A Review on Internet of Things (IoT)

Steffen Marbach
Universität zu Lübeck
Lübeck, Germany
steffen.marbach@student.uni-luebeck.de

Summary of the work with the same name by M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi, Talha Kamal [1]

Abstract

For now, we communicate either human to human or human to a device. The Internet of Things (IoT) makes a change through machine-to-machine (M2M) communication. This Paper provides a six-layered architecture of IoT and discusses the related key challenges and the associated safety threats.

1 INTRODUCTION

IoT is continually evolving. The opportunities seem infinite. It could provide a global computing network where everything and everyone connects to the Internet. The number of devices availing of internet services is increasing every day.

The first IoT device dates back to 1982. A modified coke machine was competent to report the drinks contained and whether the drinks were cold by communicating through the Internet[2].

The basic idea of IoT is to allow an autonomous exchange of information between embedded different real-world devices around us, using leading technologies like Wireless Sensor Networks (WSNs) and Radio-Frequency Identification (RFID) which are sensed by the sensor devices and further processed for decision making, based on which an automated action is performed.

2 ARCHITECTURE

The existing architecture of the Internet with TCP/ IP protocols cannot handle a network as extensive as IoT. So there is a need for a new open architecture, that can handle this issue. This architecture should ensure security and Quality of Service (QoS). Without suitable data protection, IoT will not be adopted by many. [4] proposed a six-layered architecture divided into the six layers shown in Figure 1. This section will present the six layers of the IoT architecture.

2.1 Coding Layer

In this layer, each object gets its unique ID to provide an easy discern [4].

2.2 Perception Layer

This layer consists of data sensors like RFID Tags, IR Sensors, etc. Which could sense the temperature, humidity, location, etc. It passes the sensor data onto the Network Layer for further action by converting it into a digital signal.

2.3 Network Layer

This layer receives digital signals from the Perception layer with the given information in it. The Network layer's job is to transmit this information to the Middleware layer. For this job, there are used transmission mediums like Bluetooth, WiFi, 3G, etc. with fitting protocols like IPV6, IPV4, etc.

2.4 Middleware Layer

This layer processes the information provided by the Perception layer through the Network layer. It includes technologies like Cloud computing with direct access to a database to store the data. In some Intelligent Processing Equipment, based on the processed results of the in-

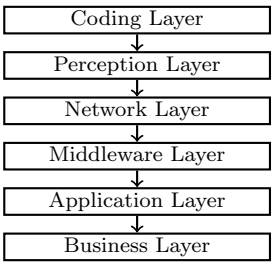

Figure 1: Six-Layered Architecture of IoT

formation a fully automated action is taken.

2.5 Application Layer

With the processed data this layer holds the bandwidth of applications of IoT. The IoT-related applications could be smart homes, transportation, planet, etc.

2.6 Business Layer

This layer combines the applications and services of IoT by managing and merging them to provide different business models.

3 APPLICATIONS

Several possible future applications can be of great advantage like smart Hospitals, smart agriculture, smart traffic systems, etc. In this section, we present two of them:

3.1 Smart Environment

IoT will predict natural disasters such as floods, fires, earthquakes, etc. Also, there will be proper monitoring of air pollution in the environment.

3.2 Smart Home

IoT will provide solutions for Home Automation. We could remotely control our appliances, monitor utility meters, energy, and water supply to help save resources, and build an encroachment detection system that could prevent burglaries. Also, gardening sensors could measure light, humidity, temperature, and other gardening vitals. IoT could water plants according to their needs.

4 SECURITY AND PRIVACY

IoT makes everything and a person localizable and addressable. So IoT must have a robust security infrastructure. This section will present some of the possible IoT-related issues.

4.1 Unauthorized Access to RFID

Unauthorized access to tags is a fundamental issue. Some real-life threats of RFID are RFID Viruses, Side Channel Attacks with a cell phone, and SpeedPass Hack.

4.2 Sensor-Nodes Security Breach

WSNs are vulnerable to attacks because sensor nodes are part of a bi-directional sensor network. [5] described some of the possible attacks that include Jamming, tampering, Sybil, Flooding, and some other kinds of attacks

4.3 Cloud Computing Abuse

The shared resources can face security threats like Man-in-the-middle attacks (MITM), Phishing, etc. The Cloud Security Alliance (CSA) draws attention to hazard like Data Loss, Accounts Hijacking, the Monstrous use of Shared Computers, etc. [3] describes this and other problems closer.

5 CONCLUSION

The IoT is getting bigger and will affect every part of our life. It ranges from automated houses to monitoring health and the environment. We discussed future applications and a six-layered architecture for their use. And the associated safety threats. The development of IoT explains solutions for its security and data protection threats.

References

[1] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi, and Talha Kamal. A review on internet of things (iot). *International Journal of Computer Applications (0975 8887)*, 113(1), 2015.

[2] Carnegie Mellon. The "only" coke machine on the internet. *The Carnegie Mellon University Computer Science Department*, 2014.

[3] S.R.Taghizadeh V. Ashktorab. Security threats and countermeasures in cloud computing. *in International Journal of Application or Innovation in Engineering and Management (IJAIEM)*, 1(2), Oct'12.

[4] Fuquan Sun Xu Cheng, Minghui Zhang. Architecture of internet of things and its key technology integration based-on rfid. *in Fifth International Symposium on Computational Intelligence and Design*, pages 294–297, 2012.

[5] G.Attebury Y.Wang and B.Ramamurthy. A survey on security issues in wireless sensor networks. *in IEEE communications Survey and Tutorials*, 2006.