Security Requirements in IoT Environments

Ftayem Binglaw[1], Murat Koyuncu[2(✉)], and Tolga Pusatlı[3]

[1] Graduate School of Natural and Applied Science, Atilim University, Ankara, Turkey
[2] Atilim University, Ankara, Turkey
mkoyuncu@atilim.edu.tr
[3] Cankaya University, Ankara, Turkey

Abstract. The Internet of Things (IoT) is a relatively new concept as it connects things (or objects) that do not have high computational power. The IoT helps these things see, listen, and take action by interoperating with minimal human intervention to make people's lives easier. However, these systems are vulnerable to attacks and security threats that could potentially undermine consumer confidence in them. For this reason, it is critical to understand the characteristics of IoT security and their requirements before starting to discuss how to protect them. In this scope, the present work reviews the importance of security in IoT applications, factors that restrict the use of traditional security methods to protect IoTs, and the basic requirements necessary to judge them as secure environments.

Keywords: Internet of Things · IoT · Security · Security requirements

1 Introduction

IoT security can be defined as all the strategies and technologies that aim to protect any information collected, exchanged, or stored in any IoT system from threats and malicious attacks [1]. This information may face many risks and threats such as theft, tampering, and destruction. Also, the security of IoT components such as sensors, devices, applications, and networks should be considered in the scope of IoT security.

Security considerations are not new in the information technology (IT) context; rather, they are critical components of any technology's success, development and adoption. Security has always been an issue since computers started communicating with each other. However, the scope of coverage of such security has so far been limited, e.g. money and intellectual property, to name two [2, 3]. The advent of the IoT with its complex environment has added a whole new dimension to this problem and, as a result, has faced new and unique security challenges. This complexity is due to various factors such as large number of heterogeneous connected devices, huge data generated and exchanged by these devices, and differences in the communication infrastructure. In addition, IoT devices are made by different manufacturers, use different security policies and communication stacks, and are based on various standards [4]. This has led to the failure in implementing a robust security system for devices, especially since most

W. Hussain and M. A. Jan (Eds.): IoTaaS 2021, LNICST 421, pp. 84–96, 2022.
https://doi.org/10.1007/978-3-030-95987-6_6

of them are not equipped with an effective security mechanism and are not primarily designed to deal with security problems [5].

The IoT is the integration and collaboration of several technologies such as WSN, RFID, cloud computing, Internet, etc. Naturally, it suffers from all the vulnerabilities of these technologies [6]. In addition, as mentioned above, the IoT has its own characteristics which aggravate the security requirements considerably. This leads to an indispensable need to review security requirements specifically from an IoT perspective.

Against this backdrop, the goal of this paper is to answer the following questions:

- Why is it so important to secure the IoT?
- What are the challenges when using the already available technologies to secure and protect information to this end?
- What are the basic security requirements that must be met in IoT to render it secure?

2 Importance of IoT Security

Attacks on IoT devices can sometimes be easy to implement, especially when they target devices with limited resources that represent the majority, such as smart TVs and baby monitors. Resource limitations represent weaknesses and flaws that hackers can use to attack the IoT system as a whole, thereby compromising its overall safety and productivity [5, 7, 8]. In addition, IoT devices may be left to operate in harsh, irregular and even hostile environments without supervision, making them more vulnerable to various security breaches [9]. The common attack strategy on IoT devices is to hack one device that has vulnerabilities, and to take fraudulent actions against other connected devices by impersonating the true identity of the hacked device [5]. As a result, it can be said that the interconnected nature of the IoT means that every insecure device connected to it has the potential to affect the security of the IoT system as a whole [10]. For example, attackers could compromise a home alarm system by intercepting the radio frequency signal used to lock and unlock home windows.

It is common for IoT devices to be targeted by attackers. F-Secure published a report titled “Attack Landscape H1 2019: IoT, SMB Traffic”, recording a 300% increase in the number of cyber-attacks on IoT devices in 2019. The attacks usually target IoT devices that are found in homes and workplaces such as medical devices, smart TVs, and smart printers, all of which are considered weak and unsafe against these attacks. More troubling is the fact that attackers find it easy to hack devices as access points to more critical and sensitive networks and systems.

