Security Challenges of the Internet of Things

Musa G. Samaila, Miguel Neto, Diogo A.B. Fernandes, Mário M. Freire and Pedro R.M. Inácio

Abstract The Internet of Things (IoT) is an environment in which ordinary and complex consumer products, buildings, bridges, animals or even people, etc. are embedded with sensors, equipped with a variety of communication technologies and given unique identifiers that can enable them connect to the Internet. This allows them to talk to each other, collect data and transfer data over the Internet. IoT has the potential to enhance the way we do things by increasing productivity and efficiency. It also has the prospects of delivering significant business benefits. Nonetheless, implementing secure communication in the IoT and integrating security mechanisms into some of its devices have been a major impediment to its progress, resulting in many privacy concerns. Although IoT is a hybrid network of the Internet, many security solutions for the Internet cannot be directly used on the resource-constrained devices of the IoT, hence the need for new security solutions. In this chapter, we discuss the security challenges of the IoT. First, we discuss some basic concepts of security and security requirements in the context of IoT. We then consider fundamental security issues in the IoT and thereafter highlight the security issues that need immediate attention.

M.G. Samaila (✉) · M. Neto · D.A.B. Fernandes · M.M. Freire · P.R.M. Inácio
Department of Computer Science, Instituto de Telecomunicações, University of Beira Interior, Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal
e-mail: mgsamaila@it.ubi.pt

M. Neto
e-mail: migasn@gmail.com

D.A.B. Fernandes
e-mail: dfernandes@penhas.di.ubi.pt

M.M. Freire
e-mail: mario@di.ubi.pt

P.R.M. Inácio
e-mail: inacio@di.ubi.pt

M.G. Samaila
Centre for Geodesy and Geodynamics, National Space Research and Development Agency, P.M.B. 11, Toro, Bauchi State, Nigeria

J.M. Batalla et al. (eds.), *Beyond the Internet of Things*,
Internet of Things, DOI 10.1007/978-3-319-50758-3_3

1 Introduction

Internet of Things (IoT) is a paradigm and concept of ubiquitous connectivity, where nearly all virtual and physical electrical *things/objects* (electrical appliances) are expected to be embedded with Internet Protocol (IP) suite to enable them to connect to each other via the Internet. Using unique identifiers, these innumerable connected smart devices can communicate over multiple networks, forming a larger IP based network of interconnected *things*, or an ecosystem of connected *devices* [1]. The devices include common *things* such as lamps, bread toasters, wearable devices, toothbrushes and virtually every useful *thing* one can imagine. Other devices that participate in this communication include embedded sensor devices used in Machine-to-Machine (M2M) communications, implantable and other medical devices, smart city, smart energy grids, Vehicle-to-Vehicle (V2V) Communications, etc. Another essential component of the IoT phenomenon is the Machine-to-Human (M2H) communication. Constrained devices with limited computational power, memory and energy resources, and having lossy network channels like Wireless Sensor Networks (WSNs) responsible for information gathering also constitute an integral part of the IoT ecosystem.

The enabling technologies that will drive the future of IoT include sensor technology, Radio Frequency Identification (RFID) [2], Micro-Electro-Mechanical Systems (MEMS) technology, nanotechnology and smart things, energy harvesting, cloud computing along with the ongoing evolution of wireless connectivity and the transition towards Internet Protocol Version 6 (IPv6). The interaction between these technologies is breeding a new form of communication that is enabling seamless exchange of information between systems, devices and humans, thereby serving as an enabling platform for the IoT. Consequently, ordinary electronic devices and many other *things* are now manufactured with communications, computing and digital sensing capabilities. Such functionalities enable these devices to sense their environment and participate in data exchange. Thus, *things* are said to have *digital voice*.

Just like the Internet, this ecosystem of connected *objects* has the potential to change virtually everything in the world [3]. Today, IoT is rapidly becoming one of the most hyped technologies in both academia and industry. Moreover, the transition from the use of traditional devices to the use of Internet connected smart devices is accelerating at an alarming pace. As a growing network of everyday *objects*, IoT represents the next major economic revolution that will be enabled by the Internet [4]. Experts believe that we are entering into a new era, one in which the IoT will replace the traditional Internet that we know today. In this new era of connectedness, business playing ground is swiftly changing as a result of the impact of IoT, which is now creating new business opportunities, new sources of revenue and improved processes. According to Gartner, the global economic benefits of IoT will be close to $2 trillion [5]. Gartner also says that 4.9 Billion *things* will be connected before the end of 2015 [6], 6.4 billion in 2016 [7], and the number is expected to reach 25 Billion in 2020 [6] as more light bulbs, wearable devices like

watches, and cars connect to the Internet. Additionally, in order to consolidate business operations around the IoT, companies and researchers are coming up with more innovative solutions for the IoT [8, 9]. This is good news for operators, investors and every player with a stake in the IoT.

In spite of the potential advantages and benefits of IoT, and the fact that it is affecting increasing number of businesses and creating new exciting opportunities, however, there are still many security and privacy challenges that need to be addressed if IoT is to be willingly embraced by the business community, policy makers and the society at large. The idea of interconnecting incalculable number of remotely controlled smart devices (some of which are resource-constrained) via the Internet is raising alarms about security and privacy of users. This chapter, therefore, is focused on examining and describing the relevant security and privacy challenges posed by IoT connected devices that have been identified in the literature, and the difficulties of dealing with them. We focus specifically on connected devices that have limited resources in terms of memory, computing power and energy.

This chapter is structured as follows. Section 1 presents a brief overview of IoT, where we briefly consider the enabling technologies, the prospects and the need for securing the IoT. Section 2 looks at the concepts of security in the IoT. Section 3 examines the fundamental IoT security issues. Section 4 highlights some IoT security issues that need immediate attention. Finally, Sect. 5 presents our conclusions.

2 Concepts of Security in the Internet of Things

In this section we discuss some basic concepts of IoT security. Specifically, we present a general overview of IoT security, security goals for IoT, where the IoT security becomes delicate, size and heterogeneity of *things*, and the privacy concerns in the IoT.

2.1 A General Overview of Internet of Things Security

As the economic, social and technical significance of IoT is growing day by day, IoT is not only attracting the interest of investors, users and researchers but also nefarious users who are working hard to turn connected devices into weapons for cyber attacks or stealing data. Although the general idea behind the creation of IoT is to make life easier, it is obvious that interconnecting a large amount of non-traditional computing devices, such as smart water sprinklers and smart refrigerators, over the Internet, can be dangerous, and will bring a major change to individual and enterprise security and privacy. This is because a couple of security issues on one device can affect a number of devices on the same or different

network. An attacker can, for example, use compromised connected devices like smart TVs to launch Denial-of-Service (DoS) or Man-in-the-Middle (MitM) attacks on other networks and services. For instance, security researchers from Proofpoint [10] revealed cyber attacks that may probably be the first IoT botnet attacks to be using about 100,000 ordinary smart household gadgets including smart TVs, home-networking routers, connected multi-media centres and a refrigerator. The attacks were observed between December 23, 2013 and January 6, 2014, in which hackers used the compromised appliances and sent out about 750,000 malicious spam emails, targeting a number of enterprises and individuals all over the world.

While security and privacy concerns in the Internet are not new and still present challenges, security and privacy issues in the IoT pose additional and unique challenges. Due to the increasing popularity of the IoT, it is certain that more and more varieties of devices that gather all sorts of data will be deployed or embedded into different systems, organizations, homes, etc. As this massive data capturing activities constantly increase, concerns for corporate and individuals security and privacy will also increase. Most of these devices pose a number of potential security risks that could be exploited by malicious entities to harm legitimate users. Given the capabilities of some of the smart devices, some users may not even know that they are being recorded or tracked.

As IoT devices generate more data, protection of data will continue to be an issue. As a consequence, IoT is hardly safe for processing sensitive information, especially as the technology become more pervasive and integrated more into our everyday lives. The staggering variety of devices comprising the IoT along with the different constraints associated with such devices further compound the problem. One motivating factor that will make the IoT data a more attractive target for malicious users is the fact that data is directly accessible over the Internet, and can potentially be accessed through poorly secured smart devices that have little or no security measures. Hence the need to ensure that each device is properly secured is of paramount importance. Addressing such challenges and ensuring security in the IoT would prevent intruders from exploiting vulnerabilities that could be used to compromise personal information.

2.2 Security Goals for the Internet of Things

As a fundamental component of every network design, security is among the biggest obstacles standing in the way of full deployment of the IoT. Recently, there have been numerous successful attacks on the IoT. Some of the attacks come from white hat hackers who want to examine the performance of these IoT devices and find out how vulnerable they are to intrusion. Other attacks come from malicious entities who exploit known vulnerabilities in such devices in order to discover sensitive information for personal gain. Considering the rising incidence of cyber attacks targeting the IoT [11], there is need to plan and implement a good security strategy for the IoT. This can only be achieved if new security goals are identified

and implemented in the design process of IoT devices and systems. Introducing security goals or requirements early in the design process can help fortify information security, reduce risks and improve risk management.

