

Internet of Things: Opportunity and Security Issue

Veena Tripathi

Assistant Professor, Computer Science and IT department, Model Institute of Engineering and Technology,
Jammu, India.

Abstract – Now-a-days, smart grid, smart homes, intelligent transportation, are infrastructure systems that connect our world beyond our expectations. The ‘Internet of Things’ is an emerging topic of technical, social, and economic significance. Internet of things is the development of the internet in which everyday objects have network connectivity, allowing them to send and receive data. In our paper we have discussed about possible usage, scenarios and technological building blocks of the “Internet of Things”[1]. As the number of Internet-enabled devices increasing with the advent of IPv6 and wide deployment of Wi-Fi network the estimated number of active wireless connected devices will exceed 40 billion. The advantage of this expansion is that, we are able to do the things we never before imagined but as with every good thing, there’s a downside of internet-enabled systems are attractive targets for cyber attack. Now the problem is that, how do we protect potentially billions of them from intrusions and interference that could compromise personal privacy. In the development of any IoT application security and testing frameworks play an important role. Our approach is to focus on problems of hacking the Internet-connected devices, create more secured and attack proof internet of things enabled devices and applications. This paper is mainly focusing on the concept of IoT architecture, security issues and area of research needed.

Index Terms – Internet of things, Device-to-Device, Back-End Data-Sharing, M2M, Cyber attack.

1. INTRODUCTION

The Internet of Things is comprised of a wildly diverse range of device types- from small to large, from simple to complex – from consumer gadgets to sophisticated systems, smart home appliances to factory control devices, medical devices and even automobiles. In Internet of Things, embedded devices are different from standard PCs or other consumer devices. Security has not been a high priority for these devices until but now it’s time to establish The “Internet of Secure Things”. Use of multiple layers of protection is the driving principle for enterprise security. It includes firewalls, authentication/encryption, security protocols and intrusion detection/intrusion prevention systems. Things require a collaborative, umbrella approach to IoT security.

Now security required for following issues first one is hacking of devices and systems to obtain information and data. The second one is cyber-attacks against the devices themselves. “A Cyber-attack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber-attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data

and lead to cybercrimes, such as information and identity theft. Cyber-attack is also known as a computer network attack (CNA)[2]. Beginning with introducing the architecture and features of IoT security, this paper expounds several security issues of IoT that exist in the three-layer system structure, among these safety measures concerned.

2. LITERATURE REVIEW & GROWTH RATE OF IOT

Data in motion will travel from a host of devices, through diverse networks to different data centers located in the cloud[5]. IoT will not reach its full potential unless users can trust that their connected devices are secure and their privacy is guaranteed. The security framework must be interconnected and coordinated to avoid breaches, snooping, hacking or accidental leaks. Data within an IoT ecosystem is either in motion or at rest. Data at rest is the one that resides within the device or the cloud, whereas data in motion is the data moving from one node to the other. Driving data, for example could be at rest in the car computer or sent over the cellular network to the cloud for fuel consumption analysis.

Ericsson’s former CEO Hans Vestburg was the first to state in 2010 presentation to share holders that, the world will have 50 billion connected devices by 2020. The following year, Dave Evans, who worked for Cisco at the time, published the same prediction in a white paper.

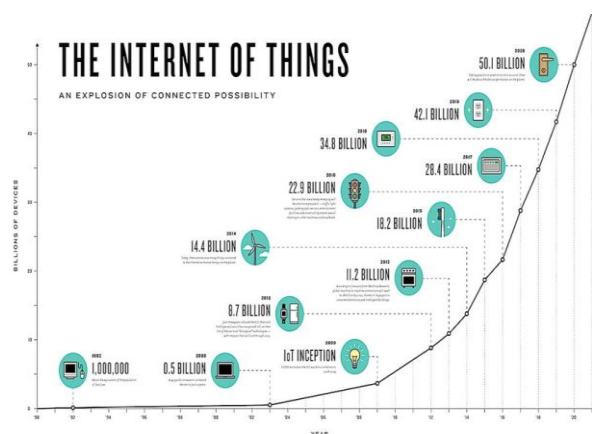


Fig-1.Growth rate of IoT devices

According To John Greenough Report In 2014 The 'Internet Of Things' Will Be The World's Most Massive Device Market And Save Companies Billions Of Dollars.

