions based on cloud-, fog-, and mobile-computing facilities. Furthermore, the applicability and integration of cutting-edge approaches like Software Defined Networking (SDN) and containers for embedded and constrained devices with IoT are investigated.

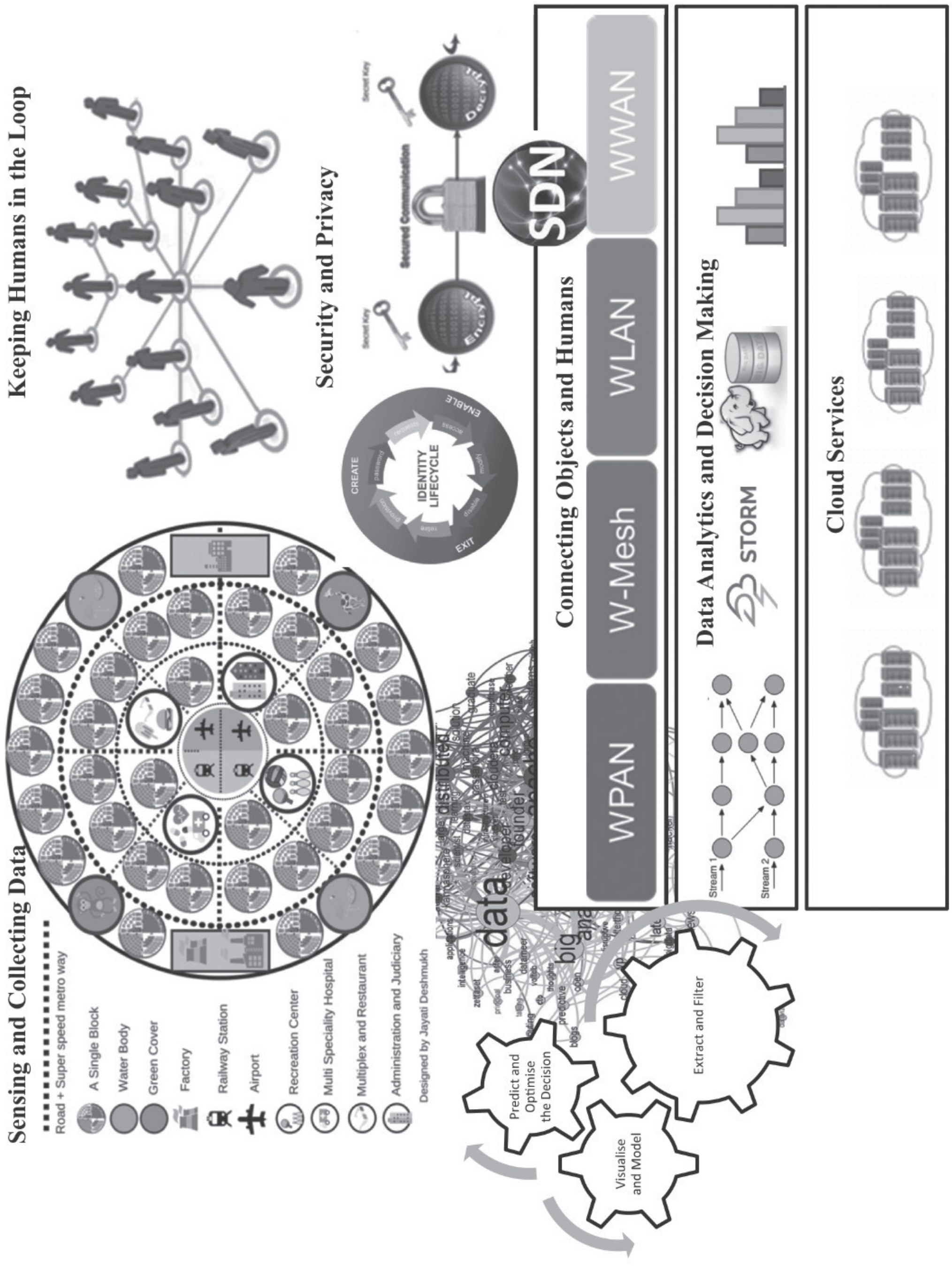


FIGURE 1.1 IoT Ecosystem

1.2 INTERNET OF THINGS DEFINITION EVOLUTION

1.2.1 IoT EMERGENCE

Kevin Ashton is accredited for using the term "Internet of Things" for the first time during a presentation in 1999 on supply-chain management [6]. He believes the "things" aspect of the way we interact and live within the physical world that surrounds us needs serious reconsideration, due to advances in computing, Internet, and data-generation rate by smart devices. At the time, he was an executive director at MIT's Auto-ID Center, where he contributed to the extension of RFID applications into broader domains, which built the foundation for the current IoT vision.

1.2.2 INTERNET OF EVERYTHING

Since then, many definitions for IoT have been presented, including the definition [7] that focuses mostly on connectivity and sensory requirements for entities involved in typical IoT environments. Whereas those definitions reflect IoT's basic requirements, new IoT definitions give more value to the need for ubiquitous and autonomous networks of objects where identification and service integration have an important and inevitable role. For example, Internet of Everything (IoE) is used by Cisco to refer to people, things, and places that can expose their services to other entities [8].

1.2.3 INDUSTRIAL IoT

Also referred to as Industrial Internet [9], Industrial IoT (IIoT) is another form of IoT applications favored by big high-tech companies. The fact that machines can perform specific tasks such as data acquisition and communication more accurately than humans has boosted IIoT's adoption. Machine to machine (M2M) communication, Big Data analysis, and machine learning techniques are major building blocks when it comes to the definition of IIoT. These data enable companies to detect and resolve problems faster, thus resulting in overall money and time savings. For instance, in a manufacturing company, IIoT can be used to efficiently track and manage the supply chain, perform quality control and assurance, and lower the total energy consumption.

1.2.4 SMARTNESS IN IoT

Another characteristic of IoT, which is highlighted in recent definitions, is "smartness." This distinguishes IoT from similar concepts such as sensor networks, and it can be further categorized into "object smartness" and "network smartness." A smart network is a communication infrastructure characterized by the following functionalities:

- standardization and openness of the communication standards used, from layers interfacing with the physical world (ie, tags and sensors), to the communication layers between nodes and with the Internet;
- object addressability (direct IP address) and multifunctionality (ie, the possibility that a network built for one application (eg, road-traffic monitoring) would be available for other purposes (eg, environmental-pollution monitoring or traffic safety) [10].

1.2.5 MARKET SHARE

In addition, definitions draw special attention to the potential market of IoT with a fast growing rate, by having a market value of $44.0 billion in 2011 [11]. According to a comprehensive market research conducted by RnRMarketResearch [12] that includes current market size and future predictions, the IoT and M2M market will be worth approximately $498.92 billion by 2019. Quoting from the same research, the value of the IoT market is expected to hit $1423.09 billion by 2020, with Internet of Nano Things (IoNT) playing a key role in the future market and holding a value of approximately $9.69 billion by 2020.

Besides all these fantastic and optimistic opportunities, for current IoT to reach the foreseen market, various innovations and progress in different areas are required. Furthermore, cooperation and information-sharing between leading companies in IoT, such as Microsoft, IBM, Google, Samsung, Cisco, Intel, ARM, Fujitsu, Ecobee Inc., in addition to smaller businesses and start-ups, will boost IoT adoption and market growth.

IoT growth rate with an estimated number of active devices until 2018 is depicted in Fig. 1.2 [13]. The increase of investment in IoT by developed and developing countries hints at the gradual change in strategy of governments by recognizing IoT's impacts and trying to keep themselves updated as IoT gains momentum. For example, the IoT European Research Cluster (IERC) (http://www.rfid-in-action.eu/cerp/) has conducted and supported several projects about fundamental IoT research by considering special requirements from end-users and applications. As an example, the project named Internet of Things Architecture (IoT-A) (http://www.iot-a.eu) aims at developing a reference architecture for specific types of applications in IoT, and is discussed in more detail in Section 1.3. The UK government has also initiated a 5 million project on innovations and recent technological advances in IoT [14]. Similarly, IBM in the USA [15] has plans to spend billions of dollars on IoT research and its industrial applications. Singapore has also announced its intention to be the first smart nation by investing in smart transport systems, developing the e-government structure, and using surveillance cameras and other sensory devices to obtain data and extract information from them [16].

