Internet of Things: Privacy and Security Implications

Mohamed A Eltayeb, Colorado Technical University, Colorado Springs, CO, USA

ABSTRACT

In the contemporary world, we are surrounded by a complex network of interconnected sensors. These allows us to share, collate, transmit, and store vast amounts of data. These systems are known as the Internet of Things (IoT), and this technological offering has attracted a large amount of interest from academics, researchers, and developers in recent years due to its highly scalable and agile nature. However, while the IoT delivers significant benefits, it also poses some risks. The data that is stored and exchanged via the IoT is extremely valuable to individuals who have malevolent intent. In more recent years, the increasing popularity of the IoT as a means of sharing information has been associated with privacy and security risks that have undermined users’ trust in the IoT. This paper examines what these risks are and some of the actions that can be taken to mitigate them.

KEYWORDS

1. INTRODUCTION

The IoT consists of a complex network of physical units that employ embedded software networks, sensors, and other electronic devices to exchange information. It was first introduced in 1999 and was initially designed as a mechanism that could link the virtual world with the physical world. However, it has significantly evolved since its early manifestation and now incorporates many different components across numerous industries and applications to the extent that it has become a significant part of everyday life in contemporary society. In simplistic terms, the IoT is often regarded as the world’s biggest small town. Each of the elements that live in this world knows and is connected to one another, and is aware of how one another functions and what one another is doing. Experts predict that the majority of components we use in everyday life will be connected to the IoT network in some way, shape or form in the future (Gubbi et al., 2013). It has been projected that the IoT market will reach a potential value of up to $11.1 Trillion by 2025 (Maier, 2016). Figure 1 illustrates the interconnection of objects in the IoT environments.

Components of the IoT network can communicate with one another and with humans using embedded sensors. These sensors connect disparate objects that can be located anywhere in the world (Xia et al., 2012). The development of this immense and powerful network has provided humanity
with access to some significant benefits. However, as with all forms of technology, the IoT is not
without its inherent disadvantages and top of the list of downsides are security and privacy exposures.

The introduction of new technologies often spurs the question “How does this impact my
privacy?” and this reservation is of particular relevance within the context of the IoT. Individuals
who are evaluating whether they would like to use the technology associated with the IoT naturally
have concerns as to the extent it delivers value, will improve their lives, will be useful to them, and
will be secure. The particular threats associated with security and privacy have been examined by
many researchers (Suo et al., 2012; Bohli et al., 2013; Neisse et al., 2014; Pohls et al., 2014; Ren
et al., 2014; Zhang et al., 2015; Ray et al., 2016) and security breaches are frequently reported
by the media. A study by Miorandi et al. (2012) found that the extent of the privacy and security
risks has prevented many people from using the IoT. To this end, it is critical that users of the IoT
are fully aware of the risks that are associated with its use and that they implement appropriate
measures through which these risks can be minimized. Furthermore, as the systems associated
with the IoT are developing at a rapid pace, it is imperative that our ability to manage exposures
evolves at an equal rate.

Due to advances in IoT technologies, every single object can potentially be attached to a sensor,
be it clothing, medical equipment, food items, animals, etc. As a result, the amount of data collected
by the IoT technologies is expanding at an exponential rate as more and more sensors are added to
the network. Today, there are a large number of entry points to Wireless Sensor Networks (WSN)
and these continue to expand at a steady rate (Perera et al., 2014). The larger the number of entry
points and sensors, the higher the level of vulnerability and risk of security breaches. Thus, many
IoT consumers have become concerned about security and the ongoing protection of their privacy.
This is somewhat expected given the fact that one function of the IoT is to store and share private
data. The main challenges and disadvantage users may encounter in the adoption of IoT is that they
lack full control over their sensitive data.

The objective of this paper is to examine the potential privacy and security threats that can arise
from the use of IoT systems. The paper will identify the underlying concepts of IoT technology and
examine how it can be used and abused. It will then progress to present some potential solutions that
can be employed to protect IoT users against security breaches and allow the real-time detection of
such breaches in the event they do occur.
Future Approach of Next Generation Cellular Mobile Communications
[www.igi-global.com/chapter/future-approach-next-generation-cellular/63295?camid=4v1a](www.igi-global.com/chapter/future-approach-next-generation-cellular/63295?camid=4v1a)

Joint Radio Resource Management in Cognitive Networks: TV White Spaces Exploitation Paradigm
[www.igi-global.com/chapter/joint-radio-resource-management-cognitive/77684?camid=4v1a](www.igi-global.com/chapter/joint-radio-resource-management-cognitive/77684?camid=4v1a)