A Survey, Design and Analysis of IoT Security and QoS Challenges

M Kesavan, Research Scholar, SITE, VIT University, Vellore, India
J Prabhu, VIT, Vellore, India

ABSTRACT

IoT is a technological exemplar with a vision of “Everything is connected” enabling everyone to publish their generated data collected from different heterogeneous and homogenous systems onto the web. The basic concept of IoT is connectivity, a set of physical objects that use network support to exchange data. These objects can be software, boards, sensors, etc. In the real end to end network deployment, IoT is a platform and cloud is one part of it. In order to turn the IoT vision into reality high reliability, security and QoS are required to support the communications between the homogenous and heterogeneous networks. The security and QoS are critical factors in the real End to End topology. In this article, the authors proposed the various challenges for IoT security, and IoT routing between the edge and cloud.

KEYWORDS
Integration, Interoperability, Quality of Service [QoS] Cloud, Security

1. INTRODUCTION

Internet plays a very important role for the devices to communicate with the help of protocols. In recent technological fields, Each IoT devices has unique identity and unique Identifier (Ip address and Url). Most of the IoT devices has an interface allows users to query the devices, monitor and control them remotely (Weber, 2010). These devices communicate to the other smart things wirelessly thus connecting them to internet and making them establish their ID and identifier status on the web. Eventually an IoT is formed, which is in turn used as an IoT application by human users. These devices can be used as tool for tracking, observing and influencing the real world. Miniatures of these devices are created and attached to other objects such as people, desk are rooted into places like home, office etc. A wireless network of these devices are formed. A good example is RFID tags.

The entity is brought from origin to a destination by routing the packets without losing the Integrity. These devices can either be an IoT or an Internet device. This approach involves routing and better security in the layers.

1.1. Background of IoT

The IoT is simply the network of interconnected things which are embedded with sensors, software, and network connectivity and embedded devices that enable them to collect and exchange data making them accessible over the Internet. IoT brings useful applications like home automation, smart health monitoring, security, automated devices monitoring and management of daily tasks. Every sector like Energy, Computing, Management, Security and transportation are going to be benefited with
this new paradigm (IEEE Internet of Thing Journal Evaluating critical security issues of the IoT world: Present and Future challenges of IoT, n.d.). Development of sensors, actuators, smart phones, RFID tags makes it possible to materialize IoT which interact and co-operate each other to make the service better and make accessible at any time, from anywhere using any network. Wireless sensor technology allows objects to provide real-time environmental information and context. IoT allows objects to become more intelligent which can think and communicate among them.

As the number of devices connected to the internet is growing in rate, the concept of IoT has gained power. Survey has revealed that there will be billions of devices connected to IoT serving various purposes in day to day life (Al-Fuqaha et al., 2015). This results in development of applications in various domains, whereas the application depends on QoS requirements.

The QoS requirements classified are Best effort, Differentiated services and guaranteed services. The guaranteed services known as hard QoS should use suitable mechanism at each layer of IoT architecture. A delay in any layer could lead to unacceptble QoS, in order to provide guaranteed services it is important to know QoS has been addressed properly at each layer (Ahsan et al., 2016).

In the real deployment, IoT is connected to different backend systems with different Vendors. Due to high heterogeneity and scalability upgrading the devices for various Malware, virus scanning, and software Functionality is highly challenging. Numerous vendors and integrators likely would be involved over the lifetime of the device, requiring a collaborative mix of standards-based, proprietary and open-sourced components (Stoimenovic & Wen, 2014; Qu &Chan 2016).

As a result, security solutions for the devices are indeed with strong hardware-based security, and legacy devices should be protected behind purpose-built gateways (Khari et al., 2016).

Also, there is no single, perfect level of security. Various devices at different companies have varying risk profiles. Creating just the right security level is achievable, through evaluating the risk, use and capability of every device. IoT security focus is more on data than the device. Due to immense use and importance of the Internet of Things, it has become paramount to secure it. IoT security is so critical because private information could be stolen from the use of connected devices.

2. ANALYSIS ON IOT

As mentioned in the introduction, the IoT is nothing but devices communicate through the internet when they are enabled and don’t communicate if they are disabled. Example: Smart TV, Online games through computer/Xbox etc. The best example of this is the RFID tags, which enables each device to communicate with each other over any network connectivity altogether resulting in exchange of information in a better and smarter manner (Al-Fuqaha et al., 2015).

IOT has given a concept of Machine to-Machine (M2M) communication. Implementing strategy to capitalize on the Internet of Things so that you can just stop your business and starts making it thrive. IOT is going to have huge impact on home automation and building automation system where every convenience will be taken care of by the interconnected devices on IOT.

The major characteristics of IoT objects are to sense, tiny in size, limited capability, and limited energy, connected to the physical world, intermittent connectivity and mobility, managed by devices and not by People (Aljawarneh, 2012).

2.1. IoT Architecture

There is no single agreement on architecture for IoT, which is agreed universally. Different architectures have been proposed by different researchers (Gubbi et al., 2013; Han et al., 2016; Hao, 2015) based on the use cases. Earlier researchers identified the three layer architecture as key for the Internet of Things (Desai et al., 2015; Van der Veer & Wiles, 2008). When we deep dive for many user deployment, the IoT architecture is decoupled and the layers are well augmented for better understanding and requirements. This could be one of the reasons that the five layered architectures are proposed (IEEE Internet of Things Journal Evaluating critical security issues of the IoT world: Present and Future
Silicon Validation of GALS Methods and Architectures in a State-of-the-Art CMOS Process


www.igi-global.com/chapter/silicon-validation-of-gals-methods-and-architectures-in-a-state-of-the-art-cmos-process/108454?camid=4v1a