Chapter 77
Privacy in the Internet of Things

Jayashree Kanniappan
Rajalakshmi Engineering College, India

Babu Rajendiran
Rajalakshmi Engineering College, India

ABSTRACT

Internet of Things technology is rapidly gaining popularity, not only in industrial and commercial environments, but also in personal life by means of smart devices at home. The Internet of Things (IoT) spawn new businesses and make buildings, cities and transport smarter. The IoT allows for ubiquitous data collection or tracking, but these useful features are also examples of privacy threats that are already limiting the success of the IoT vision when not implemented correctly. Privacy should be protected in the device, in storage, during communication, and at processing. The privacy of users and their data protection have been identified as one of the important challenges that need to be addressed in the IoT. The chapter presents the IoT technology, the various applications, and privacy issues. Various other issues such as security and performance are also addressed.

INTRODUCTION

The Internet of Things (IoT) paradigm envisions the pervasive interconnection and cooperation of smart things over the Internet infrastructure. Realization of IoT paradigm depends on integration of Radio Frequency Identification (RFID) systems for tracing and addressing items non-contact and automatically, Wireless Sensor Networks (WSN) for integrating distributed information collection, transmission and processing, Machine to Machine systems and intelligent signal processing and nanometer technologies (Dey et al., 2015). The IoT encompasses a set of technologies that enable a wide range of appliances, devices, and objects to interact and communicate among themselves using networking technologies (Tarouco et al., 2012).

The IoT enables many new services for people's everyday lives, spawns new businesses and makes buildings, cities and transportation systems smarter. It is based on intelligent and self-configuring nodes interconnected in a dynamic and global network infrastructure that relies on sensory, communication,

DOI: 10.4018/978-1-5225-7113-1.ch077

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

networking, and information processing technologies (Ziegeldorf et al., 2014). The IoT is generally characterized by small things with limited storage and processing capacity, and issues regarding reliability, performance, security, and privacy have been a challenge.

Examples of IoT systems includes healthcare, emergency, advanced building management systems, smart home, smart grids for energy distribution, intelligent transport systems, public surveillance and data acquisition, smart factory and smart retail stores (Zanella et al., 2014). By employing the IoT technologies in the activities of healthcare servicing, doctors are able to access different kinds of data resources online quickly and easily, make emergency medical decisions, and reduce costs in the process (Xu et al., 2014). Health-related IoT applications are used to monitor the conditions of patients inside hospitals and old people at home (Khanna & Misra, 2014). For example, a tiny, wearable device can detect a person's vital signs and send an alert to a healthcare professional if a certain threshold is reached or if a person has fallen down. Also, when an accident occurs, the victim's medical journals are automatically made available to the ambulances to ensure that optimal treatment can be provided (Virkki & Chen, 2013).

The vision for the IoT is to make our everyday lives easier and boost the efficiency and productivity of businesses and employees. The data collected will help us to make smarter decisions. The ubiquity and interactions involved in the IoT provides many conveniences and useful services for individuals and organizations, but it is vulnerable to privacy. One of the most significant challenges in convincing users to adopt emerging technologies is the protection of data and privacy (Badkas et al., 2015). To solve the privacy problems created by IoT applications of the future, the privacy policies for each system domain must be specified. Once specified, either the individual IoT application or the IoT infrastructure must enforce privacy. The IoT system must be able to elicit users' requests for data access and the policies, and evaluate the requests against the policies in order to decide if they should be granted or denied.

In this chapter various issues related to IoT will be discussed. IoT privacy challenges and open problems will be elaborated. Finally, possible solutions and recommendations will be discussed.

BACKGROUND

The Internet security glossary (RFC) defines privacy as "the right of an entity, acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others. A Request for Comments (RFC) is a formal document from the Internet Engineering Task Force (IETF) that is the result of committee drafting and subsequent review by interested parties.

Information privacy was defined as "the right to select what personal information about me is known to what people" by Westin (1968). Westin's surveys measure attitudes and concerns about privacy and provide data on how these attitudes and concerns change over time. Westin has surveyed the general level of privacy concern of the public and has also studied the attitudes about specific privacy-related topics, for example, confidence in organizations that handle personal information, acceptance of a national identification system, and use of medical records for research. Westin classified the public into three categories. Westin has interchangeably used the following categories to refer to the groups of people that he created: (1) High and Fundamentalist, (2) Medium and Pragmatist, (3) Low and Unconcerned.

14 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/privacy-in-the-internet-of-things/213871

Related Content

E-Government, E-Surveillance, and Ethical Issues from Malaysian Perspective
Maslin Masrom (2016). *Ethical Issues and Citizen Rights in the Era of Digital Government Surveillance (pp. 249-263).*
www.irma-international.org/chapter/e-government-e-surveillance-and-ethical-issues-from-malaysian-perspective/145572

Military Expenditure and Economic Growth Relationship Revisited in Some South Asian Countries: With Special Reference to India
Kanchan Datta (2019). *National Security: Breakthroughs in Research and Practice (pp. 810-835).*
www.irma-international.org/chapter/military-expenditure-and-economic-growth-relationship-revisited-in-some-south-asian-countries/220917

Exploring Privacy Notification and Control Mechanisms for Proximity-Aware Tablets
Huiyuan Zhou, Vinicius Ferreira, Thamara Silva Alves, Bonnie MacKay, Kirstie Hawkeyand Derek Reilly (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 1748-1767).*
www.irma-international.org/chapter/exploring-privacy-notification-and-control-mechanisms-for-proximity-aware-tablets/213881

The Mode of Information – Due Process of Law and Student Loans: Bills of Attainder Enter the Digital Age
Timothy C. Bagwelland Shareka L. Jackson (2016). *Ethical Issues and Citizen Rights in the Era of Digital Government Surveillance (pp. 16-34).*
www.irma-international.org/chapter/the-mode-of-information--due-process-of-law-and-student-loans/145559

Microblogs, Jasmine Revolution, and Civil Unrest: Reassessing the Emergence of Public Sphere and Civil Society in People's Republic of China
Kenneth C. C. Yangand Yowei Kang (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 1153-1178).*
www.irma-international.org/chapter/microblogs-jasmine-revolution-and-civil-unrest/213848