

Internet of Things: Unabridged Solution

Romika Choudhary
Assistant Professor
FET, MRIIRS

Ashish Vats
Assistant Professor
FET, MRIIRS

Gagandeep Kaur
Assistant Professor
FET, MRIIRS

Ila Chaudhary
Assistant Professor
FET, MRIIRS

Swathi Sharma
Assistant Professor
CMRIT, Bangalore

ABSTRACT

In essence, all computing devices can perform only computational operation with limited communicating capabilities. Proliferation of sensor take “things” to another level and an era of Internet of Things (IoT) get start. IoT is a multilayered structure which provides ease of optimization, prediction and strategic evolution. Applications of IoT improve the quality of a common man life as it can be deployed from smart farming to smart home. IoT has the potential to provide a simplified solution to a complex real life problem [1-2]. IoT gives us abundant facilities but can cost us in terms of data security.

Keywords

Internet of Things (IoT), RFID (Radio Frequency Identification), WSN (Wireless Sensor Network)

1. INTRODUCTION

With the persistent headways in innovation, IoT provides a global solution in which everybody and everything will be connected to the Internet [3]. Internet of Things (IoT) as the name says is the wireless arrangement of multiple commutable devices(things) that can communicate with each other with the help of internet and can share the data on cloud for analytics purpose without any human involvement [4]. It is possible only due to the invent of sensors and technologies such as RFID (Radio Frequency Identification), WSN (Wireless Sensor Network) etc.



Fig. 1: Internet of Things

In 1982, concept of IoT came into the picture when in an industry a coke machine was linked with the Internet and could predict the temperature of beverage and capable of file the drinks contain [5]. Later, in 1991, Mark Weiser showed the ubiquitous computing features of IoT [6]. Bill Joy, in 1999, gave a methodology for device to device

communication in his taxonomy of internet [7]. Kevin Ashton proposed the term “Internet of Things” to describe a system of interconnected devices in 1999 [8].

The fundamental concept of IoT is to permit self-sufficient change of useful records among invisibly embedded various devices of the real world around us. These embedded devices are fueled by using the leading technologies like Radio-Frequency Identification (RFID) and Wireless Sensor Networks (WSN) [9] which can be sensed with the aid of the sensor gadgets and in addition processed for selection making, on the idea of which an automatic action is accomplished [10].

Multiple IT companies have their unique vision of IoT. An article published in Network World interviewed some key IT providers and conclude the different methodology opt by them to build IoT solutions. HP’s have a vision to continually link the people with the advent of IoT. Intel is centered on empowering billions of current gadgets with intelligence. Cisco put his emphasis on industrial automation and convergence of multiple traditional operational technologies to a new rising technique. Microsoft believes that nowadays IoT exist in powerful gadgets which can talk to each other to provide futuristic era of IoT. While IBM focused on the remote controlling of IoT based gadgets and their security challenges to smartly transform the world [11]. IoT is constantly advancing and is the latest research point where infinite opportunities exist.

This review paper on Internet of Things is organized in the total 5 sections. Section 2 describes the basic architecture of Internet of Things and subsequent section shed light on the brief description of key application areas of IoT. Section 4 describes major security challenges in the Internet of things along with the future trends and final section 5 gives the summary of the paper.

2. ARCHITECTURE

IoT Technology has two development platforms i.e. software and hardware. To understand the architecture of Internet of Things it is required to have the knowledge of hardware and the software associated with it. Hardware and software both require different skill set for managing product development. Hardware design of the product plays a vital role as it impacts the IoT products’ cost, reliability, capabilities, and more.

IoT products are designed as per the users’ demand, so different IoT products have their customized IoT packages. IoT entrepreneurs opt a package which can satisfy the customer’s requirement, so a generalize hardware architecture cannot be proposed. However, in spite of the utility, every IoT

gadgets have few common “building blocks”, as shown in the Figure 2.

