Internet of Things and Security Concerns that come with it

Submitted by:

Name – Aman Lal

Login Id – amanl

Student Number - 791650

Table of Contents

Section Number	Chapter	Page
1.0	List of Abbreviations	1
1.1	Introduction	2
1.2	Underlying Technologies	2
1.3	Applications of IoT	3
2.1	Challenges faced by IoT	4
3.1	Securing the Internet of Things	5
4.1	Conclusion	5
	References	5

1.0. List of Abbreviations

IoT – Internet of Things

IPv6 – Internet Protocol version 6

WIFI – Wireless Fidelity

NFC – Near Field Communication

RFID – Radio Frequency Identification

SSH – Secure Shell

SSL – Secure Sockets Layer

1.1. Introduction

Internet of Things (IoT) is where the physical world meets the Internet. It is a cyber-physical system connecting physical devices such as automobiles, healthcare equipment, sensors etc. which enables them to collect, transmit and exchange data.[1]

To create the Internet of Things it is required to convert things into Smart devices i.e. devices which are connected to other devices or network via a protocol like WIFI, NFC, 3G etc and can operate interactively and anonymously to some extent. [2] In order to convert things into smart devices the following parameters are required:

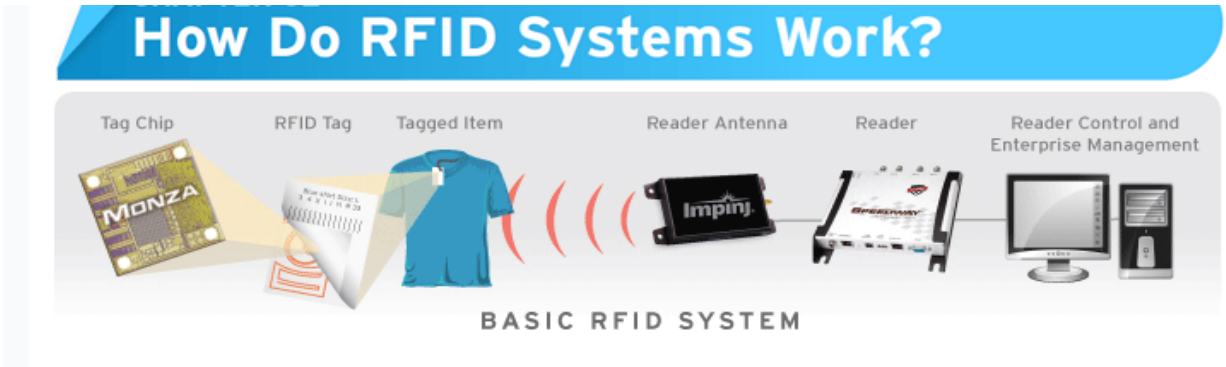
- Identity – To identify any device in IoT. [3]
- The ability to communicate – Integration with a communication protocol.
- Senses – Sensors can be added to provide some kind of senses to these things. [3]
- Controller – A Small embedded controller needs to be attached to things which require to be controlled over the Internet. [3]

1.2. Underlying Technologies

A broad range of technologies are currently used to identify objects such as WIFI for WLANs, Bluetooth for smart objects, matrix barcodes for identification of things, Near Field Communication(NFC) and Radio Frequency Identification (RFID) to digitally identify things using smart phones and card readers. [1]

IPv6 forms the backbone of IoT, and the 128 bit addressing scheme can provide unique IP addresses to each of these physical objects. The need of the hour is to integrate the existing technologies and legacy systems with Internet Protocol version 6.[4]

A new framework GlowBal IPv6 has been proposed for using low energy Bluetooth and an IPv6 addressing proxy framework has been proposed for devices using Identification tags(RFID) and legacy technologies.[1]



[5]

1.3. Applications of Internet of Things

The Internet of Things is a stepping stone in Technology for our generation, much like the World Wide Web 20 years ago. The Figure below depicts a few of its applications