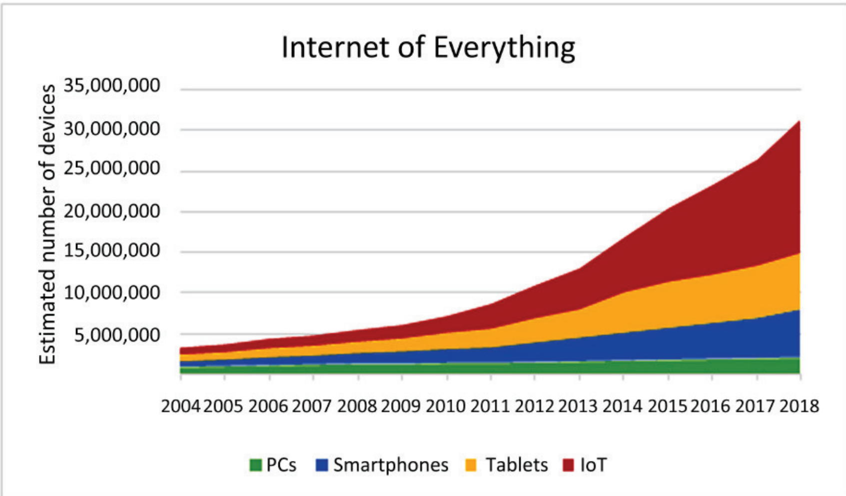


FIGURE 1.2 IoT Trend Forecast [13]

1.2.6 HUMAN IN THE LOOP

IoT is also identified as an enabler for machine-to-machine, human-to-machine, and human-with-environment interactions. With the increase in the number of smart devices and the adoption of new protocols such as IPv6, the trend of IoT is expected to shift toward the fusion of smart and autonomous networks of Internet-capable objects equipped with the ubiquitous computing paradigm. Involving human in the loop [17] of IoT offers numerous advantages to a wide range of applications, including emergency management, healthcare, etc. Therefore, another essential role of IoT is to build a collaborative system that is capable of effectively responding to an event captured via sensors, by effective discovery of crowds and also successful communication of information across discovered crowds of different domains.

1.2.7 IMPROVING THE QUALITY OF LIFE

IoT is also recognized by the impact on quality of life and businesses [8], which can revolutionize the way our medical systems and businesses operate by: (1) expanding the communication channel between objects by providing a more integrated communication environment in which different sensor data such as location, heartbeat, etc. can be measured and shared more easily. (2) Facilitating the automation and control process, whereby administrators can manage each object's status via remote consoles; and (3) saving in the overall cost of implementation, deployment, and maintenance, by providing detailed measurements and the ability to check the status of devices remotely.

According to Google Trends, the word "IoT" is used more often than "Internet of Things" since 2004, followed by "Web of Things" and "Internet of Everything" as the most frequently used words. Quoting the same reference, Singapore and India are the countries with the most regional interest in IoT. This is aligned with the fact that India is estimated to be the world's largest consumer of IoT devices by 2020 [18].

1.3 IoT ARCHITECTURES

The building blocks of IoT are sensory devices, remote service invocation, communication networks, and context-aware processing of events; these have been around for many years. However, what IoT tries to picture is a unified network of smart objects and human beings responsible for operating them (if needed), who are capable of universally and ubiquitously communicating with each other.

When talking about a distributed environment, interconnectivity among entities is a critical requirement, and IoT is a good example. A holistic system architecture for IoT needs to guarantee flawless operation of its components (reliability is considered as the most import design factor in IoT) and link the physical and virtual realms together. To achieve this, careful consideration is needed in designing failure recovery and scalability. Additionally, since mobility and dynamic change of location has become an integral part of IoT systems with the widespread use of smartphones, state-of-the-art architectures need to have a certain level of adaptability to properly handle dynamic interactions within the whole ecosystem.

Reference architectures and models give a bird's eye view of the whole underlying system, hence their advantage over other architectures relies on providing a better and greater level of abstraction, which consequently hides specific constraints and implementation details.

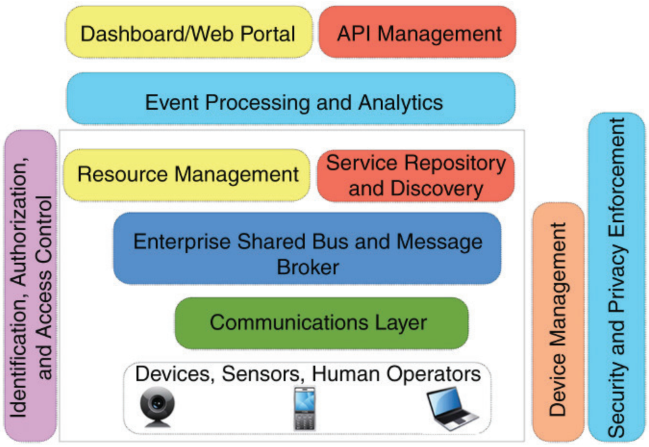


FIGURE 1.3 A Reference Architecture for IoT

Several research groups have proposed reference architectures for IoT [19,20]. The IoT-A [19] focuses on the development and validation of an integrated IoT network architecture and supporting building blocks, with the objective to be “the European Lighthouse Integrated Project addressing the Internet-of-Things Architecture.” IoT-i project, related to the previously mentioned IoT-A project, focuses on the promotion of IoT solutions, catching requirements and interests. IoT-i aims to achieve strategic objectives, such as: creating a joint strategic and technical vision for the IoT in Europe that encompasses the currently fragmented sectors of the IoT domain holistically, and contributing to the creation of an economically sustainable and socially acceptable environment in Europe for IoT technologies and respective R&D activities.

Fig. 1.3 depicts an outline of our extended version of a reference architecture for IoT [20]. Different service and presentation layers are shown in this architecture. Service layers include event processing and analytics, resource management and service discovery, as well as message aggregation and Enterprise Service Bus (ESB) services built on top of communication and physical layers. API management, which is essential for defining and sharing system services and web-based dashboards (or equivalent smartphone applications) for managing and accessing these APIs, are also included in the architecture. Due to the importance of device management, security and privacy enforcement in different layers, and the ability to uniquely identify objects and control their access level, these components are prestressed independently in this architecture. These components and their related research projects are described in more detail throughout this chapter.

1.3.1 SOA-BASED ARCHITECTURE

In IoT, service-oriented architecture (SOA) might be imperative for the service providers and users [21,22]. SOA ensures the interoperability among the heterogeneous devices [23,24]. To clarify this, let us consider a generic SOA consisting of four layers, with distinguished functionalities as follows:

- Sensing layer is integrated with available hardware objects to sense the status of things
- Network layer is the infrastructure to support over wireless or wired connections among things

- Service layer is to create and manage services required by users or applications
- Interfaces layer consists of the interaction methods with users or applications

Generally, in such architecture a complex system is divided into subsystems that are loosely coupled and can be reused later (modular decomposability feature), hence providing an easy way to maintain the whole system by taking care of its individual components [25]. This can ensure that in the case of a component failure the rest of the system (components) can still operate normally. This is of immense value for effective design of an IoT application architecture, where reliability is the most significant parameter.

SOA has been intensively used in WSN, due to its appropriate level of abstraction and advantages pertaining to its modular design [26,27]. Bringing these benefits to IoT, SOA has the potential to augment the level of interoperability and scalability among the objects in IoT. Moreover, from the user's perspective, all services are abstracted into common sets, removing extra complexity for the user to deal with different layers and protocols [28]. Additionally, the ability to build diverse and complex services by composing different functions of the system (ie, modular composability) through service composition suits the heterogeneous nature of IoT, where accomplishing each task requires a series of service calls on all different entities spread across multiple locations [29].

1.3.2 API-ORIENTED ARCHITECTURE

Conventional approaches for developing service-oriented solutions use SOAP and Remote Method Invocation (RMI) as a means for describing, discovering, and calling services; however, due to overhead and complexity imposed by these techniques, Web APIs and Representational State Transfer (REST)-based methods were introduced as promising alternative solutions. The required resources range from network bandwidth to computational and storage capacity, and are triggered by request–response data conversions happening regularly during service calls. Lightweight data-exchange formats like JSON can reduce the aforementioned overhead, especially for smart devices and sensors with a limited amount of resources, by replacing large XML files used to describe services. This helps in using the communication channel and processing the power of devices more efficiently.

Likewise, building APIs for IoT applications helps the service provider attract more customers while focusing on the functionality of their products rather than on presentation. In addition, it is easier to enable multitenancy by the security features of modern Web APIs such as OAuth, APIs which indeed are capable of boosting an organization's service exposition and commercialization. It also provides more efficient service monitoring and pricing tools than previous service-oriented approaches [30].

To this end, in our previous research we have proposed Simurgh [31], which describes devices, sensors, humans, and their available services using web API notation and API definition languages. Furthermore, a two-phase discovery approach was proposed in the framework to find sensors that provide desirable services and match certain features, like being in a specific location. Similarly, Elmangoush et al. [32] proposed a service-broker layer (named FOKUS) that exposes a set of APIs for enabling shared access to the OpenMTC core. Novel approaches for defining and sharing services in distributed and multiagent environments like IoT can reduce the sophistication of service discovery in the application development cycle and diminish service-call overhead in runtime.

Shifting from service delivery platforms (SDPs) toward web-based platforms, and the benefits of doing so are discussed by Manzalini et al. [33]. Developers and business managers are advised to focus on developing and sharing APIs from the early stage of their application development lifecycle, so that eventually, by properly exposing data to other developers and end users, an open-data environment is created that facilitates collaborative information gathering, sharing, and updating.

1.4 RESOURCE MANAGEMENT

Picturing IoT as a big graph with numerous nodes with different resource capacity, selecting and provisioning the resources greatly impacts Quality of Service (QoS) of the IoT applications. Resource management is very important in distributed systems and has been a subject of research for years. What makes resource management more challenging for IoT relies on the heterogeneous and dynamic nature of resources in IoT. Considering large-scale deployment of sensors for a smart city use-case, it is obvious that an efficient resource management module needs considerable robustness, fault-tolerance, scalability, energy efficiency, QoS, and SLA.