The importance of security in the IoT becomes even clearer with real-life incidents, giving us a better idea about the extent of the impact of IoT security problems on consumers’ lives. Here are a few examples:

BMW’s ConnectedDrive Vulnerability: In January 2015, a security flaw appeared in the BMW ConnectedDrive System, one that allows drivers whose cars have been accidentally locked to request a remote unlock of their vehicle from the BMW helpline [11]. This flaw allowed the attacker to impersonate the BMW’s servers and send instructions to unlock the locked vehicle remotely using a mobile phone network even without any request from the owner.

Hacked IoT Devices: On October 21, 2016, several websites including Twitter, Netflix, Spotify, Airbnb and The New York Times were reported to be inaccessible due to a Distributed Denial of Service (DDoS) attack [12]. To launch this attack, the attacker(s) hacked a number of IoT devices with limited resources and used them to send numerous fake requests to these sites. This overflow burdened the Web sites, rendering them unable to deal with their customers' requests and leading to their temporary shut-down.

Denial of Basic Services: According to Simo Ronella, CEO of Valtia, the company responsible for managing the overall operations and maintenance of damaged properties, in 2016, two buildings in southeast Finland were attacked [13]. This attack deprived residents of heating, which is an essential service in a cold country like Finland, as it temporarily disrupted the computer systems that controlled the central heating and hot water distribution to both buildings using a DDoS attack. According to local reports, this cyber-attack lasted about a week.

Hacked Baby Monitor: According to NBC News, in 2018, a Texas couple experienced a cyber-attack targeting the cameras they used to monitor their four-month-old baby [14]. They heard voices and insults coming from the child's room. Then they heard the voice of a man in their room telling them that their child had been kidnapped. However, when they got to their child's room, they found him alone and asleep.

Exploiting Connected Fax Machines: In 2018, Yaniv Palmas and Eyal Atkin, two security researchers from Check Point, discovered that popular HP Officejet Pro All-in-One fax printers had security flaws [15]. These flaws could allow hackers to steal data across the company's network using a phone line and fax number. They said that attackers could fax files loaded with malware that were specifically created to target networks. Fax vulnerabilities enable this malware to decrypt files and upload them to its memory, which could compromise sensitive information or cause disruption across connected networks.

Hacking Smart Bulbs: The security experts from the University of Texas stated that hackers can make use of Internet-connected light bulbs as a covert channel to exploit the user's private data [16]. Researchers used the LIFX and Phillips Hue smart light systems as a study for this purpose, stating that hackers could launch an attack by manipulating the infrared light upon creating a communication channel between the smart lights and a device that senses infrared light. Then, by installing a malicious agent on the phone, they could encode private data and transfer them through the infrared covert channel.

These are just several examples of what attacks targeting the IoT can do. The consequences of the attacks may be more dangerous when they target applications that directly affect human life, such as e-health applications or smart transportation applications, which may cause accidents that threaten people's lives. IoT devices do not only collect and manage critical personal information such as users' names and telephone numbers, medical records and prescriptions, but also monitor user activities (e.g., when users are at home) [17, 18]. Therefore, users should ensure that IoT devices and the services they provide are free from vulnerabilities and defects threatening user's security, especially as this technology is becoming more and more common in daily life [10, 19, 20]. For this reason, ensuring security in IoT products should be a major stakeholder

priority and a goal to be achieved. Otherwise, without IoT security and privacy guarantees, related solutions are unlikely to be widely adopted by stakeholders despite their benefits [21].

