

Chapter 2

Security Mechanisms for Connectivity of Smart Devices in the Internet of Things

Somayya Madakam and Hema Date

2.1 Introduction

We have already connected cars, homes, refrigerators, thermostats, spoons, and many other appliances and devices to the Internet. In fact, in the near future, even more physical things will get connected to the Future Internet (FI). A complete IoT corporate's vision is that a world of low-cost sensors will be designed, developed, and embedded into our daily eating utensils, mattresses, and home lighting systems, to name but a few, for better services to the human being through smart device connectivity. The term smart device (SD) designates any physical object associated with computing resources and capable of communicating with other similar objects via physical transmission medium and logical protocols or with humans via a standard user interface. The scale spans from big smart devices such as personal digital assistants (PDAs) to small ones such as radio-frequency identification (RFID) tags [1]. Smart devices can be programmed, sometimes hardwired, to tell us to reduce the amount of caffeine we consume after 8 pm or train one's bedroom lights to gradually increase their brightness precisely at the moment one comes out of deep sleep. Sensors can work around the clock (24×7) to measure and monitor everything from one's diet to one's sleeping behavior and then use this information to modify future actions for a better future. A recent observation at Seven Hills Hospital at Marol in Mumbai (India) was that the patient's entire blood pressure, electro cardio graphy (ECG), sugar content level, oxygen, water amount, and other allied medical parameters were completely measured by sensors, computers, and allied medical smart devices for monitoring, automation, and controlling. This was finally intimated to the concerned nurses and doctors for further treatment. This is an ideal example how smart devices can be used for better medical treatment. This

S. Madakam (✉) • H. Date

IT Applications Group, National Institute of Industrial Engineering (NITIE), Mumbai, India

e-mail: somu4smart@gmail.com

kind of device connection is called the Internet of Things. The Internet of Things is a new paradigm shift in IT world, where things have digital identities, monitoring functionalities with artificial intelligence (AI), and can be located, tracked, automated, monitored, and controlled automatically.

In the rest of this chapter, we explore the concept of smart devices and their connectivity from the viewpoint of scholars, academicians, practitioners, and developers. Furthermore, we also discuss in detail the security mechanisms of smart devices within the Internet of Things (IoT) scenario, with emphasis on both physical and logical remedy mechanisms.

2.2 Internet of Things

As discussed before, a smart device is an electronic device, generally connected to other electronic devices through high-speed bandwidth networks with the help of wireless technologies such as Bluetooth, near-field communication (NFC), Wi-Fi, and 4G, capable of communication with other devices. These smart devices can be smartphones, androids, tablets, iPads, computers, laptops, television, consoles, and IP cameras. Next-generation smart cards, also called smart devices, are regarded as personal devices providing a secured execution and storage environment for application tasks and sensitive secrecy/privacy of the data or information, respectively [2].

In the beginning, the Internet was designed and used only for communication and to access websites/web portal through mobiles or computers to download information. However, with the help of advanced technological tools and techniques and more powerful smart devices with high speed, extra capabilities, and more intelligence abilities, its connotation changed. Advances in technologies like very large-scale integration (VLSI) chips and microcontrollers are also creating smarter devices with low power consumption; this means that large networks of sensors can be created, with the ability to obtain information, process it, and act accordingly. 3D computer-aided design system uses the common multi-touch gestures associated with smart devices to keep the modeling operations simple and easy for users. However, it is difficult to input the precise geometric information to generate 3D CAD models by such gestures [3]. Here it shows how the idea of the Internet of Things arises [4]. Though the term IoT was coined by Kevin Ashton in 1999 at the Auto-ID Center in MIT, the IoT was the seventh technology in the series defined by the International Telecommunication Union (ITU) in their reports originally launched in 1997 under the title *Challenges to the Network*.

The Internet of Things describes the evolution from systems linking digital information to systems relating digital information to real-world physical items. In this sphere, the Internet connects with our routines through this network of connected objects [5]. The rise of the Internet of Things provides an environment where everyday objects are allied to the Internet and contribute together on a system, which gives way to the convergence of smart appliances and

conventionally connected to devices. There were approximately 6.3 billion people living on the planet in 2003, and 500 million devices connected to the Internet as per Cisco's statistics. This indicates that there was less than one (0.08) device for every person. Based on Cisco's Internet Business Solutions Group (IBSG)'s definition, the IoT did not exist in the year 2003. The number of connected devices was relatively very small given that ubiquitous smart devices such as smartphones were introduced only in the year 2007. Hence, Cisco's IBSG reported that the IoT was born way back between 2008 and 2009. Today, the Internet of Things is quite prosperous, as initiatives such as Cisco's planetary skin, smart grid, and intelligent vehicles continue to progress. Cisco's IBSG predicts that there will be 25 billion smart devices connected to the Internet by 2015 and 50 billion by 2020. Some other projections indicate that up to 100 billion smart devices or objects will be connected to the Internet by the end of the year 2020. According to the seventh EMC digital universe study report, India's digital universe shall grow ninefold by 2020. Out of which data generated by the IoT shall be 10 %. The IoT is considered as the world's third wave of the information industry after the inventions of computer and the Internet [6]. The base for any smart device to function efficiently is the help of embedded Internet of Things technologies. Speaking about smart devices, it includes even the existing electronic devices that have computational capabilities as well as physical things, acquiring the power of intelligence through various artificial intelligence capabilities to perform tasks efficiently and effectively.