Resource management involves discovering and identifying all available resources, partitioning them to maximize a utility function—which can be in terms of cost, energy, performance, etc., and, finally, scheduling the tasks on available physical resources. Fig. 1.4 depicts the taxonomy of resource management activities in IoT.

1.4.1 RESOURCE PARTITIONING

The first step for satisfying resource provisioning requirements in IoT is to efficiently partition the resources and gain a higher utilization rate. This idea is vastly used in cloud computing via virtualization techniques and commodity infrastructures, however, virtual machines are not the only method for achieving the aforementioned goal. Since the hypervisor, that is responsible for managing interactions between host and guest VMs, requires a considerable amount of memory and computational capacity, this configuration is not suitable for IoT, where devices often have constrained memory and processing power. To address these challenges, the concept of *Containers* has emerged as a new form of virtualization technology that can match the demand of devices with limited resources. Docker (https://www.docker.com/) and Rocket (https://github.com/coreos/rkt) are the two most famous container solutions.

Containers are able to provide portable and platform-independent environments for hosting the applications and all their dependencies, configurations, and input/output settings. This significantly reduces the burden of handling different platform-specific requirements when designing and developing applications, hence providing a convenient level of transparency for applications, architects, and developers. In addition, containers are lightweight virtualization solutions that enable infrastructure providers to efficiently utilize their hardware resources by eliminating the need for purchasing expensive hardware and virtualization software packages. Since containers, compared to VMs, require considerably less spin-up time, they are ideal for distributed applications in IoT that need to scale up within a short amount of time.

An extensive survey by Gu et al. [34] focuses on virtualization techniques proposed for embedded systems and their efficiency for satisfying real-time application demands. After explaining numerous Xen-based, KVM-based, and microkernel-based solutions that utilize processor architectures such as ARM, authors argue that operating system virtualization techniques, known as container-based virtualization, can bring advantages in terms of performance and security by sandboxing applications on top

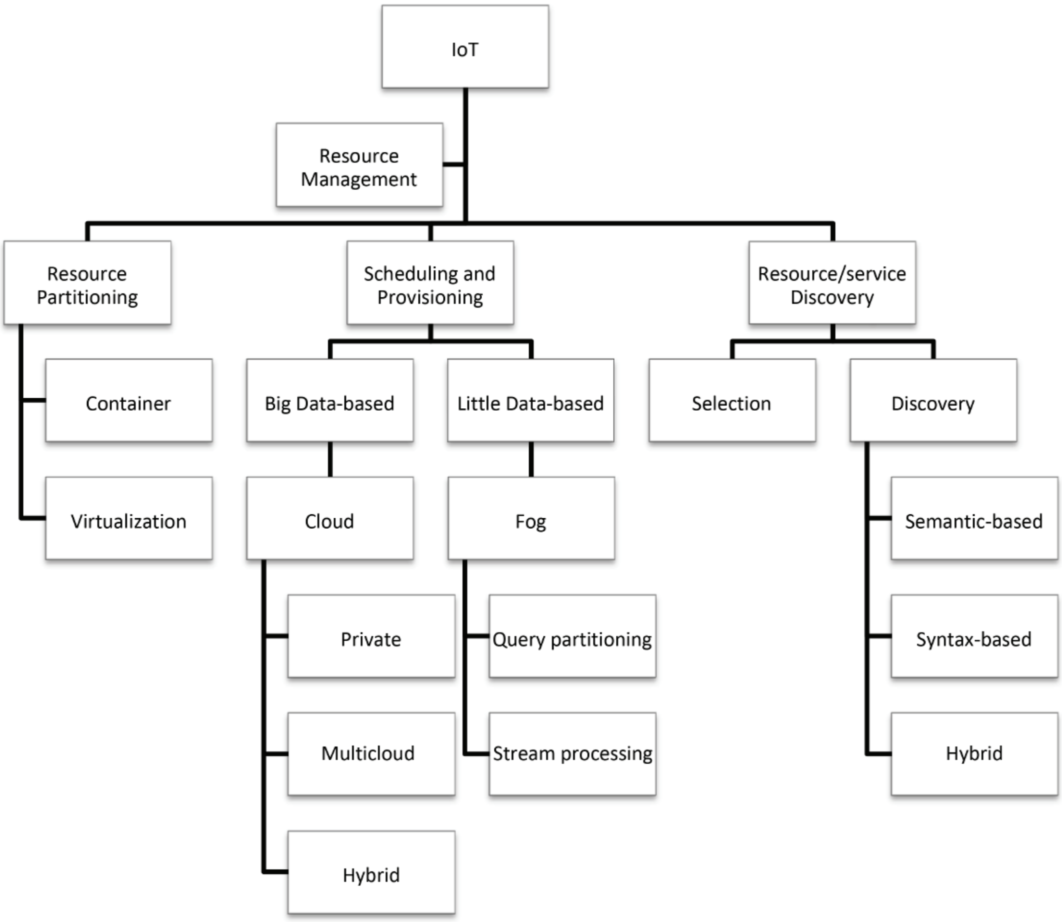


FIGURE 1.4 Taxonomy of Resource Management in IoT

of a shared OS layer. Linux VServer [35], Linux Containers LXC, and OpenVZ are examples of using OS virtualization in an embedded systems domain.

The concept of virtualized operating systems for constrained devices has been further extended to smartphones by providing the means to run multiple Android operating systems on a single physical smartphone [36]. With respect to heterogeneity of devices in IoT, and the fact that many of them can leverage virtualization to boost their utilization rate, task-grain scheduling, which considers individual tasks within different containers and virtualized environments, can potentially challenge current resource-management algorithms that view these layers as black box [34].

1.4.2 COMPUTATION OFFLOADING

Code offloading (computation offloading) [37] is another solution for addressing the limitation of available resources in mobile and smart devices. The advantages of using code offloading translate to more efficient power management, fewer storage requirements, and higher application performance. Several surveys about computation offloading have carefully studied its communication and execution requirements, as well as its adaptation criteria [38–40], hence here we mention some of the approaches that focus on efficient code segmentation and cloud computing.

Majority of code offloading techniques require the developers to manually annotate the functions required to execute on another device [39]. However, using static code analyzers and dynamic code parsers is an alternative approach that results in better adaptivity in case of network fluctuations and increased latency [41]. Instead of using physical instances, ThinkAir [42] and COMET [43] leverage virtual machines offered by IaaS cloud providers as offloading targets to boost both scalability and elasticity. The proposed combination of VMs and mobile clouds can create a powerful environment for sharing, synchronizing, and executing codes in different platforms.

1.4.3 IDENTIFICATION AND RESOURCE/SERVICE DISCOVERY

IoT has emerged as a great opportunity for industrial investigations, and is similarly pursued by research communities, but current architectures proposed for creation of IoT environments lack support for an efficient and standard way of service discovery, composition, and their integration in a scalable manner [44].

The discovery module in IoT is twofold. The first objective is to identify and locate the actual device, which can be achieved by storing and indexing metadata information about each object. The final step is to discover the target service that needs to be invoked.

Lack of an effective discovery algorithm can result in execution delays, poor user experience, and runtime failures. As discussed in Ref. [45], efficient algorithms that dynamically choose centralized or flooding strategies can help minimize the consumed energy, although other parameters such as mobility and latency should be factored in to offer a suitable solution for IoT, considering its dynamic nature. In another approach within the fog-computing context [46], available resources like network bandwidth and computational and storage-capacity metrics are converted to time resources, forming a framework that facilitates resource sharing. Different parameters like energy-consumption level, price, and availability of services need to be included in proposing solutions that aim to optimize resource sharing within a heterogeneous pool of resources.

The Semantic Web of Things (SWoT) envisions advanced resource management and service discovery for IoT by extending Semantic Web notation and blending it with IoT and Web of Things. To achieve this, resources and their metadata are defined and annotated using standard ontology-definition languages such as RDF and OWL. Additionally, search and manipulation of these metadata can be done through query languages like SPARQL. Ruta et al. [47] have adopted the SSN-XG W3C ontology to collect and annotate data from Semantic Sensor Networks (SSN); moreover, by extending the CoAP protocol (discussed in Section 1.6) and CoRE Link Format that is used for resource discovery, their proposed solution ranks resources based on partial or full request matching situations.

1.5 IoT DATA MANAGEMENT AND ANALYTICS

Although IoT is getting momentum to enable technology for creating a ubiquitous computing environment, special considerations are required to process huge amounts of data originating from, and circulating in, such a distributed and heterogeneous environment. To this extent, Big Data related procedures, such as data acquisition, filtering, transmission, and analysis have to be updated to match the requirements of the IoT data deluge.