Security goals (or requirements) are basically the fundamental principles that describe functional and non-functional objectives needed to be satisfied so as to achieve the security features of a system. Explicitly outlining security goals is key to baking security into a design process. In information security, there are three fundamental principles of security, namely confidentiality, integrity and availability, which are often referred to as the CIA triad. These fundamental principles have been broadened over time to include other security requirements such as authentication, access control, non-repudiation and privacy preservation. Essentially, these fundamental principles constitute the central objective of any security program of an Information Technology (IT) system. Usually, every security mechanism, safeguard and control is put in place in order to provide one or more of these requirements. Similarly, every threat, risk and vulnerability is evaluated for its potential ability to compromise one or more of these principles. But since every system has unique security goals, the level of security needed to achieve these requirements differ from one system to another. The same also applies to all IoT systems.

Considering the diversity in IoT system functions, device types and deployment locations, there is no *one size fits all* set of security requirements that can be effectively used for every application area within the IoT ecosystem. Although IoT systems vary considerably from one application to another, some applications may share common security goals [12]. The principal IoT security requirements to counter most security threats can be characterized according to the following fundamental security attributes [13, 14], namely confidentiality, integrity, availability, authentication, access control, non-repudiation, secure booting and device tampering detection. It is important at this juncture to state that, depending on its area of application, an IoT system or device may require some, all, or more of the above security requirements. Similarly, the degree of implementation of a particular requirement depends on the application scenario, for example, some scenarios may require low, medium or high degree of implementation. Below is a brief description of the given security requirements.

2.2.1 Confidentiality

Connecting unsecured, small and inexpensive smart devices to the Internet exposes users to massive security risks. Vulnerabilities in such devices serve as entry points through which cyber-criminals can access private or corporate assets. No doubt, IoT presents potential for greater comfort and efficiency at home and in workplace, thereby improving living conditions. However, without proper security measures, such benefits may turn into nightmare.

Data confidentiality is an important security requirement that ensures that only those authorized to view the information are given access to the data and that no sensitive information gets to unauthorized persons. Lately [15, 16], there are growing concerns over data confidentiality in the IoT, since connected devices are sometimes used for transmitting confidential data. The level of confidentiality needed depends on application scenario and implementation. For instance, the level of confidentiality required for securing smart water sprinklers will definitely not be the same as that required to secure devices in critical sectors like the healthcare industry. The measures needed to be undertaken in order to provide End-to-End (E2E) message secrecy in the case of patient confidentiality should be strong enough such that access is restricted to only those authorized to view the message.

2.2.2 Integrity

IoT devices often store sensitive user data locally. For example, a user can store bank details, social security number, contacts, travel preferences and favourite music play lists. A number of people have concerns that their sensitive data could be accessed or manipulated over the IoT. Apart from personal user information, network service providers and manufacturers of smart devices can, as well, store important data on a device. The data can contain sensitive information, such as billing and payment records, usage statistics, business secrets and decryption keys. Intentional or unintentional alteration or deletion of such data can be traumatic, hence the need for information integrity protection.

In the context of IoT, integrity is maintaining the accuracy, consistency and trustworthiness of data in transit or stored on any IoT device. There should be assurance that information cannot in anyway be modified by unauthorized entities.

2.2.3 Availability

Availability in the IoT ensures that a system or a service is available to authorized users, and that authorized users have access to every data they are authorized to access. Thus the connectivity of an IoT device or service must persist even if there is a link failure, which necessitates the need for link handover whenever a link fails.

The best way to ensure availability is by performing hardware repairs as soon as a problem occurs, carrying out a regular preventive maintenance of all hardware and ensuring that the Operating System (OS) is free of any software conflicts and is up to date. In addition, other software on the system must remain updated. It is also important to maintain an immediate and adaptive recovery in worst case scenarios. Backup copies of data should be stored in safe locations to safeguard against data loss in case of a natural disaster, such as fire or flood.

2.2.4 Authentication

Authentication is a property that ensures that a transaction or any other exchange of information is from the source it claims to be from. This implies that all IoT devices must be able to prove their identity in order to maintain authenticity. Device authenticity can be verified through authentication, which involves proof of identity. This happens whenever a device is connected to a network. Device authentication enables a device to access a network based on identical credentials stored in a safe location. The device authenticates itself prior to receiving or transmitting any information. In most cases the process of authentication involves more than one proof of identity.

Parts authentication is also an essential requirement that should be considered in IoT system design. It will ensure that no third party components with potential security risks are connected to the system. Additionally, it has the potential to allow secure in-service upgrades as a result of the code-signing confirmation that authenticate the identity of every firmware source.

2.2.5 Access Control

Access control refers to the security attribute that allows only authorized entities to access a resource, such as sensor data, file or website. In the context of IoT, access control enables secure interaction between devices. It determines who is allowed to access some resources, and limits the privileges of device Applications (apps) and components so that they can only access resources necessary for their normal operations. Access control is needed in an IoT system to ensure that only trusted entities can update device software, command actuators, perform device configuration operations or access sensor data. An efficient access control also enables the creation of new business services that allow customers to access some information like sensor data after payment.

Authentication is an essential ingredient for access control, since in order to control access both users and devices must be identified. IoT, however, poses a distinctive set of challenges due to highly constrained computational power, memory and low power requirement of many IoT devices along with the nature of deployment of some devices. As such, some standard authorization models like Access Control List (ACL) and Role Based Access Control (RBAC) may not apply directly [17].

2.2.6 Non-repudiation

In the IoT context, non-repudiation is a security property that provides available proofs that will prevent any user or device from denying an action, such as message exchange. It ensures the availability of evidence, usually through a Trusted Third Party (TTP). The evidence should make the transfer of credentials between entities

undeniable. It is also possible to use the process of data monitoring in non-repudiation to identify potentially compromised *things*.

Non-repudiation is usually not considered as an important security requirement for many IoT application scenarios. But for business applications that involve payment for services [18], non-repudiation is an indispensable security property that will prevent users and service providers from denying payment action. The greatest bottleneck, however, for implementing non-repudiation in some IoT devices is the challenge that using attestation on resource-constrained devices poses.

2.2.7 Secure Booting

As one of the foundations for security in a device, secure booting blocks any attempt to run different software on an IoT device when switching it on. It is a technique that asserts and verifies the integrity of an executable image before control is passed to it. This is the security property which ensures that device firmware has not been tampered with. As soon as power is introduced to an IoT device, the integrity and authenticity of the software running on the device is verified using digital signatures that are generated cryptographically. The digital signature on the software image that is verified by the device ensures that only authorized software that has been signed by the entity that authorized it is allowed to run on the device.

Secure booting requires specific hardware capabilities, since it is implemented using cryptographically signed code provided by the manufacturer along with the hardware support that will verify the authenticity of the code. This further highlights the need for baking security in the device itself [19].

2.2.8 Device Tampering Detection

Device tampering detection is a security requirement that ensures that any attempt to tamper with an IoT device, whether logically or physically, is detected [20]. Although some new Micro-Controller Units (MCUs) have some advanced memory and code protection capabilities that protects against unauthorized access, the use of these tamper-resistant protections may not always provide the required protection, or may not be available.

A large number of IoT devices like sensors are deployed in open environments, allowing attackers to have direct contact with them. In addition, some skilled attackers can even take them to their lab for analysis. Example of IoT devices that are likely to be targets for hardware tampering include sensor nodes and IoT wearable devices.

2.3 Where Internet of Things Security Becomes Delicate

While security considerations are not new in IT networks, IoT poses unique security challenges for both individual users and companies. Given the potential pervasive nature of the IoT devices and services, it will not be inappropriate to say that computers have now spread from our desktops to almost every aspect of our lives. They are now found as tiny devices in our pockets, on our wrists, implanted in the body of some animals and humans, and embedded in cars and almost all the everyday gadgets we use [21]. While we may not think of some of these small devices as computers, they can collect, process, store and share vast amounts of data.

In contrast to the paradigm of traditional computer systems that are usually protected inside the secure perimeter of enterprise networks, most devices comprising the IoT are poorly secured, some are poorly designed, a large proportion of them are deployed outside of the standard enterprise security perimeter and quite a number of them use lightweight specialized OSes like VxWorks, MQX and INTEGRITY [20]. As a result, standard computer security solutions may not even run on most of these devices, which makes the task of securing IoT devices and services tricky. The next section provides a discussion on the challenges of implementing security for IoT and some related hardware issues.

2.3.1 Challenges of Implementing Security for IoT

The following lists some unique security challenges and design considerations for the IoT devices and systems, which differ considerably from the traditional computers and computing devices [22–24]:

1. Some manufacturers of IoT devices that are new in the business lack security expertise, and can not afford to hire the services of security experts. Therefore they rely on the rudimentary security mechanism on the hardware and software components they acquire. Consequently, they end up producing devices with many security vulnerabilities.
2. Many companies that produce IoT devices spend less or nothing on research and development that can potentially improve the security of their products in quest of competition for inexpensive devices.
3. Virtually all devices that can be connected to the Internet have embedded OSes in their firmware. However, in view of the fact that such devices are designed to be very small and inexpensive, their OSes are usually not designed with security in mind. As a result, most of them have vulnerabilities.
4. The homogeneous nature of IoT deployments, for example, in WSNs in which almost all sensor nodes, apart from the sink node, are very identical represents a potential security risk. Because if attackers can identify some vulnerability on a single device, they can use it to compromised the remaining devices and even others that are similar in design or use the same protocols.