3 Factors that Restrict the Use of Traditional Security Methods to Protect IoT

It is well known that protecting the information stored and exchanged among devices and within a network is not a new problem as there have always been concerns for cyber-attacks targeting information. However, security has remained as a hot topic since ready-made solutions are not always satisfactory. The IoT security requires the development and creation of new solutions designed to suit the nature of this technology or, at best, solutions modified from old ones. This is because the common Internet-connected devices differ from IoT devices in terms of functionality and device resources such as memory, power source, and data processing capability. For example, a laptop differs from a baby monitor and a smartphone differs from a smart door lock. This difference makes it difficult to use traditional security, that was originally designed to protect these systems, to protect the IoT; security in this respect has to be stronger because IoT devices are connected to the physical world and, at the same time, they are not designed to withstand the new threats that this world faces on a daily basis. This section visits some of the important features that distinguish the IoT from well-known information systems as reported in [5, 10, 22–25].

3.1 Mobility

Most IoT devices are portable and often connect to the Internet via a wide range of service providers. As most of these devices are mobile, this ability can cause disconnection from a specific network, release its IP address, connect to another network, and get a new IP address. Therefore, a stable network connection cannot always be expected in such an environment. This factor makes it difficult and complicated to verify the identity of every device trying to connect to the network. In addition, what resources such a device can access, and what risks it may bring to the network are other issues to be considered.

3.2 Heterogeneity

The IoT is a heterogeneous and complex system that combines many products from different manufacturers; hence, the different technologies. These products differ from each other in terms of resources (software and hardware), security policies, and functionality. Therefore, interaction and interoperability become difficult due to the lack of a common platform. This gives rise to the problem of creating a common standard for IoT security architecture accepted by all vendors and manufacturers. Creating this architecture would enhance the interoperability of the security functions of all components of the IoT system. Obviously, the success of this will depend on collaboration among companies to create a global standard that significantly facilitates IoT network security.

3.3 Scalability

Scalability is related to the ability of the system, with all the software and hardware it contains, to meet the large increase in the number of devices and the vast amount of information circulating in addition to the increasing demand for services.

The things connected to the IoT are increasing daily and their number is expected to reach about 14.7 billion devices by 2023 [26]. This significant increase in the number of devices is matched with an increase in the number of users and an increase in the services they demand. In addition, the amount of information that users share will increase by a major amount. Such dual increase in both information and devices will lead to other problems, including providing unique addresses for devices, where the information is stored, and how to control and monitor it. On the other hand, a lot of these devices will be deployed in areas where it may be impossible or impractical to provide physical security, making it easier for intruders to physically compromise the devices on the network. In short, limited scalability makes it difficult to monitor, identify, and protect IoT devices.

3.4 The Possibility of Being Tampered

Current security solutions focus primarily on protection from remote attackers, and are based on the fact that these individuals cannot physically access the devices. This is mostly true for desktop computers and servers that are usually kept in closed buildings, or mobile devices that rarely leave their owners' pockets. However, this is not the case for IoT devices that may be located in many remote areas left unattended. In most cases, attackers can gain easy physical access to them to extract secrets, modify programs, or add malicious data.

3.5 Limited Resources

The implementation of a robust security mechanism in an IoT system depends on the availability of strong security in each IoT device. It is well known that the availability of robust security methods in any device depends to a large extent on having sufficient resources to support it, such as having adequate power supply, memory space, and processing capability.

The IoT devices are not initially built for being secure; nor are they always designed to be smart and to exchange information with other devices. As discussed previously, traditional methods may not always work; for instance, those used to secure computers cannot be used to secure IoT devices such as coffee machines, refrigerators, door locks, etc. One of the reasons is that these devices contain a limited amount of resources, unlike computers. Most IoT devices are simple, resource-constrained things that often perform one function, such as turning lights on/off or measuring the oxygen level in the blood. Such lack of resources inhibits the implementation of complex security solutions. On the other hand, since traditional security solutions are designed to run on computers, smartphones, and other devices with larger resources, they are not suitable for IoT devices with limited resources.

The devices in the IoT have many limitations and restrictions that control the level of security they can provide. This may be due to the manufacturers' strategy to produce

inexpensive and lightweight smart devices. The resource limitations on IoT devices include hardware restrictions such as computing power, energy supply and memory size; and software restrictions such as O/S security updates, and network limitations due to a variety of the communication protocols and media.