Generally, Big Data is characterized by 3Vs, namely velocity, volume, and variety. Focusing on either an individual or a combination of these three Big Data dimensions has led to the introduction of different data-processing approaches. Batch Processing and Stream Processing are two major methods used for data analysis. Lambda Architecture [48] is an exemplary framework proposed by Nathan Marz to handle Big Data processing by focusing on multiapplication support, rather than on data-processing techniques. It has three main layers that enable the framework to support easy extensibility through extension points, scale-out capabilities, low-latency query processing, and the ability to tolerate human and system faults. From a top-down view, the first layer is called “Batch Layer” and hosts the master dataset and batch views where precomputed queries are stored. Next is the “Serving Layer,” which adds dynamic query creation and execution to the batch views by indexing and storing them. Finally, the “Speed Layer” captures and processes recent data for delay-sensitive queries.

Collecting and analyzing the data circulating in the IoT environment is where the real power of IoT resides [49]. To this end, applications utilize pattern detection and data-mining techniques to extract knowledge and make smarter decisions. One of the key limitations in using currently developed data-mining algorithms lies in the inherent centralized nature of these algorithms, which drastically affects their performance and makes them unsuitable for IoT environments that are meant to be geographically distributed and heterogeneous. Distributed anomaly-detection techniques that concurrently process multiple streams of data to detect outliers have been well-studied in the literature [50]. A comprehensive survey of data-mining research in IoT has been conducted by Tsai et al. [51] and includes details about various classifications, clustering, knowledge discovery in databases (KDD), and pattern-mining techniques. Nevertheless, new approaches like ellipsoidal neighborhood factor outlier [52] that can be efficiently implemented on constrained devices are not fully benchmarked with respect to different configurations of their host devices.

1.5.1 IoT AND THE CLOUD

Cloud computing, due to its on-demand processing and storage capabilities, can be used to analyze data generated by IoT objects in batch or stream format. A pay-as-you-go model adopted by all cloud providers has reduced the price of computing, data storage, and data analysis, creating a streamlined process for building IoT applications. With cloud’s elasticity, distributed Stream Processing Engines (SPEs) can implement important features such as fault-tolerance and autoscaling for bursty workloads.

IoT application development in clouds has been investigated in a body of research. Alam et al. [53] proposed a framework that supports sensor-data aggregation in cloud-based IoT context. The framework is SOA-based and event-driven, and defines benefits from a semantic layer that is responsible for event processing and reasoning. Similarly, Li et al. [54] proposed a Platform as a Service (PaaS) solution for deployment of IoT applications. The solution is multitenant, and users are provided with a virtually isolated service that can be customized to their IoT devices while they share the underlying cloud resources with other tenants.

Nastic et al. [55] proposed PatRICIA, a framework that provides a programming model for development of IoT applications in the cloud. PatRICIA proposes a new abstraction layer that is based on the concept of intent-based programming. Parwekar [56] discussed the importance of identity detection devices in IoT, and proposed a service layer to demonstrate how a sample tag-based acquisition service can be defined in the cloud. A simple architecture for integrating M2M platform, network, and data layers has also been proposed. Focusing on the data aspect of IoT, in our previous research we proposed an architecture based on Aneka, by adding support for data filtering, multiple simultaneous data-source selection, load balancing, and scheduling [57].

IoT applications can harness cloud services and use the available storage and computing resources to meet their scalability and compute-intensive processing demands. Most of the current design approaches for integrating cloud with IoT are based on a three-tier architecture, where the bottom layer consists of IoT devices, middle layer is the cloud provider, and top layer hosts different applications and high-level protocols. However, using this approach to design and integrate cloud computing with an IoT middleware limits the practicality and full utilization of cloud computing in scenarios where minimizing end-to-end delay is the goal. For example, in online game streaming, where perceived delay is an important factor for user satisfaction, a light and context-aware IoT middleware [58] that smartly selects the nearest Content Distribution Network (CDN) can significantly reduce the overall jitter.

1.5.2 REAL-TIME ANALYTICS IN IoT AND FOG COMPUTING

Current data-analytics approaches mainly focus on dealing with Big Data, however, processing data generated from millions of sensors and devices in real time is more challenging [59]. Proposed solutions that only utilize cloud computing as a processing or storage backbone are not scalable and cannot address the latency constraints of real-time applications. Real-time processing requirements and the increase in computational power of edge devices such as routers, switches, and access points lead to the emergence of the Edge Computing paradigm.

The Edge layer contains the devices that are in closer vicinity to the end user than the application servers, and can include smartphones, smart TVs, network routers, and so forth. Processing and storage capability of these devices can be utilized to extend the advantages of using cloud computing by creating another cloud, known as Edge Cloud, near application consumers, in order to: decrease networking delays, save processing or storage cost, perform data aggregation, and prevent sensitive data from leaving the local network [60].

Similarly, Fog Computing is a term coined by Salvatore Stolfo [61] and applies to an extension of cloud computing that aims to keep the same features of Cloud, such as networking, computation, virtualization, and storage, but also meets the requirements of applications that demand low latency, specific QoS requirements, Service Level Agreement (SLA) considerations, or any combination of these [62]. Moreover, these extensions can ease application development for mobile applications, Geo-distributed applications such as WSN, and large-scale systems used for monitoring and controlling other systems, such as surveillance camera networks [63,64]. A comparison of Cloud and Fog features is presented in Table 1.1 and Fig. 1.5 shows a general architecture for using cloud and fog computing together.

Stonebraker et al. [65] pointed out that the following requirements should be fulfilled in an efficient real-time stream processing engine (SPE):

- Data fluidity, which refers to processing data on-the-fly without the need for costly data storage
- Handling out-of-order, missing, and delayed streams
- Having a repeatable and deterministic outcome after processing a series or bag of streams
- Keeping streaming and stored data integrated by using embedded database systems
- Assuring high availability, using real-time failover and hot backup mechanisms
- Supporting autoscaling and application partitioning

Table 1.1 Cloud Versus Fog

	Fog	Cloud
Response time	Low	High
Availability	Low	High
Security level	Medium to hard	Easy to medium
Service focus	Edge devices	Network/enterprise core services
Cost for each device	Low	High
Dominant architecture	Distributed	Central/distributed
Main content generator—consumer	Smart devices—humans and devices	Humans—end devices

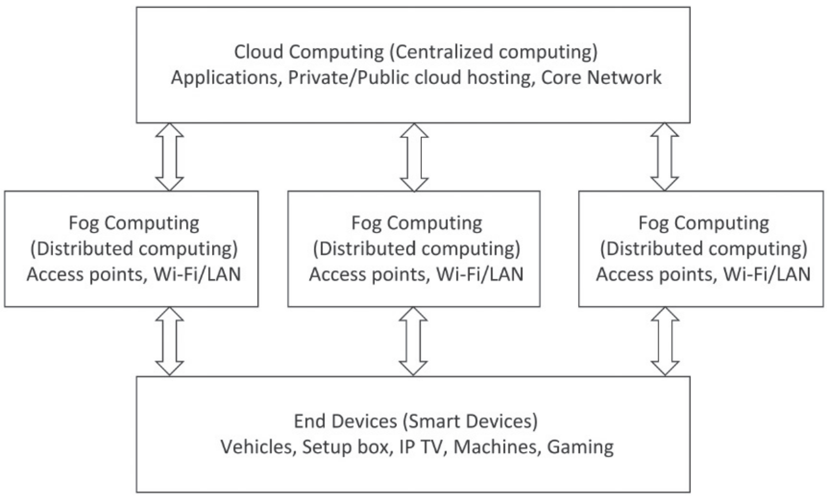


FIGURE 1.5 Typical Fog Computing Architecture

To harness the full potential of Fog computing for applications demanding real-time processing, researchers can look into necessary approaches and architectures to fulfill the aforementioned requirements.

1.6 COMMUNICATION PROTOCOLS

From the network and communication perspective, IoT can be viewed as an aggregation of different networks, including mobile networks (3G, 4G, CDMA, etc.), WLANs, WSN, and Mobile Adhoc Networks (MANET) [21].

Seamless connectivity is a key requirement for IoT. Network-communication speed, reliability, and connection durability will impact the overall IoT experience. With the emergence of high-speed mobile networks like 5G, and the higher availability of local and urban network communication protocols such

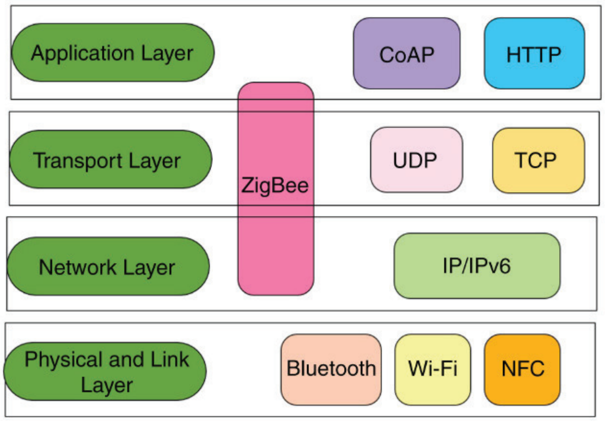


FIGURE 1.6 Use of Various Protocols in IoT Communication Layers

as Wi-Fi, Bluetooth, and WiMax, creating an interconnected network of objects seems feasible, however, dealing with different communication protocols that link these environments is still challenging.