5. As the number of connected devices increases, the techniques used in exploiting potential entry points or vulnerabilities also increase. Now one does not have to be a professional hacker to be able to hack some IoT devices because of the availability of tools and tricks on-line coupled with simplicity in design of some of the devices. Cyber criminals can reprogram poorly designed devices and cause them to malfunction in order to steal sensitive information.
6. A vast number of IoT devices deployed in difficult terrains are expected to be placed there unattended for years, and due to the nature of the terrains, it may be difficult to perform some upgrade or configuration on them. For some applications that involve a very large number of devices, IoT devices are designed without provision for upgrade or update, probably due to the complications that will be involved because of the large number. On the other hand, there are some upgradeable *things* that are only replaced every few years, such as smart refrigerators and smart cars, and may have long life cycle. Some of these *things* may even outlive the companies, thereby leaving them without further support. It is obvious that the security mechanisms on the devices in the above scenarios will be outdated, thereby raising serious security concerns.
7. A number of applications may require the deployment of IoT devices in locations where it will be very difficult to provide physical security. In such instances, malicious entities may physically capture some devices in order to reverse engineer them, and possibly access sensitive data.
8. IoT is designed to provide seamless connections among diverse devices in different systems and subsystems using the Internet. As such, a compromised washing machine in a given country can be used to send thousands of risky spam emails across the globe using its Wi-Fi connection.

2.3.2 Hardware Issues

As the IoT technology grows, attention is mostly focused on applications, such as sensing, wireless transmission, smartness and other aspects of the IoT, and forgetting about the underlying hardware that enables such functionalities [25]. In recent years, there are significant technological advancements in hardware manufacturing processes, such as miniaturization of chips, which has inherent advantages, including, but not limited to, smaller size, lower cost and higher speed. Investment in this industry is increasing considerably, and hardware giants like Intel and ARM along with other companies are making significant improvements in their hardware. Nevertheless, in the race for smaller, more energy efficient, lighter and lower cost IoT hardware, the hardware community is facing a number of challenges.

First and foremost, in order for the miniature chips to consume less battery power, outdated architecture is used on at least the first-generation of Intel Edison platform, which is based on Quark processors. Fortunately, the processor speed is improving, because the next-generation of Edison that followed is based on Atom Silvermont cores that is on some Android and Windows tablets [26]. This processor

is significantly faster. Presently, the Edison platform for IoT applications has a *Tangier* System-on-a-Chip (SoC) that mixes a dual-core Atom running Linux with a Quark chip [27]. Eventually, the modern 64-bit x86 CPU cores may end up being used in the next generation of Edison microcomputers for IoT applications. But if the modern 64-bit x86 CPU cores are used in wearable devices, it is not likely that they will be cheap again, and considering their complexity, their power requirement will definitely be more than what a disposable IoT device can withstand.

Another issue is that improving the processing power of the microcomputers will make them to dissipate more heat, which will result in bigger packaging, and hence bigger size. Additionally, processors with hardware-assisted security will consume more power, which implies bigger and more expensive batteries [26].

2.4 Size and Heterogeneity of Things

IoT is characterized by large number of heterogeneous devices. It is expected that this heterogeneity will allow seamless connection of combinations of smart *things* via highly constrained and non-constrained network environments. Connected devices range from very simple and lightweight devices powered by 8-bit MCUs to very sophisticated devices with powerful processing capabilities and extremely large memories. Furthermore, in order to make the IoT vision more realizable, it is expected that in the coming years there will be a growing need for more services that will interconnect multiple IoT application domains. Be that as it may, the sheer size and the growing heterogeneity in terms of device types, device resources, topology and security/communication protocols constitute a challenge to security and privacy in the IoT. The following sections elaborate on the size and heterogeneity of the IoT with more details.

2.4.1 Size of IoT

Considering that the market demand for IoT is expanding daily, the size of IoT can be described in different perspectives, such as IoT market size and IoT revenue size. For example, as IoT is fast becoming a powerful force that is transforming businesses across all industries, it is expected to generate incremental revenue that is estimated to be in billions of dollars. Nonetheless, for the purpose of this chapter, we focus only on the size of IoT in terms of number of connected devices and its impact on security. As the IoT matures, the number of connected *things* continues to grow and applications with extremely large number of devices are becoming commonplace. This number represents a security risk [22], especially if there is a security breach in one or more of the devices. Updating a large number of devices that are already deployed (which may be in millions) will be a very big challenge for manufacturers, and if an attacker successfully exploits vulnerability in a single

device he can compromise other devices on the same network, or extend the effects to other networks, until he eventually reaches his final target.

Moreover, the large number of interconnections of devices in some applications, such as WSNs, which is far more than the number of interconnections in the traditional Internet, constitutes a security concern. Considering the massive number of wireless links between devices in the IoT, malicious entities can exploit any available vulnerability and try to compromise a network.

2.4.2 Heterogeneity of the IoT

The IoT encompasses heterogeneous networks of intelligent devices with diverse network protocols and communication technologies. In the concept of IoT, these diverse *things* are expected to exchange information and data seamlessly without human intervention [28], but most smart *things* use network solutions that are proprietary to specific vendors, leading to undesirable co-location of networking technologies. Furthermore, many intelligent consumer items do not communicate with devices that use only propriety network solutions [29]. Consequently, they have to communicate via gateways, resulting in lossy connections. In addition, since the Industrial, Scientific and Medical (ISM) bands in urban environments are often congested, interference from other wireless networks may hamper the performance of IoT devices, especially where large number of devices are deployed. In the above scenarios, if, for example, there is an attempt to compromise a smart device equipped with device tampering detection mechanism, and that device raised an alarm, the alarm may not be communicated to the relevant authorities due to poor network connection. Hence the device may eventually be compromised. As such, enabling across-the-board network protocols and communication technologies is essential. This highlights the need for seamless interoperability between IoT systems [30].

Considering the level of mobility in the IoT and the fact that most of the connections are wireless, every single hand-off represents a tremendous opportunity for attackers to infiltrate IoT systems. The risk of such security breach can be exacerbated by inadequate interoperability among IoT systems and subsystems. This emphasizes the need for sustainable interoperability to be adopted across a wide range of application domains, which will provide common interface solutions. However, creating a framework to achieve the requisite degree of interoperability is not an easy task.

2.5 Privacy Concerns in the Internet of Things

Since the inception of the World Wide Web in 1989 [31], preservation of privacy has been a concern. Concerns about privacy on the Internet are exacerbated by the coming of IoT, and are expected to grow even more than was previously thought as

the IoT is beginning to take shape and gain popularity with new application domains being created daily. This can be attributed to the fact that securing IoT devices and systems presents additional challenges to security administrators than securing the traditional computers and related systems. For example, a large number of connected devices, such as sensors and smart *things* will be deployed all over the place. Such devices may operate autonomously or be controlled remotely from somewhere. When these devices interact with each other and with humans they will collect, process and transmit data about the environment, objects and of course, about humans [32].

Considering what happens with smart phone technology that sometime captures information without the consent or knowledge of the user [33], there is every reason for users of IoT devices to worry about their privacy. For instance, in some applications like smart healthcare, smart devices leave traceable signatures of behaviours and locations of users that some malicious attackers can exploit.

It is very exciting to see IoT being integrated into different aspects of our live, since it has the potential to bring positive changes to the way we do things. This, however, represents a significant privacy risk that can enable an attacker to carry out an unwanted surveillance on users. Governments can also use IoT devices to carry out unnecessary surveillance on their citizens in the name of counter-terrorism, also known as the *big brother effect* [34, 35]. Without adequate security measures, today it is possible for attackers to hack and take control of any device that has audio or visual capability and use it for malicious surveillance purposes. For example, attackers were able to hack baby monitors in April 2015 [36]. The reality is that even smart TVs can be used by malicious attackers to spy on users [37].

Additionally, as the IoT gains more momentum and acceptance, many companies and businesses have so far collected huge amounts of data about their customers and visitors. This information is being collected from web cookies, social networks, mobile apps, video cameras, RFID bracelets, etc. The stored data may contain a considerable amount of personal and sensitive information. The disturbing reality is that, in most cases, customers are not given the choice to opt-out of data collection. While the motive behind the data collection may be to improve services and customer experience, as well as enable companies identify new business opportunities based on the data, the use of such personal data may amount to infringing on the privacy of users.

3 Fundamental Internet of Things Security Issues

In this section, we examine the fundamental IoT security issues. Essentially, we consider some root causes of IoT security issues, such as *things* are not designed with security in mind; open debugging interfaces; inappropriate network configuration and use of default passwords by users; and lack of encryption of critical information before storage. We also look at current and emerging IoT cyber threat landscape and finally, overview of the IoT threat agents.

3.1 Things Are not Designed with Security in Mind

With the advent of IoT and an ever more connected public, more companies are embedding computers and sensors into their products and enabling them to connect to the Internet. Computers and sensors are now being embedded into all sorts of consumer devices, including tea kettles and clothing. Many houses, offices and factories have a number of computers and sensors embedded all over. While companies are desperately competing and rushing to be the first to launch a particular product into the emerging IoT market, they sometimes forget device security. In the quest to react to various business opportunities, many manufacturers leave a lot of devices open to vulnerabilities. Today, IoT has introduced new exploitable attack surfaces that expand beyond the web into the cloud, diverse OSes, different protocols and many more. Consequently, every day we hear news about new devices that are being compromised by hackers as a result of security vulnerabilities.

