ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 5; Issue 3; May-June: 2017; Page No. 102-108
Journal Approved by UGC

Internet of Things: Security Challenges and There Proposed Solutions

Vikas Kumar[1], Dr. Neetu Sharma[2]

[1]Scholar (M.Tech), Cyber Forensics and Information Security, GITAM, MDU, Bahadurgarh, Haryana (India)

Vikas105joon@gmail.com

[2]*Head of Department (C.S.E), Cyber Forensics and Information Security, GITAM, MDU,* Bahadurgarh, Haryana, (India)

neetush75@gmail.com

Abstract

This new amazing technology Internet of Things brings environment of standard shift in our professional and personal life. Iot becomes common which boost the transfer of goods and services in universal supply chain networks. IoT has a great effect on the security and privacy of the tangled stakeholders. A modest legal structure must take the hidden technology into account and would be the best to establish by an international administrator, which is boosted by the private sector according to their special needs and thereby becomes easy to adjust. Today, IoT is need which being realization everywhere, human interest like smart city, smart environment, security, smart business process, smart agriculture, home automation and healthcare etc. This article deliberate the Security challenges and there proposed solutions. The contents of the respective administrator must wrap the right to information, provisions restricting the use of mechanisms of the Internet of Things, rules on IT-security-legislation, provisions which supporting the use of mechanisms of the Internet of Things and the establishment of a task force doing research on the legal challenges of the IoT.

Key Words: Internet of Things; cyber security; RFID; Zigbee; ARM; Smart Home.

Introduction

The IoT is a concept where an object is assigned to an IP address and through that IP address we make that device identifiable on internet. Certainly, what IoT can do is beyond imagination. It connects plethora of heterogeneous object.

In the year 1985 a speech is given by Peter T. Lewis at the Federal Communication Commission (FCC) where the term IOT was first used by him. But at that time this concept didn't gain popularity back then, it has been gaining a lot of attraction since last five years.

The Internet of Things (IoT) has become a universal term to describe the tens of billions of devices that have sensing or instinct capabilities, and are connected with each other by the Internet. The IoT covers everything from small to big things like wearable fitness bands to smart home appliances, to factory control devices, medical devices and even automobiles. Till now security has not been a high priority for these devices. But it is now time to establish The Internet of *Secure* Things.

Many analysts announced 2015 as "the year of IoT," but so far, it has been a year of bad block. Assumed, there are still thirteen months to go, but negative reports keep piling on. A security firm Kaspersky recently ran a cussing critique of IoT security challenges, with insulting headlines, "*Internet of Crappy Things*". [1]

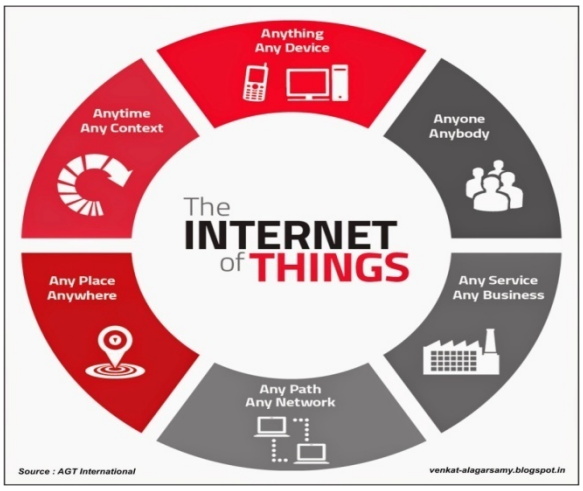

Figure 1: IoT Applications [8]

Corresponding author: Vikas Kumar

1. IoT APPLICATION DOMAINS:

In present time IoT is expected which transform every business rules, which includes health care sector, banking services, manufacturing and logistics, retail and industrial sector and home computerization. Using power of IoT in some of the domains include the following. [2]

A. Manufacturing & Logistics

- Machine-to-machine communication
- Machine-to-infrastructure communication
- Asset tracking of goods on the move

B. Health care and life sciences

- Remote monitoring of patient health
- Diagnosis and drug delivery

C. Industrial and home automation

- Smart city, smart homes and computerization
- Industrial building computerization
- Appliance monitoring, like washing machines, AC and refrigerators
- Livestock farming tagging and devices to monitor activities

D. Retail

In retail sector IoT replaces bar coding with radio frequency identification (RFID) devices that collects more data to monitoring systems, which helps in improving supply chain efficiently or Easier product learning capability and discoverability through the product and smart phone communication. Due to divergent services being planned by using IoT, which tells that any company does not capable of develop a full end-to-end solution and support IoT based innovations. Of all the business domains, retail would be the first sector to see number of IoT recognition. This is visible as Walmart has already implemented IoT for supply chain management.

