Chapter 61
Security in Cloud of Things (CoT)

Bashar Alohali
Liverpool John Moores University, UK

ABSTRACT

With IoT era, development raises several significant research questions in terms of system architecture, design and improvement. For example; the requirement of virtual resource utilization and storage capacity necessitates making IoT applications smarter; therefore, integrate the IoT concept with cloud computing will play an important role. This is crucial because of very large amounts of data that IoT is expected to generate. The Cloud of Things (CoT) is used to connect heterogeneous physical things to the virtual domain of the cloud. Despite its numerous advantages, there are many research challenges with utilization of CoT that needs additional consideration. These include high complexity, efficiency, improving reliability, and security. This chapter introduces CoT, its features, the applications that use CoT. CoT, like all other networked functions, is vulnerable to security attacks. The security risks for CoT are listed and described. The security requirements for CoT are identified and solutions are proposed to address the various attacks on CoT and its components.

INTRODUCTION

Through the years, the era of information technology and pervasiveness of digital technologies have showed an exponential growth. The rising number of technological improvements offers a wealth of new services. Recently, Internet of Things (IoT) has attracted attention since it involves several applications, including smart grid, control systems, remote healthcare, smart mobility, traffic flow management and so on. In addition, it is expected to grow in terms of its deployment as well as its applicability in various application areas. The term IoT was coined by Kevin Ashton in 1999, which meant any entity that has a chip placed inside it or addressable on a network with an IP-address and can connect to wireless or wired network infrastructure (Gratton, 2013). These are everyday objects with ubiquitous connectivity and communicating and operating constantly. The use of IoT leads to a smart world with ubiquitous computing and provides services that enables remote access and intelligent functionality (Chaouchi, 2013). IoT enables real-time analysis of data flows that could improve efficiency, reliability and economy

DOI: 10.4018/978-1-5225-8176-5.ch061

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

of systems. For example, connecting all appliances in the smart house can save electricity by efficient monitoring. Thus, IoT provides convenience in day-to-day living and makes an intelligent use of resources in a home (Parwekar, 2011).

CoT represents an important extension of IoT. CoT refers to the virtualization of IoT infrastructure to provide monitoring and control. IoT deployments typically generate large amounts of data that require computing as well as storage. A cloud infrastructure that can provide these resources can effectively offload the computing and storage requirements within the IoT network to the cloud. An added benefit is the ability to virtualize the underlying IoT infrastructure to provide monitoring and control from a single point. An application using IoT could therefore become a smart application. A CoT connects heterogeneous appliances to the virtual cloud domain. Both tangible and intangible objects (home appliances, sensor-based and network-enabled) and surrounding people can be integrated on a network or into a set of networks (Sun, Zhang, & Li, 2012).

CoT suggests a model consisting of a set of services (or commodities) that are delivered just like the traditional commodities. In other words, CoT can provide a virtual infrastructure which can integrate analytic tools, monitoring devices and visualization platforms (Parwekar, 2011). Moreover, CoT is a recent technological breakthrough that can enable end-to-end service provisioning for users and businesses to directly access applications on demand from anywhere, anytime (Sun et al., 2012).The emerging CoT services will enable a new generation and intelligent use of a collection of applications that will be fed with real time and analysis.

CoT, as a connected universe of things, can become a tangible reality in the future. Connected devices and things, ranging from sensors to public transport, will send huge of data that should be effectively managed and processed. However, cyber-attacks on critical infrastructure, recently, have highlighted security as a major requirement for CoT. A compromise of the CoT can have drastic effects, sometimes nation-wide and on people's lives. So, a CoT infrastructure should be secure. This chapter will present an overview of some of the concepts related to CoT. After introducing CoT, it continues to present the architecture and the applications of CoT. In addition, the security requirements for the CoT are discussed and the security challenges are highlighted. Specifically, the threats to the CoT are discussed. The chapter concludes with a discussion on the existing security solutions and a mention of the open research issues.

BACKGROUND

Overview of CoT

IoT on which CoT is based, is a new IT paradigm that describes an imagined reality of trillions of things connected to each other. It is transmitting valuable data that is stored, processed and analyzed by computers to control and addresses all sorts of human activities, ranging from healthcare, road traffic, emergency management, retail, crime prevention, lighting, energy and power and/or transportation. IoT is closely linked with the concepts of "smart city", "ubiquitous computing" (Vasseur & Dunkels, 2010), and other paradigms that describe new technological reality in which sensors and microcontrollers are embedded in various things and integrated into human living. This results in increased comfort and security. IoT unites several individual technologies, including machine-to-machine (M2M), supervisory control and data acquisition (SCADA), a system designed for industrial remote monitoring & control of equipment, wireless sensor networks (WSN) and radio-frequency identification (RFID). All these systems and

23 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/security-in-cloud-of-things-cot/224628

Related Content

Review on 5G Millimeter-Wave Antennas: MIMO Antennas
Mohamed Ismail Ahmed, Hala Mohammed Elsayed Mohammed Marzoukand Abdelhamid A. Shaalan (2020). *Fundamental and Supportive Technologies for 5G Mobile Networks (pp. 44-76).*
www.irma-international.org/chapter/review-on-5g-millimeter-wave-antennas/241972

Predictive Modeling for Imbalanced Big Data in SAS Enterprise Miner and R
Son Nguyen, Alan Olinsky, John Quinnand Phyllis Schumacher (2018). *International Journal of Fog Computing (pp. 83-108).*
www.irma-international.org/article/predictive-modeling-for-imbalanced-big-data-in-sas-enterprise-miner-and-r/210567

APT: A Practical Tunneling Architecture for Routing Scalability
Dan Jen, Michael Meisel, Daniel Massey, Lan Wang, Beichuan Zhangand Lixia Zhang (2018). *Fog Computing: Breakthroughs in Research and Practice (pp. 158-182).*
www.irma-international.org/chapter/apt/205974

Fog Computing: Applications, Concepts, and Issues
Chintan M. Bhattand C. K. Bhensdadia (2018). *Fog Computing: Breakthroughs in Research and Practice (pp. 198-207).*
www.irma-international.org/chapter/fog-computing/205976

From Theory to Practice: A Comprehensive Review of Osmotic Computing
P. Umamaheswari (2024). *Advanced Applications in Osmotic Computing (pp. 73-89).*
www.irma-international.org/chapter/from-theory-to-practice/340997