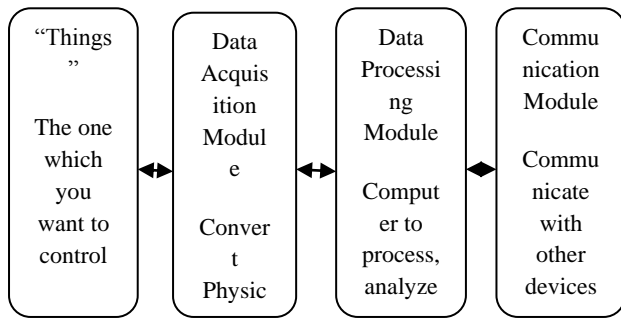


Fig. 2: Architecture of Internet of Things

“Things” is authentic as the device that you wish to control or monitor. Multiple IoT gadgets have integrated on-chip “things”. For example, IoT products like a smart vehicle, smart water pump, smart home and many more, can automatically control and monitor themselves. The function of data acquisition module is to collect physical signal from things and convert them into digital signals that can be manipulated by a computer. Data acquisition module includes all the sensors such as temperature, motion, light, vibration, etc. which can accept the real-world signals and convert them into a readable form. This block is also responsible for signal conditioning, analog-to-digital conversion, scaling, and interpretation operation.

The third block of architecture in the device is the data processing module which processes the data, interpret information by performing analytics, and store data either locally or on the cloud. The two challenges of data processing module are processing power and size of local data storage. The most important block of IoT hardware is the communications module. It is the circuitry that allows communications with cloud platform and with third-party devices. This module may additionally consist of communication ports inclusive of USB, serial (232/485), CAN, or Modbus.

Similarly, for software domain of IoT, a layered architecture was proposed to understand the data flow between various layers. Layered architecture of IoT is derived from the network hierarchical structure [12]. Normally, software architecture is divided into six layers as shown in the below Figure 3. The function of each layer of IoT architecture is described below:

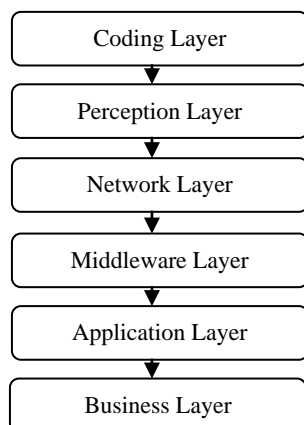


Fig.3 Layered architecture of Internet of Things

The first layer is the coding layer which provides the identification to the objects. Coding layer provides a unique identification number to each device, which uniquely identify each object in a network. Device layer of IoT, is Perception layer and its function is to provide a physical meaning to things. It consists of data sensors in multiple forms like RFID tags, IR sensors or other sensor networks [13] which could sense the temperature, velocity, humidity, health parameters and area etc of the objects. This layer converts the physical information into the digital signal with the help of sensors and passes it to the network layer for further action.

Network layer then passes on the information to the successor layer through the transmission mediums like Wi-Fi, Bluetooth, WiMax, Zigbee, GSM, 3G etc with protocols like IPv4, IPv6, MQTT, DDS etc. Middleware layer then stores the information received from perception layer to local storage or cloud. This layer consists of some intelligent processing system which processes the information and provides the necessary action required to perform a task. The application layer is responsible for data formatting and presentation. There are application layer protocols specified in context to IoT are MQT, SMQTT, CoAP, DDS, XMPP, AMQP, RESTful HTTP, MQTT-SN etc. The IoT related applications can be smart homes, smart transportation, smart planet etc.. the last layer, Business layer maintains coordination between the application and services of IOT and generates the different business model for different business.

3. APPLICATIONS

Nowadays mostly all devices that we use in our daily life are smart devices but they have limited communication capabilities with each other. IoT makes communication between these devices so that they can share useful information and a wide range of innovative devices can be developed [14]. These smart applications with some autonomous capabilities would absolutely shift the quality of our lives to next level [15]. For example, Google Car handles all the driving which makes driving more easy and safe. This self-driving car acquaintance with real-time traffic, road conditions, weather and other information exchanges [16], all due to the concept of IoT. The current section provides the details of few applications of IoT.