2. IOT ARCHITECTURE:

IoT architecture is very typical to represent, due to the net of interconnected devices, or entities. Each layer of IoT has its own defined functions and the devices that are used in that layer. There are diversified opinions about the number of layers in IoT. But this architecture consists of three layers: Perception Layer, Network Layer, and Application layer. A brief description of every layer is given according to different researches in the figure: 2 graphically represent the Architecture.

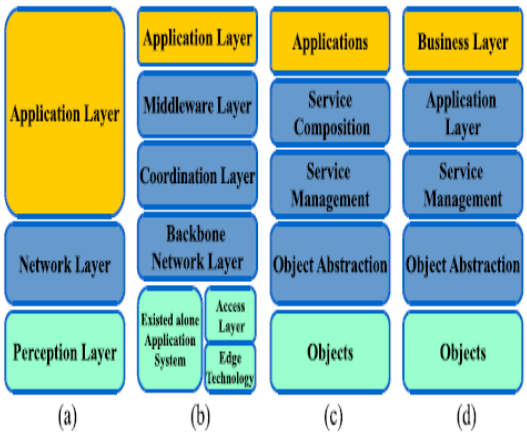

Figure.2: Three Layer IoT Architecture [9]

A. Perception Layer

The main function of the perception layer is to identify the physical properties of stuff around us which is part of the IoT. This process of analysation is based on different type of sensing technologies (e.g. RFID, WSN, GPS, NFC, etc.). In addition, this layer does the work of transforming the information into digital signals. However, some objects may not be recognized directly. Thus, microchips will be affixed to these objects to appreciate them with sensing and even processing capabilities. Nanotechnologies and planted intelligence will play an important role in the perception layer. First of all we will make chips smaller which are used in our everyday life. The second one will develops them with processing capabilities that are required for applications. [3]

B. Network Layer

The network layer is ensured for processing the received data from the Perception Layer. In addition, it is responsible for transmitting data to the application layer through various network technologies, such as wireless/wired networks and Local Area Networks (LAN). The main medium for transmission has FTTx, 3G/4G, Wifi, bluetooth, Zigbee, UMB, infrared technology, and so on. Huge quantities of data will be carried by the network. That's why, it is essential to provide a sound middleware to store and process this massive amount of data. This technology offers a reliable and dynamic interface through which data could be stored and processed. Indeed, research and development on the processing part is important for the future development of IoT.

© 2017 IJETCR. All Rights Reserved.

C. Application Layer

The application layer handles the processed data by the Network Layer. In real, application layer authorized the front end of the whole IoT architecture. Moreover, this layer provides the compulsory tools for developers to understand the IoT vision. In this vision, the range of possible applications is impressive (e.g. Intelligence transportation, identity authentication, location based services, safety, etc.). To suit IoT attention, the three-layer architecture provides a high level framework through which deferent approaches might be implemented.

3. MODELS OF IOT ARCHITECTURE:

There are some Models of IOT Architecture which are as follows.

A. IOT-A

IOT-A is also called an Architectural Reference Model (ARM) which support design choices with a common understanding. This proposed project is popularly termed as European Lighthouse mingled Project which supports interoperability. ARM also defines guidelines for designing protocols, algorithms and interfaces.

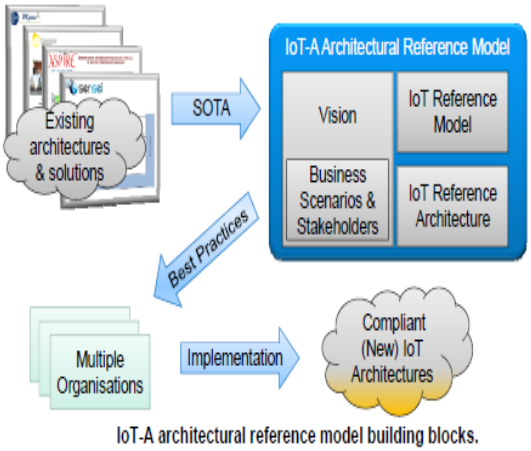

Figure.3: IoT Architectural Reference Model [10]

B. WIRELESS SENSOR NETWORK

Internet protocol and non Internet Protocol based technology solutions are used for Wireless Sensor Networks. Zigbee, Z-wave, Insteon and Wavevenis are non IP Based solution. IPv6 and 6LoWPAN are IP based solutions of WSN. However, presence of many proprietary and non proprietary Wireless networks, it is difficult for a cohesive integration of WSN with fast growing Internet Technologies. In the current context, world is moving towards IP based solutions which are based on open standard like IPv6 and 6LoWPAN.