1.6.1 NETWORK LAYER

Based on the device's specification (memory, CPU, storage, battery life), the communication means and protocols vary. However, the commonly used communication protocols and standards are listed below:

- RFID (eg, ISO 18000 series that comes with five classes and two generations, and covers both active and passive RFID tags)
- IEEE 802.11 (WLAN), IEEE 802.15.4 (ZigBee), Near Field Communication (NFC), IEEE 802.15.1 (Bluetooth)
- Low-power Wireless Personal Area Networks (6LoWPAN) standards by IEFT
- M2M protocols such as MQTT and CoAP
- IP layer technologies, such as IPv4, IPv6, etc.

More elaboration on the aforementioned network-layer communication protocols is available in Ref. [66], and a breakdown of layers in the IoT communication stack that these protocols will operate is shown in Fig. 1.6.

1.6.2 TRANSPORT AND APPLICATION LAYER

Segmentation and poor coherency level, which are results of pushes from individual companies to maximize their market share and revenue, has made developing IoT applications cumbersome. Universal applications that require one-time coding and can be executed on multiple devices are the most efficient.

Protocols in IoT can be classified into three categories:

1. general-purpose protocols like IP and SNMP that have been around for many years and are vastly used to manage, monitor, configure network devices, and establish communication links;

2. lightweight protocols such as CoAP that have been developed to meet the requirements of constrained devices with tiny hardware and limited resources;
3. device- or vendor-specific protocols and APIs that usually require a certain build environment and toolset.

Selecting the right protocols at the development phase can be challenging and complex, as factors such as future support, ease of implementation, and universal accessibility have to be considered. Additionally, thinking of other aspects that will affect the final deployment and execution, like required level of security and performance, will add to the sophistication of the protocol-selection stage. Lack of standardization for particular applications and protocols is another factor that increases the risk of poor protocol selection and strategic mistakes that are more expensive to fix in the future. In order to enhance their adoption, it is important to make sure that communication protocols are well documented; sensors and smart devices limit their usage in IoT.

Table 1.2 summarizes the characteristics of major communication protocols in IoT, while it also compares their deployment topology and environments.

M2M communication aims to enable seamless integration of physical and virtual objects into larger and geographically distributed enterprises by eliminating the need for human intervention. However, to achieve this, the enforcement of harmony and collaboration among different communication layers (physical, transport, presentation, application), as well as the approaches used by devices for message storage and passing, can be challenging [67].

The publish/subscribe model is a common way of exchanging messages in distributed environments, and, because of simplicity, it has been adopted by popular M2M communication protocols like MQTT. In dynamic scenarios, where nodes join or leave the network frequently and handoffs are required to keep the connections alive, the publish/subscribe model is efficient. This is because of using push-based notifications and maintaining queues for delayed delivery of messages.

Table 1.2 IoT Communication Protocols Comparison

Protocol Name	Transport Protocol	Messaging Model	Security	Best-Use Cases	Architecture
AMPQ	TCP	Publish/Subscribe	High-Optional	Enterprise integration	P2P
CoAP	UDP	Request/Response	Medium-Optional	Utility field	Tree
DDS	UDP	Publish/Subscribe and Request/Response	High-Optional	Military	Bus
MQTT	TCP	Publish/Subscribe and Request/Response	Medium-Optional	IoT messaging	Tree
UPnP	—	Publish/Subscribe and Request/Response	None	Consumer	P2P
XMPP	TCP	Publish/Subscribe and Request/Response	High-Compulsory	Remote management	Client server
ZeroMQ	UDP	Publish/Subscribe and Request/Response	High-Optional	CERN	P2P

On the other hand, protocols like HTTP/REST and CoAP only support the request/response model, in which a pulling mechanism is used to fetch new messages from the queue. CoAP also uses IPv6 and 6LoWPAN protocols in its network layer to handle node identification. Ongoing efforts are still being made to merge these protocols and standardize them, as to support both publish/subscribe and request/response models [68,69].

1.7 INTERNET OF THINGS APPLICATIONS

IoT promises an interconnected network of uniquely identifiable smart objects. This infrastructure creates the necessary backbone for many interesting applications that require seamless connectivity and addressability between their components. The range of IoT application domain is wide and encapsulates applications from home automation to more sophisticated environments, such as smart cities and e-government.

Industry-focused applications include logistics and transportation [70], supply-chain management [71], fleet management, aviation industry, and enterprise automation systems. Healthcare systems, smart cities and buildings, social IoT, and smart shopping are a few examples of applications that try to improve the daily life of individuals, as well as the whole society. Disaster management, environmental monitoring, smart watering, and optimizing energy consumption through smart grids and smart metering are examples of applications that focus on environment.

In a broader magnitude, Gascon and Asin [72] classified 54 different IoT applications under the following categories: smart environment, smart cities, smart metering, smart water, security and emergencies, retail, logistics, industrial control, smart agriculture, smart animal farming, domestic and home automation, and eHealth. For further reference, Kim et al. [73] have surveyed and classified research about IoT applications based on application domain and target user-groups.

In this section we present categorization of enterprise IoT applications based on their usage domain. These applications usually fall into the following three categories: (1) monitoring and actuating, (2) business process and data analysis, and (3) information gathering and collaborative consumption. The rest of this section is dedicated to characteristics and requirements of each category.

1.7.1 MONITORING AND ACTUATING

Monitoring devices via APIs can be helpful in multiple domains. The APIs can report power usage, equipment performance, and sensor status, and they can perform actions upon sending predefined commands. Real-time applications can utilize these features to report current system status, whereas managers and developers have the option to freely call these APIs without the need for physically accessing the devices. Smart metering, and in a more distributed form, smart grids, can help in identifying production or performance defects via application of anomaly detection on the collected data, and thus increase the productivity. Likewise, incorporating IoT into buildings, or even in the construction process [74], helps to move toward green solutions, save energy, and, consequently, minimize operation cost.

Another area that has been under focus by researchers is applications targeting smart homes that mainly target energy-saving and monitoring. Home monitoring and control frameworks like the ones developed by Verizon [75] and Boss support different communication protocols (Wi-Fi, Bluetooth, etc.) to create an interconnected network of objects that can control desired parameters and change configurations based on the user's settings.

1.7.2 BUSINESS PROCESS AND DATA ANALYSIS

Riggins et al. [76] categorized the level of IoT adoption through Big Data analytics usage to the following categories:

- *Society level*, where IoT mainly influences and improves government services by reducing cost and increasing government transparency and accountability
- *Industry level*, in which manufacturing, emergency services, retailing, and education have been studied as examples
- *Organizational level*, in which IoT can bring the same type of benefits as those mentioned in society level
- *Individual level*, where daily life improvements, individual efficiency, and productivity growth are marked as IoT benefits

The ability to capture and store vast amounts of individual data has brought opportunities to healthcare applications. Patients' data can be captured more frequently, using wearable technologies such as smart watches, and can be published over the Internet. Later, data mining and machine-learning algorithms are used to extract knowledge and patterns from the raw data and archive these records for future reference. Healthsense eNeighbor developed by Humana is an example of a remote controlling system that uses sensors deployed in houses to measure frequent daily activities and heath parameters of occupants. The collected data is then analyzed to forecast plausible risks and produce alerts to prevent incidents [77]. Privacy and security challenges are two main barriers that refrain people and industries from embracing IoT in the healthcare domain.

1.7.3 INFORMATION GATHERING AND COLLABORATIVE CONSUMPTION

Social Internet of Things (SIoT) is where IoT meets social networks, and, to be more precise, it promises to link objects around us with our social media and daily interaction with other people, making them look smarter and more intractable. SIoT concept, motivated by famous social media like Facebook and Twitter, has the potential to affect many people's lifestyles. For example, a social network is helpful for the evaluation of trust of crowds involved in an IoT process. Another advantage is using the humans and their relationships, communities, and interactions for effective discovery of IoT services and objects [78].

Table 1.3 contains a list of past and present open-source projects regarding IoT development and its applications.

1.8 SECURITY

As adoption of IoT continues to grow, attackers and malicious users are shifting their target from servers to end devices. There are several reasons for this. First, in terms of physical accessibility, smart devices and sensors are far less protected than servers, and having physical access to a device gives the attackers an advantage to penetrate with less hassle. Second, the number of devices that can be compromised are far more than the number of servers. Moreover, since devices are closer to the users, security leads to leaking of valuable information and has catastrophic consequences. Finally, due to heterogeneity and the distributed nature of IoT, the patching process is more consuming, thus opening the door for attackers [2,79].

Table 1.3 List of IoT-Related Projects

Name of Project/Product	Area of Focus
Tiny OS	Operating System
Contiki	Operating System
Mantis	Operating System
Nano-RK	Operating System
LiteOS	Operating System
FreeRTOS	Operating System
RIOT	Operating System
Wit.AI	Natural Language
Node-RED	Visual Programming Toolkit
NetLab	Visual Programming Toolkit
SensorML	Modeling and Encoding
Extended Environments Markup Language (EEML)	Modeling and Encoding
ProSyst	Middleware
MundoCore	Middleware
Gaia	Middleware
Ubiware	Middleware
SensorWare	Middleware
SensorBus	Middleware
OpenIoT	Middleware and development platform
Koneki	M2M Development Toolkit
MIHINI	M2M Development Toolkit

In an IoT environment, resource constraints are the key barrier for implementing standard security mechanisms in embedded devices. Furthermore, wireless communication used by the majority of sensor networks is more vulnerable to eavesdropping and man-in-the-middle (proxy) attacks.

