Privacy and Security Challenges and Solutions in IOT: A review

N Alhalafi1, *, Prakash Veeraraghavan2
1,2 Department of Computer Science and Computer Engineering, La Trobe University, Australia
E-Mail: N.alhalafi@hotmail.com

Abstract: The Internet of Things (IoT) is a revolutionary concept that heavily relies on the network infrastructure to connect large number of devices whose main purpose is to collect data and communicate among one another in the bid to enhance their decision-making capabilities. However, with this great evolution comes various challenges that threatens the information technology industry; these include security and privacy issues. The presence of a large number of interconnected technologies open a grey area in the IT field which has been worsened by the lack of capacity of various institutions to identify, assess and monitor important components to ensure compliance with security policies. Thus, there is need for a clear understanding of the issues at hand and how they can be solved in order to fully harness this capability.

1. Introduction
The Internet of Things (IoT) refers to the next evolution of the internet that will enable a networking infrastructure that connects a large number of devices to allow them to collect data and communicate with each other in order to make processed smart decisions [13]. It is noteworthy that devices, in this case, refer to any object embedded with the necessary hardware and software to support processing and networking capabilities. IoT provides businesses with applications that they can use to control their assets and come up with efficient and cost-effective business models. The technology is also an enabler of a hyper-connected society and can be used to optimize transportation and mobility [2]. However, the technology faces a lot of security and privacy challenges that need to be addressed to enhance its acceptance and use. Indeed, without a clear appreciation of the challenges posed by the security and privacy issues related to the IoT and the possible solutions to the problems, the success of the technology and the privacy of potential users face significant peril. This paper examines various security and privacy challenges associated with IoT and the possible solutions that can be used to address the challenges.

2. Review and Analysis
The IoT is a huge network comprising of interconnected networks with devices that are resource constrained. Since IoT devices have scarce resources, they cannot use complete security suites used in typical networks. This presents a challenge as one has to design a unique security framework for IoT or use existing solutions. Efforts must, however, be made to ensure that lightweight security solutions are used to secure IoT so that devices resources are not depleted on security at the expense of performance. Some of the security and privacy challenges associated with IoT include difficulty in establishing safe and secure communication. This is because the technology comprises different components at the
network edge making it challenging to ensure that all the components communicate safely and securely. There are also some data secrecy and confidentiality concerns associated with IoT. For example, the technology involves the interconnection of several networks. Where in most cases, a user may not be in control of some of the networks hence exposing data to many secrecy and confidentiality threats. Additionally, IoT involves a lot of devices and networks. This makes it challenging to identify, assess and monitor important components to ensure compliance with security policies [12]. Finally, it is challenging to ensure an adequate level of secure exchange of information and trust between different vertical information technology infrastructures.

2.1 Confidentiality and Access

Besides the above, there are a number of core technologies that support IoT networks. They include Radio Frequency Identification (RFID), Near Field Communication (NFC) and Wireless Sensor Network (WSN). RFID technology supports IoT networks by ensuring that IoT objects are equipped with identifiers and smart tags that make the objects manageable. Furthermore, RFID technology enables the IoT objects to have smart chips that give the objects the ability to sense information in their environment, compute and communicate with other objects or human beings. The RFID component is however prone to denial of service, eavesdropping, skimming, relay and side channel attacks that may compromise the security and privacy of IoT users [13].

WSNs are usually used to support remote sensing application and information gathering in IoT networks. The WSNs are preferred in such applications because they are cost effective, efficient, consume low power and have intelligent and processing capabilities. This IoT component is also susceptible to the wormhole, neighbor discovery, ping flood, ICMP, flood and syn flood attacks. NFC is the technology that supports communication within a small distance of few centimeters with low power and data rate need such as communication with smart cards and access control. NFC component is prone to phishing, user tracking, relay and data forging attacks [14]

2.2 Cybersecurity

In relation to the IoT, the cybersecurity issues revolve around confidentiality, authentication, and access. In this case, confidentiality refers to the need to ensure that data is kept private with only the authorized users allowed to access the data [2]. For IoT, cryptography emerges as the most important technology in ensuring confidentiality. In turn, authentication refers to the verification of data to ensure that there has been no tampering and that the information has been delivered by the supposed sender or author. On the other hand, access is about ensuring that only the authorized users can retrieve or obtain the infrastructure, communications, and information while making sure that the authorized users are not blocked from acquiring the data [2].

