Chapter 81
Critical Issues in the Invasion of the Internet of Things (IoT):
Security, Privacy, and Other Vulnerabilities

Shravani Devarakonda
Charles Sturt University, Australia

Malka N. Halgamuge
https://orcid.org/0000-0001-9994-3778
The University of Melbourne, Australia

Azeem Mohammad
Charles Sturt University, Australia

ABSTRACT

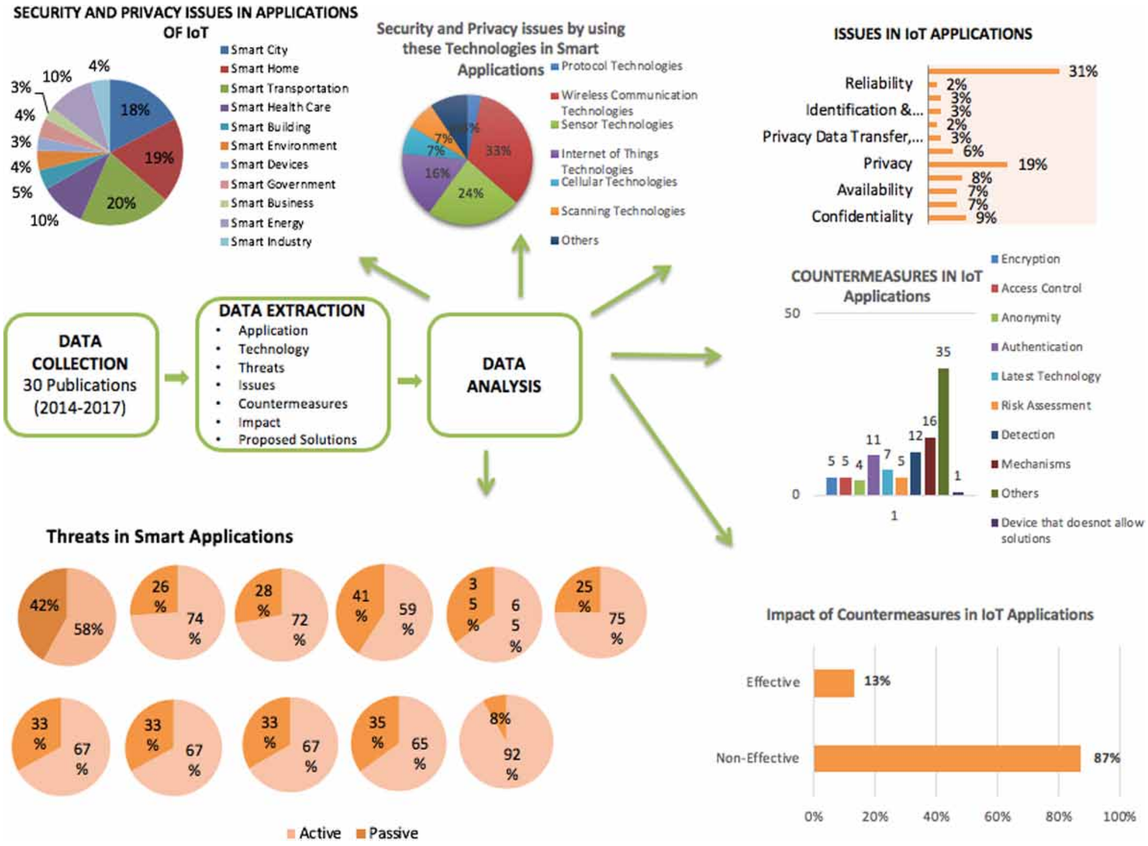
In this chapter, the authors collected data from issues related to threats in the applications of IoT-based technologies that describe the security and privacy issues from 30 peer reviewed publications from 2014 to 2017. Further, they analyzed each threat type and its percentages in each application of the internet of things. The results indicated that the applications of smart transportation (20%) face the highest amount of security and privacy issues followed by smart home (19%) and smart cities (18%) compared to the rest of the applications. Further, they determined that the biggest threats were denial of service attack (9%) followed by eavesdropping (5%), man in the middle (4%), and replay (4%). Denial of service attacks and man in the middle attack are active attacks that can severely damage human life whereas eavesdropping is a passive attack that steals information. This study has found that privacy issues have the biggest impacts on people. Therefore, researchers need to find possible solutions to these threats to improve the quality of IoT applications.

DOI: 10.4018/978-1-7998-8954-0.ch081

INTRODUCTION

In the most recent decade, there has been economic growth and social transformation that has prompted the urbanization rush in the world (Zhang et al., 2017). There is a continued growth in technologies due to the Internet of Things (IoT) is in every part of the people's lives in the 21st century (Pishva, 2017). By 2030, it is estimated that urban areas population will reach 5 billion (Zhang et al., 2017) and a few experts are estimating that more than 50 billion things would be connected to the networking world. Most of these associates to unsecured actuators and sensors (Ronen et al., 2017) for a lower marketplace and customers demand services (Geneiatakis et al., 2017). The mission of smart cities in urban areas is quick growth that increases the opportunities (Srivastava, 2017). Some of the applications which come under the smart city concept which are shown in the Table 1.

Figure 1. Graphical abstract of this study



In today's world nearly, all appliances are connected to internet technologies. Making use of electronics with a few specialized programs that have Internet access and creates intelligent networks (Pishva, 2017). The Smart Cities architecture consists of 3 worlds: Information, Communication, and Physical. Furthermore, the sensing components that make up the Physical world of IoT include wearable devices, smart sensing devices, environmental sensors, and operating and control components. Similarly, the het-