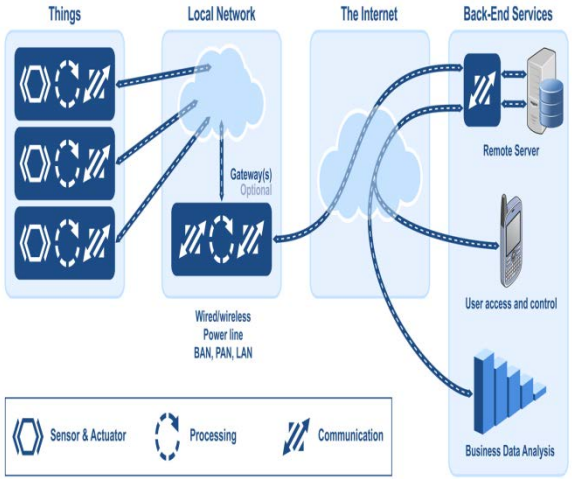

Figure 4: IoT Wireless Sensor Network [11]

C. SENSEI

European Union project of SENSEI was an initial action during 2010 on IoT architecture and initiatives. The primary objective of this project is to design a network of the future by interconnecting the physical and digital world. These projects arrange, operate and interconnect sensors, network nodes and actuators everywhere. SENSEI does not differentiate physical object and virtual object. [4]

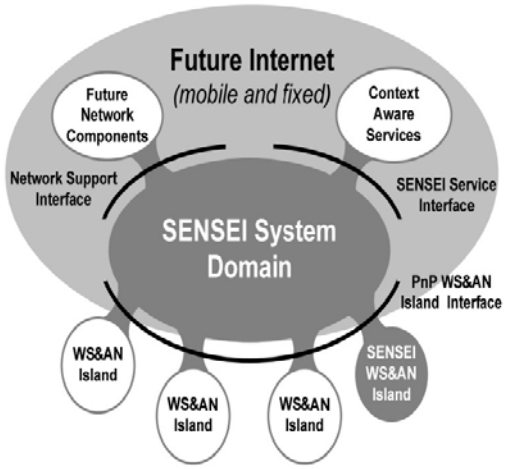

Figure.5: IoT Sensei System Domain [12]

4. CHALLENGES OR BIGGEST THREAT TO IOT:

The Internet of Things (IoT) is already starts to give rising to real-world applications, from connected homes, cars to health monitoring and smart utility meters.

© 2017 IJETCR. All Rights Reserved.

Analyst Gartner predicts there will be 26 billion IoT devices – excluding PCs, tablets and smart phones till 2020.But IoT represents a completely different level of complexity when it comes to the application.

Applications, like smart TVs and cash machines to can be infected with high-risk. And in its latest internet threat assessment report by the European crime agency; Europol warns tells that the IoT creates new types of risks and threats not only in consumer applications but also in critical infrastructure control systems.

It goes on to say: "We can expect to see (more) targeted attacks on existing and emerging infrastructures, including new forms of blackmailing and extortion schemes (e.g. ransomware for smart cars or smart homes), data theft, physical injury and possible death, and new types of botnets."[5]

A present example of Friday, 12 May 2017 is The Wanna Cry ransomware attack. This attack was a big disaster in worldwide cyber attack by ransomware cryptoworm till now, which targeted computers running with Microsoft old Windows operating system XP by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.[6]

Below, we've compiled a list of some of the biggest IoT security and privacy issues as we head toward this truly connected world.

- A trillion points of vulnerability

In Iot setup there are large number of sensors used to collect data and every single device and sensor in the IoT have a hidden risk. Each of these devices has the controls in place to contain the confidentiality of the data collected and the integrity of the data which sent. And one weak link in whole setup could open up access to thousands of devices on a network with possibly serious consequences.

- Trust and data integrity

In IoT there is large number of sensors collect date and in corporate lobby this bombardment of data from all manner of connected sensors. But how sure can an organisation that the data which they get by iot devices is safe or not been compromised with any kind of interference? But in the IoT that security efficiency doesn't exist due to presence of large number of devices that are connected with each other. Security should be embedded inside the design of these IoT devices and systems to create trust in both the hardware and integrity of the data.

- Data collection, protection and privacy

The perception of the IoT is to make everyone lives easier and boost the efficiency and productivity of businesses. Use of IoT to collect data will help in taking smarter decisions. But this will also create an effect on privacy forecast. If data will collect by cheap connected IOT devices will be compromised it will undermine trust in the IoT.