2.3 Security and Privacy

In order to address the security issues associated with the IoT, researchers like Brumfitt et al. recommended that there is need to move away from the traditional view of security that focuses on transport, physical, cryptography and application security since the approach is not ideal for IoT. The researcher further recommended that a new security framework that has a lightweight forensic, inter-device coordination and network-based user interface should be used.

On the other hand, Chen et al. (340) proposed an information fusion approach to secure IoT networks. This approach averages on techniques found in medical and biological fields to enhance the security of the networks. There are also researchers like Ding et al. who proposed allowing IoT systems to use their autonomous potential to self-organize and defend themselves against security threats. The security of IoT networks can also be assured by implementing secure authentication mechanisms. For example, one can use certificate-based credentials to secure the IoT networks. It is, however, important to ensure that appropriate measures are put into consideration when developing a key based authentication mechanism to minimize the chances of an attacker taking advantage of a week design to bypass the authentication.
2.4 Challenges

2.4.1 Identification and Localizing and Tracking

The evolving features and technologies of the IoT along with the emerging systems of the IoT interaction have led to specific privacy and security challenges. One of the privacy and security challenges of the IoT is related to identification with regard to the risk of associating an identifier such as an address with the individual and related data [12]. In this case, the main challenge is related to associating the identity to a particular context that violates the individual’s privacy by providing the identifying information to entities outside the user’s personal sphere, increasing the possible cyber attack vectors. Another privacy and security challenge linked to the IoT is localizing and tracking. In this case, the threat is related to the determination and recording of the individual’s location across space and time. While localization and tracking are already possible through various means such as internet traffic and mobile phone GPS location, many users may perceive it as a violation of privacy if the data is used inappropriately or if they do not have any control of the sharing of their location data [12]. As such, the IoT faces a challenge in ensuring awareness of tracking and control of the localization data.

2.4.2 Profiling and Authentication

The IoT also poses significant privacy and security challenges related to profiling as well as interaction and presentation that violate privacy. In relation to profiling, the IoT poses a risk in the compilation of data about users so as to determine their interests through correlation with other sources of data and profiles [1]. In this case, profiling methods may be used in e-commerce for consumer personalization as well as for internal targeting and optimization on the basis of the customers’ interests and demographics. However, profiling could lead to privacy violations if the data is used for unsolicited ads, price discrimination, and social engineering. Moreover, the gathering and sale of user profiles in the data marketplace without the individual’s consent is considered as a privacy violation. In turn, the IoT may also pose privacy and security challenges where private information on the individual user is conveyed inadvertently through the public media, thus disclosing the data to unwanted audiences. Various applications used in the IoT such as healthcare, transportation, and retail are reliant on significant user interactions. Majority of the mechanisms used to interact with the user and present feedback information are inherently public in nature, posing a threat to the individual’s privacy in case other people can observe the data [11]. Thus, the IoT must solve the challenge posed by the easy visibility of personal user data.

2.4.3 Lifecycle Transitions and Inventory Attacks

Finally, IoT poses privacy and security challenges with regard to lifecycle transitions and inventory attack. In this case, the users’ private information collected during the IoT device’s lifetime may be disclosed during changes to the gadget’s control spheres during their lifecycle [4]. The smart devices interact with numerous services and persons and amass the data on such interactions in their history logs. Considering that the lifecycle of most consumer goods is based on the customer owning the products forever, the sale or sharing of such devices could result in the buyer accessing sensitive data about the previous owner, thus violating the individual’s privacy. In turn, the privacy and security of the IoT are challenged by the threat of an inventory attack. As the IoT interconnection capacities evolve with the development of end-to-end vision, the smart devices can be queried over the internet by both legitimate and non-legitimate parties. When the IoT gadgets are queried by the non-legitimate entities, the latter may exploit the device to collect unauthorized information regarding the characteristics and existence of the user’s personal effects [10]. Thus, the IoT can allow for the disclosure of comprehensive data about the users’ life and belongings, posing a threat to their security and privacy.

2.5 Solutions to Identified Privacy and Security Issues
The most capable solution in enhancing the privacy and security of the IoT should rely on ensuring the availability of less user-identifying data outside the individual’s personal sphere. To achieve the goal of reducing the availability of such data, the IoT could focus more on local processing of data rather than centralized information processing as well as enhancing horizontal communication between the smart devices instead of vertical communication [5]. In addition, current approaches to privacy and security preservation such as data perturbation, client-side personalization, encryption, and data anonymity and obfuscation apply to the IoT. However, such techniques should be adapted to account for the distributed nature of data in the IoT networks. Moreover, smart devices should have the capacity to authenticate queries and respond only to requests from legitimate entities [9]. This can be implemented in an IoT network using a PUFs based security protocol as discussed in the section below.