The Internet of Things is the next evolution of the Internet, which is positively affecting human life. The Internet of Things is a technological revolution that represents the future of computing and communications, and its development depends on the dynamic technical innovation in a number of important fields, from wireless sensors to nanotechnologies. Primarily, the Internet of Things is aimed at making our daily life more sophisticated and flexible. The IoT is a network of smarter objects, which includes people too. These devices will have communication and computation capabilities [7]. The IoT, also called Cyber-Physical Systems, is now going to reign over all earthly things, living as well as nonliving. It will be present everywhere (omnipresent) through various connected technologies and will have the potential to automate, monitor, and control things even in situations of disasters. According to one estimate, there could be around 86,000 trillion devices that connect to the future Internet, soon.

In the Internet of Things, everything real becomes virtual, which means that each person and thing has a locatable, addressable, and readable counterpart on the Internet [8]. In the Internet of Things, every existing object can be connected to the Internet and can exchange data with other objects. By allowing everything to be interconnected, objects will have recognition, localization, sensing, control, and management. The basic objective of any device or thing or object connection to the Internet varies from device to device. This connection can be done through various technologies including RFID, IPv6, EPC, bar code, ZigBee, Wi-Fi, Bluetooth, NFC, sensor, actuator, data analytic, ambient intelligence (AI), and Web 2.0.

The IoT is a paradigm shift that takes advantage of sensor networks. It is rapidly gaining ground in modern wireless communications, with its position and status

known, where services and intelligence are added to this expanded Internet, fusing the digital and physical world. The basic concept is the pervasive presence of objects, such as radio-frequency identification (RFID) tags, actuators, mobile phones, and sensors [9]. The benefits of the IoT to developing and emerging economies are significant, and strategies to realize these need to be found. As a result, applying the IoT for modeling logistic system is a promising solution for researchers [10]. The prospects of a world of smart things that virtually talk to each other are fascinating, leading to many new applications and opportunities [11]. The pervasive and ambient intelligence (AI) will involve interaction coordination and cooperation among more and more smart devices [12].

2.3 Security in the IoT

Security is not a new concept. Right from birth to death, one has to take care of several security mechanisms in terms of food, shelter, children, articles, finance, and many more aspects, in which we are experiencing very well. Similarly, when the billions of smart devices are connecting to the Internet under the umbrella of IoT phenomena, there needs to be robust security mechanisms to get the right information to the right things, at the right place at the right time through the right channel. At the same time, when the communication is happening among all people, objects, and machines, security is absolutely required. Sometimes one may be unable to receive data due to device failure, due to in turn, to noise or channel failure. Besides, there may be more hackers who often try to hack strategic information for their own business without following any cyber laws or ethics. Organizations need to protect their own information from attackers or competitors as these could lead to loss of professional data. Information security refers to measures adopted to prevent the unauthorized use, misuse, modification, or denial of knowledge, facts, data, or capabilities [13]. The basic security issues in the IoT are the same as the security issues in general IT; however, in the case of the IoT, much more sensitivity and confidentiality are a must. The sensitivity of IoT technologies is based on different security requirements such as confidentiality, integrity, authenticity, privacy, availability, and regulation. As every player with a stake in the IoT is well aware, security is paramount for the safe and reliable operation of connected devices. The security of smart device issues generally includes physical and logical issues. The logical issues are many in the form of malware counting into virus, worms, Trojan horse, and spyware. Smart devices have limited capabilities, in terms of computational power and memory, and might be battery-powered devices, thus raising the need to adopt particularly energy-efficient technologies. These devices generate a large amount of data per second, even in peta-bytes per second. The deployment of the IoT raises many security issues coming from (1) the very nature of smart objects, e.g., the adoption of lightweight cryptographic algorithms, in terms of processing and memory requirements, and (2) the use of standard protocols, e.g., the need to minimize the amount

of data exchanged between nodes [14]. The integration of the physical world into the fabric of Web imposes advanced security requirements that need to be satisfied in order to ensure a stringent control over IoT service interaction. Security and privacy trials of the Internet of Things (IoT) that appear are due to the connection of diverse technologies [15].

The Internet of Things is a topic that has been studied by many researchers, either trying to create a trustworthy infrastructure to enhance the privacy of the Internet of Things or creating developments secure enough to provide applications on fields as healthcare [16]. Design principles and methods for securing the IoT are yet to be explored. Security in the IoT device is a crucial aspect that applies at different levels, ranging from technological issues to more philosophical ones, such as privacy and trust, especially in scenarios like smart toys. The security challenges derive from the very nature of smart objects and the use of standard protocols. In [17], the security challenges and requirements for an IP-based IoT have been presented by analyzing existing Internet Protocols to be applied to the IoT and the limitations and problems that such a solution might introduce. The technique of the Internet of Things is a new application technique, and people are often more focused on novel applications, neglecting the security problem, which is more important in the case of wireless sensor network in the IoT [18]. Towards particular IoT security, there are several open issues such as cryptographic algorithms, authentication protocols, access control, trust or privacy, and governance frameworks [19]. Hence, the research status of key technologies including encryption mechanism, communication security, protecting sensor data, and cryptographic algorithms must be taken care of [20]. However, it is the need of the hour that we need to work for more advanced security mechanisms in the forthcoming years in securing smart device communications under the umbrella of the Internet of Things.