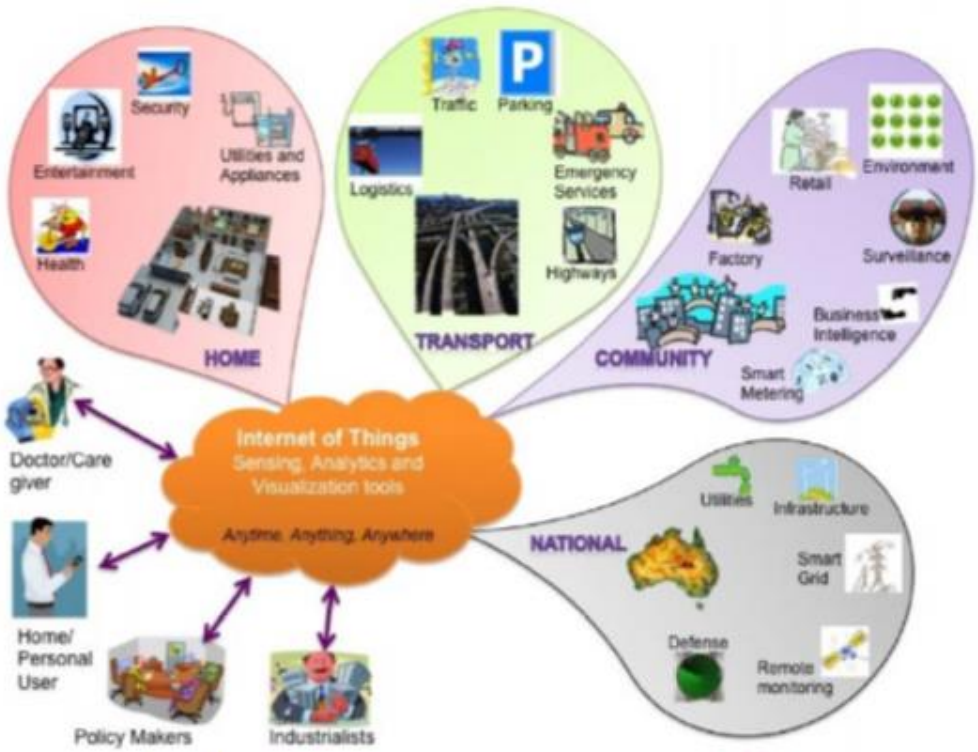


Fig. 1. Internet of Things showing users and applications, [11].

[1]

Surrounded by the Internet of things one could

- Walk up to anything and learn anything about it by extending your smart phone towards it, For instance going to a supermarket and learning about the ingredients and expiry of products.[3]
- Monitor things – Continuously monitor the vitals of a patient and predict events like a cardiac arrest well in advance.[3]
- Search for things – Ask Google questions like where are my keys? or Where is my child? [3]
- Manage Things – Smart Cities – Traffic Problems might just become a thing of the past with smart congestion control and traffic alerts. [3]
- Control Things – Smart Grids and Meters can be used to balance the load and decide when to use renewable energy, effectively reducing electricity bills. [3]

Given all of these widespread application of IoT, it remains a double edged sword and has serious implications on privacy and security.

Privacy might become meaningless in the concept of Internet of Things because everyone can be monitored anytime without people even knowing about it.