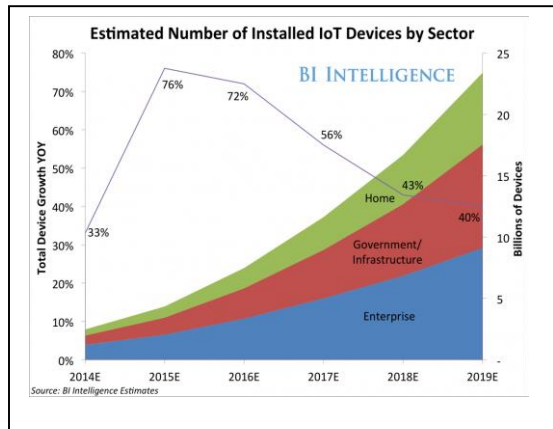


Fig-2. Estimated Numbers of Installed IoT Devices by Sector

As it can be seen, since IoT has come into existence, search volume is consistently increasing with the falling trend for Wireless Sensor Networks. As per Google’s search forecast (line no-3 in Fig-3), this trend is likely to continue as other enabling technologies converge to form a genuine Internet of Things.

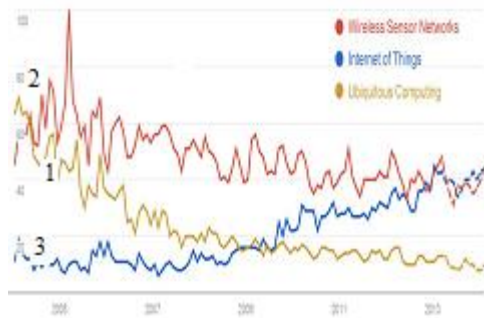


Fig-3. Google search trends since 2004 for terms Internet of Things, Wireless Sensor Networks, Ubiquitous Computing.[12]

3. OPPORTUNITY OF INTERNET OF THING (IOT)

Internet of thing is sensing, analytics and visualization tool. Fig-4[3] depicting the interconnection among things like smart television, phones/laptops, smart refrigerator and smart individual etc. via internet. One can say that by the smart use of IOT, it would be possible to know when the things need to repair, recall or replace without any human interference; which greatly reduce the waste and loss of the objects. There are several application domains which will be impacted by the emerging Internet of Things. The applications can be classified based on the type of network availability, coverage, scale, heterogeneity, repeatability, user involvement. We categorize the applications into four application domains: Personal and Home, Transport, Community and National.

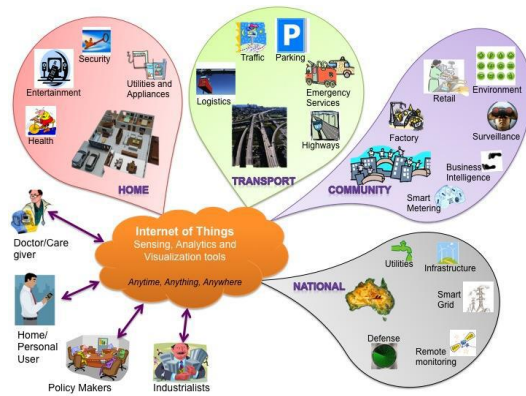


Fig -4. Internet of Things Schematic showing the end users and application areas[12] .

Now-a-days in every field of life IoT is playing an important role for example- Healthcare, emergency, defense services, transport management and environmental services also. To easily understand the different opportunities, we classify these opportunities according to fields. Table-1 shows Potential IoT applications of it.