- Lazy consumers

Computers have option of automatic updates but most of users are very lazy to execute even the basic steps to keep their computer safe. Than how we can say that these type of lazy consumers protecting the multiple IoT devices will be even harder than a single computer, this problem will get even worse.

- Data Authentication

Problem can be faced after successful encryption of data there are more chances of device can be hacked. Due to the failure to establish the authenticity of the data, which can be communicated to and from an IoT device, than security is compromised.

- IoT Security-Side-channel Attacks

Encryption and authentication both in place still leave scope for side channel attacks. Such attacks focus less on the information and more on how that information is being presented. For instance if someone can access data like timing information, power consumption or electromagnetic leak, all of this information can be used for side channel attacks.

- IoT Security-Hardware Issues

From the very starting phase of the internet of things, hardware has being the problem. It's assumes that with all the promotion and rapid interest of IoT devices. Chipmakers like ARM and Intel are boosting their processors for more security with every new generation but in real this doesn't match with that security gap. The main problem is budget for modern architecture of the chips which is very less for the IoT devices, if the prices will go up in making them chip will become expensive. Also the complex design will require more battery power which is finally becomes a challenge for IoT applications. Affordable wearable IoT devices won't use such chips, this means there we need better approach.

- Weak Password Protection

© 2017 IJETCR. All Rights Reserved.

A big number of users create weak and simple passwords for authorizations. Many devices accept passwords such as "1234."

- Insecure web/mobile interface

Most IoT-based solutions have a web/mobile interface for device management or for utilization of collected data. This web interface is found insecure due to be sluggish development of the Open Web Application Security Project. That will invite Vulnerabilities, such as poor session management, weak default credentials and cross-site scripting vulnerabilities.

- Default credentials

Most devices and sensors are configured to use the default username/passwords.

- Privacy concerns

Devices used in the health care domain collect at least one piece of personal information; the big majority of devices collect details such as username and date of birth. However, the fact is that many devices transmit information across networks without encryption poses even more privacy risk. Privacy risk arises as the objects within the IoT collect and cumulative portion of data that relate to their service. For example, the regular purchase of different food types may divulge the religion or health information of the buyer. This is one condition of the privacy challenges with respect to IoT.

5. PROPOSED SOLUTIONS:

There are some proposed solutions for the security of internet of things take a look at a few basic points, such as what should be done, and what is being done, to improve IoT security now.

- Formulation for security breaches

We should always be prepared for hidden security breaches. Sooner or later any day any time it can be happened, to anyone else. It is also necessary to educate customers, employees and everyone about the security problems and their solutions to overcome those problems else involved in the process about the risks of such breaches. Instruct them in what to do in case of a breach, and what to do to avoid breaches.

- IoT Security -Data Encryption

Internet of things applications collects hues amount of data. And for that collection of Data and processing is essential part of the whole IoT environment. Always Most of this type of data is personal and needs to be protected through encryption. To overcome this IoT security issue we can use of Secure Sockets Layer protocol or SSL wherever your data is present online. Websites already use SSL certification to encrypt and protect the user's data online. This is only first half of the equation seconds half is to protect the wireless protocol side. While data is being transferred wirelessly it also needs encryption. Assure you self use a wireless protocol with inbuilt encryption.

- Digital Signature

When the device is first developed and ready to use, then by a cryptographically generated digital signature it should verifies the authenticity and integrity of the software on the device, i.e., Here only the software that has been authorized to run on that device and signed by the entity that will be authorized, and it will be loaded. [7]

- Firewall

For the security reasons Firewall is must for each and every device to make deep packet analysis capability to control traffic, It is designed to terminate at the device in a way that makes excellent use of the limited computational resources available.

- Software Updates

Software updates and security patches must be delivered in a way that uphold the limited bandwidth and regular connectivity of a planted device and absolutely terminate each and every possibility of compromising functional security.

- Latency and Capacity

Here Latency means the total time taken in data transfer between the application endpoints and Capacity. That is calculated in the bps also known as handling speed of network. Developers of IoT devices always try to find out different ways to increase capacity and latency of their IoT applications for improving performance. Problem is both these factors are inversely proportionate, improving one degrades the other. Data intensive devices and applications should be thoroughly tested for latency and capacity balance.

- Manufacturability Test

Manufacturers always do the assembly line testing on their end but you should also verify the same. It is also suggested that we must use all the modules together on a board testing which is required to make sure there are no errors because of soldering and wiring. Manufacturability testing is necessary to make sure your application works as it is intended to. At Last initiative to teach customers and

© 2017 IJETCR. All Rights Reserved.

employees on latest IoT security threats and solutions should always take.