Cryptographic algorithms need considerable bandwidth and energy to provide end-to-end protection against attacks on confidentiality and authenticity. Solutions have been proposed in RFID [80,81] and WSN [82] context to overcome aforementioned issues by considering light cryptographic techniques. With regard to constrained devices, symmetric cryptography is applied more often, as it requires fewer resources; however, public key cryptography in the RFID context has also been investigated [83].

WSN with RFID tags and their corresponding readers were the first infrastructure for building IoT environments, and, even now, many IoT applications in logistics, fleet management, controlled farming, and smart cities rely on these technologies. Nevertheless, these systems are not secure enough and are vulnerable to various attacks from different layers. A survey by Borgohain et al. [84] investigates these attacks, but less attention is given to solutions and counter-attack practices.

1.9 IDENTITY MANAGEMENT AND AUTHENTICATION

When talking about billions of connected devices, methods for identifying objects and setting their access level play an important role in the whole ecosystem. Consumers, data sources, and service providers are essential parts of IoT; identity management and authentication methods applied to securely connect these entities affect both the amount of time required to establish trust and the degree of confidence [4]. IoT's inherent features, such as dynamism and heterogeneity, require specific consideration when defining security mechanisms. For instance, in Vehicular Networks (VANETs), cars regularly enter and leave the network due to their movement speed; thus, not only do cars need to interact and exchange data with access points and sensors along the road, but they also need to communicate with each other and form a collaborative network.

Devices or objects in IoT have to be uniquely identified. There are various mechanisms, such as ucode, which generate 128-bit codes and can be used in active and passive RFID tags, and also Electric Product Code (EPC), which creates unique identifiers using Uniform Resource Identifier (URI) codes [85,86]. Being able to globally and uniquely identify and locate objects decreases the complexity of expanding the local environment and linking it with the global markets [84].

It is common for IoT sensors and smart devices to share the same geographical coordinates and even fall into same type or group, hence identity management can be delegated to local identity management systems. In such environments, local identity management systems can enforce and monitor access-control policies and establish trust negotiations with external partners. Zhou et al. [87] investigated security requirements for multimedia applications in IoT and proposed an architecture that supports traffic analysis and scheduling, key management, watermarking, and authentication. Context-aware pairing of devices and automatic authentication is another important requirement for dynamic environments like IoT. Solutions that implement a zero-interaction approach [88] to create simpler yet more secure procedures for creating a ubiquitous network of connected devices can considerably impact IoT and its adoption.

1.10 PRIVACY

According to the report published by IDC and EMC on Dec. 2012 [89], the size of the digital universe containing all created, replicated, and consumed digital data will be roughly doubled every 2 years, hence, forecasting its size to be 40,000 exabytes by 2020, compared to 2,837 exabytes for 2012. Additionally, sourced from statisticbrain.com, the average cost of storage for hard disks has dropped from $437,500 per gigabyte in 1980 to $0.05 per gigabyte in 2013. These statistics show the importance of data and the fact that it is easy and cheap to keep the user's data for a long time and follow the guidelines for harvesting as much data as possible and using it when required.

Data generation rate has drastically increased in recent years, and consequently concerns about secure data storage and access mechanisms has be taken more seriously. With sensors capable of sensing different parameters, such as users' location, heartbeat, and motion, data privacy will remain a hot topic to ensure users have control over the data they share and the people who have access to these data.

In distributed environments like IoT, preserving privacy can be achieved by either following a centralized approach or by having each entity manage its own inbound/outbound data, a technique known as privacy-by-design [84]. Considering the latter approach, since each entity can access only chunks

Table 1.4 IoT Standards

Organization Name	Outcome
Internet of Things Global Standards Initiative (IoT-GSI)	JCA-IoT
Open Source Internet of Things (OSIoT)	Open Horizontal Platform
IEEE	802.15.4 standards, developing a reference architecture
Internet Engineering Task Force (IETF)	Constrained RESTful Environments (CoRE), 6LOWPAN, Routing Over Low power and Lossy networks (ROLL), IPv6
The World Wide Web Consortium (W3C)	Semantic Sensor Net Ontology, Web Socket, Web of Things
XMPP Standards Foundation	XMPP
Eclipse Foundation	Paho project, Ponte project, Kura, Mihini/M3DA, Concierge
Organization for the Advancement of Structured Information Standards	MQTT, AMPQ

of data, distributed privacy- preserving algorithms have been developed to handle data scattering and their corresponding privacy tags [90]. Privacy-enhancing technologies [91,92] are good candidates for protecting collaborative protocols. In addition, to protect sensitive data, rapid deployable enterprise solutions that leverage containers on top of virtual machines can be used [93].

1.11 STANDARDIZATION AND REGULATORY LIMITATIONS

Standardization and the limitation caused by regulatory policies have challenged the growth and adoption rate of IoT and can be potential barriers in embracing the technology. Defining and broadcasting standards will ease the burden of joining IoT environments for new users and providers. Additionally, interoperability among different components, service providers, and even end users will be greatly influenced in a positive way, if pervasive standards are introduced and employed in IoT [94].

Even though more organizations and industries make themselves ready to embrace and incorporate IoT, increase in IoT growth rate will cause difficulties for standardization. Strict regulations about accessing radio frequency levels, creating a sufficient level of interoperability among different devices, authentication, identification, authorization, and communication protocols are all open challenges facing IoT standardization. Table 1.4 contains a list of organizations that have worked toward standardizing technologies either used within IoT context or those specifically created for IoT.

1.12 CONCLUSIONS

IoT has emerged as a new paradigm aimed at providing solutions for integration, communication, data consumption, and analysis of smart devices. To this end, connectivity, interoperability, and integration are inevitable parts of IoT communication systems. Whereas IoT, due to its highly distributed and heterogeneous nature, is comprised of many different components and aspects, providing solutions to integrate this environment and hide its complexity from the user side is inevitable. Novel approaches that utilize SOA architecture and API definition languages to service exposition, discovery, and composition will have a huge impact in adoption and proliferation of the future IoT vision.

In this chapter, different building blocks of IoT, such as sensors and smart devices, M2M communication, and the role of humans in future IoT scenarios are elaborated upon and investigated. Many challenges ranging from communication requirements to middleware development still remain open and need further investigation. We have highlighted these shortcomings, have provided typical solutions, and have drawn guidelines for future research in this area.

REFERENCES

[1] Hafner K, Lyon M. Where wizards stay up late: the origins of the Internet. New York: Simon and Schuster; 1998.

[2] Atzori L, Iera A, Morabito G. The internet of things: a survey. Comput Netw 2010;54(15):2787–805.

[3] Li S, Xu LD, Zhao S. The internet of things: a survey. Inform Syst Front 2014;17(2):243–59.

[4] Perera C, Zaslavsky A, Christen P, Georgakopoulos D. Context aware computing for the internet of things: a survey. Commun Surv Tutorials IEEE 2014;16(1):414–54.

[5] Miorandi D, Sicari S, De Pellegrini F, Chlamtac I. Internet of things: vision, applications and research challenges. Ad Hoc Netw 2012;10(7):1497–516.

[6] Ashton K. That 'internet of things' thing. RFiD J 2009;22(7):97–114.

[7] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gener Comput Syst 2013;29(7):1645–60.

[8] L.R. LLC. An introduction to the Internet of Things (IoT). http://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf; 2013.

[9] Vilajosana X, et al. OpenMote: Open-source prototyping platform for the industrial IoT. In: Ad hoc networks. Springer International Publishing; 2015. p. 211–222.

[10] Da Xu L, He W, Li S. Internet of Things in industries: a survey. Ind Inform IEEE Trans 2014;10(4):2233–43.

[11] M.R. Group. Internet of Things (IoT) & M2M communication market—advanced technologies, future cities & adoption trends, roadmaps & worldwide forecasts 2012–2017. http://www.prnewswire.com/news-releases/internet-of-things-iot--machine-to-machine-m2m-communication-market---advanced-technologies-future-cities--adoption-trends-roadmaps--worldwide-forecasts-2012---2017-216448061.html; 2012.

[12] RnRMarketResearch. Internet of Things technology and application market by communication technology (ZigBee, Z-Wave, Bluetooth, Wi-Fi, NFC, RFID), application vertical (building automation, consumer, wearable electronics, industrial, automotive & transportation, agriculture) & geography—global trends & forecasts to 2014–2020. http://www.marketsandmarkets.com/Market-Reports/iot-application-technology-market-258239167.html; 2014.

[13] BI Intelligence. Research for the digital age. https://intelligence.businessinsider.com/; 2015.

[14] Wang F, Hu L, Zhou J, Zhao K. A survey from the perspective of evolutionary process in the Internet of Things. Int J Distrib Sens Netw 2015;2015:9.

