

International Journal of Computer Science and Mobile Computing



A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IJCSMC, Vol. 5, Issue. 2, February 2016, pg.312 – 316

Internet of Things- A Review

Sukhdev Singh Ghuman

Assistant Professor, SBDSM Khalsa College

Domeli (Kapurthala) , Punjab (India)

ghumanggg@gmail.com

Abstract: *Internet of things is the network of physical objects where every object can share data and information with other devices in the network. IoT is spreading very fast and it wil soon become ubiquitous. Everything is on the way to becoming a smart of offer you convenience and services which they never did before. IoT was coined by RIFD community. There are many challenges like connectivity, security, power management and security to be addressed for successful implementation of IoT.*

Keywords: IoT, Network, Security, Middleware, Access Control

I. INTRODUCTION

The internet of things is the network of physical objects, devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data [7]. Internet of things is a world where billions of devices communicate with each other and share data and information through public or private network. It is based on the concept of Wireless Sensor Networks (WSN) which are used in many fields to measure different parameters and send data to a central node for processing [1]. The IoT concept was coined by Radio Frequency Identification (RFID) development community in 1999. Due to exponential growth in the mobile devices, embedded systems, cloud computing and communication, IoT has become more

practical and relevant in this world. In analogy to the definition that a universe is commonly defined as the totality of existence, an Internet of Things universe might potentially connect everything. As a further analogy to new theories about parallel universes, different Internet of Things worlds might develop and exist in parallel, potentially overlap and possess spontaneous or fixed transfer gates [2]. In this paper the fundamental challenges has been discussed in section II. The main security problems have been discussed in section III and finally the topic is concluded in section IV.



Internet of things [3]

The Internet of Things (IoT) is becoming the technology of the day very fast. It is also evolving very fast. There is a need to understand challenges faced by this technology so that these challenges can be addressed to attain the expected 50 billion connected devices in 2020 [4].

II. FUNDAMENTAL CHALLENGES

The fundamental challenges faced by IoT are as discussed below [4]:

Connectivity:

There should be single connectivity standard that must be followed by others. There will be a large variety of wired and wireless standards used to connect the things in the IoT. The challenge is getting the connectivity standards which can communicate with one another.

Power management:

Power management the IoT is very fundamental because every device consumes power. These devices will be battery powered and use energy conservation techniques to be more portable. Line-powered equipment will need to be more energy efficient. Power management feature should be added to these devices and equipment. Adding Power management feature is a big challenge. Wireless charging will also incorporate connectivity with charge management.

Security:

This is the most important challenge in IoT because huge amount of data being sent within the IoT. This can be done by using built in hardware security and different connectivity security protocols. After doing all this, still security is not fool proof if consumer is not using security features integrated into the device. So, educating the user about the security features is also important challenge.

Complexity:

Manufacturers are trying hard to add connectivity to devices and equipment that has never been connected to internet. The challenge is to keep the design and development easy to get more things connected especially when typical RF programming is complex. Novice users should be able to set-up and use their devices without seeking help from a technical person.

Rapid evolution:

The Internet of things is a new technology so it will evolve and change constantly. More devices are being added every day to the complicated world of IoT and the industry is still in its infancy. The industry faces many challenges like unknown devices, unknown applications and unknown use cases. A wide variety of wired and wireless connectivity technologies are needed to meet the various requirements of the market. Last, a wide selection of sensors, mixed-signal and power-management technologies are required to provide the user interface to the IoT and energy-friendly designs.

III. SECURITY ISSUES

There are many challenges involved while building IoT. This section is concerned with major security related challenges while building IoT.

