

## Chapter 5

# IoT Security, Future Challenges, and Open Issues

**Noshina Tariq**

 <https://orcid.org/0000-0002-9754-253X>

*Air University, Pakistan*

**Tehreem Saboor**

*Air University, Pakistan*

**Muhammad Ashraf**

*Air University, Pakistan*

**Rawish Butt**

*Air University, Pakistan*

**Masooma Anwar**

*Air University, Pakistan*

**Mamoona Humayun**

 <https://orcid.org/0000-0001-6339-2257>

*Jouf University, Saudi Arabia*

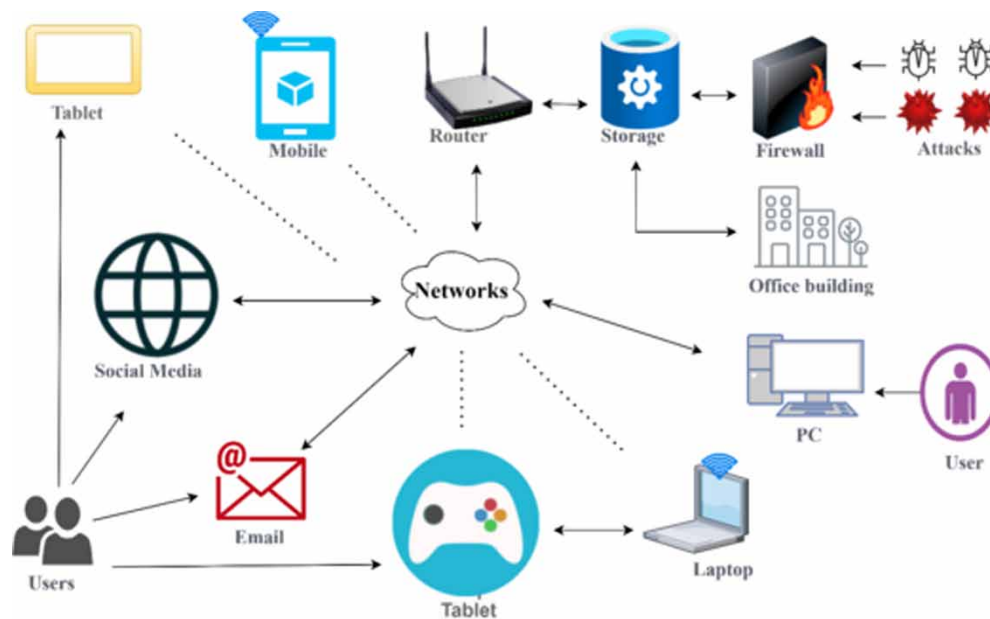
### ABSTRACT

*The internet of things (IoT) refers to the network of connected devices embedded in everyday objects that enable digital transformation. The rapid proliferation of IoT devices has led to significant advancements in technology and data exchange capabilities. However, the security of user data and IoT systems has become a paramount concern. This chapter focuses on the security challenges and approaches in IoT. Various attacks, such as denial of service, password guessing, replay, and insider attacks, pose significant threats to IoT security. It investigates the state-of-the-art technologies, future challenges and open issues currently facing IoT security. The findings from this chapter serve as a foundation for future work in improving IoT security and protecting user data effectively.*

## INTRODUCTION

The Internet of Things (IoT) is a rapidly growing technology that has the potential to revolutionize many aspects of our lives. It enables us to connect physical objects and systems with each other, allowing for unprecedented levels of automation and control over everyday tasks. However, this increased connectivity also brings new security challenges which must be addressed for IoT devices to remain secure and reliable. This paper provides an overview of the current state-of-the-art in IoT security research, focusing on future challenges and open issues that need to be addressed to ensure the safe deployment of these technologies. The concept behind the Internet of Things (IoT) was first proposed by Kevin Ashton in 1999 (Akhtar, N. 2020). Since then, it has grown into one of the most important emerging technologies today due its ability to enable seamless communication between different types of connected devices such as sensors, actuators, controllers etc., thus enabling various applications ranging from smart homes and cities through industrial automation up until healthcare monitoring systems (Shafiq et al., 2022) As more and more “things” are being connected via networks like Wi-Fi or Bluetooth Low Energy (BLE), there is an increasing demand for robust security solutions that can protect them against malicious actors who might try to gain unauthorized access or disrupt their normal operation. A general representation of IoT is depicted below in Figure 1.

*Figure 1. Internet of things*



The Internet of Things (IoT) is a rapidly evolving technology that has become an integral part of our daily lives, allowing us to connect and interact with the physical world in ways never before possible. IoT devices are becoming more powerful, interconnected, and ubiquitous every day; however, this also raises significant security concerns surrounding these technologies. As the number and complexity of

23 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/iot-security-future-challenges-and-open-issues/339249](http://www.igi-global.com/chapter/iot-security-future-challenges-and-open-issues/339249)

## Related Content

---

### Impact of Brand Trust and Technology Readiness on the Willingness to Use Autonomous Cars in Brazil

José Carlos Rodrigues and Mateus Canniatti Ponchio (2020). *International Journal of Business Strategy and Automation* (pp. 56-72).

[www.irma-international.org/article/impact-of-brand-trust-and-technology-readiness-on-the-willingness-to-use-autonomous-cars-in-brazil/265496](http://www.irma-international.org/article/impact-of-brand-trust-and-technology-readiness-on-the-willingness-to-use-autonomous-cars-in-brazil/265496)

### Auditing in the New Age of Industry 4.0: The Need for More Research

Chijioke E. Nwachukwu, Timothy Onechojon Usman, Sadiq Oshoke Akhor and Agboola Omoniyi Oladipupo (2021). *International Journal of Business Strategy and Automation* (pp. 17-28).

[www.irma-international.org/article/auditing-in-the-new-age-of-industry-40/269494](http://www.irma-international.org/article/auditing-in-the-new-age-of-industry-40/269494)

### Securing the Digital Supply Chain Cyber Threats and Vulnerabilities

Siva Raja Sindiramutty, Noor Zaman Jhanjhi, Chong Eng Tan, Navid Ali Khan, Bhavin Shah and Loveleen Gaur (2024). *Cybersecurity Measures for Logistics Industry Framework* (pp. 156-223).

[www.irma-international.org/chapter/securing-the-digital-supply-chain-cyber-threats-and-vulnerabilities/339251](http://www.irma-international.org/chapter/securing-the-digital-supply-chain-cyber-threats-and-vulnerabilities/339251)

### Similarity Measure Optimization for Target Detection: A Case Study for Detection of Keywords in Telephone Conversations

Batuhan Gundogdu and Murat Saraclar (2019). *Operations Research for Military Organizations* (pp. 347-374).

[www.irma-international.org/chapter/similarity-measure-optimization-for-target-detection/209812](http://www.irma-international.org/chapter/similarity-measure-optimization-for-target-detection/209812)

### An Overview of Feeder Services in the Era of Mega Containerships

Olcay Polat (2017). *Global Intermediation and Logistics Service Providers* (pp. 317-339).

[www.irma-international.org/chapter/an-overview-of-feeder-services-in-the-era-of-mega-containerships/176046](http://www.irma-international.org/chapter/an-overview-of-feeder-services-in-the-era-of-mega-containerships/176046)