International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 12, No.1 (Oct-2022)

https://dx.doi.org/10.12785/ijcds/120198

Challenges for Security in IoT, Emerging Solutions, and Research Directions

Iraq Ahmad Reshi[1] **and Sahil Sholla**[1]

[1]*Department of Computer Science and Engineering, Islamic University of Science and Technology, Kashmir, JK, India*
Received 22 Jan. 2021, Revised 15 Jul. 2022, Accepted 23 Jul. 2022, Published 1 Oct. 2022

Abstract: : Internet of Things (IoT) systems have gained huge popularity in the past decade. This technology is developing as a back boon from the day-to-day utility in smart homes to intelligent power grids. It has become ubiquitous in the past decade while gaining popularity in academia and industry. As the devices used are usually sensors without a well-developed user interface, they are vulnerable to various threats. In this survey article, we have undergone some of the security challenges the technology faces and how the recently emerging technologies can provide an escape. Emerging technologies like blockchain, AI, and Deep learning techniques provide a platform where IoT operations are carried out successfully and securely. However, specific challenges need to be dealt with before implementing these in practice. We have briefly reviewed the role of particular technologies in securing IoT devices.

Keywords: Fog Computing, Blockchain, Quantum Cryptography, Tiny Encryption, Machine Learning, Deep Learning

1. Introduction

By 2025, the total deployment of Internet of Things (IoT) linked devices is predicted to reach 30.9 billion elements, a significant increase from the 13.8 billion devices that were expected by the end of 2021[1]. IoT architecture include Sensing layer, which is the data collection layer, the Network layer which undertakes the communication part, and the application layer that enables services and user interface. A typical IoT architecture where data collected from sensors is transmitted to the cloud via a gateway as shown in figure 1. The data can be visualized at a user interface. The four-layer architecture includes separation of application and services and the five-layer architecture further adds a business layer over the application layer. Though IoT has found a vast application in several areas including Healthcare, Vehicular traffic management, smart homes, smart cities, and a lot more, still it poses certain challenges that need to be addressed. Since an IoT network is mainly composed of sensors with limited device capabilities like battery and processing so there is a lot of management and operational issues other than traditional networks. A lot of IoT features have included vulnerabilities. With the heterogeneous nature of devices and by their interconnection a lot of interfaces need to be integrated. Hence it becomes more difficult to secure the system using one security protocol[2].

As IoT is the fusion of sensor networks with traditional network systems, it brings extra security vulnerabilities with its existence. Some researchers call it the Internet of Threats due to its weak secure infrastructure [3]. With the number of connected devices still on the rise, users feel insecure about the privacy and security issues, due to the heterogeneity of protocols and devices. In the past decade, several important surveys have been written on the topic. Tables 1 and 2 discuss the contribution of multiple researchers. Moreover, table 2 summarizes the contribution of proposed research articles considering the technological solutions discussed. The primary focus of our survey is to introduce the subjects to the broader scope of cutting-edge technologies that are enormously promising security solutions for IoT systems. These technologies will revolutionize the context of IoT networks in the near future. The rest of the paper is organized as follows. Section 2 briefs about various IoT security challenges. Section 3 describes the emerging technology solutions including Machine Learning (ML), Blockchain, Tiny encryption, Quantum resistant approaches, and Fog and edge computing. Section 4 briefs about the future research motivation. In section 5, we conclude the survey.

2. Security Challenges

The lack of a proper interface in IoT devices adds to their vulnerability. In past years we witnessed various large-scale IoT attacks that changed the whole perspective of security. Mirai malware generated data in terabytes by using common factory default User-id and passwords. It took down thousands of systems in 2016 and is still active [15]. Similarly, Stuxnet targets programmable logic controllers (PLCs), initially destroyed plants in Iran, and is active still and not domain-specific [16]. According to a CNN report in 2017, implantable medical devices possess vulnerabilities

E-mail address: rshiraq333@gmail.com, sahilsholla@gmail.com