# Chapter 7
# Future Challenges of IoT Sensor Networks

**Pendukeni Phalaagae, Adamu Murtala Zungeru, Boyce Sigweni, Joseph M. Chuma, and Thabo Semong**

## 7.1 Introduction

Chapter 6 describes the security challenges at various layers (perception, network, cloud, and the user interface) of a wireless IoT sensor network and reviews the proposed mitigation procedures for the security threats at those layers. Chapter 6 also gave a brief overview of the future wireless sensor technologies such as IoE and IoP driven by advances in technology connecting IoT. An increase in IP-enabled devices and the global availability of the Internet is a major driving factor of The IoE and IoP technology. As devices increase in number, threats become prevalent, and hence there is a need for further research to mitigate the challenges that will come with the advance in the IoT technology. This chapter aims to shed some light on the areas that need further research to come up with robust and lightweight security mechanisms for future IoT Networks. Some of these areas that need further research are highlighted in the subsequent sub-chapters.

## 7.2 Hardware Security

An increase in the number of IoT devices has led to an increase in the in-network security challenges and privacy concerns. However, recent research work has put emphasis on software-based security schemes leaving IoT hardware vulnerable to attacks. Security is IoT devices that are often neglected or treated as an afterthought by IoT device manufacturers. Research has proven that a non-secure hardware platform inevitably leads to a non-secure software stack. Existing security solutions are inadequate since the techniques do not offer strong security and protection against threats. Henceforth future work should work towards the design of security techniques for resource-constrained IoT hardware by considering both hardware security implementations such as cryptographic coprocessor or anti-tampering technologies

A. Murtala Zungeru et al., *Green Internet of Things Sensor Networks*,
https://doi.org/10.1007/978-3-030-54983-1_7

(e.g., chip or memory protection, self-destruction, etc.) and software solutions in a hybrid manner [1, 2]. However, further research is required to design and develop security mechanisms with low overhead costs for lightweight IoT hardware.

## 7.3 Lack of Lightweight Cryptographic Algorithms

Lightweight security will always be one of the key future research areas in IoT because of the resource-constrained nature of IoT sensor networks. The process of encrypting communication in the IoT sensor networks is computationally complex regarding cost, energy, and memory for small-sized and resource-constrained IoT devices. Complex security algorithms affect the performance of devices. Therefore, algorithms targeted at security and optimized resource utilization at low computation cost for IoT devices should be further investigated for lightweight IoT solutions such as key management, access authentication, access control for specific requirements for specific IoT sensor networks [3].

## 7.4 Lack of Lightweight Trust Management Systems

Trust needs to be established between neighboring nodes in the network. However, an attacker can join the network, masquerade, and recommend itself to other nodes in the network and attract traffic, which then makes it easy for them to forward attacks in the network. Therefore, a secure trust management system needs to be deployed to maintain a high level of trust between resources-constrained nodes in the network. Similarly, future research work should look at the assessment of correlation agreement among IoT nodes and its role of autonomous and intelligent trust management among nodes at all layers of the IoT sensor networks. Precision knowledge apprehension is another security goal to be considered in future works to increase the high level of trust among nodes in a network include owing to the requirement of maintaining confidentiality, quality of service, and reliable communication. For these reasons, it is essential to appropriately enforce trust management starting from the characterization of different threats and attacks at each specific level of the IoT architecture [2].

## 7.5 Lack of Lightweight Secure Routing Protocols

Assuring end-to-end secure communication among devices is a major challenge in IoT sensor networks. Data encryption has been proven to be the most effective method for secure communication across wireless sensor network communication where communication channels are more prone to attacks and data breaches.

According to research, using efficient encryption methods with low computational costs can play an important role in reducing security risks and attacks in wireless IoT communication. However, an encryption algorithm must be chosen properly to cater for the resource-constrained nature of IoT nodes. The key issues in designing secure mechanisms or algorithms are to deal with the trade-off between security, performance, and cost. Therefore, a secure routing algorithm proposed should have the capacity to secure the network with optimal use of memory-constrained IoT devices to make IoT deployment sustainable.

## 7.6 Lack of Lightweight Anti-Malware Solutions

The widespread adoption of IoT devices has attracted attackers to abuse them by causing an increase in malicious software (malware). Several types of malware can affect IoT software applications and IoT sensor networks hardware devices. Research has demonstrated that malware is a serious threat that can destroy an IoT device or have the attacker get authority and control over the IoT system. The most common adverse malware include rootkits, ransomware, bots, logic bombs, virus, worms, and Trojans. In order to keep pace with the increased adoption of IoT devices and an increased number of malware attacks, researches need to design lightweight malware detection solutions for IoT resource-constrained environments. This opens up new research challenges that need to be addressed by implementing a physical level cryptosystem with emphasis on low-power and low-cost security mechanisms against malware [4]. For future work malware, obfuscation may be considered to increase the malware detection rate, and the efficiency of the mechanisms may be assessed for their implementation in resource-constrained IoT devices [5].

## 7.7 Summary

The rapid evolution of IoT sensor networks has brought along many benefits. However, IoT has also brought about ambiguity and several security concerns to IoT adopters. Security issues are the most critical challenges that need to be addressed in promoting the adoption and development of IoT systems. This work presents security and privacy issues and their solutions. The work suggests a layered approach to expose security issues and challenges at each layer of the IoT architecture and proposes techniques used to mitigate these challenges. IoT sensor networks undergo security and privacy issues such as hardware vulnerabilities, secure routing issues, and a lack of interoperable standards for heterogeneous networks. Finally, directions and perspectives are drawn and discussed for future directions in securing IoT sensor networks IoT covering evolving areas such as artificial intelligence, Blockchain technology, sensor Internet of People, context-aware sensing, cloud infrastructure, security and privacy, and the Internet of Everything. IoT has endless opportunities and application domains. However, there are shortcomings that arise with the adoption of IoT such systems' security for resource-constrained IoT devices. In conclusion, this work aims to highlight IoT sensor networks' security challenges and to unearth research opportunities to address these challenges. Therefore, from the survey, opportunities such as Blockchain, machine learning, and the development of context-aware applications, IoP and IoE, should be further investigated to review real-life examples and analysis of their effectiveness towards enhancing privacy and security in IoT sensor networks. The convergence of IoT sensor networks with neural networks, deep learning, predictive modeling, and low-power protocols and algorithms can be investigated for enhancing security in IoT sensor networks.

## References

1. F. Rahman, M. Farmani, M. Tehranipoor, Y. Jin, Hardware-assisted cybersecurity for IoT devices, in *2017 18th Int. Work. Microprocess. SOC Test Verif.*, (2017), pp. 51–56. https://doi.org/10.1109/MTV.2017.16
2. M. Frustaci, P. Pace, G. Aloi, G. Fortino, Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet Things J. **5**(4), 2483–2495 (2018). https://doi.org/10.1109/JIOT.2017.2767291
3. Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the Internet of Things: Perspectives and challenges. Wirel. Netw. **20**(8), 2481–2501 (2014). https://doi.org/10.1007/s11276-014-0761-7
4. N. Sklavos, Malware in IoT software and hardware, in *Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE'16)*, (Barcelona, 2017), pp. 8–11
5. Su, V. Danilo Vasconcellos, S. Prasad, S. Daniele, Y. Feng, K. Sakurai, Lightweight classification of IoT malware based on image recognition. Proc. Int. Comput. Softw. Appl. Conf. **2**, 664–669 (2018). https://doi.org/10.1109/COMPSAC.2018.10315