The story of data breaches in the IoT devices or networks is becoming commonplace, and if the situation is not carefully handled, something similar to what happened in the mid 1990s (i.e., when the level of insecurity in personal computers reached an alarming stage) [38] may eventually happen with the IoT. This can be attributed greatly to the fact that many vendors do not make security their top priority; they only consider it as an afterthought when their products have security issues. This makes a number of IoT devices and networks vulnerable to all sorts of attacks. As such, many IoT devices can be hacked directly over the network or indirectly using some apps.

3.1.1 Testing the Security of IoT Devices

Several organizations and security firms, including but not limited to Hewlett Packard (HP) [39], Veracode [40] and Symantec [41] have conducted research on security in the IoT. The results of these studies revealed some disturbing facts about the security and privacy status in the IoT. For example, HP carried out the study on 10 of the most popular IoT devices in use. Highlights of the results contained in an official report released by the company in 2015 are presented below:

- Six out of ten of the devices with user interfaces were found vulnerable to some issues like persistent XSS and weak credentials.
- 80 % of the devices captured one or more user information directly or using device mobile apps, or the cloud.
- 90 % of the devices have used unencrypted network service.
- 70 % of devices along with their cloud and mobile apps enable attackers to identify valid user accounts via account enumeration.
- 70 % of devices along with their cloud and mobile apps components failed to require complex and lengthy passwords.

To emphasize the fact that IoT devices, their mobile apps and associated cloud services are mostly designed without security in mind, we now consider the results of the study conducted by Veracode. Six new always-on common IoT devices with up-to-date firmware were examined, which include the following [42]:

1. Chamberlain MyQ Internet Gateway—an Internet-based remote control for garage doors.
2. Chamberlain MyQ Garage—an Internet-based remote control for controlling garage doors, interior switches and electrical outlets.
3. SmartThings Hub—a central control device for controlling home automaton sensors, switches and door locks.
4. Unified Computer Intelligence Corporation (Ubi)—an always-on voice-controlled device for answering questions, controlling home automaton and performing tasks such as sending emails and SMS messages.
5. Wink Hub—a device used as a central control for home automation products.
6. Wink Relay—a combination hub and control device for home automation sensors and products.

Within the scope of their study, the Veracode team of researchers uncovered security vulnerabilities in these devices that could negatively impact user experience. The results of the study are summarized below:

- Cyber criminals can leverage data obtained from the Ubi device to know exactly when a user is at home based on the level of noise or brightness of light in the room, which could facilitate burglary.
- Security vulnerabilities in Wink Relay or Ubi can enable malicious attackers to turn on microphones on IoT devices with such capabilities and eavesdrop on users.
- Vulnerabilities in Chamberlain MyQ system can allow an attacker to know when a garage door is closed or opened. Such information could be used to rob the house.
- Some of the vulnerabilities provide attackers with the opportunity to remotely run arbitrary code on a device.

To scrutinize the security of IoT devices, a Symantec team of researchers examined 50 smart home devices that are commonly used today. The team discovered that: none of the tested devices allow the use of strong passwords, none used mutual authentication and in addition, user accounts on those devices are not protected against brute-force attacks. They also found that about 2 out of 10 of the mobile apps for controlling those devices did not use Secure Socket Layer (SSL) for encrypting information exchange between the devices and the cloud.

The team further highlighted a number of attacks surfaces of smart home devices, including physical access, local attacks over Wi-Fi/Ethernet, cloud polling, direct connection, cloud infrastructure attacks and malware. They went further to describe several possible attack scenarios based on each attack surface.

3.2 Open Debugging Interfaces

The importance of building security into IoT devices at the outset, rather than considering it as an afterthought was mentioned earlier. One of the important approaches to implementing security by design is to make sure that the attack surface is minimized as much as possible [43]. As such, there is need for manufacturers of IoT gateways to implement only the necessary interfaces and protocols that will enable an IoT device to perform its intended functionalities. Manufacturers should put a limit on the services of all interfaces on the device for debugging purposes, which, in most cases, may not be even needed by the user, and can allow hackers to have direct channel into the local area network using the Wi-Fi.

Although leaving such interfaces may be indispensable for the manufacturer and researchers for development and testing purposes, a user may not even know that such interfaces exist throughout the lifespan of the device, hence he does not need them. In addition, these open debugging interfaces are potentially dangerous and present opportunities for malicious entities to hack the device or access important information. Moreover, through them, malicious attackers can remotely run some harmful code, such as virus and spyware on the device [43].

For instance, in the research study conducted by Verocode [40], reported earlier, the research team discovered that some debugging interfaces were left open and unsecured on two of the devices they examined, through which a malicious attacker can run arbitrary code and harm the system. Even though some of these interfaces may be hidden, a malicious person can go to any length to discover them. Once discovered, all one needs to do is to go to Android developer site and download a simple toolkit that can enable him have an access into the gateway within few minutes.

In order to implement a workable security in the IoT, the concept of security by design should be given the priority it deserves so that unnecessary security flaws can be avoided. For example, it is important for manufacturers to include some mechanism in their design that will prevent even a legitimate user from running malicious code that can be dangerous to the gateway device or a smart device.

3.3 Inappropriate Network Configuration and Use of Default Passwords by Users

With the continued rise in production of diversity of IoT devices, more smart *things* hit the market by the day, and now the connected versions of almost every household appliance is available in the market. Additionally, as manufacturers are seriously competing to grab their share of the predicted $1.7 trillion revenues in the IoT market by 2019 [44], the prices of these *things* are getting cheaper by the day. For these reasons, people are now using connected devices more than ever before. A recent survey carried out by TRUSTe [45] showed that 35 % of U.S. and 41 % of

British domestic online consumers own at least one smart *thing* apart from their phone. The survey further revealed the most popular devices in use, which include: smart TVs (20 %), in-car navigation systems (12 %), followed by fitness bands (5 %) and home alarm systems (4 %). Even though percentage and popularity of devices may differ, the results of this survey are likely to be true for other European Countries, China and many other developing Countries.

Unfortunately, it seems that many consumers are not aware of IoT security concerns and their associated implications on their privacy and security. This is evident from the manner in which some consumers install, configure and use their smart devices. A significant portion of the security concerns revolves around appliances for smart homes. The *do-it-yourself* syndrome, where some consumers use default passwords and settings on their smart devices, as in the case of the security cameras reported in [46–48], has resulted in inappropriate network design and implementation and consequently leaving their Internet routers and smart devices open for hackers to access [49]. This is one of the reasons why many smart home internal networks are badly configured [50].

Another issue is the use of weak passwords. In most cases when some users are smart enough to change default passwords, they, however, use simple passwords that are easy to guess. Sometimes, a user that is enlighten about security may want to use a long and complex password that would be difficult for an attacker to guess, but the restrictions on some devices may not allow such setting. In addition, many of the devices do not have keyboards, and since all configurations must be done remotely, some users become reluctant about security settings.

It is possible that some users are unaware that attackers usually look for poorly configured networks and devices to exploit. Therefore, it is important for vendors to find a way of educating consumers on current security best practice, which include changing passwords regularly and proper network configuration.

3.4 Lack of Encryption of Critical Information Before Storage

It is an obvious known fact that many IoT devices, with or without the consent of their owners, do collect some kind of personal information. Such information may include name, date of birth, address, zip code, email address, location, health information, social security number, and in some cases even credit card number. A leading global data privacy management company, TRUSTe [51], conducted an online survey in the U.S. on 2,000 Internet users aged between 18 and 75, and found that 59 % of users are aware that smart *things* can capture sensitive information about their personal activities. 22 % believed that the benefits and conveniences that come with the IoT innovation are worth sacrificing their privacy for and, surprisingly, 14 % were comfortable with such companies collecting their personal information. The question now is not, if these devices are really collecting

personal data from users, but, as rightly posed by HP [39]: "Do these devices really need to collect this personal information to function properly?" One of the obvious reasons that most companies would give for capturing personal user data is that they need such data in order to improve their products. Another reason could be to know the habits of their valuable customers so they can better serve them by creating new services that would meet their needs as individuals.

Now that it is established that some IoT devices collect sensitive personal information from their users, limiting the amount of data collected by these devices is crucial. Of course, this is a difficult thing to do because of the business opportunities such data collections have created for these companies [52, 53]. However, data stored on IoT devices constitutes a tempting target for attackers, either due to the value of information it refers to, or because of the simplicity involved in accessing it. As these devices store data locally on their memories or transmit it over a variety of networks, such as home and hospital networks (which on many occasions are insecure) [54], there are concerns that the data could be accessed or manipulated over the Internet. Hence, the most appropriate thing to do irrespective of the amount of data that a device collects is to ensure that this data is well protected, whether stored on the device internal memory or on transit. So far, encryption is the best way to protect data against unauthorized access [55, 56], and hence protecting its integrity and confidentiality. Unfortunately, many IoT devices store data on their memories in an unencrypted form, making it easy for hackers to lay hands on it [14].

While encryption is widely believed to be the best approach to securing data, implementing it on many IoT devices presents some unique challenges for security experts. For example, the use of SSL for securing communication in some IoT devices is not an option, since it requires more processing power and memory, which are very scarce resources on the resource-constrained devices. One other option is to think of using Virtual Private Network (VPN) tunnel, which requires a fully featured OSes. However, smart devices run very light versions of OSes [57].

