


# Chapter 7

## Analysis of Vulnerabilities in IoT and Its Solutions

**Puspanjali Mallik**

 <https://orcid.org/0000-0002-3896-3457>

*Shailabala Women's Autonomous College, India*

### ABSTRACT

*The internet of things (IoT) fulfils abundant demands of present society by facilitating the services of cutting-edge technology in terms of smart home, smart healthcare, smart city, smart vehicles, and many more, which enables present day objects in our environment to have network communication and the capability to exchange data. These wide range of applications are collected, computed, and provided by thousands of IoT elements placed in open spaces. The highly interconnected heterogeneous structure faces new types of challenges from a security and privacy concern. Previously, security platforms were not so capable of handling these complex platforms due to different communication stacks and protocols. It seems to be of the utmost importance to keep concern about security issues relating to several attacks and vulnerabilities. The main motive of this chapter is to analyze the broad overview of security vulnerabilities and its counteractions. Generally, it discusses the major security techniques and protocols adopted by the IoT and analyzes the attacks against IoT devices.*

### INTRODUCTION

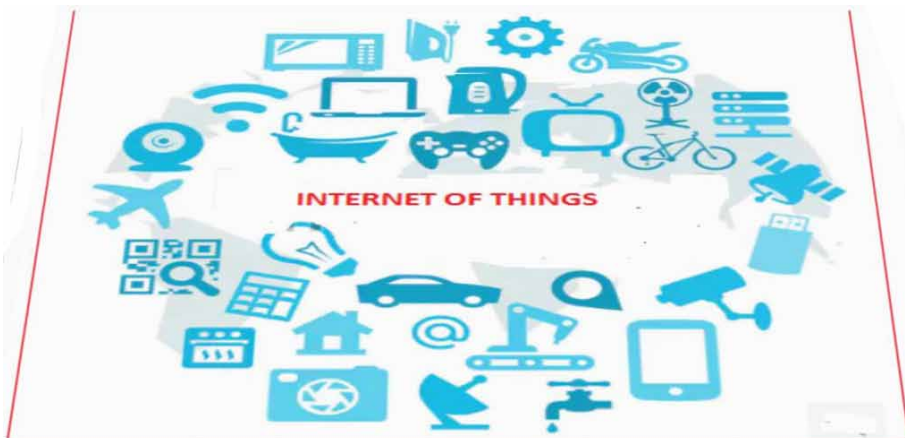
Everyday information security brings new challenges because of its wide availability in each field starting from personal to commercial lives. Data must be protected from interception, theft and attack caused by unauthorized persons or hackers (F.Meneghello et.al, 2019). Network security is one part of information security

DOI: 10.4018/978-1-5225-9493-2.ch007

which may be challenged by Denial-of-Service attack and Cloning attack . Several countermeasures have been introduced to reduce the vulnerability risk and to strengthen the network security (M.Irshad et.al, 2016) Among the counter measures the best form is prevention action that includes monitoring control to detect threats. This network security expanding in dimension becomes complex every day as per as the varying mode of uses and applications. Traditionally, only the edge devices (J.W.Jones et.al, 2018) were included in the formation of network but towards the last part of twentieth century all devices within a proposed area became enable to communicate with each other. Fig 1. shows the types of devices integrated within a common area satisfying the communication criteria to form the IoT.

This newly formed network linked to Internet by following cloud technology

*Figure 1. IoT Devices*



and facilitates the automation of applications such as smart agriculture, smart healthcare, smart home, smart city, smart car, and smart transportation system etc. By the year 1999, this idea was first introduced by Kevin Ashton, founder of one automated organization at MIT to describe a system where the Internet is connected to the physical world via ubiquitous sensors. He successfully implemented the data connectivity and after this communication started between any two devices where as previously it was only limited between any two routing devices. Fig.2 includes the list of number of connected devices used in IoT . According to this, in the year 2015, there were only 3.8 billion IoT devices were connected, the number will reach to 9.9 billion in this year 2020 and the number is expected to reach by 21.5 billion by the year 2025.

19 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/analysis-of-vulnerabilities-in-iot-and-its-solutions/262551](http://www.igi-global.com/chapter/analysis-of-vulnerabilities-in-iot-and-its-solutions/262551)

## Related Content

---

### Toward Intelligent Fuzzy QoS Model in Wireless Ad Hoc Networks

Lyes Khoukhi, Ali El-Masri and Dominique Gaiti (2012). *Wireless Multi-Access Environments and Quality of Service Provisioning: Solutions and Application* (pp. 218-244).

[www.irma-international.org/chapter/toward-intelligent-fuzzy-qos-model/61842](http://www.irma-international.org/chapter/toward-intelligent-fuzzy-qos-model/61842)

### 6G With Integration of Sensing and Communication

Aswatha R., Seethalakshmi V., Gunanandhini S., Senthilkumar B. and Prabhakar G. (2022). *Handbook of Research on Design, Deployment, Automation, and Testing Strategies for 6G Mobile Core Network* (pp. 93-113).

[www.irma-international.org/chapter/6g-with-integration-of-sensing-and-communication/302181](http://www.irma-international.org/chapter/6g-with-integration-of-sensing-and-communication/302181)

### QoS-Constrained Resource Allocation Scheduling for LTE Network

Hung-Chin Jang and Yun-Jun Lee (2015). *International Journal of Wireless Networks and Broadband Technologies* (pp. 1-15).

[www.irma-international.org/article/qos-constrained-resource-allocation-scheduling-for-lte-network/125815](http://www.irma-international.org/article/qos-constrained-resource-allocation-scheduling-for-lte-network/125815)

### Multi-Standard Multi-Band Reconfigurable LNA

Mohd Tafir Mustaffa (2012). *Advances in Monolithic Microwave Integrated Circuits for Wireless Systems: Modeling and Design Technologies* (pp. 1-23).

[www.irma-international.org/chapter/multi-standard-multi-band-reconfigurable/58485](http://www.irma-international.org/chapter/multi-standard-multi-band-reconfigurable/58485)

### The Urban Communication Infrastructure: Global Connection and Local Detachment

Susan Drucker and Gary Gumpert (2012). *Wireless Technologies: Concepts, Methodologies, Tools and Applications* (pp. 1150-1169).

[www.irma-international.org/chapter/urban-communication-infrastructure/58836](http://www.irma-international.org/chapter/urban-communication-infrastructure/58836)