3.1 Smart Environment

An ample of research work in IoT has been carried out in developing countries like on the environment in India. IoT devices can be utilized in various domain of environment like pollution, weather, prediction of natural disaster etc. Air pollution is one of the major global issues. With the help of IoT devices, we can continuously monitor the quality of air and can also predict the natural disaster like fire, flood, earthquake etc. A huge number of industries put emphasis on connecting tiny devices and objects to infer and to measure environmental and ecological resources in their Research and Development units.

3.2 Smart Home

IoT also provides solutions for Home Automation with which we will be able to control our accessories remotely, as per our needs. IoT enables multiple features in our home like controlling appliances, monitoring of energy meter, home security, emergency identification and other similar applications. Outside the home, in garden we can use gardening sensors which can monitor the environmental factors like intensity of light, humidity, temperature, moisture and other gardening parameters.

3.3 Smart Educational Environment

IoT devices are widely used in the educational sector to record the attendance of student and staff, for tracking library books, to identify Laboratory equipment, to provide campus security and emergency alert and much more.

3.4 Smart Hospitals

IoT will facilitate life-saving applications in the healthcare domain. Hospitals can provide the smart flexible wearable bands with RFID tags to the patients, which can monitors the multiple parameters like heart rate, blood pressure, temperature and other condition of patient. In case of any emergency, it can send an alarm signal to the doctor as well as nurses irrespective of the presence of patients i.e. inside or outside the premises of hospital [17].

3.5 Smart Business System:

IoT plays a major role in business advancement. Sensors and the RFID tags make the business environment smarter. With RFID equipped products, a stock record can be easily maintained. Inventory control, goods and commodities identification, purchase or sales billing, surveillance, customer identification can also be done with the help of IoT. Moreover, the retailer can even accomplish the sales blueprint and graphs for effective strategies.

3.6 Government E- Services

Government E-Services can become much smart then today, if deployed the IoT technology in it. We can use RFID tags in Aadhar cards, Voter Id cards etc. People identification and tracking become easier with these smart cards.

4. SECURITY IN IoT

IoT has made the life easier than before, but every technology also has its dark side as well. The IoT make a step change in individuals “quality of life” at a cost of privacy of user’s data. If one affair can anticipate the Internet of things from transforming the way we reside and work, it will be a breakdown in security. The attributes of vast implementations of IoT present new and unique aegis challenges. Addressing these challenges and ensuring secure services must be a fundamental priority. The users must feel that they can control the privacy of data.

IoT is a network of interconnected devices, so if any device is poorly secured then it interns data threat to all network. This challenge becomes more complex when we use such poorly secured device on a mass scale in a network. So, a robust approach is needed to provide the security to IoT infrastructure [18].

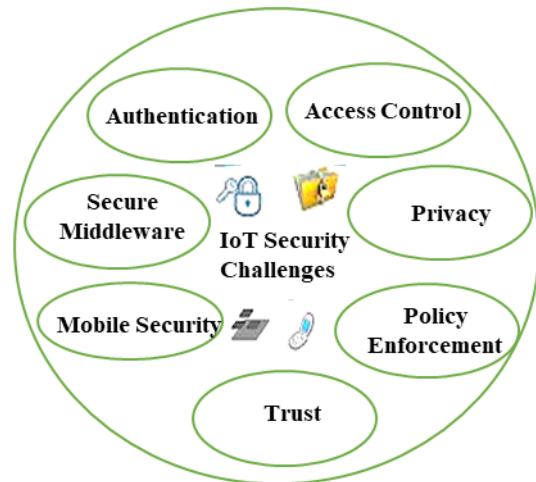


Fig. 4. Security Challenges in IoT

In designing of any IoT product, its security and testing framework plays an important role. For developing a robust IoT product we should be focused on the following key points:

Data Encryption: IoT applications collect tons of data. Data encryption can be made by using Secure Sockets Layer (SSL) protocol with some wireless protocol to protect the personal data like location, bank details etc.

Data Authentication: Data Authentication is required to prevent the hacking of IoT device. Due to data encryption, identification of data source cannot be made. So anyone can create a false data to misguide the IoT device. IoT devices without data authentication definitely pose a security risk.

