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

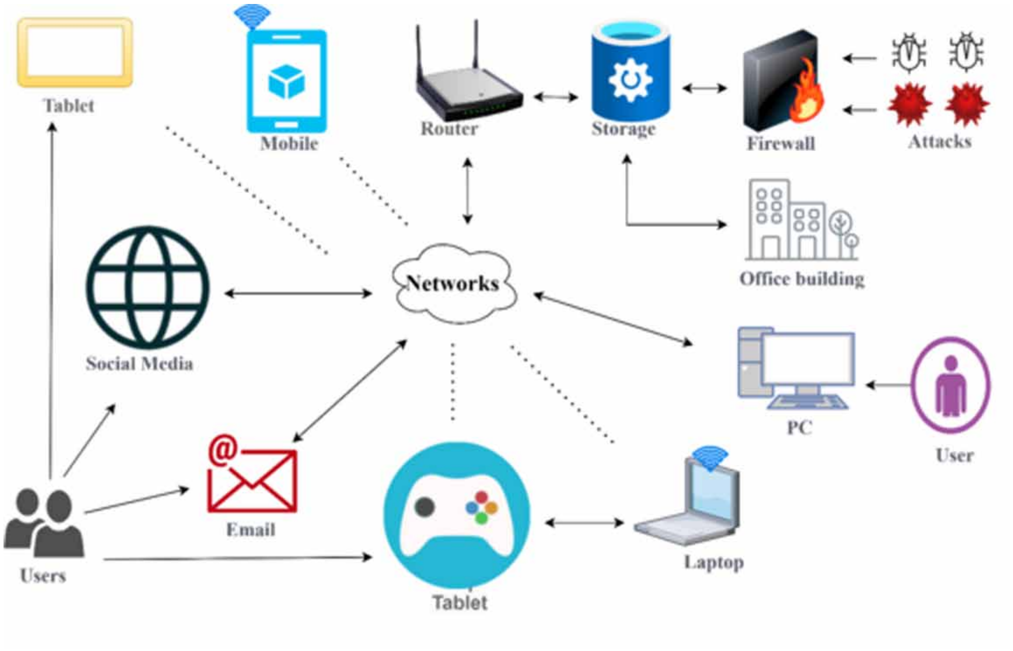
The internet of things (IoT) refers to the network of connected devices embedded in everyday objects that enable digital transformation. The rapid proliferation of IoT devices has led to significant advancements in technology and data exchange capabilities. However, the security of user data and IoT 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.

DOI: 10.4018/978-1-6684-7625-3.ch005

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