3.5 Current and Emerging IoT Cyber Threat Landscape

As IoT enters deep into our daily lives, and more *things* are getting connected and tapping into the Internet than people, security risks associated with the IoT continue to grow in both number and sophistication. Today, an increasingly massive amount of personal information and business data captured by numerous connected *things* and sensors (that may have exploitable vulnerabilities) are being transferred among smart *things* and between *things* and the cloud, thereby expanding the threat landscape. On top of that, a single weak link on any of such devices is enough to provide hackers with unlimited doorways through which they can gain unauthorized and unlawful access to an IoT system.

In the context of computer security, a threat is a potential to exploit a vulnerability or a potential to violate a security policy, and hence expose a computer

system to harm [58]. Thus, a threat may or may not happen, but if it happens, it is capable of inflicting damage on a system. The Proliferation of highly vulnerable smart devices in the enterprise, homes and in everyday life is creating an unprecedented increase in the number and sophistication of cyber threats in the IoT. Since every *thing* that connects with the Internet creates potential entry point for cyber criminals, and considering the large number of smart devices involved in the connections, effective cyber security in general is becoming increasingly complex to provide.

Given the complex protection model of resource-constrained devices of the IoT, point solutions like security suite or antivirus software that can be easily installed on laptops, smart phones and tablets cannot be used to protect these devices against threats. They lack advanced OSes that can handle the requirements of such functionalities. Furthermore, in view of the diversity of threats, delivering perimeter security in the context of IoT will require much skills and efforts. Hence, understanding threats is crucial, as it often allows security administrators to provide proper countermeasures against these threats. The most common threats that are known across different ecosystems include, but are not limited to, DoS, MitM, attacks on privacy and physical attacks. The effects of threats vary considerably depending on their nature. For instance, some may affect the confidentiality, integrity or availability of data, while others may damage a system completely. To fully understand the growing trend of cyber threats in the IoT, we need to identify the valuable assets and the diverse vulnerabilities in the IoT.

3.5.1 Internet of Things Cyber Assets

In the context of the IoT, an asset can be defined as any tangible or intangible item that is considered valuable to a person or an enterprise, which is also subject to threats. Assets in any IoT ecosystem can be hardware, software, or a piece of data (belonging to individuals or cooperate organizations), services, or the data therein [59]. As IoT is revolutionizing many industries, the manufacturing industry is also changing. Currently, cyber assets for industrial IoT do not only refer to computing devices, but include different machines, such as boilers, conveyors, compressors and some other equipment [60]. These factory devices may not necessarily be in the same geographical location, but are being connected via the Internet in order to optimize performance and efficiency. For a company, assets may also refer to things that are related to the business, but are not really electronic or infrastructure embodiment, such as the reputation of the company [61]. In Fig. 1 we provide an overview of typical IoT assets for five different application domains.

3.5.2 Vulnerabilities Associated with IoT Devices

Vulnerabilities represent weaknesses or mistakes in a device or system that allow an unauthorized entity to locally or remotely execute commands, access or modify unauthorized data, interrupt normal operation of a system, and/or damage a system

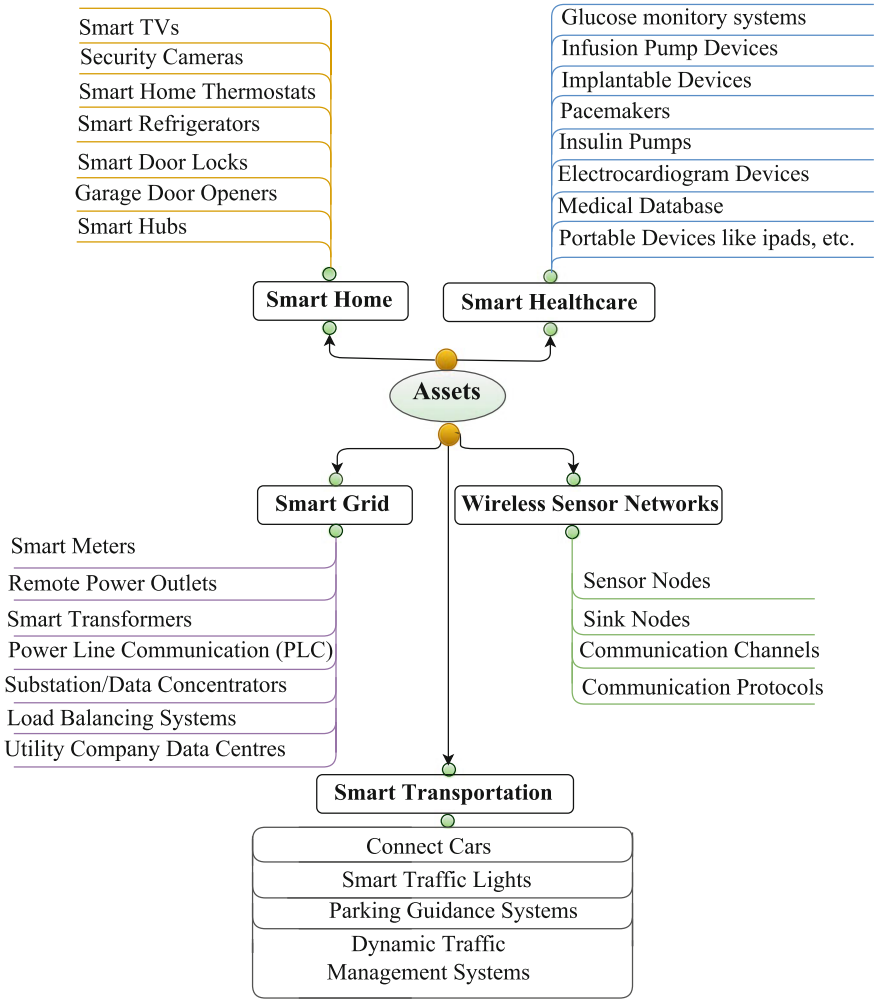

Fig. 1 Overview of typical IoT assets for five application domains

[61]. In computer security, vulnerability is popularly defined as "the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw" [62, 63]. Security flaws can be found on any or both of the two major components of an IoT system, namely software and hardware. Usually, hardware vulnerabilities are not easy to figure out, and fixing such vulnerabilities is typically much harder. The hardware of most IoT devices have a considerable number of embedded micro programs in them, and fixing vulnerabilities in these micro programs is no trivial task for different reasons, which include cost, lack of expertise, incompatibility and interoperability with bigger hardware, and it requires a lot of effort and time. Software vulnerabilities can exist

in the device OSes, communication protocols and other apps software. A number of factors are responsible for software vulnerabilities, which include design flaws and software complexity [59].

The Open Web Application Security Project (OWASP), under the IoT Top 10 project has highlighted top ten security vulnerabilities that are associated with many IoT devices [64]. The top ten security vulnerabilities presented below serve as guide for manufactures to take into consideration to secure IoT devices:

1. Insecure web interface
2. Insufficient authentication/authorization
3. Insecure network services
4. Lack of transport encryption
5. Privacy concerns
6. Insecure cloud interface
7. Insecure mobile interface
8. Insufficient security configurability
9. Insecure software/firmware
10. Poor physical security.

3.6 Overview of Internet of Things Threat Agents

Threats are normally manifested through threat agents (which can be individuals or groups), also known as threat actors, who maliciously break through systems using a variety of techniques, causing different levels of damages. There exist multitudes of threat actors with diverse motives targeting the IoT, including business competitors seeking advantage, criminals seeking financial gain, foreign governments perpetrating espionage for economic or military purpose, just to mention a few [59]. Over the years these potential adversaries have proven remarkably innovative, resourceful and very determined in exploiting vulnerabilities [65]. The OWASP IoT project, under the threat agent category [66], has formulated a mathematical expression that describes threat agent as:

$$\text{Threat Agent} = \text{Capabilities} + \text{Intentions} + \text{Past Activities} \quad (1)$$

The expertise of threat agents pose a greater challenge than the monitoring of malicious code scheme, and much bigger challenge than monitoring changes to system configuration using intrusion detection techniques. Therefore, identifying these entities who can potentially exploit the assets of individuals or companies in the IoT is very fundamental. The OWASP [66] IoT project has also broadly classified threat agents, which we have summarize in Table 1 below. Seven threat agents are shown in Table 1 with each having its class and typical examples.

Table 1 Classification of IoT threat agents

Threat agent	Class	Typical examples
Non-targeted specific	Software	Computer viruses, worms, trojans, logic bombs
Employees	Insider	Disgruntled staff, contractors, security guards
Organized crime and criminals	Outsider	Criminals that target valuable information, such as credit card numbers and bank accounts
Corporations	Outsider	Corporations, government agencies, partners, competitors
Human	Unintentional	Accidents, carelessness
Human	Intentional	Insider, outsider
Natural disasters	Non-human factors	Flood, fire, lightning, meteor, earthquakes

4 IoT Security Issues that Need Immediate Attention

In this section we highlight IoT security issues that need immediate attention. Particularly, we discuss efficient lightweight authentication schemes for IoT, robust and flexible lightweight cryptography, need for efficient key revocation schemes and need for standardization of security solutions.