4 Security Requirements for the IoT

In the short term, the IoT is expected to enter various areas of our daily life such as our cities, homes, hospitals and schools. However, this prevalence heavily depends on an important factor, which is the degree of security that the IoT provides to consumers [27]. If IoT service providers want this technology to spread widely, they should think of security requirements when manufacturing or deploying IoT technology. In this way, IoT user can be sure that his sensitive and private information is essentially protected from any kind of abuse. Also, the services and applications provided by the IoT must be available whenever the user needs them.

Table 1. Example IoT threats and possible attack consequences.

Threat	Target	Possible consequences
Eavesdropping	Confidentiality	Disclosure of sensitive data
Eavesdropping	Privacy	Disclosure of private data
Impersonation	Authentication, Authorization	Unauthorized access to data or devices
Tampering	Availability	Physical damage
False data injection	Integrity	May cause false reports and wrong decisions

In order to ensure security in the IoT and to create readily available IoT devices and services, a set of security requirements have to be taken into consideration. Failure to do so could mean failure to provide security and privacy, resulting in serious problems and dire consequences. The minimum main security requirements to be met in any IoT system can be listed as providing confidentiality, integrity, availability, authentication, authorization, and privacy [4, 7, 24, 28–30]. These requirements are extracted considering the most popular potential threats to these systems and their targets as given in Table 1. Note that the table does not include all threats, but only examples; also that, even though these requirements may not be new as regards computer security, they still need to be considered when it comes to IoTs.

4.1 Confidentiality

Confidentiality refers to granting only authorized users the right to access certain information, ensuring the security of that information, and protecting it from disclosure.

Even if this information is stolen, the presence of such a security measure prevents the perpetrators from understanding the stolen data and exploiting it.

IoT devices may deal with sensitive information important to individuals, institutions and governments, including medical records, banking transactions and military secrets. Therefore, the protection of this information is important and is closely related to the user's degree of confidence in the IoT technology and their willingness to use it and benefit from its services. For example, eavesdropping or tampering with information exchanged by health devices may lead to the disclosure of personal health information or even lead to life-threatening situations for individuals. As another example, the data related to the composition of any product that guarantees its quality and distinguishes it from other products should be confidential because its spread can harm the company's reputation and competitive advantage [8].

To achieve confidentiality, protect information and gain user confidence, specific technologies need to be developed, such as encrypting data before it is transmitted, and creating mechanisms for securely distributing cryptographic keys [24, 31, 32]. Most of the techniques used previously to provide confidentiality in the network are considered heavy on the IoT system and, for this reason, cannot be implemented for this purpose. For example, some asymmetric encryption methods, which encode data through a complex calculation that require adequate power and high computational capacity, will not be suitable for use in IoT devices with limited resources. One of the well-known encryption methods is the symmetric key encryption method. In this method, the sender and receiver use the same secret key to encrypt and decrypt the data [33]. However, before defining these technologies, one should take into account the heterogeneous nature of the IoT and the limited resources of most of its devices. In the literature, there are studies to develop symmetric key-based lightweight encryption algorithms aiming to produce solutions to this specific requirement.

4.2 Integrity

This requirement is necessary to give users confidence in the accuracy and completeness of the information provided by the IoT. As mentioned before, the IoT is often based on the exchange of private, sensitive and valuable information among many different devices that greatly affect consumers. For this reason, it is important to ensure that accurate, original, legal, unaltered, timely and complete information reaches consumers [22]. Incorrect information may appear as a result of changing or tampering with the original information, and this change may be intentional or unintentional. In an intentional alteration, a malicious attacker picks up the information before it reaches its target, changes it, and then sends it back to its destination. Thus, the recipient receives information other than what was sent to them from the authorized sender. As a result, the attacker can modify, alter, or completely destroy the data, endangering the integrity of the IoT system, which entails great risks. As for the unintended change, it could sometimes result from a transmission error or unintended noise, or as a result of weather factors [5, 34].