Different fields	Application of IoT
Healthcare	Patient monitoring, personnel monitoring, disease spread modelling and containment- real-time health status and predictive information to assist practitioners in the field, or policy decisions in pandemic scenarios.
Emergency services, defence	Remote personnel monitoring (health, location); Resource management and distribution, Response planning; Sensors built into building infrastructure to guide first responders in emergencies or disaster scenarios
Crowd monitoring	Crowd flow monitoring for emergency management; Efficient use of public and retail spaces; workflow in commercial environments
Traffic management	Intelligent transportation through real-time traffic information and path optimisation
Infrastructure monitoring	Sensors built into infrastructure to monitor structural fatigue and other maintenance; Accident monitoring for incident management and emergency response coordination
Water	Water quality, leakage, usage, distribution, waste management
Building management	Temperature and humidity control, activity monitoring for energy usage management,

	Heating, Ventilation and Air Conditioning (HVAC)
Environment	Air pollution, noise monitoring, waterways, industry monitoring

Table:1 Potential IoT applications

4. IOT ARCHITECTURE

IoT is a world-wide network of interconnected objects these objects are uniquely addressable based on standard communication protocol. In WSN application architecture there are three layers Perception layer, Network layer, Application layer. These layers perform following functions as shown in fig-5.

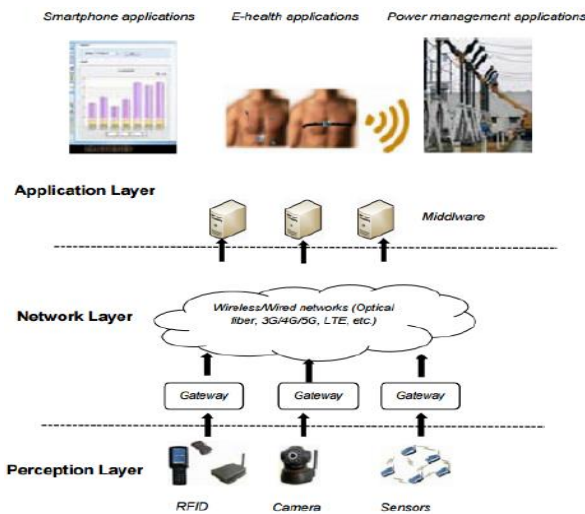


Fig. 5. IoT Architecture

4.1) *Perception Layer*: In the perception layer, the system aims to acquire, collect and process the data from the physical world. Perception layer mainly includes: Smart card, Reader, RFID tag, Sensor network. Each RFID electronic tag has a unique ID called Electronic Product Code (EPC) which is the only searchable ID allocated for each physical target[5].

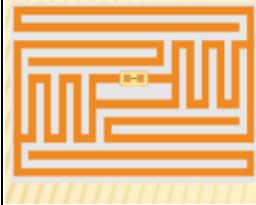

Each of these devices has following vulnerability which leads to be a security issue of IOT such as sensor attacks, sensor abnormalities, radio interference. Perception of things require a large number of terminals, terminals are used for real-time data collection to be presented to the user. This process needs an authentication and data integrity. Due to the wireless nature of communication, IOT can face threat from the hackers, virus attacks etc. The main problems existed in perception terminals include leakage of confidential information, tampering, terminal virus, copying and other issues.

4.2) *Network Layer*: In IoT, each alliance has it’s own network address. For instance, ZigBee is one alliance with its own network addresses. Similarly Z-Wave is a low-power MAC protocol designed for home automation and has been used for

IoT communication, especially for smart home and small commercial domains. It covers about 30-meter point-to-point communication and is suitable for small messages in IoT applications, like light control, energy control, wearable healthcare control and others. Wi-Fi devices come with IP stack in their chip, enabling IP-based connectivity. The IP layer aids the respective devices to effectively communicate within their operating range. 6LoWPAN (IPv6 Low Power Wireless Personal Area Network) devices also operate in IEEE 802.15.4, but they have the network stack with IP connectivity (IPv6). As an analogy, consider TV remotes which could be operated on the internet.

4.3) *Application Layer*: Data processing and services providing are two major purposes of the application layer. At this layer information received and decision are taken place for controlling of device. The application layer serves as the interface between the user and the desired sensor application. Protocols such as HTTP/HTTPS (Hyper Text Transfer Protocol – Secure) have been in existence ever since IP began. A common browser makes use of HTTP. With the emergence of IoT, protocols such as Message Queuing Telemetry Protocol (MQTT), Advanced Message Queuing Protocol (AMQP), Constrained Application Protocol (CoAP), etc. have emerged significantly. For instance, Adhaar card makes use of AMQP(Advanced Message Queuing Protocol), and Facebook Messenger uses the MQTT(Message Queuing Telemetry Transport) protocol, all these are lighter version of the heavyweight HTTP protocol and are more effective when used in combination with 6LoWPAN.