[15] Ortutay B. IBM to invest $3-billion in new 'Internet of Things' unit. http://www.reuters.com/article/us-ibm-investment-idUSKBN0MR0BS20150331; 2015.

[16] Yu E. Singapore unveils plan in push to become smart nation. http://www.zdnet.com/article/singapore-unveils-plan-in-push-to-become-smart-nation/; 2014.

[17] Dastjerdi AV, Sharifi M, Buyya R. On application of ontology and consensus theory to human-centric IoT: an emergency management case study. In: Proceedings of the eighth IEEE international conference on Internet of Things (iThings 2015, IEEE CS Press, USA), Sydney, Australia, Dec. 11–13, 2015.

[18] Ryan A. India to be the largest Internet of Things market by 2020. http://www.metering.com/india-to-be-the-largest-internet-of-things-market-by-2020/; 2015.
[19] IoT-A, IoT-A Internet of Things—architecture. http://www.iot-a.eu/; 2012.
[20] WSO2, A reference architecture for the Internet of Things. http://wso2.com/wso2_resources/wso2_whitepaper_a-reference-architecture-for-the-internet-of-things.pdf; 2014.
[21] Castellani A, Bui N, Casari P, Rossi M, Shelby Z, Zorzi M. Architecture and protocols for the internet of things: a case study. In: Eighth IEEE international conference on pervasive computing and communications workshops (PERCOM workshops); 2010. p. 678–683.
[22] Ishaq I, Hoebeke J, Rossey J, De Poorter E, Moerman I, Demeester P. Enabling the web of things: facilitating deployment, discovery and resource access to IoT objects using embedded web services. Int J Web Grid Serv 2014;10(2):218–43.
[23] Guinard D, Trifa V, Karnouskos S, Spiess P, Savio D. Interacting with the SOA-based Internet of Things: discovery, query, selection, and on-demand provisioning of web services. IEEE Trans Serv Comput 2010;3(3):223–35.
[24] Stirbu V. Towards a restful plug and play experience in the web of things, In: IEEE international conference on semantic computing; 2008. p. 512–517.
[25] Guinard D, Trifa V, Mattern F, Wilde E. From the internet of things to the web of things: resource-oriented architecture and best practices. Architecting the Internet of Things. Berlin Heidelberg: Springer; 2011. pp. 97–129.
[26] Li B, Yu J. Research and application on the smart home based on component technologies and Internet of Things. Procedia Eng 2011;15:2087–92.
[27] Su K, Li J, Fu H. Smart city and the applications. In: International conference on electronics, communications and control (ICECC); 2011. p. 1028–1031.
[28] Dohr A, Modre-Opsrian R, Drobics M, Hayn D, Schreier G. The internet of things for ambient assisted living. In: Seventh international conference on information technology: new generations (ITNG); 2010. p. 804–809.
[29] Valipour MH, Amirzafari B, Maleki KN, Daneshpour N. A brief survey of software architecture concepts and service oriented architecture. In: Second IEEE international conference on computer science and information technology (ICCSIT 2009); 2009. p. 34–38.
[30] Datta SK, Bonnet C, Nikaein N. An iot gateway centric architecture to provide novel m2m services. In: IEEE world forum on Internet of Things (WF-IoT); 2014. p. 514–519.
[31] Khodadadi F, Dastjerdi AV, Buyya R. Simurgh: a framework for effective discovery, programming, and integration of services exposed in IoT. In: International conference on recent advances in Internet of Things (RIoT); 2015. p. 1–6.
[32] Elmangoush A, Magedanz T, Blotny A, Blum N. Design of RESTful APIs for M2M services. In: Sixteenth international conference on intelligence in next generation networks (ICIN); 2012. p. 50–56.
[33] Manzalini A, Minerva R, Moiso C. If the Web is the platform, then what is the SDP? In: Thirteenth international conference on intelligence in next generation networks (ICIN 2009); 2009. p. 1–6.
[34] Gu Z, Zhao Q. A state-of-the-art survey on real-time issues in embedded systems virtualization; 2012.
[35] Soltesz S, Pötzl H, Fiuczynski ME, Bavier A, Peterson L. Container-based operating system virtualization: a scalable, high-performance alternative to hypervisors. ACM SIGOPS Oper Syst Rev 2007;41(3):275–87.
[36] Andrus J, Dall C, Hof AV, Laadan O, Nieh J. Cells: a virtual mobile smartphone architecture. In: Proceedings of the twenty-third ACM symposium on operating systems principles; 2011. p. 173–187.
[37] Zhou B, Dastjerdi AV, Calheiros RN, Srirama SN, Buyya R. A context sensitive offloading scheme for mobile cloud computing service. In: Proceedings of the eighth IEEE international conference on cloud computing (Cloud 2015, IEEE CS Press, USA), New York, USA, June 27–July 2, 2015.
[38] Enzai M, Idawati N, Tang M, A taxonomy of computation offloading in mobile cloud computing. In: Second IEEE international conference on mobile cloud computing, services, and engineering (MobileCloud); 2014, p. 19–28.

[39] Cuervo E, Balasubramanian A, Cho D, Wolman A, Saroiu S, Chandra R, Bahl P. MAUI: making smartphones last longer with code offload. In: Proceedings of the eighth international conference on mobile systems, applications, and services; 2010. p. 49–62.
[40] Satyanarayanan M, Bahl P, Caceres R, Davies N. The case for vm-based cloudlets in mobile computing. Pervasive Comput IEEE 2009;8(4):14–23.
[41] Chun B-G, Ihm S, Maniatis P, Naik M, Patti A. Clonecloud: elastic execution between mobile device and cloud. In: Proceedings of the sixth conference on computer systems; 2011, p. 301–314.
[42] Kosta S, Aucinas A, Hui P, Mortier R, Zhang X. Thinkair: dynamic resource allocation and parallel execution in the cloud for mobile code offloading. In: INFOCOM, 2012 proceedings IEEE; 2012. p. 945–953.
[43] Gordon MS, Jamshidi DA, Mahlke SA, Mao ZM, and Chen X. COMET: code offload by migrating execution transparently. In: OSDI; 2012. p. 93–106.
[44] Wei Q, Jin Z. Service discovery for internet of things: a context-awareness perspective. In: Proceedings of the fourth Asia-Pacific symposium on Internetware; 2012. p. 25.
[45] Liu W, Nishio T, Shinkuma R, Takahashi T. Adaptive resource discovery in mobile cloud computing. Comput Commun 2014;50:119–29.
[46] Nishio T, Shinkuma R, Takahashi T, and Mandayam NB. Service-oriented heterogeneous resource sharing for optimizing service latency in mobile cloud. In: Proceedings of the first international workshop on mobile cloud computing & networking; 2013. p. 19–26.
[47] Ruta M, Scioscia F, Pinto A, Di Sciascio E, Gramegna F, Ieva S, Loseto G. Resource annotation, dissemination and discovery in the Semantic Web of Things: a CoAP-based framework. In: Green computing and communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE international conference on Cyber, Physical and Social Computing; 2013. p. 527–534.
[48] Nathan Marz JW. Big Data: principles and best practices of scalable realtime data systems. Greenwich, CT: Manning Publications; 2013.
[49] Misra P, Simmhan Y, Warrior J. Towards a practical architecture for the next generation Internet of Things, arXiv Prepr. arXiv1502.00797; 2015.
[50] Moshtaghi M, Bezdek JC, Havens TC, Leckie C, Karunasekera S, Rajasegarar S, Palaniswami M. Streaming analysis in wireless sensor networks. Wirel Commun Mob Comput 2014;14(9):905–21.
[51] Tsai C-W, Lai C-F, Chiang M-C, Yang LT. Data mining for internet of things: a survey. Commun Surv Tutorials IEEE 2014;16(1):77–97.
[52] Rajasegarar S, Gluhak A, Ali Imran M, Nati M, Moshtaghi M, Leckie C, Palaniswami M. Ellipsoidal neighbourhood outlier factor for distributed anomaly detection in resource constrained networks. Pattern Recognit 2014;47(9):2867–79.
[53] Alam S, Chowdhury MMR, Noll J. SenaaS: an event-driven sensor virtualization approach for Internet of Things cloud. In: Proceedings of the 2010 IEEE international conference on networked embedded systems for enterprise applications (NESEA); 2010.
[54] Li F, Vogler M, Claessens M, Dustdar S. Efficient and scalable IoT service delivery on cloud. In: Proceedings of the sixth international conference on cloud computing (CLOUD); 2013.
[55] Nastic S, Sehic S, Vogler M, Truong H-L, Dustdar S. PatRICIA— a novel programming model for IoT applications on cloud platforms. In: Proceedings of the sixth international conference on service-oriented computing and applications (SOCA); 2013.
[56] Parwekar P. From Internet of Things towards cloud of things. In: Second international conference on computer and communication technology (ICCCT); 2011, p. 329–333.
[57] Khodadadi F, Calheiros RN, Buyya R. A data-centric framework for development and deployment of Internet of Things applications in clouds. In: IEEE tenth international conference on intelligent sensors, sensor networks and information processing (ISSNIP); 2015. p. 1–6.
[58] Medvedev A, Zaslavsky A, Grudinin V, Khoruzhnikov S. Citywatcher: annotating and searching video data streams for smart cities applications. Internet of Things, smart spaces, and next generation networks and systems. Springer International Publishing; 2014. pp. 144–155.

