


Chapter 7

Analysis of Vulnerabilities in IoT and Its Solutions

Puspanjali Mallik

 <https://orcid.org/0000-0002-3896-3457>

Shailabala Women's Autonomous College, India

ABSTRACT

The internet of things (IoT) fulfils abundant demands of present society by facilitating the services of cutting-edge technology in terms of smart home, smart healthcare, smart city, smart vehicles, and many more, which enables present day objects in our environment to have network communication and the capability to exchange data. These wide range of applications are collected, computed, and provided by thousands of IoT elements placed in open spaces. The highly interconnected heterogeneous structure faces new types of challenges from a security and privacy concern. Previously, security platforms were not so capable of handling these complex platforms due to different communication stacks and protocols. It seems to be of the utmost importance to keep concern about security issues relating to several attacks and vulnerabilities. The main motive of this chapter is to analyze the broad overview of security vulnerabilities and its counteractions. Generally, it discusses the major security techniques and protocols adopted by the IoT and analyzes the attacks against IoT devices.

INTRODUCTION

Everyday information security brings new challenges because of its wide availability in each field starting from personal to commercial lives. Data must be protected from interception, theft and attack caused by unauthorized persons or hackers (F.Meneghello et.al, 2019). Network security is one part of information security

DOI: 10.4018/978-1-5225-9493-2.ch007

19 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/analysis-of-vulnerabilities-in-iot-and-its-solutions/262551

Related Content

Taxonomy of Computer Network Congestion Control/Avoidance Methods

Mirza Waseem Hussain, Sanjay Jamwal, Tabasum Mirza and Malik Mubasher Hassan (2021). *Managing Resources for Futuristic Wireless Networks* (pp. 178-212).

www.irma-international.org/chapter/taxonomy-of-computer-network-congestion-control/avoidance-methods/262552

Impact of Frame Duration and Modulation Coding Schemes With WiMAX Bandwidth Asymmetry in Transmission Control Protocol Variants

Kailash Chandra Bandhu and Ashok Bhansali (2019). *International Journal of Wireless Networks and Broadband Technologies* (pp. 35-45).

www.irma-international.org/article/impact-of-frame-duration-and-modulation-coding-schemes-with-wimax-bandwidth-asymmetry-in-transmission-control-protocol-variants/237190

GAIA Bus: Cloud Computing Services for Agro-Food Chain

Georgios Kormentzas (2015). *International Journal of Wireless Networks and Broadband Technologies* (pp. 16-28).

www.irma-international.org/article/gaia-bus/125816

Link Failure Avoidance Mechanism (LFAM) and Route Availability Check Mechanism (RACM): For Secure and Efficient AODV Routing Protocol

Meeta Singh and Sudeep Kumar (2018). *International Journal of Wireless Networks and Broadband Technologies* (pp. 1-14).

www.irma-international.org/article/link-failure-avoidance-mechanism-lfam-and-route-availability-check-mechanism-racm/209431

Node Localization: Issues, Challenges and Future Perspectives in Wireless Sensor Networks (WSNs)

Noor Zaman, Azween Abdullah and Muneer Ahmed (2012). *Wireless Sensor Networks and Energy Efficiency: Protocols, Routing and Management* (pp. 223-235).

www.irma-international.org/chapter/node-localization-issues-challenges-future/62737