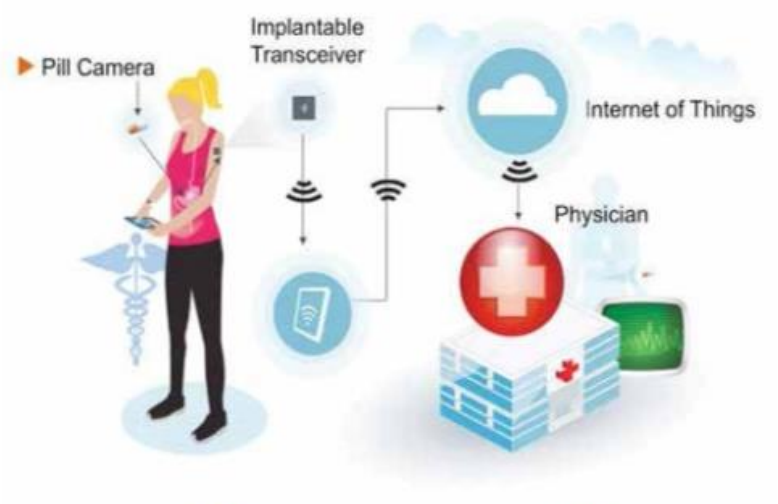


Fig. 2. Internet of Things in medical care, [13].

[1]

2.1 Challenges faced by IoT

The problem with Internet of Things is that we are producing these “smart things” way faster than we can secure them

- These devices have limited resources in terms of processing, memory and energy. – These resources are not enough to implement traditional security solutions.[1]
- Security features reduce performance and increase costs.
- No Established standards as the technology is still new.[6]
- Hardware and Software backdoors created by developers become easy targets to attackers with physical access to these things.[6]
- Hackers can become the next generation of terrorists since they can get into things and control everything, things could be safety critical devices such as pacemakers or nuclear reactor sensors.[6]
- Technocracy – Sensors on everything means explosion of Data, all going through Technology giants which gives them an insight into the everyday life of user.[3]
- Communication between things is a sweet target for attackers as it contains a lot of information which might not be encrypted because of resource constraints of sensors.[7]

3.1. Securing the Internet of Things

Security Boot – It allows that only cryptographically signed code from the manufacturer can be loaded onto the boot of the device. Similar to what Microsoft has done for Windows 8.[8]

- Data Security – Access Authentication – To make sure that the authenticity of users accessing these things via protocols like Kerberos.[9]
- Communication between things can be secured using public key cryptography tunnelling protocols such as SSH and SSL.[10]
- Encryption – Encrypting the communication between things using Advanced Encryption Standard.[11]
- Protection against cyber-attacks – Embedded Firewalls – Limit communication with only known and trusted hosts[6].
- Intrusion detection and Security monitoring – Log hack attempts so that policies can be updated to mitigate known threats[6].
- Embedded Security Management to provide a layer of security within the device itself
- Device Tampering detection

4.1. Conclusion

It is imperative to understand that the above Security measures need to be implemented for devices which have resource constrains.

Sensors connected to IoT have only enough resources to send and transmit. Authenticity, Integrity and Confidentiality is still a large hurdle that needs to be crossed to successfully move towards Utopia.

IoT scares a lot of people because of its gaping security loop holes but well, the internet was in the same state 20 years ago and we now have a very secure and somewhat usable Internet.

REFERENCES

1. Qazi Emad-ul-Haq1, H.A., Abdelfettah Belghith1, Muhammad Hussain1, Wadood Abdul2, Mostafa H. Dahshan2 and Sanaa Ghouzali3 *Challenges and solutions for Internet of Things Driven by IPv6* KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS, Dec. 2015 **VOL. 9, NO. 12**.
2. Wikipedia, *Smart Device.* 2016.
3. YouTube, *The Internet of Things: Dr. John Barrett at TEDxCIT.* 2012.
4. NetworkWorld, *ARIN Finally Runs Out of IPv4 Addresses.*
5. IMPINJ, *How do RFID systems work?* 2016.
6. YouTube, *Internet of Things: Security and Privacy.* 2015.
7. Britton, K., *Handling Privacy and Security in the Internet of Things* J O U R N A L O F I N T E R N E T L AW, Apr. 2016.
8. Microsoft, *Security Boot.*
9. Microsoft, *Kerberos Explained.* 2015.
10. Wikipedia, *Transport Layer Security.* 2016.
11. Wikipedia, *Advanced Encryption Standard.* 2016.