This security requirement is important to the IoT and, if not available, there may be serious consequences. For example, tampering with medical information and readings produced by medical devices, such as an insulin pump or pacemaker, may lead to life-threatening consequences [18]. Apart from this, if the data is not reliable, then it cannot

be used for the purposes for which it was designed; hence, any service that relies on this data could be compromised. An even more dangerous incident is using this data without knowing that it has been tampered with, sometimes resulting in wrong decisions, e.g. giving the wrong medication to a patient. Therefore, there is a need to come up with and use technologies whose mission is to verify the integrity of the data provided by the IoT. One simple technique to do so is the Cyclic Redundancy Check (CRC), which ensures data integrity by adding a fixed-length value to detect network errors in the IoT. A request to resend the correct data goes to the sender if this technology observes the arrival of incorrect data [9, 24, 32].

4.3 Availability

The requirement of IoT availability is necessary to provide a fully functional Internet-connected environment. This ensures that services are available to consumers whenever they need them and without interruption [18]. In other words, availability ensures that authorized users can access all related devices, services and data provided by the IoT whenever they need it and without any delay. Availability is essential even in the event of attacks and crashes; it also guarantees the ability to provide minimum services in the event of a power outage and blackout [5, 22]. In IoT, most services are requested in real time, meaning that if the request is not answered in time due to unavailability of the service, this request cannot be rescheduled at any other time [35]. For example, if the information about an intruder in a house is sent to the police station the next day, that information loses its value. Likewise, if the blood glucose meter registers disturbing readings, which are then received late by the doctor, this can result in significant harm to the patient, even death. Therefore, certain techniques should be devised and applied to ensure uninterrupted availability in IoT. Additionally, an IoT system needs to provide backup of vital information to prevent data loss and ensure data availability. Firewalls and IDSs can be installed on a network to prevent attacks and provide availability of IoT devices [32].

4.4 Authentication

Authentication is a major requirement of the IoT because it provides confidence in the devices participating in the IoT network and is critical for improving network performance. This security requirement is for everything intended to connect to an IoT system. Typically, the authentication and identity management work together to manage and secure access to information and resources, and to connect to the network. Identity management identifies objects individually, while authentication enables the IoT objects to confirm the identity of the peer they are communicating with. In other words, authentication enables the recipient to verify whether she or he has actually received the data from the sender who claims who they are. This means ensuring the legitimacy of the data presented in the networks, as well as the legitimacy of the objects sending and requesting that data. In brief, to provide security, no IoT entity should have the ability to directly access available resources unless its identity is authenticated first [5, 7, 32, 34].

The process of authenticating and verifying the identity of an object is a prerequisite for allowing access to resources and requests for any data or service in the IoT. This

process ensures that no attacker can enter the network using a false ID and password, and send out false messages. This further demonstrates the importance of having a mechanism that enables the recipient to ensure that the message received comes from a reliable source and, at the same time, enables the senders to ensure that the requester of information is reliable.

The nature of scalability in the IoT is a major concern when authentication is taken into account. Identifying a large number of devices and authenticating each object directly in real time can be a daunting task due to the vast number of objects connected to the IoT [36]. Because of all this, it is necessary to propose a mechanism that effectively deals with the scalability of devices in the IoT environment while enabling entities to confirm each other's identity in every interaction in it. To work around this issue, different schemes and algorithms and pre-shared keys are proposed that are lightweight and do not adversely affect battery life within devices and their performance. For example, symmetric key encryption depends on both parties having the same encryption key to confirm their identity [37, 38]. Also, one of the methods used for authentication is what is known as the 'direct authentication method' for humans and machines. The user can open the office door using biometric identification (such as a fingerprint) or an object within a personal network, such as an ID card or smartphone. The combination of authentication methods can prevent any overall system security loss.

