Chapter 6
Security Issues of IoT

Neha Gupta
Symbiosis University of Applied Sciences, Indore, India

ABSTRACT

Wireless communication networks are highly prone to security threats. The major applications of wireless communication networks are in military, business, healthcare, retail, and transportations. These systems use wired, cellular, or adhoc networks. Wireless sensor networks, actuator networks, and vehicular networks have received a great attention in society and industry. In recent years, the internet of things (IoT) has received considerable research attention. The IoT is considered as future of the internet. In the future, IoT will play a vital role and will change our living styles, standards, as well as business models. The usage of IoT in different applications is expected to rise rapidly in the coming years. The IoT allows billions of devices, peoples, and services to connect with others and exchange information. Due to the increased usage of IoT devices, the IoT networks are prone to various security attacks.

IOT – SECURITY

Every connected device creates opportunities for attackers. These vulnerabilities are broad, even for a single small device. The risks posed include data transfer, device access, malfunctioning devices, and always-on/always-connected devices. The main challenges in security remain the security limitations associated with producing low-cost devices, and the growing number of devices which creates more opportunities for attacks.

Security Spectrum: The definition of a secured device spans from the simplest measures to sophisticated designs. Security should be thought of as a spectrum of vulnerability which changes over time as threats evolve. Security must be assessed

DOI: 10.4018/978-1-7998-2414-5.ch006

based on user needs and implementation. Users must recognize the impact of security measures because poorly designed security creates more problems than it solves. Example: A German report revealed hackers compromised the security system of a steel mill. They disrupted the control systems, which prevented a blast furnace from being shut down properly, resulting in massive damage. Therefore, users must understand the impact of an attack before deciding on appropriate protection.

1.1 Challenges

Beyond costs and the ubiquity of devices, other security issues plague IoT:

i. **Unpredictable Behaviour** – The sheer volume of deployed devices and their long list of enabling technologies means their behaviour in the field can be unpredictable. A specific system may be well designed and within administration control, but there are no guarantees about how it will interact with others.
ii. **Device Similarity –** IoT devices are fairly uniform. They utilize the same connection technology and components. If one system or device suffers from a vulnerability, many more have the same issue.
iii. **Problematic Deployment** – One of the main goals of IoT remains to place advanced networks and analytics where they previously could not go. Unfortunately, this creates the problem of physically securing the devices in these strange or easily accessed places.
iv. **Long Device Life and Expired Support –** One of the benefits of IoT devices is longevity, however, that long life also means they may outlive their device support. Compare this to traditional systems which typically have support and upgrades long after many have stopped using them. Orphaned devices and abandon ware lack the same security hardening of other systems due to the evolution of technology over time (Weyrich & Ebert, 2015).
v. **No Upgrade Support –** Many IoT devices, like many mobile and small devices, are not designed to allow upgrades or any modifications. Others offer inconvenient upgrades, which many owners ignore, or fail to notice.
vi. **Poor or No Transparency –** Many IoT devices fail to provide transparency with regard to their functionality. Users cannot observe or access their processes, and are left to assume how devices behave. They have no control over unwanted functions or data collection; furthermore, when a manufacturer updates the device, it may bring more unwanted functions (Weyrich & Ebert, 2015).

Predictive Modeling for Imbalanced Big Data in SAS Enterprise Miner and R
Son Nguyen, Alan Olinsky, John Quinnand Phyllis Schumacher (2018). *International Journal of Fog Computing (pp. 83-108).*
www.irma-international.org/article/predictive-modeling-for-imbalanced-big-data-in-sas-enterprise-miner-and-r/210567