4.1 Efficient Lightweight Authentication Schemes for IoT

As the IoT leads us to the Internet of Everything (IoE) with people, *things*, data and processes as its core components, authentication is among the most critical functionalities that will enable secure communication between these entities. Authentication, in the context of the IoT, simply refers to the process of identifying and validating users and connected *things* like smart devices, computers and machines. It allows authorized users or devices to access resources as well as denies malicious entities access to such resources [67]. It can also restrict authorized users or devices from accessing compromised devices. Furthermore, authentication reduces the chances for an intruder to establish multiple connections with the gateway, thereby reducing the risks of DoS attacks.

In a secure IoT communication, prior to any communication between two or more entities that will involve accessing a resource, each participating entity must be validated and authenticated so as to establish its real identity in the network. It implies that each legitimate node or entity must have a valid identity in order to participate in the communication. In spite of the importance of secure identity in IoT communications, however, many of the IoT devices in the market today lack security identities and have fallen victim to a number of security violations [68].

An authentication process typically relies on the use of usernames and passwords. For example, on the traditional Internet, websites authenticate users by

requiring usernames and passwords, and browsers authenticate websites using SSL protocol. But one contending issue in the IoT is that the devices usually deployed at the core of the communication system and the terminal nodes in most ecosystems are made up of sensors, and in some cases RFID tags. These terminal devices are used for gathering information and transmitting the gathered information to the various platforms. Consequently, in absence of identity validation and authentication, an adversary can connect to these sensors and also access the data, or carry out a wide range of malicious activities. Considering that most of them are energy-starved nodes and have limited computation and memory resources [69], traditional secure authentication schemes, most of which are based on public key cryptography that need a lot of computation and memory space [70], cannot be used directly on them. Hence the need for secure and efficient lightweight authentication schemes for IoT ecosystems cannot be overemphasized.

4.2 Robust and Flexible Lightweight Cryptography

Lightweight Cryptography (LWC) is an emerging field for developing cryptographic algorithms or protocols for implementation in constrained environments, such as WSNs, RFID tags, smart health-care devices, and embedded systems among many others [71]. LWC is expected to play a vital role in securing the IoT and ubiquitous computing in general [72]. The term *lightweight* can be considered from two perspectives, namely hardware and software. However, lightweightness in hardware does not necessarily imply lightweightness in software and vice versa. Besides, there are even design trade-offs between them [73]. For a more thorough discussion on this subject, we refer the reader to [73, 74].

In the last few years, a number of lightweight ciphers have been developed tailored for small scale embedded security, including KLEIN, PRESENT, XTEA, CLEFIA, Hummingbird 2, just to mention a few. But the reality is that most of these primitives guarantee only a low level of security, which restricts their deployment [75]. Since trade-offs invariably exist between security and performance, balancing the trade-offs between security and efficiency for LWC will continue to be a challenge. Similarly, the power consumption of resource-constrained devices and the issues associated with the hardware weight and the software weight for LWC need to be addressed in order to develop more robust and flexible LWC for IoT applications.

4.3 Need for Efficient Key Revocation Schemes

Many resource-constrained devices of the IoT are often deployed in open and hash environments where disruption of connectivity and device failures are not rare phenomena. A good example is WSNs, a key technology for collecting a variety of

data from different environments in the IoT. As these highly constrained devices are deployed in such hostile environments [76], they are susceptible to all manner of attacks. Hence it is important to devise a mechanism that can effectively and efficiently revoke secret-keys (or private-keys) as soon as a sensor node or any other smart device is compromised.

In the Internet, secure communication between two or more entities relies on trust of digital certificates. Clients can present certificates to servers and vice versa. In cryptography, a digital certificate is simply an electronic document that ties up an attribute such as a public-key with an identity. Pubic Key Infrastructure (PKI) is a system that manages the creation, distribution and revocation of digital certificates and private-keys. Digital certificates and secret-keys have an expiration date. They can also be revoked prior to expiration for a number of reasons, such as compromise of private-keys or change in the status of an entity that holds the key. PKI allows users to revoke a public-key at the Certificate Authority (CA) if the corresponding private-key is compromised. Revoking any certificate associated with a compromised key is very critical so as to mitigate the possible damages that a compromised key can cause. When a certificate is revoked, certificate revocation information must be made available to participating entities through Certificate Revocation List (CRL), On-line Certificate Status Protocol (OCSP), or some other means. For more details on this topic, we refer the reader to [77].

Like in the traditional Internet, trust within the IoT is also a fundamental requirement. There is need for entities to trust that smart devices and their associated data and services are secure from every form of manipulation. However, implementation of key revocation is more challenging in the IoT than in the traditional Internet. There are many reasons for the complications in the implementation, including the size of network, diversity of devices, and constrained nature of many devices. For instance, connecting low cost devices with limited resources makes it difficult for cryptographic algorithms based on Public Key Cryptography (PKC) to function without impacting on the quality or level of security to be provided. Moreover, many smart devices completely ignore CRL, thereby giving opportunity to malicious entities to use keys that were obtained through a data breach to perform malicious activities [41]. Developing efficient and reliable key revocation schemes that will cope with the diverse issues in the IoT is therefore crucial.

4.4 Need for Standardization of Security Solutions

The variety of devices comprising the IoT is stunning; as a result, IoT is crowded with a number of wireless communication technologies like Wi-Fi, Bluetooth, IEEE 802.154, Zigbee, Long-Term Evolution (LTE), etc. This mixture of different physical layers makes interoperability among connected devices very difficult. While devices using different communication technologies can still communicate through IP routers, a gateway must be used when the incompatibility issues in the

protocol stack go beyond the physical and link layers [78], which increases the cost of deployment. It also complicates the use of security solutions across devices with diverse wireless communication technologies. As such, standardized solutions that can be used across multiple domains are required.

Recognizing the above challenges, some standardization initiatives for the IoT are already underway. Discussions about the establishment of standards for the IoT began in 2013. By 2014, few of the standards started taking shape, and quite a handful of them have already started certifying a few products on a preliminary basis as at September 2015 [79]. The standards include Thread Group, AllSeen Alliance/AllJoyn, Open Interconnect Consortium/IoTivity, Industrial Internet Consortium, ITU-T SG20, IEEE P2413 and Apple HomeKit [79]. While some efforts have gone into development of some standards, real standards supporting the IoT are yet to be fully operational. As a consequence, the market is left open for manufacturers to compete without specific guiding rules using different approaches. This gives rise to the development of different protocols and platforms, which in turn results in products with so many vulnerabilities.

A major obstacle in the development of standards for IoT is lack of uniform definition for the smart devices. For example, harmonizing a standard for light bulbs and a standard for pacemakers will definitely be an issue. Again, considering that IoT requires many technologies to work, a single standard cannot cover them all. This is completely different from the desktop and laptop computers where a single standard covers the way they work [79]. Furthermore, due to the number of the standardizing bodies, there may be overlap in their functions, or even conflicts in their strategies. Thus, there is need for the various standards to harmonize their work in order to realize standardized security solutions for the IoT.

5 Conclusions

Through the IoT, an increasing number of people and all types of devices like consumer products communicate and collaborate over the Internet via various accessing methods. This is a clear indicator that the world is moving so fast towards ubiquitous connectivity that is already revolutionizing interactions in almost every human endeavour, including transportation, health-care, economics, work, education, entertainment, among many others. IoT also encompasses the M2H and M2M communication technologies that are creating many business opportunities worldwide. Notwithstanding, such big promises, benefits and opportunities usually come with some risks, and for the IoT, the risks are just as important as the benefits. Security and privacy concerns are among the risks likely to hamper its growth. Presently, there are a number of security and privacy challenges that need to be addressed in order for the IoT to reach its full potential and be fully applicable in an efficiently utilized manner.

In this chapter, we have discussed security and privacy challenges of the IoT, and showed that protecting enterprise intellectual property, customer information

and operational infrastructures is needed now more than ever before. We also pointed out some issues that emphasized the need for the IoT to be secured so that we can fully realize its value and benefits. Furthermore, we highlighted some challenges that are standing as obstacles to the realization of secure communications in the IoT. Some of these issues are the cause of the numerous vulnerabilities that were uncovered in so many smart devices lately. Finally, we discussed some issues that need immediate attention if IoT security and privacy challenges must be addressed.

Acknowledgments The authors wish to thank the Centre for Geodesy and Geodynamics, National Space Research and Development Agency, Toro, Bauchi State, Nigeria for supporting this work. This work was partially supported by the UID/EEA/50008/2013 Project.

