


# Privacy and Security Challenges in the Internet of Things

**Fernando Almeida**

 <https://orcid.org/0000-0002-6758-4843>

*Polytechnic Institute of Gaya, Portugal*

**Justino Lourenço**

*Polytechnic Institute of Gaya, Portugal*

## INTRODUCTION

The Internet of Things (IoT) is a concept that describes the large and growing number of digital devices that operate between networks of potentially global scale. Unlike the conventional Internet, in which interaction is essentially performed by people, IoT is composed only of sensors and other intelligent devices (Chou, 2016). Therefore, we are facing a technological revolution that includes the interaction between objects and simple actions of daily life to the most complex processes of organizing entire industrial productions. IoT provides new and innovative ways for organizations to manage and monitor remote operations (Vermesan & Friess, 2014). Conceptually, it offers the possibility of connecting the physical world with the digital world through the Internet.

Significant social and material vulnerabilities can appear with the advancement of IoT. The Internet exposes people to new risk situations, which although they already exist in the physical world, are enhanced in the virtual world, due to the greater exposure and range that technologies provide. Several risks may arise due to IoT's lack of privacy and security. For example, hackers can open the door of a house remotely by knowing access security codes, can know user behaviors through access to the network of home light sensors or temperature sensors, can spy a person through access to security cameras, etc. (Eastwood, 2017; Karlov, 2017). Therefore, it is critical that IoT provides strong security mechanisms in a way that the benefits of this technology could be safely exploited by people.

The large network of connected devices and the enormous flow of data that IoT will generate turn data security and privacy a fundamental challenge. In this sense, this study aims to characterize how IoT service providers address the challenge of data privacy and security. By conducting case studies with leading companies in this sector we seek: (i) to identify the main privacy risks that IoT devices can expose; (ii) analyze the main privacy and security barriers in IoT devices; and (iii) propose counter-measures that can be adopted by companies and users to increase the security of IoT. The manuscript is organized as follows: initially a literature review on the concept of IoT and security and data protection is performed. After that, the adopted methodology is presented. Consequently, the main identified solutions and recommendations are presented and discussed. After that, some indications for future research are given. Finally, the main conclusions are drawn.

## BACKGROUND

### Concept, Evolution and Technologies of IoT

IoT is a concept in which the devices and objects of our day-to-day life are equipped with sensors capable of intelligently communicating between them. According to Hanes et al. (2017) a “thing” in the context of the IoT is a connected object which may be, for example, a person with a heart monitor, an industrial tank with level sensors, a car with sensors that warn of tire pressure, a public lighting of a city, an outlet at home, or any other natural or man-made object. IoT collects information from various devices (computers, vehicles, smartphones, traffic lights, etc.) and applications (anything from a social media application like Twitter to an e-commerce platform, from a production system to a traffic control).

IoT has the potentiality to transform the way we live, work and learn. It is the beginning of a cycle of technological renewal that will aid in the optimization and automation of basic daily tasks. In addition, it may bring important information for the public benefit, and for private companies to be more assertive in their products and services rendered. The virtual connection of data, people, processes and things promises to create a world of new economic opportunities, including Smart Cities, Smart Environment, Smart Metering, Security & Emergencies, Retail, Logistics, Industrial Control, Smart Agriculture, Smart Animal Farming, home automation and e-Health (Talari et al., 2017). For Kash (2014), some practical examples of IoT application are:

- Intelligent parking systems for cities will provide real-time visibility into the availability of parking spaces throughout the city;
- Teleworking can eliminate the daily path of the workplace, allowing employees to work from home. In remote locations, it would reduce costs and improve productivity for employers and employees. The impacts would result in reduced employee spending, office maintenance and cleaning, increased employee retention, increased productivity and new job opportunities;
- Intelligent transportation solutions improve traffic flows and reduce fuel consumption;
- Intelligent power grids more efficiently connect renewable resources, improve system reliability, and consumers are charged based on the efficiency of the operation;
- Through intelligent medicine, doctors and hospitals can receive and organize data from connected medical devices, including wearable and health monitors installed in patients' homes. By receiving the data in real-time, medical professionals thus obtain more complete information of their patients, improving care through more effective diagnoses and treatments;
- Machine monitoring sensors diagnose and anticipate pending maintenance problems and lack of stock.

IoT encompass every aspect of our daily lives, because it literally enables billions of things to be connected anytime, anywhere, to anything or any person. Its applications are many, such as smart houses, connected cars, energy systems, agriculture, transport, health, etc. A single technology cannot effectively meet all the needs of IoT's many applications. Therefore, although some objects use wired connections like Ethernet, Wireless communication technologies play a crucial role in enabling IoT connectivity. According to Kranz (2016), an ideal IoT communication network will be a mixture between the two types, Wired and Wireless. Several technologies can be used in IoT, respectively:

12 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-and-security-challenges-in-the-internet-of-things/248082](http://www.igi-global.com/chapter/privacy-and-security-challenges-in-the-internet-of-things/248082)

## Related Content

---

### Determinants of Forensic Accounting: The Case of Northwestern States of Nigeria

Sagir Lawal, Junaidu Muhammad Kurawaand Kabir Tahir Hamid (2021). *Handbook of Research on Theory and Practice of Financial Crimes* (pp. 250-269).

[www.irma-international.org/chapter/determinants-of-forensic-accounting/275463](http://www.irma-international.org/chapter/determinants-of-forensic-accounting/275463)

### Victimization, Cultural Imperatives, and Empowerment of People of Color in the United States

Tamanna M. Shah (2020). *Global Perspectives on Victimization Analysis and Prevention* (pp. 96-113).

[www.irma-international.org/chapter/victimization-cultural-imperatives-and-empowerment-of-people-of-color-in-the-united-states/245030](http://www.irma-international.org/chapter/victimization-cultural-imperatives-and-empowerment-of-people-of-color-in-the-united-states/245030)

### Recognition and Protection of Women's Rights and Gender in FDRE Constitution and Other Laws of Ethiopia

Yetimwork Anteneh Wondim (2022). *Research Anthology on Child and Domestic Abuse and Its Prevention* (pp. 284-296).

[www.irma-international.org/chapter/recognition-and-protection-of-womens-rights-and-gender-in-fdre-constitution-and-other-laws-of-ethiopia/301155](http://www.irma-international.org/chapter/recognition-and-protection-of-womens-rights-and-gender-in-fdre-constitution-and-other-laws-of-ethiopia/301155)

### Language, Social Pragmatic Communication, and Childhood Trauma

Yvette D. Hyter (2022). *Research Anthology on Child and Domestic Abuse and Its Prevention* (pp. 874-908).

[www.irma-international.org/chapter/language-social-pragmatic-communication-and-childhood-trauma/301189](http://www.irma-international.org/chapter/language-social-pragmatic-communication-and-childhood-trauma/301189)

### The Aileen Wuornos Case: Bending the Criminal Binary of Monsters and Martyrs

Christine Bussey (2023). *Cases on Crimes, Investigations, and Media Coverage* (pp. 192-200).

[www.irma-international.org/chapter/the-aileen-wuornos-case/313706](http://www.irma-international.org/chapter/the-aileen-wuornos-case/313706)