2.4 Security in Smart Devices

Security has been defined as the ability to deal with a specific threat by somehow neutralizing it. A broader definition refers to relative freedoms from various kingdoms of dangers and risks. This definition includes cognitive and psychological aspects innate in a security system. Security is, thus, an attitude which depends heavily upon the perceived nature of an environment [21]. The market for devices like mobile phones, multi-functional watches, and personal digital assistants is growing rapidly. Most of these mobile user devices need security for their prospective electronic commerce applications. While new technology has simplified many business and personal transactions, it has also opened the door to high-tech crime [22]. Many corporate people for their business activities, and common people for their daily work, use smart devices around the clock and throughout the globe. Tablets, Apple iPads, and Android-based phones are now being used by millions of employees worldwide to send and receive official information for business operations. These smart devices are embedded with many applications like software

utilities in office applications, phone call, email, WhatsApp, LinkedIn, Facebook, and Instagram are sending the data including audio, video, and entertainment apps. These devices need to be secured from the vulnerabilities from both physical mode and logical point of view. Not astonishingly, security has emerged as the primary challenge posed by the smart devices at par with BYOD (bring your own device). Therefore, both physical and logical security of devices is the need of the hour. Security services, like authentication and access control, have to be non-intrusive, intelligent, and able to adapt to the rapidly changing contexts of the spaces [23].

2.4.1 Physical Security

Physical security is one of the essential parts of smart and Internet of Things devices. Physical security includes not only the area containing system hardware but also locations of wiring used to connect the systems, supporting services, backup provisions, and any other part of the systems counting as smart devices. Physical things in a house include beds, fans, curtains, windows, bedsheets, chairs, and other home appliances like kitchen utensils among others. When installing a network or connecting our home to the home area network (HAN) and wide area network (WAN) or the Internet, we are building an infrastructure that people depend on. Security measures exist to ensure that the network and devices are reliable for home owners and their family members. For many installations, outages often occur due to human tampering, whether accidental or non-accidental. Networks have physical components, such as wires, modems, firewalls, boxes, and Wi-Fi devices, which can be easily disturbed. In many installations, people will not understand the purpose of the installed electronic equipment, and curiosity may lead them to experiment. They may not realize the importance of a cable connected to an I/O ports. Someone may unplug an Ethernet cable or turn our camera direction so that they can connect their laptop or smart mobile for 5–10 min or consecutively carry out the theft or move a switch because it is in their way. A plug might be removed from a power bar because someone needs that receptacle. Assuring the physical security of an installation is supreme, signs and labels will only be useful to those who can read our language. Putting things out of the way and limiting the access are the best means to assure that accidents and tinkering do not occur. Sometimes, people are so fond of smart devices, the latest gadgets, and electronic devices and do the theft by taking the opportunity. Smart washing machines, tumble dryers, air conditioners, refrigerators, electric water heaters, and electric space heating may come under this section. Hence, physical security is one of the vital aspects in smart devices communication security.

2.4.2 Logical Security

Logical security uses technology to allow individuals to access the data, information, things, devices, and systems based on who they are and what is their role within an organization or residential place or could be a network. Access to information resources should be restricted to those individuals with a need to access. Determining data and information ownership and access rights to the process for a monitor that individuals have appropriate access are all a part of an effective security strategy. The elements of logical security include authentication, privacy, policies' standardization, and monitoring. Security services, like authentication and access control, have to be nonintrusive, intelligent, and able to adapt to the rapidly changing contexts of the spaces. Logical security is in different methods as explained in the next following sections.

2.4.2.1 Authentication

Before being granted access to network resources and devices in the Internet of Things, users should first be authenticated. In an ideal world, every wired and wireless user would have an identifier that is unique, unchangeable, and addressable, which cannot be impersonated by other users. Otherwise, this will turn out to be a very difficult problem to solve in the realistic world. Consider a medical application in which patient's information is stored in medical information system (MIS) and health information system (HIS) records. The medical data access for authentication by several users including the hospital, medical practitioners, staff nurses, medical researchers, and insurers should be authentic. Devices should be secured with the help of CCTV/IP cameras/physical security guards. This authentication of smart people and smart devices is by different means including MAC address, QR codes, RFID, and IPv4/IPv6.

2.4.2.2 Medium Access Control (MAC)

One of the closest features in authentication is to have a unique identifier like the medium access control (MAC) address. This is the 48 bit number assigned by the manufacturer to every wireless and Ethernet device. By employing MAC filtering on our access points, we can authenticate users based on their MAC address. With this feature, the access point keeps an internal table of approved MAC addresses. When a wireless user tries to associate to the access point, the MAC address of the client must be on the approved list; otherwise, association will be denied. Alternately, the access point (AP) may keep a table of known and bad MAC addresses and not permit other devices that are not in the list. IEEE 802.15.4 MAC layer offers some facilities, which can be used by upper layers to achieve a good level of security. It is said that companies like alarm.com are taking advantage of wireless

networks to let one arm or disarm their system remotely, watch live videos, detect water in the basement, trigger real-time email notifications, and control critical systems like lights, thermostats, and small appliances remotely.

2.4.2.3 The Radio-Frequency Identification (RFID)

The radio-frequency identification (RFID) technology has advanced significance over several other technologies. RFID is a powerful technology, not only for automated inspection or identification of products but also for augmenting conventional positioning systems [24, 25]. Radio-frequency identification applications are in military, airline, library, security, healthcare, sports, animal farms, and others below. RFID is the wireless, noncontact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. Without proper security controls, tags embedded in consumer products could leak potentially embarrassing information. Even if the tag contents are secured, predictable tag responses could be tracked, violating one's location privacy [26]. In a bottom-up approach, cryptography is the cornerstone for network infrastructure protection. Although it is possible to implement existing standards, such as Advanced Encryption Standard (AES), some IoT devices, such as passive RFID tags, might be extremely constrained. Cryptographic mechanisms must be smaller and faster but with little or no reduction in security level.

2.4.2.4 Quick Response (QR) Code

QR code is one of the latest authentication techniques in which objects, things, or events can be identified or distinguished from the world. Once scanned through mobile, this code will take one to the main home page of that particular product description, which is given in detail. QR codes are two-dimensional barcodes that visually encode bits of information characterized as black square dots placed on a white square grid. QR code security protocols allow the code creator to protect data stored in QR codes by encryption. This allows the end users to verify that message did not tamper with the previous one. The initial usage of these codes is spread more in Japan, China, and the rest of world.

