Analysis of Threats and Challenges in IoT

Divya Gautam
Asst. Prof.
Dept. of Computer Science Engineering
Amity University, Madhya Pradesh
Gwalior, India
divyagautam06@gmail.com

ABSTRACT

A new emerging technology is internet of things where we number of objects connected through internet for sending and receiving data like various automation systems, vehicles, sensors etc. There are various security challenges which IoT is facing now a days because of connectivity of various personal properties through internet. It's very easy to attack on such kind of systems to hack personal properties. This research focuses on various technologies used in IoT. It also gives a brief review of various challenges and threats in Internet of Things.

Keyword: - IoT (Internet of Things), EPC (Electronics product code), ONS (Object Name Service).

INTRODUCTION

The EPC Technology which was investigated by Auto-ID Center of MIT [1] [2] and the investigation reports given by ITU [3] [4] is called IoT. Before accepting a new concept, people generally think about 2 theoretical questions:

1. To which human activity does it related to? Namely to analyze the similarities and Differences between it and these related human activities, Which is to added its various features which are different from Others. It can exist as a new type of object in order to support.

2. Which model is to be described by it? A model is a formal absence of a mind of an objective thing, which also indicates that human have a deep cognition about this thing. An explanatory model expands to a further theoretical work on every Element of the model, on other hand; it provides the Technology activities and engineering practices which gives the new thing. The IoT is a system of equivalent computing devices, machines of digital and mechanical, gadgets, pets or person which are provided with an uncommon identifiers and the capacity to passing the data over a network with no requirement of person-to-person or person-to-machine interaction. A object, in the IoT, may be a human with a heart monitor implantation, animal with a biochip transponder, an land vehicle that has included sensors to make the driver attentive when pressure is low in tire, or another natural and/or man- made objects that can be allow an IP address and provided the ability to send the data over a network. Internet of Things has progressed from the union of wireless technologies, MEMS system and the Internet.

II TECHNOLOGIES USED IN IOT

A- EPC (Electronic Product Code):

Basically IoT derives are with the help of "Things Oriented" perspective where things are considered as the things were very simple items radio frequency identification (RFID) tags. The concept of IoT architecture to several scenario like the Auto-ID labs, EPC, object name service (ONS), all these concepts have target to architect the IoT with global design. The main Aim of Electronic Product Code is to support the use of RFID and spread it to the world-wide network for modern future of network and also creates the smart industry for standard global for EPC global network. Electronic Product Code was developed by Auto-ID of Massachusetts institute of technology for data sharing purpose in real time by discovering a unique identifier and the use of RFID, wireless communication technology through internet infrastructure and platform.

EPC: This code is of 96-bits and divided into 4 categories, first partition is Header, 0-7 bits; which describes some future information parts like the numbers, types and length. The target of header is to provide extensibility for required future information. Second partition is Manager, 8-35 bits; it defines responsibility to maintain two cases in their domain that is, object type code and serial numbers. Third is Object Class, 36–59 bits; the duty of object class is to be used for a large number otherwise another object - grouping which is developed by the EPC manager. Fourth is Serial Number, 60-95 bits; it describes the encoding a unique object id-number for all kinds, it provides 2^{36}= 68,719,476,736 unique identifiers [5].

EPC have different element, EPC encoding, EPC tags, reader, EPC savant, Object Name Server, PML, EPC-IS [6].

1. EPC encoding: It has 4 fields which includes EPC header, electronic product code manager, serial number, object classification. The coding length should be of 64 bits,

between 46 bit and 256 bit which should be unique number for all goods in the entire world.

2. EPC tags: Similarly to RFID tags, it is so simple and cheaper then all data and it should store in Electronic product code tags. EPC tags can be classified into two categories, read-only tags and read/write tags.

3. Reader: The target of reader is to get and capture required information from EPC tags.

4. EPC savant: It manages and will deliver information that comes to reader parts.

5. Object Name service (ONS): In traditional internet, any host address should be identified by query server called domain name server (DNS). The motive of DNS is to provide IP address for every host from a certain unique input-name, but in case of IoT communication, it will occur between objects instead of hosts therefore the concept of Object Name Service (ONS) introduce with integration and description of specific object related to RFID tags identifier. Object Name Service is based on Electronic Product Code encoding and users, to identify that which data are stored in EPC-IS.

6. Physical Markup Language (PML): it is developed from XML and adopted a common standard syntax to describe natural objects.

7. EPC-IS: Its target is storage and it provides different product information to the EPC code hence this information store in PML format.

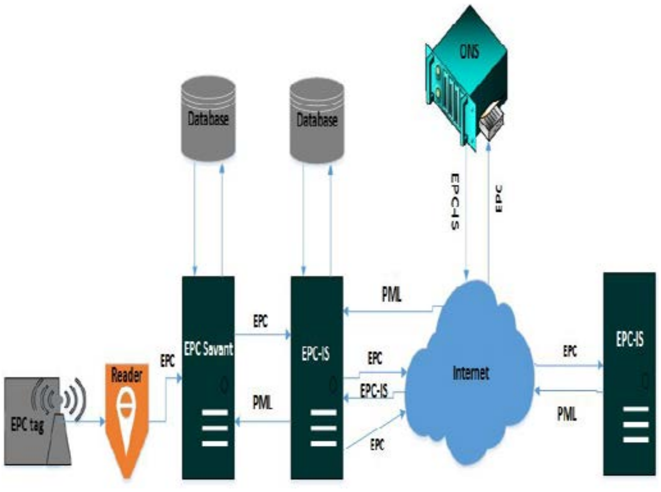

Figure 1: The architecture of EPC network.

