International Journal of Computing and Network Technology
ISSN (2210-1519)
Int. J. Com. Net. Tech. 7, No. 3 (Sept.-2019)

http://dx-doi.org/10.12785/ijcnt/070302

Internet of Things Security: Issues, Challenges and Counter-Measures

Asifa Nazir[1], Sahil Sholla[2] and Adil Bashir[3]

1,2,3Department of Computer Science & Engineering,Islamic University of Science &Technology, Awantipora, India

Received: 25 May. 2019, Accepted: 13 Augs. 2019, Published: 1 Sept. 2019

Abstract: The Internet of Things (IoT) is one of the most promising technologies that seeks to improve quality of life by providing smart civic amenities. Several smart application domains that are envisaged include agriculture, industry, healthcare, transportation etc. IoT nodes are provided with unique identification numbers having ability to transfer data over the network without requiring human intervention. The ubiquitous communication among IoT devices leads to several security vulnerabilities. This paper presents a survey of security issues, challenges and attacks at different layers of IoT architecture. Moreover, we discuss counter-measures that can be adopted as well as possible future research directions. Security issues along with possible counter-measures are discussed in a layer wise manner with the aim to provide researchers with a bird's eye view of IoT security landscape.

Keywords: Internet of things (IoT), Security, Challenges, Attacks, Counter-measures

1. Introduction

The term Internet of Things was first introduced by Kevin Ashton in 1999, which actually now grows into reality by interconnecting real world things present in the universe around people to the internet [2]. In recent years IoT has been drawing wide attention of researchers. An annual report on "Internet of Things" was released by International Telecommunication Union (ITU) in 2005 [3].ITU in this report mainly focussed on the RFID and smart computing era that interconnects things at large level globally. IoT applications have been growing rapidly these days due to the presence of technologies like Radio Frequency Identification (RFID) and wireless communicating sensor technology. The RFID technology enables us to uniquely label every single node in network thereby serving as fundamental identification technique in IoT [1].

Internet of Things (IoT) is a system of interconnected computing devices, services and humans provided with unique identification numbers having ability to transmit, share, and communicate data over IoT network without requiring human intervention. IoT has different application domains like healthcare, retail, agriculture, transportation, manufacturing and business. Things in IoT trail an identity method (UID'S) by which each and everything can be identified in an environment of homogenous and heterogeneous devices. Further, every area in IoT is identified by unique IP. With the increased prevalence of IoT there is significant growth in the number of links and networks via which almost everyone connects using devices like desktop, smartphone, PDA, etc. Due to presence of large number of low-cost and small sized sensor devices, technology is putting forward new demands to the Internet technology. Also, IPV6 has made IoT services available more efficiently by accommodating large amount of addresses so as to provide IP address to each thing in IoT network. It has been anticipated that very soon all the smart things that we have around us are going to be internet worked with the aim to provide better services. Therefore, the main aim is to revolutionize the manner people live today by making smart devices around them performing daily tasks whether simple or complex in much more simpler way like smart homes, smart cities, smart transportation, smart grid, smart building, smart environmental monitoring etc. [1].

Since IoT has become a key element of future internet technology, therefore it becomes important to provide satisfactory security mechanism for IoT devices. In IoT context awareness has its own role to play as it refers to the idea of a smart things being aware of their

E-mail address: malikasifa356@gmail.com, sahilsholla @ gmail.com adilbashir.445@ gmail.com

http://journals.uob.edu.bh