2.4.2.5 IPv4/IPv6

In comparison with IPv4, IPv6 has an increased set of capabilities to simplify end-system auto-configuration, which includes the automated discovery of routers, neighbor's resolution, duplicate address detection, and neighbor unreachability detection. Refer to Table 2.1. These enhancements bring along with them a different set of security vulnerabilities that must be addressed. According to Scott Hogg, IPv6 security author and CTO of GTRI, "All security practitioners should

Table 2.1 Comparison between IPv4 and IPv6

IPv4	IPv6
The address space is 32 bits	The space is 128 bits
The length of the header is 20 bytes	The length of the header is 40 bytes
Four bytes for each address in the header	Fifteen bytes for each address in the header
The number of header field is 12	The number of header field is 8
Checksum field, used to measure error in the header, required	Checksum field eliminated from the header as error in the IP header is very crucial
Internet Protocol Security (IPSec) with respect to network security is optional	Internet Protocol Security (IPSec) with respect to network security is mandatory
No identification to the packet flow (lack of QoS handling)	The flow-level field on the header portion identifies the packet flow and directs to the router (efficient QoS handling)
The fragmentation is done both by sending host and routers	The fragmentation is done both by sending host; there is no role of the routers
No identification to the packet flow (lack of QoS handling)	The flow-level field on the header portion identifies the packet flow and directs to the router (efficient QoS handling)
Clients have to approach the dynamic host configuration server (DHCS) whenever they connect to a network	Clients do not have to approach any such server as they are given permanent addresses
www.certiology.com , website accessed dated on	12/12/2015

learn about IPv6 now because all organizations have IPv6 capable and enabled operating systems in their environments. Failure to secure the IPv6 system is like allowing a back-door to exist.” There are 16 different tunnels and transition methods, not to mention upper layer tunnels. A general myth and misunderstanding about IPv6 is that it is more secure than IPv4. This assertion stems from the original mandated use of IPSec in host-to-host communication, as specified in RFC 2401. Certainly, if IPSec is implemented, it would provide confidentiality and integrity between two hosts, but it still would not address any link operation vulnerabilities, attacks, and most of the denial-of-service (DoS) attacks. DoS is one of the most aggressive and menacing intrusive behaviors. It severely degrades availability of a victim, such as a smart device or even the network by imposing computationally intensive tasks, using exploitation of system vulnerability. The victim is then forced to stop providing services for some time to other devices of the network. Hence, effective approaches for detecting DoS attack are significantly important to protect on-line services, and many efforts have been made to enable this process.

2.4.3 Security Tools and Software

Software is a set of logical instructions executed for problem solving. Securing software is a computer program designed to enhance information security. The

explosion of Internet traffic has created enormous demand for information system security professionals. In this mode, all files that the operating system (OS) opens or uses are scanned first before they are fully opened. Security must be addressed throughout the smart device software life cycle, right from the initial design, coding, and development to operational and maintenance environment. To deal with the distributed denial-of-service attacks, the information security personnel should ensure that critical network connections have enough bandwidth and redundancy to prevent easy attacks [27]. Authors of [28] have reported that lower connection speeds can easily be overwhelmed by the attacker. The distributed denial-of-service attacks cannot just be eliminated by having sufficient bandwidth; additional techniques for dealing with these attacks should also be employed [29]. This includes the installation of intrusion detection systems to foresee a possible attack [30], the intrusion detection systems as network burglar alarms, and listening to the network for traffic that matches common attack signatures stored in the database [31]. Security codes, motion detectors, and cameras provide information to a smart home security system, allowing it to determine whether an individual is a resident, a cleared visitor, or an intruder. Motion detectors trigger an alert, letting the artificial intelligence program know that there is someone or something to be evaluated. Facial recognition software and security codes allow the security system to allow residents into the home, while based on preprogrammed information restrict access to other individuals [32, 33]. The malfunctioning software in smart environments is of two/many forms including:

- **Mobile Viruses:** These can be the main threat, particularly with devices that have significant computational capabilities. Mobile devices, in general, are susceptible to viruses in several ways. Viruses can take advantages of security holes in applications or in underlying OS and cause damage. Applications downloaded to mobile devices like android can be as virus prone as desktop applications. In some of the mobiles, malfunctioning SMS can also crash the OS.
- **Bluejacking:** This refers to sending nameless, unwanted messages to other users with Bluetooth-enabled mobile phones or laptops. Bluejacking depends on the capability of Bluetooth phones to detect and contact another Bluetooth-enabled device. Bluejacking can be a problem if it is used to send obscene or threatening messages or images or to send advertising. If we want to avoid such malicious messages, we can turn off Bluetooth or set it to “undiscoverable.”

Apart from this, secure boot, when electrical power is first supplied to a smart device, and the authenticity and integrity of the system software on the smart device should be verified using cryptographically generated digital signatures. In the same way, the person who signed on a legal certificate through a digital signature attached to the software copy should be verified by the device to ensure only the duly authorized software to run on that device at the time of booting. The foundation of reliance has been established, but the device still needs protection from various runtime threats and malicious intents. Infineon Pvt. Ltd. and many other companies have developed a broad range of semiconductor technologies for counter-growing security threats. These technological solutions permit system

and device manufacturers as well as service providers to capitalize on growth opportunities by integrating the right level of security without compromising on user experience. Complemented by software and supporting services, their hardware-based products also create an anchor of trust for security, supporting device integrity checks, authentication, and secure key management.