For the workmanship of Electronic Product Code system, the reader is required to read Electronic Product Code data which is present in Electronic Product Code tags and send it to savant, after processing and analyzing, that EPC data will pass into EPC savant for its complexity, savant tries to check product data in local EPC-IS then if the savant finds any data, it will rapidly send to savant and if not, then the EPC-IS will send a request for query which is used in EPC cods for getting keyword to the Object Name Service server. When ONS server returns to the IP address of remote EPC-IS, local EPC-IS will send it back to the request of the EPC-IS by query and the purpose of it is to getting product data and pass it to electronics product code savant and wait for the PML cache, Thus EPC savant is a core position.

B. RFID Technology:

RFID technology is one of the most essential factors in the embedded communication technology, which has simple design for wireless data communication. RFID can help to positional the automatic identification of object. RFID is used for acting as electronic barcode. It is the concept of detecting an object automatically for storing and retrieving the data remotely by using radio signals. Generally, RFID components Composed of: Tags, Antenna, Tags Reader Database, Information management software. The Data is transferred between sending and receiving device by radio waves [7]. The sending data is named as tags and recipient information as reader (tag reader). Tags are generally allocated on the objects. If tags will putted in categories based on the supplied power then there would be of mainly three kinds:

i. Semi-active tags
ii. Active tags
iii. Passive tags

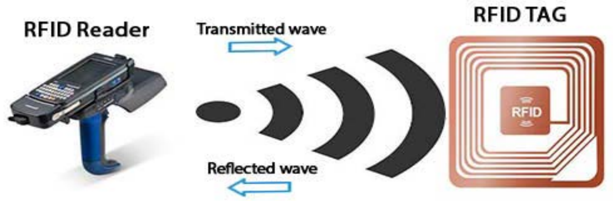

Figure 2: RFID Reader block diagram.

Active & passive tags are quite different, but it can be seen that active tags obtains the energy required from battery of mobile, while passive tags having range and scope reading than active tags and have no supplied power by them, using electro-magnetic radiated energy emitted from the reader. Passive tags have a long life with less cost, and it is also small in dimensions. Another kind of tag is semi-active tag. In terms of its internal battery use, it may use the emitted energy waves from the reader. The transmission of radio signals between the reader and tag itself is possible by using an antenna. There is software of information management for processing the data and collection of the data. In case of any need, this software (usually on a local server) allows the data which is exchanged from the tag reader being accepted, stored & retrieved in its data-base. For barcodes, RFID technology can be a substitute. Factually, a barcode is less than RFID because RFID has a scanner's automatic system. There are major differences between these two technologies. One main difference is that RFID technology is able to handling a large volume of data which important for collect the data by tags reader.

III CHALLENGES IN IOT

To achieve the vision of IoT, there are large numbers of challenges which we are needed to be overcome. These challenges vary from applications, contextual through the technical. A world where everything is connected to each other, information to communicate and the data regarded to its local environment and human in a direct/indirect ways to a centralized location opens the path for “Big Boss”. One’s right of privacy requires to be protected. Trust enhances interesting technological challenges: how and when we can control sensors in an environment? Its necessary having Governance in the IoT is crucial. Public authorities have an amenability to make sure that IoT impact, from economic development to address the issues of the people. Technological Standardizations are also very beneficial, as it grows to good interoperability, hence lowering the basic problems. At Present, A large number of manufacturers are inventing solutions with the help of their own technologies and difficult services. Some standards are required to create to change the “Intranet of Things” in “Internet of Things” which would be more complete.

One beneficial aspect in IoT is a big amount of things being related to the Internet, each one supplying data. Searching few paths to reliably store and understanding the masses of data via scalable uses remain a major challenge in technologies. To narration in this section, we will draw a few key challenge areas:
a) Access control, Security, Privacy, Management of identity.
b) Standardization and Interoperability.
c) Data deluge.

Threats to the Internet of Things Security

We can sort potential attacks against the Internet of Things into three primary categories based on the target of the attack—attacks against a device, attacks against the communication between devices and masters, and attacks against the masters. To protect end users and their connected devices, we need to address all three of these IoT attacks.

1. Attacks against IoT Devices:-
To a potential attacker, a device presents an interesting target for several reasons. First, many of the devices will have an inherent value by the simple nature of their function. A connected security camera, for example, could provide valuable information about the security posture of a given location when compromised.

2. Attacks against Communications:-
A common method of attack involves monitoring and altering messages as they are communicated. The volume and sensitivity of data traversing the IoT environment makes these types of attacks especially dangerous, as messages and data could be intercepted, captured, or manipulated while in transit. All of these threats jeopardize the trust in the information and data being transmitted, and the ultimate confidence in the overall infrastructure.