References

1. J. M. Batalla, G. Mastorakis, C. X. Mavromoustakis, and J. Zurek. On Cohabitating Networking Technologies with Common Wireless Access for Home Automation Systems Purposes. IEEE Wireless Communication Magazine, 2016.
2. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of Things: A Survey on Enabling Technologies, Protocols and Applications. IEEE Commun. Surveys & Tuts., 2015. ISSN 1553-877X. doi:10.1109/COMST.2015.2444095.
3. C. Prasse, A. Nettstraeter, and M. T. Hompel. How IoT will Change the Design and Operation of Logistics Systems. In IEEE Int Conf IoT, Oct 2014. doi:10.1109/IOT.2014.7030115.
4. World Economic Forum. Industrial Internet of Things: Unleashing the Potential of Connected Products and Services. Available via World Economic Forum, Jan 2015. URL http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf. Cited 12 Dec 2015.
5. C. Pettey. The Internet of Things Is a Revolution Waiting to Happen. Available via Gartner, Inc., April 2015. URL http://www.gartner.com/smarterwithgartner/the-internet-of-things-is-a-revolution-waiting-to-happen/. Cited 20 Nov 2015.
6. Gartner. Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015. Available via Gartner, Inc., Nov 2014. URL http://www.gartner.com/newsroom/id/2905717. Cited 20 Nov 2015.
7. P. Gutierrez. Gartner Predicts 6.4 Billion 'Things' in 2016. Available via IoTHUB, Nov 2015. URL http://www.iothub.com.au/news/gartner-predicts-64-billion-things-in-2016-411686. Cited 21 Nov 2015.
8. J. M. Batalla, M. Gajewski, W. Latoszek, P. Krawiec, C. X. Mavromoustakis, and G. Mastorakis. ID-based Service Oriented Communications for Unified Access to IoT. Computers & Electrical Engineering, pages –, 2016. ISSN 0045-7906. doi:10.1016/j.compeleceng.2016.02.020.
9. M. A. Al Faruque and K. Vatanparvar. Energy Management-as-a-Service Over Fog Computing Platform. IEEE Internet of Things Journal, 3(2):161–169, April 2016. ISSN 2327-4662. doi:10.1109/JIOT.2015.2471260.
10. Proofpoint. Proofpoint Uncovers IoT Cyberattack. Available via Proof-point, Inc., Jan 2014. URL http://investors.proofpoint.com/releasedetail.cfm?ReleaseID=819799. Cited 26 Nov 2015.
11. A. Ukil, J. Sen, and S. Koilakonda. Embedded Security for Internet of Things. In IEEE 2nd National Conf Emerging Trends & Appls Comput Sci, March 2011. doi:10.1109/NCETACS.2011.5751382.

12. Symantec. Securing IoT Devices and System. Available via Symantec Corporation, 2015. URL https://www.symantec.com/iot/. Cited 12 Dec 2015.
13. WIND. Security in the Internet of Things. Available via Wind River Systems, Inc., January 2015. URL http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf. Cited 1 Nov 2015.
14. S. Raza. Lightweight Security Solutions for the Internet of Things. Dissertation, Malardalen University Sweden, Jun. 2013.
15. A.M. Gamundani. An Impact Review on Internet of Things Attacks. In IEEE Int. Conf. Emerging Trends Netws. & Comput. Commun, May 2015. doi:10.1109/ETNCC.2015.7184819.
16. M. Abomhara and G.M. Koien. Security and Privacy in the Internet of Things: Current Status and Open Issues. In IEEE Int. Conf. Privacy Secur. Mobile Syst., May 2014. doi:10.1109/PRISMS.2014.6970594.
17. S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini. Security, Privacy and Trust in Internet of Things: The Road Ahead. Comput Netws., 2015. ISSN 1389-1286. doi:10.1016/j.connect.2014.11.008.
18. I. Alqassem and D. Svetinovic. A Taxonomy of Security and Privacy Requirements for the Internet of Things (IoT). In IEEE Int. Conf. Ind. Eng. Eng. Manag., Dec 2014. doi:10.1109/IEEM.2014.7058837.
19. T. Xu, J.B. Wendt, and M. Potkonjak. Security of IoT Systems: Design Challenges and Opportunities. In IEEE/ACM Int Conf Comput-Aided Design (ICCAD), Nov 2014. doi:10.1109/ICCAD.2014.7001385.
20. A. Grau. The Internet of Secure Things - What is Really Needed to Secure the Internet of Things? Available via ICON LABS, 2015. URL http://www.iconlabs.com/prod/internet-secure-things-%E2%80%93-what-really-needed-secure-internet-things. Cited 16 Dec 2015.
21. The Economist. Embedded Computers: Hacking the Planet. Available via The Economist Newspaper, Jul 2015. URL http://www.economist.com/news/leaders/21657811-internet-things-coming-now-time-deal-its-security-flaws-hacking. Cited 27 Nov 2015.
22. J. Dixon. Who Will Step Up To Secure The Internet Of Things? Available via Crunch Network, Oct 2015. URL http://techcrunch.com/2015/10/02/who-will-step-up-to-secure-the-internet-of-things/. Cited 4 Dec 2015.
23. K. Rose, Scott Eldridge, and Lyman Chapin. The Internet of Things: An Overview-Understanding the Issues and Challenges of a More Connected World. The Internet Society, pages 1–50, Oct 2015.
24. A. Kumar. Internet of Things (IOT): Seven Enterprise Risks to Consider. Available via TechTarget, 2015. URL http://searchsecurity.techtarget.com/tip/Internet-of-Things-IOT-Seven-enterprise-risks-to-consider. Cited 4 Nov 2015.
25. T. Lee. The Hardware Enablers for the Internet of Things - Part I. IEEE Internet of Things Newsletter, Jan 2015.
26. N. Hajdarbegovic. Are We Creating An Insecure Internet of Things (IoT)? Security Challenges and Concerns. Available via Toptal, 2015. URL http://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things. Cited 23 Nov 2015.
27. E. Brown. Edison IoT Module Ships with Atom/Quark Combo SoC. Available via LinuxGizmos.com, Sep 2014. URL http://linuxgizmos.com/edison-iot-module-ships-with-atom-plus-quark-combo-soc/. Cited 7 Dec 2015.
28. E. Baccelli, O. Hahm, M. Gunes, M. Wahlisch, and T.C. Schmidt. RIOT OS: Towards an OS for the Internet of Things. In IEEE Conf. Comput. Commun. Workshops, April 2013. doi:10.1109/INFCOMW.2013.6970748.
29. E. D. Poorter, I. Moerman, and P. Demeester. Enabling Direct Connectivity Between Heterogeneous Objects in the Internet of Things through a Network-Service-Oriented Architecture. EURASIP J Wireless Commun & Netw., 2011. doi:10.1186/1687-1499-2011-61.

30. V. L. Shivraj, M. A. Rajan, M. Singh, and P. Balamuralidhar. One Time Password Authentication Scheme Based on Elliptic Curves for Internet of Things (IoT). In IEEE 5th National Symp. Info. Technol.: Towards New Smart World, Feb 2015. doi:10.1109/NSITNSW.2015.7176384.
31. W. Coomans, R. B. Moraes, K. Hooghe, and J. Maes. The 5th Generation Broadband Copper Access. In Proceedings of IEEE 9th ITG Symp. Broadband Coverage in Germany, pages 1–5, April 2015.
32. M.J. Covington and R. Carskadden. Threat Implications of the Internet of Things. In M. Maybaum K. Podins, J. Stinissen, editor, IEEE 5th Int. Conf. Cyber Conflict, pages 1–12, June 2013.
33. B. Contos. Security and the Internet of Things - are we Repeating History? Available via CSO, Jul 2015. URL http://www.csoonline.com/article/2947477/network-security/security-and-the-internet-of-things-are-we-repeating-history.html. Cited 11 Nov 2015.
34. D. Bradbury. How can Privacy Survive in the Era of the Internet of Things? Available via The Guardian, Apr 2015. URL http://www.theguardiancom/technology/2015/arp/07/how-can-privacy-survive-the-internet-of-things. Cited 12 Nov 2015.
35. R. Benest. The Internet of Things: Big Progress or Big Brother? Prospect J Int. Affairs UCSD,, Jun 2015. URL http://prospectjournal.org/2015/06/04/the-internet-of-things-big-progress-or-big-brother/. Cited 18 Dec 2015.
36. D. Storm. 2 More Wireless Baby Monitors Hacked: Hackers Remotely Spied on Babies and Parents. Available via ComputerWorld, Apr 2015. URL http://www.comput-erworld.com/article/2913356/cybercrime-hacking/2-more-wireless-baby-monitorshacked-hackers-remotely-spied-on-babies-and-parents.html. Cited 28 Nov 2015.
37. G. Walters. It's Not Just Smart TVs. Your Home is Full of Gadgets that Spy on You: How Internet Giants are Collecting Your Personal Data Through their High-tech Devices. Available via MailOnline, Feb 2015. Security Challenges of the Internet of Things 29 URL http://www.dailymail.co.uk/sciencetech/article-2950081/It-s-not-just-smart-TVs-home-gadgets-spy-internet-giants-collecting-personal-data-high-tech-devices.html. Cited 10 Dec 2015.
38. B. Schneier. The Internet of Things is Wildly Insecure - And often Unpatchable. Available via WIRED, Jun 2014. URL http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/. Cited 13 Dec 2015.
39. Hewlett Packard. Internet of things Research Study. Available via HP Enterprise, 2015. URL http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf. Cited 9 Dec 2015.
40. Veracode. Veracode Study Reveals the Internet of Things Poses Cybersecurity Risk. Available via VERACODE, APr 2015. URL https://www.veracode.com/veracode-study-reveals-internet-things-poses-cybersecurity-risk. Cited 15 Nov 2015.
41. M. B. Barcena and C. Wueest. Insecurity in the Internet of Things. Available via Symantec, Mar 2015. URL https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/insecurity-in-the-internet-of-things.pdf. Cited 17 Dec 2015.
42. C. Osborne. Internet of Things Devices Lack Fundamental Security, Study Finds. Available via ZDNet, Apr 2015. URL http://www.zdnet.com/article/internet-of-things-devices-lack-fundamental-security-study-finds/. Cited 2 Dec 2015.
43. C. Fife. Securing the IoT Gateway. Available via CITRIX, Jul 2015. URL https://www.citrix.com/blogs/2015/07/24/securing-the-iot-gateway/. Cited 19 Nov 2015.
44. J. Greenough. The 'Internet of Things' will be the World's most Massive Device Market and Save Companies Billions of Dollars . Available via Business Insider, Apr 2015. URL http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10. Cited 24 Nov 2015.
45. TRUSTe. Majority of Consumers Want to Own the Personal Data Collected from their Smart Devices: Survey. Available via TRUSTe, Jan 2015. URL http://www.truste.com/blog/2015/01/05/majority-consumers-want-own-personal-data-survey/. Cited 4 Dec 2015.