2.4.3.1 System-Level Security

System-level security is essential for smart devices, computers, tablets, and servers. The firewall of smart devices should be always enabled in the operating system (OS) level. The device protocols in which the object or electronic device in a home area network (HAN), local area network (LAN), or world area network (WAN) should be defined very specifically. All the connected home devices are protected with login names and passwords. If it is required, one should keep double-level entry password security mechanisms like banking security systems. This ensures that third-party or rouge devices cannot steal personal home information. One should clearly caution one's children against even sharing the smart home security passwords with their friends. The same also applies to one's laptop and computer passwords, smart door key, smart gas connection, smart meter distribution, and any other locking smart fridge. Along with these, one should always update the latest versions of software. The patches will help for better smart device security operation level, leading to better and safe communication.

2.4.3.2 Antiviruses

Any smart device can be affected by malware. Malware software is an all-inclusive term for malicious programs like viruses, Trojan horse, worms, and spyware, which are designed to poison and take control of smart devices. One's smart device has been infected, rogues can capture all the keystrokes, steal one's vital information, and use the devices. Hence, antivirus software is required. Antivirus consists of computer programs that attempt to identify, prevent, and eliminate computer viruses and other malware software. Antivirus typically uses two different techniques to accomplish its mission: (1) examining files to look for known viruses matching definitions in a virus dictionary and (2) identifying suspicious behavior from any computer program that might indicate infection. Such analysis may include data captures, port monitoring, and other methods. These programs have two basic modes: (1) static file scanning, useful for when you have to scan a file to check to see if any of the files are currently infected with malware, and (2) real-time "dynamic" scanning, which is really what is needed to prevent the computer from getting infected in the first place. For better security, one should use fully licensed software with the latest/updated patches.

2.4.3.3 Firewalls

The firewall is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system as well as IoT devices. The same principle will work for all smart devices. A network firewall is similar to firewalls in building construction, because in both cases they are intended to isolate one “network” or “compartment” from one another. The successful use of a firewall is dependent on the selection of an appropriate product. Packet filtering in firewalls accepts or denies based on numerous rules that depend on the source and destination ports of packets and other diffusion criteria. The level of security for smart devices in the Internet of Things (IoT) depends on the customization/settings of the firewall software.

2.4.3.4 Monitoring

Monitoring the people or things or events using smart devices is one of the vital tasks in home/building/company. This can be done by CCTV (closed-circuit television) or IP (Internet Protocol) camera or human physical security. It is extremely difficult to monitor the objects/procedures in continuous in all the places without CCTV/IP cameras. For example, the number of participants and their safety in NITIE, Mumbai, in its convocations for 6 h without any hazardous can be possible using IP cameras. Another example is the monitoring of growth patterns of rose/lotus/jasmine plant using Koubachi sensor for its life. The Sensor will give notifications to its user’s smart mobile about basic requirements of light, hydrogen, humidity, oxygen, and carbon dioxide measurements.

CCTV/IP Camera

We know that an IP camera [34] is a video camera that can be directly connected to the Internet without the need of a separate computer. Camera devices are in use in public places as well as in homes which have the capacity to gather large amounts of image material. Fortunately, for the time being, there are effective ways to analyze the mass of video data automatically and recognize potential risk situations in advance by analytical software. In industrial plants, CCTV equipment may be used to observe parts of the process from a central control room, when the environment is not suitable for humans. CCTV [35] systems may operate continuously or only as required to monitor a particular event. [36] have worked upon calibration techniques of CCTV camera. CCTV is one part of the solution and not a panacea for public safety and security. CCTVs improve public perception of safety and deter and displace antisocial behavior and crime. For applications network security is an important concern; the deployment of IP cameras in the network address translation (NAT) environments with dynamic locations is usually desired. However, without static IP address information, accessing the Web server

associated with IP Cameras will be difficult [37]. In the mining applications, IP cameras and RFID devices are being used very effectively in order to provide security for workers and detection of landslides or unexpected explosion of water sprouts in 24×7 round the years.

Wireless Sensor Network (WSN)

WSN is one of the most popular forms of connected smart devices deployed in smart home or smart office security systems. They often integrate various wireless devices into our home to enable remote intruder detection and image streaming to our cell phone over a combined security platform, which can be remotely controlled from our mobile device. Security plays an important role in WSN since the nodes are exposed to attacks even in a ruthless environment. The original motivation behind the research into WSNs was military applications. Examples of military sensor networks include large-scale acoustic ocean surveillance systems for the detection of submarines, self-organized and randomly deployed WSNs for battlefield surveillance, and attaching microsenors to weapons for stockpile surveillance [38]. According to the author Suraiya Tarannum in his book *Wireless Sensor Networks*, the application space for WSNs is quite large and continues to expand vigorously, encompassing habitat, ecosystem, seismic and industrial process monitoring, security, and surveillance as well as rapid emergency response and wellness maintenance. The lifetime of the network can be enhanced by providing security and privacy against network layer attacks when the nodes are scattered in an unsupervised environment. In order to protect a network, few of the routing protocols such as sensor protocols for information via negotiations [39] and path redundancy-based security algorithm for homogeneous-based wireless sensor networks [40] address the security mechanism and authentication against the various attacks. Some of the secured routing protocols of heterogeneous sensor networks [41] can detect the malicious nodes and deliver the packets to sink successfully. wireless sensors networks are vulnerable to many types of attacks.

As WSNs are based on communication standards and data sent over a broadcast channel, it is possible to make packet sniffing and data spoofing attacks. In recent years, there have been many proposals using cryptography to ensure secure communication [42]. Nevertheless, cryptography alone is not sufficient for node compromise attacks and novel misbehavior in sensor networks [43]. However, in the future, the security software developers or coders should keep in mind 100 % security mechanisms while writing the codes of applications.