5. TECHNOLOGIES

Key Technologies	Performance Specification	Diagrammatic Representation
RFID	<ul style="list-style-type: none"> It stands for Radio frequency Identification Used to track & Identify the data of things. It’s similar as a register and helpful for inquiring. Easy to deploy RFID tags can be either passive, active or battery assisted passive. 	 <p>EPC RFID tag</p>
Sensor Technology	<ul style="list-style-type: none"> The “Senses” of IoT, it provides the original information. To detect changes in physical status of things. 	

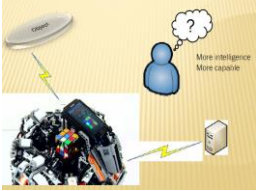
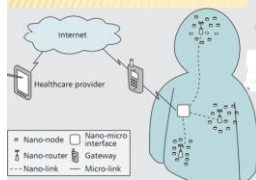
<p>Embedded Technology</p>	<ul style="list-style-type: none"> It can make an object in IoT have certain degree of Intelligence 	<p>Animal Identification</p>  <p>Embedded Technology</p>
<p>Nanotechnology</p>	<ul style="list-style-type: none"> It can realize smaller volume things interact, connect and decrease the consumption of system. 	 <p>Intrabody Nanonetworks</p>

Table:2 Key Technologies and Performance Specification

6. SECURITY ISSUES AND PARAMETERS

As we have discussed earlier there are number of security issues and parameters which are responsible for it. In this section we will discuss these parameters. Security at the device, network and cloud level are critical to the efficient and safe operation of IoT, protecting data in motion and at rest.

Here are some examples of key threats:

- ✓ **Phishing** The fraudulent practice of sending emails pretending to be from a reputable company in order to entice individuals to reveal sensitive information such as credit card numbers.
- ✓ **App hacking** The low hanging fruit in the hacking world. There are automated tools easily available on the market and lots of them are free. Unlike centralized Web environments, apps exist in an unregulated mobile device ecosystem. Unprotected binary code in mobile apps makes them fast and easy to modify and exploit. Binary code is the code that devices read to make an app work. It is basically what you download when you access mobile apps in an app store such as iTunes or Google Play.
- ✓ **DOS attacks** Denial of Service attacks are designed to temporarily or indefinitely crash a network. Fixes are available, but like viruses, hackers are continually thinking up new ones.
- ✓ **DDoS attacks** Distributed Denial of Service attacks are designed to make an online service unavailable by flooding it with traffic from multiple sources.
- ✓ **Physical intrusion** Hacking normally happens remotely. But a physical intrusion is when a device and its components are actually tampered with.

Based on the IOT security issues, the need of security is required for IOT system. Therefore looking at the traditional

parameters of security demand it needs to build a safe internet system of things, which are as follows,

- **Authenticity:** Received information by a reader should be noticeable whether is sent from authenticated electronic tag or not.
- **Confidentiality:** Sensitive Information shall not be leak to any unauthorized reader by using an RFID electronic tag.
- **Integrity:** While transmitting the information to IOT, data integrity can ensure the originality of information. It should ensure that the information transmitting is not fabricated i.e. not rewritten, copied or replaced by the attacker.
- **Privacy:** Privacy such as identity or commercial interest of an individual user should be protected by the secure IOT system.
- **Availability:** An authorized user can able to use various services provided by IOT and can prevent DOS attack for the availability of the services. DOS attack is major cause for threat to the availability

In the following table we have summarized the components which are used at different layer of IoT, security issues and security parameter [5].