46. M. Smith. Peeping into 73,000 Unsecured Security Cameras Thanks to Default Passwords. Available via NetworkWorld, November 2014. URL http://www.networkworld.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cam-Eras-thanks-to-default-passwords.html. Cited 7 Nov 2015.
47. D. Bisson. 73,000 Security Cameras Viewable Online Due to Use of Default Passwords. Available via Tripwire, November 2014. URL http://www.tripwire.com/state-of-security/latest-security-news/73000-security-cameras-viewable-onlin-due-to-use-of-default-passwords/. Cited 7 Nov 2015.
48. K. Zetter. Popular Surveillance Cameras Open to Hackers, Researcher Says. Available via WIRED, May 2012. URL http://www.wired.com/2012/05/cctv-hack/. Cited 7 Nov 2015.
49. M. Kostyukov. Smart Home Security. Available via Home Toys, January 2006. URL http://www.hometoys.com/content.php?post-type=763. Cited 27 Nov 2015.
50. J. T. Ho, D. Dearman, and Khai N. Truong. Improving Users' Security Choices on Home Wireless Networks. In Proc. 6th ACM Symp. Usable Privacy Secur., 2010. ISBN 978-1-4503-0264-7. doi:10.1145/1837110.1837126.
51. TRUSTe. 59 % of U.S. Internet Users Know Smart Devices Can Collect Information About Their Personal Activities. Available via TRUSTe, May 2014. URL http://www.truste.com/events/iot/2014/05/59-of-u-s-internet-users-know-smart-devices-can-collect-information-about-their-personal-activities/. Cited 8 Dec 2015.
52. M. Rozenfeld. The Value of Privacy: Safeguarding your Information in the Age of the Internet of Everything. The Institute - IEEE News Source, Mar 2014.
53. T. Olavsrud. Internet of Things Connections to Quadruple by 2020. Available via CIO, Mar 2015. URL http://www.cio.com/article/2899643/data-analytics/internet-of-things-connections-to-quadruple-by-2020.html. Cited 19 Nov 2015.
54. A. Grau. Hackers Invade Hospital Networks Through Insecure Medical Equipment. IEEE Spectrum, Jun 2015.
55. G. Singh and Supriya. Modified Vigenere Encryption Algorithm and Its Hybrid Implementation with Base64 and AES. In IEEE 2nd Int. Conf. Adv. Comput. Netw. & Secur., Dec 2013. doi:10.1109/ADCONS.2013.33.
56. A. Fragkiadakis, P. Charalampidis, S. Papadakis, and E. Tragos. Experiences with Deploying Compressive Sensing and Matrix Completion Techniques in IoT Devices. In IEEE 19th Int. Workshop Comput. Aided Modeling & Design Commun. Links & Netw., Dec 2014. doi:10.1109/CAMAD.2014.7033237.
57. J. Horn. 5 Security Questions for Your Next IoT Deployment. Available via RacoWireless, Dec 2014. URL http://embedded-computing.com/guest-blogs/5-security-questions-for-your-next-iot-deployment/#. Cited 1 Dec 2015.
58. M. Alhabeeb, A. Almuhaideb, P. D. Le, and B. Srinivasan. Information Security Threats Classification Pyramid. In IEEE 24th Int. Conf. Adv. Inf. Netw. Appl. Workshops, Apr 2010. doi:10.1109/WAINA.2010.
59. M. Abomhara and G. M. Kien. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. J Cyber Secur., 2014. doi:10.13052/jcsm2245-1439.414.
60. P. Reynolds. The Industrial Internet of Things Will Flip Cyber Security on Its Head. Available via Industrial IoT/Industrie 4.0 Viewpoints, Jun Security Challenges of the Internet of Things 31 2015. URL http://industrial-iot.com/2015/06/the-industrial-internet-of-things-will-flip-cyber-security-on-its-head/. Cited 12 Nov 2015.
61. E. Bertino, L. D. Martino, F. Paci, and A. C. Squicciarini. Security for Web Services and Service-Oriented Architectures. Springer, 2010. ISBN 978-3-540-87741-7. doi:10.1007/978-3-540-87742-4.
62. Y. Ilyin. Can we Beat Software Vulnerabilities? Available via Kaspersky Lab, Aug 2014. URL https://business.kaspersky.com/can-we-beat-software-vulnerabilities/2425-/. Cited 3 Dec 2015.
63. ExpressVPN. What is a Security Hole and How can it Get you Hacked? Available via ExpressVPN, 2015. URL https://www.expressvpn.com/internet-privacy/guides/what-is-a-security-hole-how-can-it-get-you-hacked/. Cited 19 Nov 2015.

64. OWASP. OWASP Internet of Things Top Ten Project. Available via OWASP IoT Project, 2014. URL https://www.owasp.org/index.php/OWASP_Internet_of_Things_ Project. Cited 5 Dec 2015.
65. S. Pramanik. Threat Motivation. In IEEE 10th Int. Conf. & Expo. Emerging Technol. Smarter World, Oct 2013. doi:10.1109/CEWIT.2013.6851346.
66. OWASP-Threat Agent Category. What is a Threat Agent? Available via OWASP IoT Project, May 2012. URL https://www.owasp.org/index.php/Category:Threat_Agent. Cited 9 Dec 2015.
67. O. O. Bamasag and K. Youcef-Toumi. Towards Continuous Authentication in Internet of Things Based on Secret Sharing Scheme. In Proceedings of the WESS'15: Workshop Embedded Syst. Secur. ACM, 2015. ISBN 978-1-4503-3667-3. doi:10.1145/2818362.2818363.
68. M.A. Jan, P. Nanda, Xiangjian He, Zhiyuan Tan, and Ren Ping Liu. A Robust Authentication Scheme for Observing Resources in the Internet of Things Environment. In IEEE 13th Int. Conf. Trust, Secur. & Privacy Comput. Commun., Sept 2014. doi:10.1109/TrustCom.2014.31.
69. K. Fan, J. Li, H. Li, X. Liang, X. Shen, and Y. Yang. ESLRAS: A Lightweight RFID Authentication Scheme with High Efficiency and Strong Security for Internet of Things. In IEEE 4th Int. Conf. Intell. Netw. Collab. Systs., Sept 2012. doi:10.1109/iNCoS.2012.48.
70. G. Zhao, X. Si, J. Wang, X. Long, and T. Hu. A Novel Mutual Authentication Scheme for Internet of Things. In IEEE Proceedings of Int. Conf. Modeling, Identification & Control, June 2011. doi:10.1109/ICMIC.2011.5973767.
71. G. Bansod, N. Raval, N. Pisharoty, and A. Patil. Modified SIMON and SPECK: Lightweight Hybrid Design for Embedded Security. Cryptology ePrint Archive: Report 2014/1016,, Dec 2014. URL https://eprint.iacr.org/2014/1016. Cited 12 Nov 2015.
72. M. Katagi and S. Moriai. Lightweight Cryptography for the Internet of Things. Sony Corporation, pages 1–4, 2011. URL https://www.iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf. Cited 3 Dec 2015.
73. Universite du Luxembourg. On Lightweightness, Mar 2015. URL https://www.cryptolux.org/index.php/On_Lightweightness. Cited 11 Nov 2015.
74. J. Woods and P. Muoio. Practical Applications of Lightweight Block Ciphers to Secure EtherNet/IP Networks. ODVA Industry Conf & 17th Annual Meeting, pages 1–15, Oct 2015. URL https://www.odva.org/Portals/0/Library/Conference/2015_ODVAConference_Woods_Practical-applications-of-Lightweight-Block-Ciphers.pdf.
75. I. Mansour, G. Chalhoub, and P. Lafourcade. Key Management in Wireless Sensor Networks. J Sensor & Actuator Netws., 2015. doi:10.3390/jsan4030251.
76. M. Ge and K. R. Choo. A Novel Hybrid Key Revocation Scheme for Wireless Sensor Networks. Springer International Publishing Switzerland, 2014. doi:10.1007/978-3-319-11698-3 35.
77. Cisco Systems. Public Key Infrastructure Certificate Revocation List Versus Online Certificate Status Protocol. White Paper, pages 1–6, 2004.
78. S. L. Keoh, S. S. Kumar, and H. Tschofenig. Securing the Internet of Things: A Standardization Perspective. IEEE Internet of Things J, June 2014. ISSN 2327-4662. doi:10.1109/JIOT.2014.2323395.
79. C. Null. The State of IoT Standards: Stand by for the Big Shakeout. Available via TechBeacon, Sep 2015. URL http://techbeacon.com/state-iot-standards-stand-big-shakeout. Cited 24 Nov 2015.