2.5 Privacy of Smart Devices

The term privacy is derived from the Latin word “privatus” [44] and “privo”, meaning to deprive [45]. In English language dictionaries, privacy is defined as “withdrawal from public view or company and one’s private life” [46]. The term

privacy is used frequently in ordinary language as well as in philosophical, political, legal discussions and the Internet of Things (IoT), yet there is no standard single definition or analysis or meaning of the term. Perceived privacy has long been accepted as the right of individuals, groups, or institutes, and they decide for themselves when, how, and what kind of information they need to deal with during communication with others [47].

With the advancement of the digital age and IoT technology, personal information vulnerabilities have increased. Information privacy may be applied in numerous ways, including encryption, authentication, and data masking—each attempting to ensure that it is available only to those with authorized access. Information privacy is considered an important aspect of information sharing during smart devices' communication. The need to maintain information privacy is applicable to collected personal information, such as medical records, financial data, criminal records, and political information. According to [48], perceived privacy includes both reliability and credibility dimensions, which are related to sharing of information among users of IT. During communication on the website, many users handle a lot of information on certain procedures. Credibility and reliability, thus, are important issues in these transactions [49]. Jingjun [50] says that mobile nodes in the IoT often move from one cluster to another, in which cryptography-based protocols are required to provide rapid identification authentication and privacy protection. In an advanced technological communication of the Internet of Things, where each and every object is connecting to object-human-machine to communicate, credibility and reliability are essential. All the private data generated by things should strictly follow security standards.

A single-step protocol was presented for the occasion that the mobile node joins a new cluster. The literature describes teenagers as active users of social media, who seem to care about privacy, but who also reveal a considerable amount of personal information. There is an evidence that concerns about who would get access to their health information or learn about their medical consultation affect actual or intended healthcare-seeking behaviors by adolescents [51, 52]. Burgoon defined social privacy as having control over the actual interaction with others and the frequency, length, and content of that interaction. Psychological privacy protects the individual from intrusions upon one's thoughts, feelings, and values and the freedom to decide to whom to disclose certain personal thoughts and feelings. Informational privacy refers to the ability to control whoever gathers and disseminates information about oneself and under what circumstances. Hence it is an eleventh hour that we need to work for the development of devices with privacy.

2.6 IT Act 2000

Much has been talked about the Internet of Things and smart devices. Embedded networked devices including sensors and actuators are everywhere nowadays. They are in our fridges and on our washing machines. They are in our smartphones, our

houses, hospitals, offices, ships, planes, buses, trains, and automobiles. Some of the smart devices are helping us do exercise enough for good health and measuring our sleep. In this light, Internet of Things security mechanisms are essential in the mushrooming Cyber-Physical Systems arena. Indian (Information Technology) IT Act 2000 started in 2000 to look after IT communication issues. Later, the Indian Ministry of IT department released a new version in 2008, in the form of IT Act 2008. Besides, the Energy Independence and Security Act (EISA) of 2007 gave the National Institute of Standards and Technology (NIST) primary responsibility to coordinate development of a framework that includes protocols and model standards to achieve interoperability of smart grid devices and systems. In the same way, there needs to be an IoT act, device standards to cooperate, monitor, and control miscommunication of text, pictures, audio, and videos. In October 2012, the government of India unveiled its plan of training around 500,000 cybersecurity professionals in its 5 year plan. However, India's cybersecurity industry was practically nonexistent. Most of the Indian IT companies depend on international service providers to overcome their security threats. The consequent lack of a job market has also resulted in the education system completely ignoring the cyber security field. Most of Indian technical educational institutes do not even offer the cyber security subject as a specialization. They concentrate more on lucrative subjects like software design, development, and languages like C, C++, testing, DBMS, Oracle, and Web portal. The best part is that recently Gujarat University started a course on data, forensic, and Cyber laws. In today's technological arena, data and information are perchance the key to fighting any kind of crime. That is why safe city projects got initiated in 1992. In India with an investment of circa 1200 crore rupees, the security project is aiming to install approximately 1700 CCTVs. These are being mounted at more than 50 public markets and 15 national borders. In addition to these places, they are present at almost every critical traffic intersection. This array of IP Cameras and CCTVs would create a web of surveillance setup that would form a foundation of the integrated intelligence surveillance systems. In this light, Surat City in Gujarat (India) is also one of the best examples in IP camera installations in the city public places for prevention of crimes. This project was mainly supported by public funds. These security systems generally seamlessly pass the data to police departments through their PDAs for crime analysis. Even in Delhi, the capital city of India, the public places are fixed with IP cameras for social security. Mobile apps can also be downloaded in smart mobiles at no charge. During emergencies, anybody can easily call number (911), which will give complete details of a victim with the location using GIS technologies. At the global level, the New Zealand Police, a national law enforcement agency, is using Intergraph Mobile Responder apps (software), which allow police officers to access real-time data about events for enhanced public safety.

Software can be protected by hardware. Secured hardware protects the processing and storage of code using encryption, fault and manipulation detection, and secure code and data storage. Software programs thus become trustworthy by combining it with secured hardware. This has been proven by extensive experience

in trusted computing, the use of secured elements in mobile phones, and protection of smart grids. In all of these cases, secured hardware provides the extra protection needed for security-sensitive code and data. To protect both privacy and smart device data security, M/s Emory Company has created a new smart device security policy that lays out security requirements for both Emory-owned and personally owned devices that access Emory exchange email or store-sensitive information. This policy does not grant Emory access to information stored on our devices; it only requires a handful of security settings to be enabled, including a four-digit password and data encryption technique.