3. Attacks against the Master of Devices:-
For every device or service in the Internet of Things, there must be a master. The master’s role is to issue and manage devices, as well as facilitate data analysis. Attacks against the masters – including manufacturers, cloud service providers, and IoT solution providers – have the potential to inflict the most amount of harm. These parties will be entrusted with large amounts of data, some of it highly sensitive in nature. This data also has value to the IoT providers because of the analytics, which represent a core, strategic business asset and a significant competitive vulnerability if exposed.

4. In factory floor automation, deeply embedded programmable logic controllers (PLCs) that operate robotic systems are typically integrated with the enterprise IT infrastructure. How can those PLCs be shielded from human interference while at the same time protecting the investment in the IT infrastructure and leveraging the security controls available? Similarly, control systems for nuclear reactors are attached to infrastructure. How can they receive software updates or security patches in a timely manner without impairing functional safety or incurring significant recertification costs every time a patch is rolled out?

5. A smart meter one which is able to send energy usage data to the utility operator for dynamic billing or real-time power grid optimization must be able to protect that information from unauthorized usage or disclosure. Information that power usage has dropped could indicate that a home is empty, making it an ideal target for a burglary or worse.

I. Current Available Solutions

Following are the available solutions for the threats :-
Device ID Certificates issued to each device at the point of manufacturing to establish identity and facilitate authentication to service and other devices.

As sensitive data travels through the cloud and IoT environment, it should be encrypted to prevent interception. Likewise, stored data should be transparently and seamlessly encrypted to prevent theft.

Code signing of firmware/software updates using code signed with digital certificates. Additionally, all communication with devices in the field should use SSL certificates.

IV SUGGESTED FRAME WORK

1. IT STARTS IN THE OS -Security cannot be thought of as an add-on to a device, but rather as integral to the device’s reliable functioning. Software security controls need to be introduced at the operating system level, take advantage of the hardware security capabilities now entering the market, and extend up through the device stack to continuously maintain the trusted computing base. Building security in at the OS level takes the onus off device designers and developers to configure systems to mitigate threats and ensure their platforms are safe. As a pioneer in deeply embedded operating systems, Wind River understands what it takes to ensure functional safety in trusted devices, delivering software that performs tasks on which everyday lives depend. Often the only difference between safety and security considerations is the intent behind them. Wind River is uniquely positioned to implement and deliver security for IoT because of where our products reside in the device software stack. Wind River products and solutions support secure booting with hardware roots of trust, various access control mechanisms, secure package management and software

updates, firewalling and IPS, and integration with network management and event correlation products.

2. THE END-TO-END SECURITY SOLUTION- Security at both the device and network levels is critical to the operation of IoT. The same intelligence that enables devices to perform their tasks must also enable them to recognize and counteract threats. Fortunately, this does not require a revolutionary approach, but rather an evolution of measures that have proven successful in IT networks, adapted to the challenges of IoT and to the constraints of connected devices. Instead of searching for a solution that does not yet exist, or proposing a revolutionary approach to security, Wind River is focusing on delivering the current state-of-the-art IT security controls, optimized for the new and extremely complex embedded applications driving the Internet of Things.

V CONCLUSION

IoT networks are challenging to secure. Meanwhile given that the nature of the risk emphasizes system availability as a high-priority security attribute means that the threat environment is very polarized: IoT networks need to be worried about both sophisticated targeted attacks from competitors and nation-states, as well as accidental misuse from employees, contractors, and vendors. However, by using historical attack patterns, vulnerabilities, and lessons learned from previous incidents, IoT network owners can build a threat model that effectively mitigates security risk while also addressing compliance requirements. This risk-based approach is cost effective, practical, and emphasize the most critical areas of risk first. It’s an important foundation to an ongoing information security program that can enable organizations to continue to use the benefits of increased system interconnectedness as dictated by proven ROI, while minimize the very real human and economic risks associated with IoT.

REFERENCES:-

[1] Wikimedia Foundation Lnc., “Electronic product code: from Wikipedia, the free encryclopedia” Available at: http://en.wikipedia.org/wiki/Electronic_Product_code.

[2] MIT Auto-ID Center, “The Auto-ID Savant specification1.0”. Available: http://www.epcglobalinc.org/.

[3] International Telecommunication Union, “ITU internet reports 2005: the internet of things”. Available: http://www.itu.int/internetofthings.

[4] International Telecommunication Union, “The internet of things 2009: Executive summary” Available at: http://www.itu.int?osg/spu/publications/internet of things/.

[5] David L. Brock, Integrating the Electronic Product Code (EPC) and the Global Trade Item Number (GTIN), Updated edition published November 1, 2001. Distribution restricted to sponsors until February 1, 2002, MIT auto-id center.

[6] Luigi Atzori, Antanio Lera,Giacomo Morabiti, The Internet of Things: Survey. July 2010ScienceDirect.

[7] Lu Yan ,Yan Zhang LaurenceT. Yang Huansheng Ning, The internet of things--from RFID to the next-generation, Pervasive network system.2008s.