IoT Layers	Components	Security Issues	Security Parameters
Perception Layer	Smart Card, RFID tag, Sensors	Terminal Security issue Sensor network security issue	Authentication Confidentiality
Network Layer	Wireless or wired network, computer, components	Information transmission security	Integrity Availability Confidentiality
Application Layer	Intelligent devices	Information processing safety of IOT	Privacy

Table:3 Components, Security Issues and Security Parameters

7. CONCLUSIONS & CHALLENGES

To prevent cyber attacks, organizations must ensure that they educate consumers about the correct security procedures to be followed while using an IoT system. Several European initiatives have defined different architectures, in-order to design IoT services and applications under security [9]. Typically, these approaches have been tailored to specific domains addressing a small subset of requirements regardless of the global nature of the IoT. After studying the security threats and parameters used in it, it's suggested to implement the security policy for different layers of structure.

As we have discussed earlier following are two main security challenges in IoT devices.

- ✓ Hacking of devices and systems to obtain information and data.
- ✓ Cyber-attacks against the devices themselves.

There is need to protect IoT devices or alarm it as these security threat is going to actually happen. Embedded devices are designed for low power consumption, with a small silicon form factor, and often have limited connectivity. They typically have only as much processing capacity and memory as needed for dealing with security issues. There is a requirement of policy to judge that who can input authentication credentials or decide whether an application should be trusted[11]; they must make their own judgments and decisions about whether to accept a command or execute a task.

REFERENCES

- [1] <http://whatis.techtarget.com/definition/Internet-of-Things>
- [2] <https://www.techopedia.com/definition/24748/cyberattack>
- [3] Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions.
- [4] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, T. Razafindralambo, A Survey on Facilities for Experimental Internet of Things Research, IEEE Communications Magazine 49 (2011) 58–67.
- [5] Gemalto's Guide To Making the "Internet of Things A Safe Place To Connect"
- [6] Kai Zhao1, LinaGe1 "A Survey on the Internet of Things Security", School of information science and engineering Guangxi University China

2013 Ninth International Conference on Computational Intelligence and Security.

- [7] Conner, Margery (May 27 2010). Sensors empower the "Internet of Things" pp. 32–38. ISSN 0012-7515
- [8] Shao Xiwen "Study on Security Issue of Internet of Things based on RFID" 2012 Fourth International Conference on Computational and Information Sciences
- [9] Fei Hu "Security and Privacy in Internet of Things" Model, Algorithms and Implementation
- [10] Zhuankun Wu. "Initial Study on IOT Security architecture Strategy and decision-making" research -2010
- [11] "Security In The Internet Of Things" Lessons from the Past for the Connected Future.
- [12] Jayavardhana Gubbi Internet of Things (IoT): "A Vision, Architectural Elements, and Future Directions" Department of Electrical and Electronic Engineering, The University of Melbourne, Vic - 3010, Australia
- [13] Mayuri A. Bhabad Internet of Things: "Architecture, Security Issues and Countermeasures" P.G. Scholar Dept. of Computer Science and Technology International Journal of Computer Applications (0975 – 8887) Volume 125 – No.14, September 2015
- [14] Jing Liu and Yang Xiao, Department of Computer Science "Authentication and Access Control in the Internet of Things" The University of Alabama Tuscaloosa, AL 35487-0290 USA 2012 32nd International Conference on Distributed Computing Systems Workshops
- [15] Sogeti High Tech, "Security in the Internet of Things Survey", 2014 November.

Author



Ms Veena Tripathi is an Assistant Professor in Model Institute of Engineering and Technology, Jammu (India). She has done her MS in Software Engineering from Dipartimento di Informatica e Telecomunicazioni University Of Trento, Italy. She has completed her Internship of MS in the field of Software Testing (European Union Project) in Computer Science Research center:FONDAZIONE BRUNO KESSLER Trento, Italy. She has more than 10 years of teaching Experience. She has Worked On YAKSHA project (for online preparation of Medical Entrance Examination). She has worked on many research projects during her MS program. She has the membership of International Association of Engineers (IAENG). She has published papers in reputed International Journal. She has many certifications in the field of Computers such as EMC Academic Associate Certification (Data Science and Big Data Analytics), IIT Bombay LaTeX Certification, University of California (IoT Certification) etc. She has attended more than 25 workshop, trainings, seminar and conferences. She has strong holding on programming languages. Her research interests are in Software Testing, Reverse Engineering, Software Maintenance, IoT, and Cloud Computing.