Security of the IoT raises numerous open legal and ethical issues that are currently being addressed at academic, research, corporate, government, and personal levels. Many of these issues are raised for some clear conflicts between the global versus national interests and government versus public interests. These IoT security policies and associated Codes of Practice set out the responsibilities for ensuring the security of IoT devices within personal or within the organization or within the home network or global level. The contents of respective legislation must encompass right to information, provisions prohibiting or restricting the use of mechanisms of the Internet of Things, and rules on IT security legislation [53]. The procedures to be followed to safeguard resources provide confidentiality and integrity of the information held thereon.

2.7 Methodology

This chapter is basically conceptual and grounded on the secondary data in various research articles, general articles, and corporate white papers which are grounded on on-line database. Besides the experience of the authors in the same domain on both information technology (IT) and computer science (CS) and working on the research topic “Internet of Things Technologies” since 2012 made the concepts very clear to authoring this manuscript. The beauty of this artifact is that it is composed of various thought processes gathered from authors’ and experts’ discussions in conferences, workshops, and symposiums on this topic. The data was in different formats including text, picture, and videos. The research method used here is exploratory, qualitative research type, and with a thematic narration.

2.8 Discussion and Conclusion

When all things are connected to the Internet and are ready to be accessed from the smartphones and other PDAs from anywhere at anything for any services, the security issues should not be nullified. Security of smart devices, basically into the assessment of the risk of threats which causes some loss of value to devices, is heightened through device vulnerabilities. For better security, the safeguards can be

detection, prevention, and correction. Today's development of smart labels, memory amplifiers, and smart dust seems to mirror the sudden technology shifts by Warren and Brandeis, opening up new forms of social interactions that change one's expectation of privacy or secrecy.

Devices may be left unsecured because their owners expect that they will remain in their physical control; however, if they leave the physical control of their owners, they are open to be used by anyone. Hence, physical security through surveillance systems is essential. There should be ethical design, development of smart hardware, and software from the software coders or developers along with proper deployment in appropriate applications. The international standardization bodies have to monitor the development of devices, software, and networks. Ultimately, there should be trustworthy interoperability among the Internet of Things devices to get connected. The end user/netizen also plays an important role in accessing the data and information. People have to practice international cybersecurity laws for smooth and better communication. There should be punishment for cybercrimes in order to prevent data miscommunication. The International Telecommunication Union (ITU), Institute of Electrical and Electronics Engineers (IEEE), Internet of Things-Architectures (IoT-A), and National Institute of Standards and Technology (NIST) are some of the global standardizing institutes in device standards and communication without any security breaches. The smart device security is becoming a basic need nowadays in this technical world. Hence, it is a need of hour for smart device security under the umbrella of the IoT.

References

1. Carabelea C, Boissier O (2003) Multi-agent platforms on smart devices: dream or reality. In: Proceedings of the Smart Objects Conference (SOC03), Grenoble, France, pp 126–129
2. Noda C, Walter T (2005) Smart devices for next generation mobile services. In: Construction and analysis of safe, secure, and interoperable smart devices. Springer, Berlin Heidelberg, pp 192–209
3. Kang Y, Kim H, Suzuki H, Han S (2015) Editing 3D models on smart devices. *Comput Aid Des* 59:229–238
4. Doukas C (2012) Building internet of things with the arduino. CreateSpace, North Charleston
5. Doody P, Shields A (2012) Mining network relationships in the Internet of things. In: Proceedings of the 2012 international workshop on Self-aware Internet of Things. ACM, pp 7–12
6. Yuan Y, Ma L, Zhang J (2014) Patented network analysis on cloud computing technology in internet of things. In Identification, information and knowledge in the internet of things, 2014 International Conference, Beijing, IEEE, pp 248–251
7. Agrawal S, Das ML (2011) Internet of things: a paradigm shift of future internet applications, Engineering (NUICONe), Nirma University International Conference, Ahmedabad (India) IEEE, pp 1–7
8. Yong W et al (2006) A Survey of security issues in wireless sensor networks. *Commun Surv Tutorials IEEE* 8:2–23
9. Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. *Comput Netw* 54:2787–2805

