Chapter 9

A Survey on Emerging Security Issues, Challenges, and Solutions for Internet of Things (IoTs)

Anish Khan
UIET, Kurukshetra University, Kurukshetra, India

Dragan Peraković
https://orcid.org/0000-0002-0476-9373
University of Zagreb, Croatia

ABSTRACT

The internet of things is a cutting-edge technology that is vulnerable to all sorts of fictitious solutions. As a new phase of computing emerges in the digital world, it intends to produce a huge number of smart gadgets that can host a wide range of applications and operations. IoT gadgets are a perfect target for cyber assaults because of their wide dispersion, availability/accessibility, and top-notch computing power. Furthermore, as numerous IoT devices gather and investigate private data, they become a gold mine for hostile actors. Hence, the matter of fact is that security, particularly the potential to diagnose compromised nodes, as well as the collection and preservation of testimony of an attack or illegal activity, have become top priorities. This chapter delves into the timeline and the most challenging security and privacy issues that exist in the present scenario. In addition to this, some open issues and future research directions are also discussed.

INTRODUCTION

Since from the beginning till the present day there are numerous definitions coined by different authors and researchers. The term "Internet of Things" refers to a network of physical devices or embedded devices which are capable of sending and receiving information or data via internet know as "Internet of Things (IoT)" (Oracevic et al., 2017, Adat et al., 2018, Lv, Z., 2020, Liu et al., 2017), Khattak et al.,

DOI: 10.4018/978-1-7998-7789-9.ch009

2019). A technology that combines real-world with virtual world offers a rich ground for imagination and innovative ideas. The IoT is next phase in evolution of communication technologies. We caught a glimpse in the manner of utilization of technologies is an eye catching transformation that moulds the world from off the beaten track systems to ubiquitous Internet-enabled “things” (Sain et al., 2017).

For trouble free identification and communication purposes, digital identities are issued to every smart object that will help in sharing data and opportunity to use various services. A unique detection-system-radio frequency identification (RFID) has been developed using the concept of digitally identifying many gadgets (Aldowah et al., 2018, Aly et al., 2019, Sahmim & Gharsellaoui, 2017, Arıs et al., 2018). Wireless sensor networks are crucial in the execution of cutting-edge technologies because they are resource constrained. The use of cloud computing results in the creation of a virtual platform for integrating storage devices, development and research tools, and so on (Jose, D. V., & Vijyalakshmi, A., 2018). Users can access applications on demand without considering their physical location. As IoT is a vast area and offers number of applications in every possible way in routine life. For example, health care monitoring systems, smart transportation systems, retail, surveillance, wearable gadgets and many more (Jose, D. V., & Vijyalakshmi, A., 2018, Alaba et al., 2017, Bhattarai, S., & Wang, Y., 2018). Figure 1: Illustrate some of the common applications of Internet of things.

As far as IoT becomes burning matters nowadays, in contrast with this many security and privacy challenges have pop-up and become the bottle neck issues for IoT as the number of edge devices has increased dramatically (Yousefi, A., & Jameii, S. M., 2017). Various real-time attacks, such as zero-day attacks, ransomware, phishing attacks, and DDoS attacks (Sadeeq et al., 2018, Chahid et al., 2017, Hassan, W. H., 2019), have been introduced in recent years. The motive of this paper is to highlight various attacks that make edge devices vulnerable.

The road map of this paper contains eight sections. Section I gives a short and crisp introduction to IoT. Section II tells us about history and growth of IoT. Section III highlights the main elements of IoT. Section IV illustrates the three layer architecture of Internet of Things. Section V gives brief introduction of taxonomy of attacks. Section VI gives bird eye view of security challenges to each layer of IoT and Section VII illustrates some counter measures of various threats. Section VIII tells some future research directions and some open challenges to IoT. Finally, Section VIII concludes this paper.

TIMELINE OF IoT

The “Internet” is a worldwide group of combined servers, PCs, tablets and mobiles that are administered by standard protocols for combined frameworks. This enables users to send, receive and communicate the information (Sfar et al, 2018, Ande et al., 2020, Conti et al., 2018, Maple et al., 2017). The word “Things” has many meanings in English dictionary. The word thing refers to an object, action and situation. For example, a mobile is referred to an object, ‘those kinds of things are expected from her’- here things are referred as action (Li, S., & Da Xu, L., 2017).

With the combination of above mentioned terms, a new term originates called “Internet of Things” that means a network of physical devices or embedded devices which are capable of sending and receiving information or data with the help of internet know as “Internet of Things” (Madakam et al., 2015). Vision of Internet of Things is to make things (tube-light, AC, fan, door bell, table etc) smart and to act like living entities by using internet. Internet becomes ubiquitous and spread almost in every part of the world and human life is directly influenced by internet.