Chapter 6
Security Vulnerabilities, Threats, and Attacks in IoT and Big Data:
Challenges and Solutions

Prabha Selvaraj
https://orcid.org/0000-0002-0820-9146
VIT-AP University, India

Sumathi Doraikannan
https://orcid.org/0000-0003-2920-4640
VIT-AP University, India

Vijay Kumar Burugari
https://orcid.org/0000-0002-7871-2396
KL University, India

ABSTRACT

Big data and IoT has its impact on various areas like science, health, engineering, medicine, finance, business, and mainly, the society. Due to the growth in security intelligence, there is a requirement for new techniques which need big data and big data analytics. IoT security does not alone deal with the security of the device, but it also has to care about the web interfaces, cloud services, and other devices that interact with it. There are many techniques used for addressing challenges like privacy of individuals, inference, and aggregation, which makes it possible to re-identify individuals' even though they are removed from a dataset. It is understood that a few security vulnerabilities could lead to insecure web interface. This chapter discusses the challenges in security and how big data can be used for it. It also analyzes the various attacks and threat modeling in detail. Two case studies in two different areas are also discussed.

DOI: 10.4018/978-1-5225-9742-1.ch006

INTRODUCTION

The main usage of Big Data is identify and optimize the processes in business, financial trading, enhancing and optimizing smart cities and nations, better relationship management of customers, enhancing healthcare, sports, transport services etc. IoT refers to the connection of a huge number of physical devices that are located all around the world are now connected to the internet in such a way that data could be collected and shared. Nowadays, IoT make sure that the environment which we live in could be made as smart i.e. makes our homes, offices and vehicles to be smarter and chattier. In addition, a few sensors play a vital role in assessing the noise present in the environment, pollution in the environment. A variety of techniques are used by IoT devices in order to connect with other devices for data sharing. Technologies like Standard Wi-Fi, Bluetooth low energy, Local Terminal Equipment (LTE), satellite connections are used for connecting several devices at various levels. Low Power Wide Area Networks (LPWAN) initiated its deployment of IoT devices with Sigfox, LORa and recently LTE Cat-M, Narrow Band IoT (NB-IOT) as discussed by Usman Raza et al (2017) are used and a comparison is given below in the Figure 1.

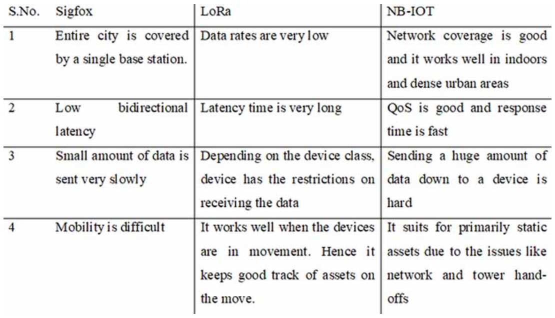
Recently enterprises augment the dependency of IoT devices which leads to more focus in security of these devices. IoT security does not alone deals with the security of the device but it also has to care about the web interfaces, cloud services and other devices that interact with it. Hence enterprise IoT systems must be free from vulnerabilities M Mowbray (2017). Therefore, many researchers put their attention on detection and countermeasures of security attacks in IoT systems.

Challenges and Issues in Big Data

Big data challenges and issues are discussed below:

- **Privacy**: The large of volume of data need to be safeguarded in order to prevent the misuse of these big data stores.
- **Veracity**: Data must meet the trustworthiness.
- **Volume**: Large volume of data need to be stored and processed in case of big data but RDBMS tools cannot be used to store or process it. So the traditional SQL based queries are not used to solve this challenge, instead compression technology can be used to compress the data at rest and also in memory.

Figure 1. Comparison of LPWAN technologies



S.No.	Sigfox	LoRa	NB-IOT
1	Entire city is covered by a single base station.	Data rates are very low	Network coverage is good and it works well in indoors and dense urban areas
2	Low bidirectional latency	Latency time is very long	QoS is good and response time is fast
3	Small amount of data is sent very slowly	Depending on the device class, device has the restrictions on receiving the data	Sending a huge amount of data down to a device is hard
4	Mobility is difficult	It works well when the devices are in movement. Hence it keeps good track of assets on the move.	It suits for primarily static assets due to the issues like network and tower hand-offs