Side-channel Attacks: Side channel attacks are more focused on the power consumption, timing information and the style of data presentation rather than contents of information.

Hardware Issues: IoT devices have a limitation of size and battery power consumption. Although the various chip designing company like Intel, upgrade their new generation processor with more security features, but battery power consumption and the cost will get increased. An affordable IoT gadget was unable to use these processors. So, still, there is a large gap between current security level of hardware and realistic scenarios.

5. CONCLUSION

This paper provides the overview of the Internet of Things and functional description of each building block of IoT architecture. An exponential growth of IoT makes it visible in various aspects of human life. We found the application of IoT from our home to our business. Sensors play a vital role in the development of IoT products, but due to heterogeneous nature of sensor, security of IoT products are also a key challenge for us. This paper also shed some light on the security aspects of IoT products and what solution can be made to provide a robust product. So, this is very precise with the insights that IoT is the next mega trend in lots of industries. IoT will potentially be contributing to industries like businesses in the utilities, oil & gas, healthcare, insurance, manufacturing, transportation, infrastructure and retail. Research efforts are required to develop a technology which integrates the IoT and communication technologies in a secure manner. We hope this paper will help in understanding the all key points for designing an IoT product.

6. REFERENCES

- [1]. L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, *Comput. Netw.* 54 (15) (2010) 2787–2805.
- [2]. D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, Survey internet of things: vision, applications and research challenges, *Ad Hoc Netw.* 10 (7) (2012) 1497–1516.
- [3]. Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer and Shahid Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in *Proceedings of Frontiers of Information Technology (FIT)*, 2012, pp. 257-260
- [4]. M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, M. Dohler, Standardized protocol stack for the internet of (important) things, *IEEE Commun. Surv. Tutorials* 15 (3) (2013) 1389–1406
- [5]. "The "Only" Coke Machine on the Internet," Carnegie Mellon University, School of Computer Science.
- [6]. M. Weiser, "The computer for the 21st century", *Sci. Amer.* 1991, pp.66 -75
- [7]. Jason Pontin, "Bill Joy's Six Webs," *MIT Technology Review*, 29 September 2005
- [8]. Kevin Ashton, "That 'Internet of Things' Thing", *RFID Journal*, 22 June 2009
- [9]. Karimi, Kaivan, and Gary Atkinson. "What the Internet of Things (IoT) needs to become a reality." White Paper, *FreeScale and ARM* (2013).
- [10]. Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, Internet of Things: A vision, architectural elements and future directions, *Future Generation Computer systems* 29 (2013) 1645–1660, Elsevier.
- [11]. Bob Violino, "Top IT Vendors reveal their IOT strategies". It can be accessed at: <http://www.networkworld.com/article/2604766/internet-of-things/top-it-vendors-reveal-their-iot-strategies.htm>
- [12]. Xu Cheng, Minghui Zhang, Fuquan Sun, "Architecture of internet of things and its key technology integration based-on RFID," in *Fifth International Symposium on Computational Intelligence and Design*, pp. 294-297, 2012
- [13]. Debasis Bandyopadhyay, Jaydip Sen, "Internet of Things -Applications and Challenges in Technology and Standardization" in *Wireless Personal Communications*, Volume 58, Issue 1, pp. 49-69
- [14]. R. Abdmeziem, D. Tandjaoui, "Internet of Things: Concept, Building blocks, Applications and Challenges, Computers and Society, Cornell University" in *International Journal of Computer Applications*, Volume 113, 2015.
- [15]. L. Atzori, A. Iera, G. Morabito, "The Internet of Things: A survey," in *Computer Networks - Science Direct* Volume 54, Issue 15, 28 October 2010, Pages 2787-2805.
- [16]. "What we're driving at," *Google Official Blog*. It can be accessed at: <http://googleblog.blogspot.com/2010/10/what-were-drivingat.html>.
- [17]. P. Fuhrer, D. Guinard, "Building a Smart Hospital using RFID technologies," in *1st European Conference on eHealth (ECEH06)*, Fribourg, Switzerland, October 12 - 13, 2006.
- [18]. "Internet of Things: An overview" by Internet Society https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf.