

An Analysis on the Challenges of IoT

L. Christina¹, T. Nithyakamala²

Assistant Professor, Department of Computer Science, Parvathy's Arts and Science College, Dindigul,
Tamilnadu. India^{1,2}

ABSTRACT: Today, Internet is one of the most important and powerful creations in all of human history. Internet of Things is a new concept for industries and it offers a platform to transfer the digital world. The impact of the Internet already has had on education, communication, business, science, government, and humanity. This paper mainly focuses on the key challenges associated with the development of IoT.

KEYWORDS: Definition of IoT and Challenges of IoT

I. INTRODUCTION

Internet of Things is a worldwide network communications between physical and virtual things through the development of data capture and communication capabilities. Cisco IBSG predicts there will be 25 billion devices connected to the Internet by 2015 and 50 billion by 2020[3]. The IoT is an intelligent network which connects all things to the Internet for the purpose of exchanging information and communicating through the information sensing devices in accordance with agreed protocols[2]. The definition of internet is not only a network of computers, but it has a network of device in different size and type, it may be smart phones, Transportation, Building, City, Lifestyle, Retail, Agriculture, Factory, Supply chain, Emergency, Healthcare, User interaction, Culture and tourism, Environment and Energy[8]. The definition of "thing" is very flexible, and may refer to: intelligent machines, drones, self-driving cars, sensor nodes measuring parameters such as temperature and humidity, actuators that turn on and off devices or make adjustments in real time, and much more[6].

The most accepted definition is "The Internet of Things is a global infrastructure for the information society that is able to provide advanced services through existing or evolving physical or virtual connections based on objects, compatible information and communication technologies. By expanding and developing the technology of the Internet of Things, each device in our environment will be able to communicate with another device and send information to them or control them, according to the information collected", defined by ITU in 2005[11].

II. CHALLENGES

The more devices are connected to the internet which emanates the large amount of data. The development of the IoT exposed many challenges including the architecture, standards and hardware and software issues.

A. Architecture

The communications among these devices are in a wireless, autonomic, and ad hoc manner. Infrastructure solutions will require systems to combine different volumes of data with their related features, to compare data to historical information, and support decision-making. Single reference architecture cannot be a suitable for all applications. Heterogeneous reference architectures have to coexist in IoT. IoT architectures should be flexible for RFID identification, intelligent devices, and smart objects [2]. The external architecture on the internet makes it possible for a substantial collaboration between billions of objects. The IoT needs an open architecture to increase providers and end user participation. Single-domain systems will become multi-domain, which will cause new challenges. IoT nodes may require decentralized autonomic and dynamic architectures based on peering of nodes. The architectural design also need Cloud computing, event-driven architectures, disconnected operations and synchronization technologies for processing, storing and retrieval of information.

B. Network Technology

The IoT deployment requires RFID, short-range wireless technologies and sensor networks for development. Different applications and environments need different networking technologies, and the ranges as well as other characteristics of cellular, WLAN, and RFID technologies are much different from each other. Communication technologies are either simple or complicated, should be low cost and with reliable connectivity. So, the new scalable sensor network communication architecture is needed to allow billions of devices. Applications have different requirements on what parties need to communicate with each other, what kind of security solutions are appropriate, and so on [2].

C. Hardware and Software Challenge

Smart devices with enhanced inter-device communication will lead to smart systems with high degrees of intelligence. The RFID and sensor network technologies consist of logic and analogue circuits with n and p type Thin Film Transistors (TFTs), power converters, batteries, memories, sensors and active tags. It forced to develop a cheap, non-toxic and disposable hardware device. Therefore, hardware researches are focusing on designing wireless identifiable systems with low size, low cost. As the bandwidth of IoT terminals could vary from kbps to mbps from sensing simple value to video stream, requirements on hardware are diverging. However, two essential requirements are low power consumption in sleep mode and the ultra low cost. The sleeping time is so far impossible when an IoT terminal is sleeping and receiving RF signals. It will be even difficult when using advanced CMOS silicon with relatively more leakage power. Hardware and protocol code design for sleeping has been the first hardware challenge of IoT [2]. One of the essential challenges in IoT is how to interconnect "things" in an interoperable way while taking into account the energy constraints, knowing that the communication is the most energy consuming task on devices [8].

Low active power is also a challenge for low-cost terminal. Traditionally, low cost equals to lower performance or longer process latency. Longer processing latency ends up to higher energy consumption. As the spectrum resource is very limited at the lower part in L band, IoT may use higher RF such as the frequency bands higher than 5 GHz. In another way, not yet used very narrow spectrum band between two used bands may have to be used by future IoT [2].

D. Heterogeneity

The devices can interact with one another and provide service through different networks [8]. IoT devices have different functionalities, configuration and hierarchies. The integration of these devices is very complex. The degree of complexity increases many folds when some of these simple devices are merged to form a complex network [6].

E. Scalability

The rapid development of embedded technologies is leading to enormous deployment of miniaturized devices (sensors, actuators, etc.). As the number of devices grows, the data produced by these devices grow unboundedly. Thus, handling the growth of number of devices and information they produce is a massive challenge in IoT [6].

F. Interoperability

Each devices and protocols are integrated to work with one another. The different platforms are used in different IoT systems. Seamless interaction among the various devices is crucial to predict the vision of IoT [6]. In IoT, data integrations over different environments are thus tough and will be supported by modular interoperable components [2]. To achieve the interoperability, all the shared information interprets correctly. So the developer needs to handle both application and hardware devices.

G. Cost versus Usability

The cost of components that are needed to support capabilities such as sensing, tracking and control mechanisms need to be relatively inexpensive [8].

H. Data Management

The vast amount of data is available in either local or global systems. The local systems can be indexed within a bounded area but the global system there will be a need new indexing methods for managing addresses and identifiers. Devices are interconnected to exchange all types of information, so the handling of these data becomes critical [8].

I. Standards

The universal standards are needed to communicate with such heterogeneous environment of devices as well as communications, applications and services. The ETSI and IETF communities are working towards the development of standard IoT [14]. When the process will be open, it can be freely available to all participants. IEEE organization is also working with standards to solve these challenges by ensuring that IPv6 packets can be routed across different network types [3].

J. Security

Many technologies are used in IoT, therefore they have different security issues. The internet devices have low power consumption, light calculations and energy resources, so there is a need for standard encryption techniques and key management scheme to secure a data in long time.

K. Business Challenge

Businesses need to profit and grow capital in order to survive in their area of activity and this depends on security in the business. The business executives have to spend more attention to the storage location, media and method of transmission, encryption, and retrieval, etc. to increase the security of Internet of Things[11].The IoT business model and application development model is easily mapped into the technical aspects. But, the business-technology alignment, and one solution will not fit possibilities for all scenarios. Although small-scale applications have been profitable in some industries, it is unsustainable when extended to other industries. In the early stage of IoT development, business aspects should be considered to reduce the risk of failure[2].

III. CONCLUSION

IoT represents the next evolution of the Internet. The IoT encompasses several technologies such as communications, sensors, big data, cloud technology, fog computing etc., therefore they have development and implementation challenges. This paper addressed some key challenges associated with the IoT technology. The IoT deployment could be hard and require large research efforts to tackle with the challenges but it can provide significant personal, professional and economic benefits in the near future.

REFERENCES

- [1] Luka Milic and Leonardo Jelenkovic, "A novel versatile architecture for Internet of Things", MIPRO 2015/CTS, pp.1229-1234.
- [2] Shanzhi Chen, Hui Xu, Dake Liu, Bo Hu, and Hucheng Wang, "Vision of IoT: Applications, Challenges, and Opportunities With China Perspective", IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 4, AUGUST 2014, pp.349-359.
- [3] Dave Evans, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything", Cisco Internet Business Solutions Group, 2011.
- [4] Kai-Di Chang and Jiann-Liang Chen, "A survey of Trust Management in WSNs, Internet of Things and Future Internet", KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 6, NO. 1, Jan 2012, pp.5-23.
- [5] Xiruo Liu, Meiyuan Zhao, Sugang Li, Feixiong Zhang and Wade Trappe, "A Security Framework for the Internet of Things in the Future Internet Architecture", Future Internet 2017.
- [6] Slavica Tomovic, Kenji Yoshigoe, Ivo Maljevic, Igor Radusinovic, "Software-Defined Fog Network Architecture for IoT", Springer Science+Business Media New York 2016, 24 October 2016.
- [7] Keyur K Patel, Sunil M Patel, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", International Journal of Engineering Science and Computing, Volume 6 Issue No. 5, May 2016, pp.6122-6131.
- [8] Zonia Fayyaz, Azra Rehmat, "Internet of Things: A Future Emerging Technology", MDSRC - 2017 Proceedings, 27-28 December, 2017 Wah/Pakistan.
- [9] Sana BENZ ARTI, Bayrem TRIKI and Ouajdi KORBA, "A Survey on Attacks in Internet of Things Based Networks", ICEMIS2017, Monastir, Tunisia, IEEE, 2017.

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization

Volume 7, Special Issue 8, September 2018

International Conference on Emerging Trends in Science, Technology and Mathematics (ICETSTM-2018)"

22nd August 2018

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

- [10] H.Reza Ghorbani, M.Hossein Ahmadzadegan, "Security challenges in Internet of Things: survey", IEEE Conference on Wireless Sensors,2017,pp.6-11.
- [11] Aditya Parashar,Sachin Rishishwar,"Security Challenges In IoT",3rd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB17),IEEE,2017.
- [12] Hanisha Verma and Rajanpreet Kaur Chahal, "A review on security problems and measures of Internet of Things", International Conference on Intelligent Computing and Control Systems ICICCS 2017, IEEE,2017.
- [13] Habib Ur Rehman,Muhammad Asif and Mudassar Ahmad, "Future Applications and Research Challenges of IOT",IEEE,2017,pp.68-74.
- [14] Gurpreet Singh Matharu, Priyanka Upadhyay and Lalita Chaudhary, "The Internet of Things: Challenges & Security Issues",IEEE,2014,pp.54-59.
- [15] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer and Shahid Khan, "Future Internet: The Internet of Things Architecture,Possible Applications and Key Challenges",2012 10th International Conference on Frontiers of Information Technology, IEEE,2012,pp.257-260.