4.5 Authorization

There is sometimes confusion between authentication and authorization requirements although these requirements differ completely in meaning. Authentication means confirmation of identity, while authorization means allowing access to the system. In simple terms, authentication is the process of self-verification, while authorization is the process of checking what the self has access to. Authorization enables determining if the person or object, after authenticating their identity, is permitted to, for example, access, use, or read the resource. These privileges or permissions are determined by the device or by the identity of the users. As such, given proper identity, anyone can access an IoT system while without permission, no one can access any resources in it [5, 39]. Therefore, it can be said that the authorization policy determines which specific resources can be accessed by which entity or user.

Authorization is typically implemented through the use of access control. Access control is important in establishing a secure connection among a number of devices and resources. After determining whether an object has the right to access a specific resource, the access control mechanism either allows or denies it to access the related resource. One important issue that should be addressed in access control is to make it easier to create and modify its rules, and to make these rules easy to understand and follow [7, 40].

4.6 Privacy Requirement

Privacy is the ability to protect data from eavesdropping and to control how it is shared and distributed. It is also concerned with concealing the identity of the owner and the

recipient of the information, which is an important aspect especially in the case of personal and sensitive information [28].

Since many people, devices and services communicate and share everything online, such as photos, videos, health records, etc., it has become important to consider privacy as an important security requirement [32]. In an open environment like the IoT, a lot of personal information about individuals can be collected without their knowledge if there are no security measures to prevent this. In an IoT environment, individuals will be able to take advantage of a large number of services that require personal information related to, for example, a consumer. These services may require photos, emails, phone numbers, bank account information, and many more. Moreover, the environment itself may be able to obtain this information automatically as a result of the interconnection among its services and devices. For example, some smart TV companies collect information about their customers in order to assess viewing behavior, usually without the knowledge or desire of customers. In this case, privacy should provide protection to individuals by giving them full control over their personal data. They should know who is responsible for collecting their data and where it is stored, and they should also be notified before such data is shared through the system [4, 39].

The privacy requirement should ensure that consumers' information and identities are in safe hands and completely protected from disclosure or leakage. The inability to access personal data except by the authorized person means that no other authenticated customer who has nothing to do with this information or any other individual can access it [4]. For example, hospital administration personnel need access to patient data for administrative purposes (registration, billing, etc.), but they are not allowed to know anything about the patient's history and health status. In this case, privacy concerns granting employees the right to access information related to their work only without disclosing sensitive medical information not related to their work [20].

IoT has become integral in various applications, namely remote patient monitoring, energy consumption control, traffic control, and smart parking. In all of these applications, users need the protection of personal information related to their movements, habits, and interactions with other people. Therefore, there is an urgent need to propose protocols and administrative frameworks for dealing with privacy, determining who stores them where, and who manages and provides access to information in IoT. For example, individuals' personal information should be destroyed when it is no longer needed. As another solution, all communication between IoT nodes can be encrypted using proper encryption algorithms. This solution ensures that the connection is not open to intruders trying to eavesdrop and, at the same time, guarantees privacy. Access control mechanisms are also among the steps that help protect individuals' privacy. This mechanism controls who has the right to access the data and what action can be taken on it.

5 Conclusions

This paper provides answers related to three key questions listed in the Introduction concerning IoT security. First, the importance of IoT security is explained by providing real-life examples. Then, the reasons that make it difficult to use the available security methods and techniques to protect the IoT are discussed. Finally, the basic security

requirements that should be met in the IoT are elaborated. Since these security requirements are primarily targeted by cyber-attacks, they need special attention to secure any IoT system.

The findings of this study are as follows: 1) IoT systems are targets of cyber-attacks, such as eavesdropping, compromising the confidentiality of data exchanged among IoT nodes. 2) IoT devices are very sensitive to intentional or unintentional data changes. 3) There are different types of attacks which can affect the availability of IoT devices and service. 4) Authentication and authorization of users and devices become complex in such a heterogeneous environment. 5) Large amounts of personal information about individuals can be collected without their knowledge. Considering all these findings, confidentiality, integrity, availability, authentication, authorization and privacy are taken as the basic security requirements for an IoT environment.

