Medicon Engineering Themes
Volume 1 Issue 2 November 2021
Perspective

Security of Internet of Things

Smita Sanjay Ambarkar*

Lokmanya Tilak college of Engineering, India

***Corresponding Author:** Smita Sanjay Ambarkar, Lokmanya Tilak college of Engineering, India.

Received: October 22, 2021; **Published:** November 08, 2021

Introduction

Internet of Things (IoT) escalates the technology to new heights thereby tremendously increasing the ranges of the connected applications [1]. The applications of IoT mainly include healthcare, agriculture, smart homes, vehicles, mart cities, smart grids etc. The IoT creates revolution in all the applications using the interconnection of embedded devices like sensors, actuators, gateways. The services provided by these IoT based applications are resultantly excellent. However this ubiquitous computing generates the huge data and therefore the protection i.e. providing privacy and security to this data is a prime concern. If the security and privacy of this data is not taken care of then it highly impedes the future development. Many IoT devices uses the open source software which further enhances the insecurity in these devices [2]. The major difficulties while incorporating the security and privacy are the highly dynamic topology, unattended deployment, heterogeneous architecture, multi hop routing and resource constrained devices. The world witnessed the Mirai Attack on oct 2016 because of the proliferation of the tiny devices. The Mirai malware is able to exploit the tiny IoT devices only because of the lack of inherent security mechanism [3]. Nowadays a lot of research is going on to secure IoT devices [4]. The basic aim of this issue is to gather information about the recent research contribution and efforts by academia, industry practitioners to improve the security and privacy of the tiny IoT devices. The issue will also focus on the new proposals to enhance the existing protocols of the IoT stack so that the inherent security and communication mechanism will get strengthened. The studies must explore the lightweight techniques to achieve CIA (Confidentiality, authentication, Integrity) triads. The studies must further include the other challenging aspects of IoT like implementation of Intrusion Detection System, fog computing, data analytics etc. The enhancement of IoT security not only enhances the efficiency of the application but also protects the leakage of user confidential data.

References

1. Yongrui Qin., et al. "When things matter: A survey on data-centric internet of things". J. Netw. Comput. Appl 64 (2016): 137-153.
2. Hu H., et al. "REPLACE: A reliable trust-based platoon service recommendation scheme in vanet". IEEE Trans. Veh. Technol 66.2 (2017): 1786-1797.
3. Wang H., et al. "Special issue on Security, Privacy and Trust in network-based Big Data". Inf. Sci. Int. J 318.C (2015): 48-50.
4. Wang H., et al. "Editorial: Special Issue on Security and Privacy of IoT". World Wide Web 21 (2018): 1-6.

Volume 1 Issue 2 November 2021