10. Coetsee L, Eksteen J (2011) The internet of things—promise for the future? An introduction. In: Proceedings of the IST Africa 2011, Gaborone, Botswana, 11–13 May
11. Mattern F (2003) From smart devices to smart everyday objects. In: Proceedings of smart objects conference, April 2003
12. Ramparany F, Boissier O, Brouchoud H (2003) Cooperating autonomous Smart Devices. In Proceedings of the Smart Objects Conference (sOc'2003), Grenoble, France (pp.182–185)
13. Maiwald E (2004) Fundamentals of network security. McGraw-Hill Technology Education, New York
14. Cirani S, Ferrari G, Veltri L (2013) Enforcing security mechanisms. In: IP-based internet of things: an algorithmic overview algorithms, ISSN 1999-4893
15. Mayer CP (2009) Security and privacy challenges in the internet of things. In: Proceedings of the KiVS workshop on Global Sensor Networks (GSN09)
16. Gessner D, Olivereau A, Segura AS, Serbanati A (2012) Trustworthy infrastructure services for a secure and privacy-respecting internet of things, pp 998–1003
17. Zhang XM, Zhang N (2011) An open, secure and flexible platform based on internet of things and cloud computing for ambient aiding living & telemedicine, pp 1–4
18. Heer T, Garcia-Morchon O, Hummen R, Keoh SL, Kumar SS, Wehrle K (2011) Security challenges in the IP-based internet of things. *Wirel Pers Commun* 61:527–5421
19. Srivastava L (2006) Pervasive, ambient, ubiquitous: the magic of radio. In: European Commission conference, From RFID to internet of things, Bruxelles, Belgium
20. Suo H, Wan J, Zou C, Liu J (2012) Security in the internet of things: a review. In: Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on, vol 3, pp 648–651, IEEE
21. Gariup M (2013) European security culture: language, theory, policy. Ashgate Publications
22. Pfitzmann A, Pfitzmann B, Schunter M, Waidner M (1997) Trusting mobile user devices and security modules. *Computer* 2:61–68
23. Al-Muhtadi J, Ranganathan A, Campbell R, Mickunas MD (2003) Cerberus: a context-aware security scheme for smart spaces. In: Pervasive computing and communications, (PerCom 2003), Proceedings of the first IEEE international conference on. IEEE, pp 489–496
24. Roman R, Najera P, Lopez J (2011) Securing the internet of things. *Computer* 44(9):51–58. doi:[10.1109/MC.2011.291](https://doi.org/10.1109/MC.2011.291)
25. Takizawa O, Hosokawa M, Takanashi K, Hada Y, Shibayama A, Jeong B (2008) Pinpointing the place of origin of a cellular phone emergency call using active RFID tags. In: Proceedings of 22nd international conference on advanced information networking and applications—workshops, Gino Wan, Okinawa, Japan, pp 1123–1128
26. Weis SA (2003) Security and privacy in radio-frequency identification devices. Doctoral dissertation, Massachusetts Institute of Technology
27. Li B, Li W (2008) Logistics information fusion application research based on RFID and GPS. In: Proceedings of 27th Chinese control conference, China, pp 389–393
28. Manion M, Goodrun A (2000) Terrorism or civil disobedience: towards a hacktivist Ethic. *ACM SIGCAS Comput Soc* 30(2):14–19
29. Katz FH (2006) Campus-wide spyware and virus removal as a method of teaching information security. In: Proceedings of the 3rd annual conference on information security curriculum development, 1–4
30. Nolan J, Levesque M (2005) Hacking human: data-archaeology and surveillance in social Networks. *SIGGROUP Bull* 25(2):33–79
31. Sukhai NB (2004) Hacking and cybercrime. In: Proceedings of 1st annual conference on information security curriculum development, pp 128–132
32. Nicks V (2009) AI enhances the smart home security system
33. Robles RJ, Kim TH, Cook D, Das S (2010) A review on security in smart home Development. *Int J Adv Sci Technol* 15: 13–22
34. Yung, Nelson HC, Pang Grantham KH, Fung George SK (2000) A novel camera calibration technique for visual traffic surveillance. In Proc

35. Ganeriwal S, Srivastava MB (2004) Reputation-based framework for high integrity sensor networks. In Proceedings of ACM SASN
36. CCTV Digital Video Recorders (DVRs), sourcesecurity.com. Retrieved 29 June 2013
37. Hintermaier W, Steinbach E (2010) A system architecture for IP camera based driver assistance applications, IEEE Intelligent Vehicles Symposium (IV), San Diego, 21–24 June, pp 540–547
38. Dagada R, Eloff MM (2013) Integration of policy aspects into information security issues in South African organizations. 7(31):3069–3077, 21 doi:[10.5897/AJBM12.979](https://doi.org/10.5897/AJBM12.979)
39. Pister KSJ (2000) Military applications of sensor networks, of Institute for Defence Analyses, Paper P-3531, Defense Science Study Group
40. Perrig A, Szewczyk R, Wen V, Culler D, Tygar JD (2001) SPINS: security protocols for sensor networks. In: Proceedings of ACM annual international conference on mobile computing and networking, pp 189–199, ISBN:1-58113-422-3, Rome, Italy
41. Sami, Al-Wakeel S, Al-Swailem A (2007) PRSA: a path redundancy based security algorithm for wireless sensor networks. Proceedings of IEEE wireless communication and networking conference, pp 4156–4160, ISBN: 1-4244-0658-7, Kowloon, China
42. Xiaojiang Du, Sghaier Giyani, Yang Xiao, Hsiao-Hwa Chen (2006) A secure routing Protocol for heterogeneous sensor networks. In: Proceedings of IEEE Global Telecommunication Conference (GLOBECOM'06), pp 1–5, ISBN: 1-4244-0356-1, San Francisco, California, December, IEEE
43. Perrig A (2001) SPINS: security protocols for sensor networks. In Proceedings of ACM MobiCom
44. Chien-Min Ou, Wei-De Wu (2012) Automatic service discovery of IP cameras over wide area networks with NAT traversal. Adv Int Things 2:23–36
45. Curtin L (1981) Privacy: belonging to oneself. Perspect Psychiatry Care 19(3–4):112–115
46. Rawnsley M (1980) The concept of privacy. Adv Nurs Sci 2(2):25–31
47. Webster's New World Dictionary (1986) Prentice-Hall, New York
48. Westin A (1967) Privacy and freedom. Atheneum, New York
49. Yousafazi SJ, Plister JG, Foxall GR (2003) A proposal model of e-trust for electronic banking. Technovation 23:847–860
50. Choate T (2000) 5 keys to customer conversion, Catalog Age, I Merchant, August, 14–15
51. Jingjun Miao, Liangmin Wang (2012) Rapid identification authentication protocol for mobile nodes in internet of things with privacy protection. J Netw 7(7):1099–1105
52. Britto MT, Tivorsak TL, Slap GB (2010) Adolescents' needs for health care privacy. Paediatrics 126:1469e76
53. Weber RH (2010) Internet of things – new security and privacy challenges. Comput Law Secur Rev 26(1):23–30

Connectivity Frameworks for Smart Devices
The Internet of Things from a Distributed Computing
Perspective

Mahmood, Z. (Ed.)

2016, XIX, 356 p. 98 illus., 57 illus. in color., Hardcover

ISBN: 978-3-319-33122-5