If enough security measures are in place to protect an IoT system, then the system can be considered secure. For this reason, it is very important to know such security requirements in full before starting to implement related actions. With the increasing use and popularity of IoT devices worldwide, it is only natural and inevitable to guarantee secure applications before any dire consequences come about as a result of compromised systems being in use.

References

1. Kouicem, D.E., Bouabdallah, A., Lakhlef, H.: Internet of things security: a top-down survey. Comput. Netw. **141**, 199–221 (2018)
2. Cvitić, I., Vujić, M., Husnjak, S.: Classification of security risks in the IoT environment. In: Proceedings of the 26th International DAAAM Symposium, pp. 731–740, DAAAM International, Vienna (2016)
3. Patel, K.K., Patel, S.M.: Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. Int. J. Eng. Sci. Comput. **6**(5), 6122–6131 (2016)
4. Razzaq, M.A., Gill, S.H., Qureshi, M.A., Ullah, S.: Security issues in the Internet of Things (IoT): a comprehensive study. Int. J. Adv. Comput. Sci. Appl. **8**(6), 383 (2017)
5. Hossain, M.M., Fotouhi, M., Hasan, R.: Towards an analysis of security issues, challenges, and open problems in the internet of things. In: IEEE World Congress on Services, pp. 21–28. IEEE (2015)
6. Andrea, I., Chrysostomou, C., Hadjichristofi, G.: Internet of Things: security vulnerabilities and challenges. In: IEEE Symposium on Computers and Communication (ISCC), pp. 180–187. IEEE (2015)
7. Abomhara, M., Køien, G.M.: Security and privacy in the Internet of Things: current status and open issues. In: International Conference on Privacy and Security in Mobile Systems (PRISMS), pp. 1–8. IEEE (2014)
8. Jha, A., Sunil, M.C.: Security considerations for Internet of Things. L&T Technol. Serv. (2014)
9. Krishna, B.S., Gnanasekaran, T.: A systematic study of security issues in Internet-of-Things (IoT). In: International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 107–111. IEEE (2017)
10. Iqbal, M.A., Olaleye, O.G., Bayoumi, M.A.: A review on internet of things (IoT): security and privacy requirements and the solution approaches. Glob. J. Comput. Sci. Technol. **16**(7) (2017)