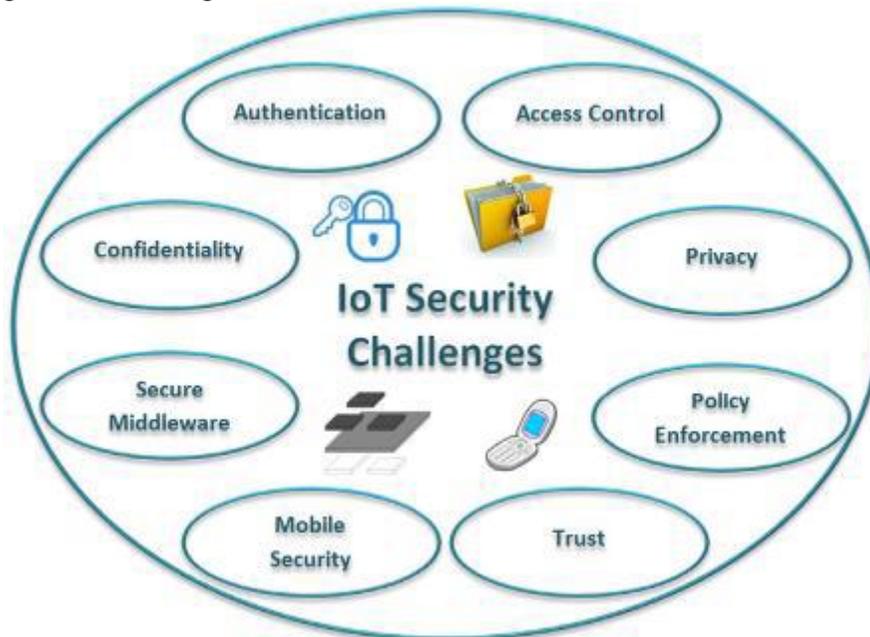


Fig. 2. Major security issues in IoT [5].

Access Control

Access control is very important parameter in IOT as the devices connected to the internet require different types of accesses. Different forms of resource and access control are applied for different form of devices. Mandatory or role-based access controls limits the privileges of devices and applications. They can access only the resources they need to do their jobs. If any component is compromised, access control ensures that the system is saved by giving as minimal access to other parts of the system as possible [6].

Privacy

The privacy is one the biggest challenge and it occurs when a static domain name is assigned to a specified IoT node. Only some of the privacy issues related to IoT are touched by recent researches, there is still a large scope to create privacy preserving mechanisms in IoT context. Today various encryption and authentication technologies are used for the confidentiality and authenticity of transaction data.

Policy Enforcement

Policy enforcement implies to the approaches used to cause the application of a set of defined efforts in a system. Policies can be defined as are performing rules which are forced for the purpose of acknowledging order, security, and consistency of data. Several efforts have already been accomplished to define the conventional languages for the specification of privacy policies, although an approved version of the language which can be applied to IoT paradigm is still insufficient.

Trust

The trust idea is used in different contexts and with different explanations. Trust is a complicated concept and its importance is dimensionally identified. A core problem with many applications towards defining the trust is that they do not contribute themselves to the demonstration of metrics and computation methodologies. The trust constraints are exactly related to the identity negotiation and access control effects.

Mobile Security

The security of the nodes is very important when they are moving like mobile phones. In mobile phones protocols are used for identification, authentication and privacy protection. The security issues of mobile devices are continuously explored by the scientific community, the available solutions partially address these needs. It poses a big challenge to intensify efforts in order to allow the integration with the other IoT technologies.

Secure Middleware

Middleware is a mechanism which joins all the different components together and enables smooth communication. It is an interface that facilitates the interaction between the 'Internet' and the 'Things', which may mean hardware or applications [8]. IoT need a number of technologies to be used to achieve the goal so middleware layer is used for the integration and security of devices. With many different technologies are in place within the IoT bench mark, numerous types of middleware layer are also engaged to effect the integration and the security of devices and data within the information network.

Authentication and Confidentiality

Many different protocols and mechanisms are with us to deal with authentication of a user and confidentiality of data in the context of IoT. Some of the major works related to authentication and confidentiality in IoT are as follows:

- Smart business security IoT application Protocol: - It combines cross-platform communications with encryption, signature, and authentication, in order to improve IoT applications development capabilities.
- Two-way authentication security scheme: - It is used as far as confidentiality and integrity is concerned.

IV. CONCLUSIONS

The IoT is going to change the way we live, work and play. From factory automation and automotive connectivity to wearable body sensors and home appliances, the IoT is going to touch every aspect of our lives. We will be living in a life with networks around us that constantly change and evolve based on our surroundings and inputs from other systems. It will help to make our lives safer with cars that sense each other to avoid accidents. It will make our lives more joyful with lighting systems that adjust based on the amount of daylight from windows. It will make our lives healthier with wearables that can detect different ailments before they happen. There is a long road ahead to the IoT of 2020. But one thing is for sure, it is going to be amazing [4].

REFERENCES

- [1] Jayavardhana Gubbia, Rajkumar Buyya, Slaven Marusic , Marimuthu Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions”, *Future Generation Computer Systems* 29 (2013) 1645–1660
- [2] Dr. Ovidiu Vermesan, Dr. Peter Friess , “Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems” , River Publishers.
- [3] Ovidiu Vermesan, Peter Friess, Patrick Guillemin, Harald Sundmaecker et al., “Internet of Things Strategic Research and Innovation Agenda”
- [4] Jim Chase, “The evolution of internet of things”, White Paper
- [5] S. Sicari, A. Rizzardi, L.A Grieco and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead”, *Comput. Netw.* 76, 146–164, 2015
- [6] “Security in the internet of things”, White Paper, Wind River Systems, Inc. 2015
- [7] https://en.wikipedia.org/wiki/Internet_of_things
- [8] <http://www.digitalservicecloud.com/iot-middleware.html>