- Verification of Network traffic

For security reasons it is requirement of Network traffic (wired or wireless) should be analyzed for any indisputable, unencrypted or modifiable data. There is a compromise between performance and security when encryption is recommended. Here Lightweight encryption algorithms can be used to cater to performance requirements.

- Verification of functional security requirements

Due to the higher level of functional security requirements must be approved. They should also be dominating to negative testing (subversion or fuzzing). For IoT security solutions we can use Software like Service (SaaS) based identity management solutions for authorization and authentication requirements.

- Secure code reviews

Early secure code reviews migrate to early moderation techniques. Sensitive and security impact areas such as boot process, security enforcement and encryption modules should go through secure code reviews. The cost of fixing a security defect is greatly reduced when the security vulnerability is discovered during the development cycle.

- End-to-end penetration test

Establishment of secure IoT network of inter connected devices it ie very essential to apply end-to-end penetration testing should be arranged through the signal path to identify any vulnerabilities in the web interface, mobile interface and cloud interface of the IoT solutions. The penetration testing would give the security condition of the IoT solution for each of its components.

6. CONCLUSION:

After the continuous warnings of security experts rate of cyber-attacks an ever-growing tendency of targeting IoT devices most of the companies nowadays do not consider adequate privacy and security safeguards for their Internet-enabled sensor products. Only 34% of surveyed executives express firm belief that their products are strong enough to suffer persistent cyber-threats.

Without any doubt, IoT enterprises that demonstrate readiness to strong with privacy, data protection and ethical method will win costumer trust and gain competitive advantage in this new type of connected world. Like BlackBerry's marketing strategy, for prove, aims at leveraging its network and mobile data security primacy to become a leader in the market of the Internet of Things. What is new and different than the game plan of its rivals is that the IoT platform will enable its customers to build up secure IoT applications. This platform will further contain time to time wi-fi software updates. BlackBerry has aims to dominate in market first at automotive and shipping sectors together, and then to constantly extend its influence to other global industry verticals, like energy and healthcare. Project Ion is an impressive initiative organized by BlackBerry that will lay the authority for an efficient and secure IoT platform. It will be based on a secure platform for data collection from across a divergent range of devices and environments, as well as establishing a aggressive policy for building durable strategic partnerships between business partners, carries and application developers.

So a plugging economy forces companies to innovate in every sensible way so as to remain competitive. For many companies, this means to connect their "thing" to the Internet, just because this is the current market trend or fashion. We can say that IoT devices are becoming modest, and this is based on their target market, which today are mostly made up of home users.

7. REFERENCES:

1. Drozhzhin,Internet of Crappy Things, Availabl https://blog.kaspersky.com/inter-net ofcrappy things/7667/(17/11/2015).
2. Fahim,ISACAJournalVolume4, 2015,https:// www.isaca.org/Journal/archives/2015/Volu me-4/Pages/security-and-privacy-challenges-of-iot-enabled-solutions.aspx, on 05 Oct 2016.
3. Shao Xiwen "Study on Security Issue of Internet of Things based on RFID" 2012 Fourth International Conference on Computational and Information Sciences.
4. http://www.meet-iot.eu/deliverables-IOTA/D1_ 3.pdf
5. RajSamani,https://securingtomorrow.mcafe e.com/business/3-key-security-challenges-internet-things/ Oct 29, 2014.
6. Wikipedia,thefreeencyclopedia,WannaCryra nsomwareattackhttps://en.wikipedia.org/w

© 2017 IJETCR. All Rights Reserved.

iki/WannaCry_ransomware_attack , *Proposed since May 2017.*.

7. AssafRegev,ShmulikRegev Coauthored ,https://securityintelligence.com/innovative-new-solutions-for-securing-the-internet-of-things/
8. https://content.mactores.com/2016/06/18120915/Internet-of-Things.png
9. https://www.researchgate.net/profile/Viviane_Schmidt/publication/305222860/figure/fig3/AS:388771083243522@1469701657316/Figure-3-The-IoT-architecture-a-Three-layer-b-Middle-ware-based-c-SOA-based.ppm
10. https://www.researchgate.net/profile/Viviane_Schmidt/publication/305222860/figure/fig3/AS:388771083243522@1469701657316/Figure-3-The-IoT-architecture-a-Three-layer-b-Middle-ware-based-c-SOA-based.ppm
11. http://web2.bilkent.edu.tr/wp-content/uploads/sites/84/photo-gallery/bckim3.png
12. http://cordis.europa.eu/pub/fp7/ict/docs/future-networks/projects-sensei-ec-summary_en.pdf

© 2017 IJETCR. All Rights Reserved.