A Critical Analysis on the Security Concerns of Internet of Things (IoT)

M.U. Farooq
Electronic Engg. Dept.
PAF-Karachi Institute of Economics and Technology, Pakistan

Muhammad Waseem
Telecommunication Engg. Dept.
Sir Syed University of Engg. and Technology, Pakistan

Anjum Khairi
Electronic Engg. Dept.
Sir Syed University of Engg. and Technology, Pakistan

Sadia Mazhar
Electrical Engg. Dept.
Sir Syed University of, Engg. and Technology, Pakistan

ABSTRACT

Internet of Things (IoT) has been a major research topic for almost a decade now, where physical objects would be interconnected as a result of convergence of various existing technologies. IoT is rapidly developing; however there are uncertainties about its security and privacy which could affect its sustainable development. This paper analyzes the security issues and challenges and provides a well defined security architecture as a confidentiality of the user's privacy and security which could result in its wider adoption by masses.

Keywords:

Internet of Things, IoT, IoT security goals, IoT security challenges and issues, IoT security architecture.

1. INTRODUCTION

The term, Internet of Things, a system of interconnected devices, was first proposed by Kevin Ashton in 1999 [1]. It is a major technological revolution that has updated the current Internet infrastructure to a concept of much more advanced computing network where all the physical objects around us will be uniquely identifiable and ubiquitously connected to each other [2]. By this continually emerging technology everything around us like televisions, refrigerators, cars and clothes etc will be collecting some useful data with the help of various existing technologies, which will then be autonomously flowing the data to the concerned devices and on the basis of which automated actions will be taken.

With a number of researches being carried out, the vision of IoT is likely to be a reality very soon. According to Gartner, around 25 billion uniquely identifiable objects are expected to be a part of this global computing network by the year 2020 [3], which is impressively a big number, however prevalence of such a big network of interconnected devices will pose some new security and privacy threats and put all those devices at a high risk of hackers as they clutch at the security gaps to make the devices work for their personal benefits.

IoT definitely has a great potential for flexibility and promises a great future but it has a potential of security disaster too. There are many questions for its wide adoption and without answering them and coming up with proper solutions for the newly posed threats, it does not seem to have any future [4]. Due to easy accessibility of the objects, it can be easily exploited by the evil-minded hackers [5]. No matter how much secure companies think their products are, they are still prone to various kinds of attacks so they must ensure proper security by making the patches available as soon as any vulnerability is detected in the system. Since the devices have a direct impact on the lives of users so security considerations must be a high priority and there must be some proper well-defined security infrastructure with new systems and protocols that can limit the possible threats related to scalability, availability and security of IoT [6].

The paper is organized as follows. Section 2 describes the generic architecture of IoT. Section 3 describes the security goals. Section 4 discusses the major security challenges and issues on each layer. Section 5 presents the security architecture of IoT and finally Section 6 concludes the paper.

2. GENERIC ARCHITECTURE

Generally, IoT has four main key levels as shown in Fig. 1, which are described below [7]:

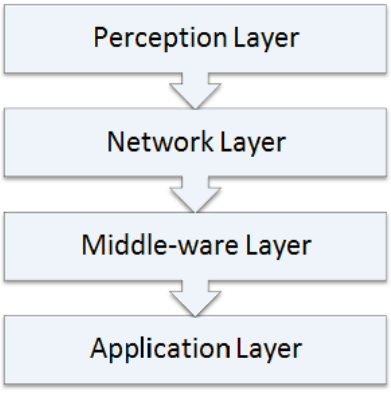

Fig. 1. Generic Architecture of IoT