11. PCWorld: BMW cars found vulnerable in Connected Drive hack. https://www.pcworld.com/article/431610/bmw-cars-found-vulnerable-in-connected-drive-hack.html. Accessed 22 Nov 2021
12. The New York Times: Hackers used new weapons to disrupt major websites across U.S. https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html. Accessed 22 Nov 2021
13. The Hacker News: DDoS attack takes down central heating system amidst winter in Finland. https://thehackernews.com/2016/11/heating-system-hacked.html. Accessed 22 Nov 2021
14. NBC News: Nest camera hacker threatens to kidnap baby, spooks parents. https://www.nbcnews.com/news/us-news/nest-camera-hacker-threatens-kidnap-baby-spooks-parents-n949251. Accessed 22 Nov 2021
15. The Hacker News: Hackers can compromise your network just by sending a Fax. https://thehackernews.com/2018/08/hack-printer-fax-machine.html. Accessed 22 Nov 2021
16. SciTechDaily: Warning: smart light bulbs could open up your personal information to hackers. https://scitechdaily.com/warning-smart-light-bulbs-could-open-up-your-personal-information-to-hackers/. Accessed 22 Nov 2021
17. Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H.: A survey on security and privacy issues in Internet-of-Things. IEEE Internet Things J. **4**(5), 1250–1258 (2017)
18. Mosenia, A., Jha, N.K.: A comprehensive study of security of internet-of-things. IEEE Trans. Emerg. Top. Comput. **5**(4), 586–602 (2016)
19. ENISA: Baseline security recommendations for IoT in the context of Critical Information Infrastructures. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot. Accessed 15 Sept 2021
20. Sfar, A.R., Natalizio, E., Challal, Y., Chtourou, Z.: A roadmap for security challenges in the Internet of Things. Digit. Commun. Networks **4**(2), 118–137 (2018)
21. Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I.: Internet of things: vision, applications and research challenges. Ad Hoc Netw. **10**(7), 1497–1516 (2012)
22. Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I.: Internet of things (IoT) security: current status, challenges and prospective measures. In: 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 336–341. IEEE, London (2015)
23. Haroon, A., Shah, M.A., Asim, Y., Naeem, W., Kamran, M., Javaid, Q.: Constraints in the IoT: the world in 2020 and beyond. Constraints **7**(11), 252–271 (2016)
24. Al-Sharekh, S.I., Al-Shqeerat, K.H.A.: Security challenges and limitations in IoT environments. Int. J. Comput. Sci. Netw. Secur. **19**(2), 193–199 (2019)
25. Elrawy, M.F., Awad, A.I., Hamed, H.F.A.: Intrusion detection systems for IoT-based smart environments: a survey. J. Cloud Comput. **7**(1), 1–20 (2018). https://doi.org/10.1186/s13677-018-0123-6
26. Cisco, Cisco Annual Internet Report (2018–2023), White paper. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf. Accessed 15 Sept 2021
27. Shamsi, K., Mazhar, A.: IoT implementation using secure communication protocols. Int. J. Comput. Eng. Res. (IJCER) **7**(12), 2250–3005 (2017)
28. Ngu, A.H., Gutierrez, M., Metsis, V., Nepal, S., Sheng, Q.Z.: IoT middleware: a survey on issues and enabling technologies. IEEE Internet Things J. **4**(1), 1–20 (2016)
29. Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., Kikiras, P.: On the security and privacy of Internet of Things architectures and systems. In: International Workshop on Secure Internet of Things (SIoT), pp. 49–57. IEEE, Vienna (2015)
30. Batalla, J.M., Vasilakos, A., Gajewski, M.: Secure smart homes: opportunities and challenges. ACM Comput. Surv. (CSUR) **50**(5), 1–32 (2017)
31. Chinanu, U.E., Oche, O.E., Okah-Edemoh, J.O.: Architectural layers of internet of things: analysis of security threats and their countermeasures. Sci. Rev. **4**(10), 80–89 (2018)

32. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W.: A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J. **4**(5), 1125–1142 (2017)
33. Ashraf, Q.M., Habaebi, M.H.: Autonomic schemes for threat mitigation in Internet of Things. J. Netw. Comput. Appl. **49**, 112–127 (2015)
34. Laeeq, K., Shamsi, J.A.: A study of security issues, vulnerabilities and challenges in internet of things. In: Securing Cyber-Physical Systems, 1st edn. CRC Press (2015)
35. Kozlov, D., Veijalainen, J., Ali, Y.: Security and privacy threats in IoT architectures. In: Workshop on Security Tools and Techniques for Internet of Things (SeTTIT). ACM, Oslo (2012)
36. Khattak, H.A., Shah, M.A., Khan, S., Ali, I., Imran, M.: Perception layer security in Internet of Things. Futur. Gener. Comput. Syst. **100**, 144–164 (2019)
37. Rehman, S.U., Khan, I.U., Moiz, M., Hasan, S.: Security and privacy issues in IoT. Int. J. Commun. Networks Inf. Secur. **8**(3), 147 (2016)
38. Zhao, K., Ge, L.: A survey on the internet of things security. In: Ninth International Conference on Computational Intelligence and Security, pp. 663–667. IEEE, Emeishan (2013)
39. Joshitta, R.S.M., Arockiam, L.: Security in IoT environment: a survey. Int. J. Inf. Technol. Mech. Eng. **2**(7), 1–8 (2016)
40. Roman, R., Najera, P., Lopez, J.: Securing the internet of things. Computer **44**(9), 51–58 (2011)