2.5.1 Devices Authentication

Authentication is an effective approach that can enhance security in IoT networks. It is, however, challenging to authenticate a large number of devices associated with IoT networks in real time. In order to address the challenge and protect against security threats like a man in the middle or attackers tempering with IoT objects to steal data, Physical Unclonable Functions (PUFs) can be used to authenticate IoT objects [7]. PUFs offer low cost primitive that can be used for secure key generation and agreement.

![Figure 1: Use of PUFs for device identification](Source: [7])

Figure one above shows a PUF based protocol that can be used to secure communication in IoT networks. In the setup, it is assumed that two IoT devices are connected to the same server. The server is used to store a list of challenge-responses pairs for each device in the network. The security infrastructure also comprises of a PUF based key agreement protocol and a secure communication protocol [7]. The system is capable of providing security services using secrete keys to secure information in a given IoT network. It is important to note that PUFs are physical primitives that can be used to develop unclonable device specific measurements on Integrated Circuits. The unique measurements can then be used as fingerprints for network devices to support identification and authentication.

3. Conclusion and Limitations

Security is a major challenge on IoT networks that need to be addressed if the networks are to be accepted and used in various aspects of human activities like commerce and entertainment. One of the promising technologies that can be used to identify and authenticate IoT objects is the PUFs based security protocol which uses unique keys and timestamps to verify nodes and messages exchanged in a given network. The approach is limited in that it requires a lot of computing power to authenticate all the objects, messages and devices in a given IoT network. The use of an authentication server to may also introduce a bottleneck that can degrade performance.
4. References

[1] Abomhara, Mohamed, and Geir M. Koien. "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders, and Attacks." *Journal of Cyber Security*, vol. 4, no. 1, 2015, pp. 65-88.

[2] Albishi, Saad, Soh Ben, Ullah, Azmat and Algarni, Fahad. “Challenges and Solutions for Applications and Technologies in the Internet of Things.” *Procedia Computer Science* 124 (2017) 608–614.

[3] Albishi, Saad, et al. "Challenges and Solutions for Applications and Technologies in the Internet of Things." *Procedia Computer Science*, vol. 124, 2017, pp. 608-614.

[4] Baldini, Gianmarco, et al. "Ethical Design in the Internet of Things." *Science and Engineering Ethics*, vol. 24, no. 3, 2018, pp. 905-925.

[5] Borgia, Eleonora, et al. "Special issue on" Internet of Things: Research challenges and Solutions." *Computer Communications*, vol. 89, no. 90, 2016, pp. 1-4.

[6] Brumfitt, Angela, Askwith, Robert and Zhou, Bo. A framework for device security in the Internet of Things. http://www.cms.livjm.ac.uk/PGNet2014/papers/1569961261.pdf (2014)

[7] Braeken, An, “PUF Based Authentication Protocol for IoT.” *Symmetry*, vol 10, 2018, pp. 1-15.

[8] Chen, Pin-Yu, Cheng, Shin-Ming, and Chen, & Kwang-Cheng. “Information fusion to defend intentional attack in Internet of Things.” IEEE Internet of Things Journal, 1, no 4, 2014, 337–348.

[9] Farooq, Muhammad Umar, et al. "A Critical Analysis on the Security Concerns of Internet of Things (IoT)." *International Journal of Computer Applications*, vol. 111, no. 7, 2015, 1-6.

[10] Lin, Huichen, and Neil W. Bergmann. "IoT Privacy and Security Challenges for Smart Home Environments." *Information*, vol. 7, no. 3, 2016, pp. 44-54.

[11] Razzaz, Mirza Abdur, et al. "Security Issues in the Internet of Things (IoT): A Comprehensive Study." *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, no. 6, 2017, pp. 383-388.

[12] Rose, Karen et al. "The Internet of Things: An Overview." The Internet Society (ISOC), vol. 1, 2015, pp. 1-50.

[13] Rehman, Aqeel et al. Security and Privacy Issues in IoT. International Journal of Communication Networks and Information Security 8, no. 3. 2017, pp. 147-157

[14] Yousuf, Tasneem, et al. "Internet of Things (IoT) Security: Current status, challenges, and countermeasures." *International Journal for Information Security Research (IJISR)*, vol. 5, no 4, 2015, pp. 608-616.