[59] Belli L, Cirani S, Ferrari G, Melegari L, Picone M. A graph-based cloud architecture for big stream realtime applications in the internet of things. Advances in service-oriented and cloud computing. Springer International Publishing; 2014. pp. 91–105.
[60] Bonomi F, Milito R, Natarajan P, Zhu J. Fog computing: a platform for internet of things and analytics. Big Data and Internet of Things: a roadmap for smart environments. Springer International Publishing; 2014. pp. 169–186.
[61] Shachtman N. Feds look to fight leaks with fog of disinformation; 2012.
[62] Bonomi F, Milito R, Zhu J, Addepalli S. Fog computing and its role in the internet of things In: Proceedings of the first edition of the MCC workshop on mobile cloud computing; 2012. p. 13–16.
[63] Vaquero LM, Rodero-Merino L. Finding your way in the fog: towards a comprehensive definition of fog computing. ACM SIGCOMM Comput Commun Rev 2014;44(5):27–32.
[64] Aazam M, Khan I, Alsaffar AA, Huh E-N. Cloud of Things: integrating Internet of Things and cloud computing and the issues involved. In: Eleventh international Bhurban conference on applied sciences and technology (IBCAST); 2014. p. 414–419.
[65] Stonebraker M, Çetintemel U, Zdonik S. The 8 requirements of real-time stream processing. ACM SIGMOD Rec 2005;34(4):42–7.
[66] Rimal BP, Choi E, Lumb I. A taxonomy and survey of cloud computing systems. In: Fifth international joint conference on INC, IMS and IDC. NCM'09; 2009. p. 44–51.
[67] Elmangoush A, Steinke R, Magedanz T, Corici AA, Bourreau A, Al-Hezmi A. Application-derived communication protocol selection in M2M platforms for smart cities. In: Eighteenth international conference on intelligence in next generation networks (ICIN); 2015. p. 76–82.
[68] Teklemariam GK, Hoebeke J, Moerman I, Demeester P. Facilitating the creation of IoT applications through conditional observations in CoAP. EURASIP J Wirel Commun Netw 2013;2013(1):1–19.
[69] Kovatsch M, Lanter M, Shelby Z. Californium: scalable cloud services for the internet of things with CoAP. In: Proceedings of the fourth international conference on the Internet of Things (IoT 2014); 2014.
[70] Yuqiang C, Jianlan G, Xuanzi H. The research of Internet of Things supporting technologies which face the logistics industry. In: International conference on computational intelligence and security (CIS); 2010. p. 659–663.
[71] Chaves LWF, Decker C. A survey on organic smart labels for the internet-of-things. In: Seventh international conference on networked sensing systems (INSS); 2010. p. 161–164.
[72] Gascon D, Asin A. 50 sensor applications for a smarter world. http://www.libelium.com/top_50_iot_sensor_applications_ranking; 2015.
[73] Kim S, Kim S. A multi-criteria approach toward discovering killer IoT application in Korea. Technol Forecast Soc 2015;102:143–55.
[74] Moreno M, Úbeda B, Skarmeta AF, Zamora MA. How can we tackle energy efficiency in IoT based smart buildings? Sensors 2014;14(6):9582–614.
[75] Lee I, Lee K. The Internet of Things (IoT): applications, investments, and challenges for enterprises. Bus Horiz 2015;58(4):431–40.
[76] Riggins FJ, Wamba SF. Research directions on the adoption, usage, and impact of the Internet of Things through the use of Big Data analytics. In: Fourty-eighth Hawaii international conference on system sciences (HICSS); 2015. p. 1531–1540.
[77] Fox GC, Kamburugamuve S, Hartman RD. Architecture and measured characteristics of a cloud based internet of things. In: International conference on collaboration technologies and systems (CTS); 2012. p. 6–12.
[78] Atzori Luigi, et al. The social internet of things (SIoT)—when social networks meet the internet of things: concept, architecture and network characterization. Comput Netw 2012;56(16):3594–608.
[79] Babar S, Mahalle P, Stango A, Prasad N, Prasad R. Proposed security model and threat taxonomy for the internet of things (IoT). Recent trends in network security and applications. Springer Berlin Heidelberg; 2010. pp. 420–429.

[80] Poschmann A, Leander G, Schramm K, Paar C. New light-weight crypto algorithms for RFID. In: IEEE international symposium on circuits and systems (ISCAS 2007); 2007, p. 1843–1846.
[81] Fu L, Shen X, Zhu L, Wang J. A low-cost UHF RFID tag chip with AES cryptography engine. Secur Commun Netw 2014;7(2):365–75.
[82] Ebrahim M, Chong CW. Secure force: a low-complexity cryptographic algorithm for Wireless Sensor Network (WSN). In: IEEE international conference on control system, computing and engineering (ICCSCE); 2013. p. 557–562.
[83] Arbit A, Livne Y, Oren Y, Wool A. Implementing public-key cryptography on passive RFID tags is practical. Int J Inf Secur 2014;14(1):85–99.
[84] Borgohain T, Kumar U, Sanyal S. Survey of security and privacy issues of Internet of Things. arXiv Prepr. arXiv1501.02211; 2015.
[85] Mainetti L, Patrono L, Vilei A. Evolution of wireless sensor networks towards the internet of things: a survey. In: Nineteenth international conference on software, telecommunications and computer networks (SoftCOM); 2011. p. 1–6.
[86] Zorzi M, Gluhak A, Lange S, Bassi A. From today's intranet of things to a future internet of things: a wireless- and mobility-related view. Wirel Commun IEEE 2010;17(6):44–51.
[87] Zhou L, Chao H-C. Multimedia traffic security architecture for the internet of things. IEEE Netw 2011;25(3):35–40.
[88] Miettinen M, Asokan N, Nguyen TD, Sadeghi A-R, Sobhani M. Context-based zero-interaction pairing and key evolution for advanced personal devices. In: Proceedings of the 2014 ACM SIGSAC conference on computer and communications security; 2014. p. 880–891.
[89] McLellan C. Storage in 2014: an overview. http://www.zdnet.com/article/storage-in-2014-an-overview/; 2014.
[90] Aggarwal CC, Philip SY. A general survey of privacy-preserving data mining models and algorithms. USA: Springer; 2008.
[91] Argyrakis J, Gritzalis S, Kioulafas C. Privacy enhancing technologies: a review. Electronic government. Berlin Heidelberg: Springer; 2003. pp. 282–287.
[92] Oleshchuk V. Internet of things and privacy preserving technologies. In: First International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology; 2009. p. 336–340.
[93] Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed internet of things. Comput Netw 2013;57(10):2266–79.
[94] Jiang H, Zhao S, Zhang Y, Chen Y. The cooperative effect between technology standardization and industrial technology innovation based on Newtonian mechanics. Inf Technol Manag 2012;13(4):251–62.

Internet of Things

Principles and Paradigms

Edited by **Rajkumar Buyya & Amir Vahid Dastjerdi**

Describes the fundamental concepts, algorithms, tools, technologies, and best practices that enable Internet of Things applications and architectures.

The Internet of Things (IoT) paradigm makes "things" such as medical devices, fridge, smart meters, cameras, and road traffic sensors part of the Internet. It is expected that trillions of IoT devices will be deployed by 2025 for applications such as smart cities and digital agriculture. This new paradigm opens the doors to new innovations and interactions between people and things that will enhance the quality of life and utilization of scarce resources.

Internet of Things: Principles and Paradigms captures the state-of-the-art research in Internet of Things, its applications, architectures, and technologies. The book identifies potential future directions and technologies that provide insights into numerous scientific, business, and consumer applications.

Internet of Things: Principles and Paradigms addresses numerous challenges and develops the conceptual and technological solutions for tackling them. The challenges include the development of scalable architecture, lightweight application development platforms, autonomic management, and as well as the privacy and ethical issues around data sensing, sharing, and processing.

Rajkumar Buyya is a Fellow of IEEE, Professor of Computer Science and Software Engineering, and Director of the Cloud Computing and Distributed Systems (CLOUDS) Laboratory at the University of Melbourne, Australia. He is also serving as the founding CEO of Manjrasoft, a spin-off company of the University, commercializing its innovations in Cloud Computing. He has authored over 500 publications and 6 text books including Mastering Cloud Computing published by McGraw Hill, China Machine Press, and Morgan Kaufmann for Indian, Chinese, and international markets, respectively. He is currently serving as Co-Editor-in-Chief of ***Journal of Software: Practice and Experience***. For further information, please visit www.buyya.com

Amir Vahid Dastjerdi is a research fellow with the Cloud Computing and Distributed Systems (CLOUDS) laboratory at the University of Melbourne. He received his PhD in computer science from the University of Melbourne and his areas of interest include Internet of Things, Big Data, and Cloud Computing.

Data Science

ISBN 978-0-12-805395-9

9 780128 053959

MORGAN KAUFMANN PUBLISHERS

AN IMPRINT OF ELSEVIER

elsevier.com