Security Challanges In IoT

Aditya Parashar
Dept. of Computer Science Engineering
Amity University, Madhya Pradesh
Gwalior, India
adparashar13.nri@gmail.com

Sachin Rishishwar
Dept. of Electronics & Communications Engineering
Amity University, Madhya Pradesh
Gwalior, India
sachin.rishishwar@gmail.com

***Abstract*— Internet of things is a latest technology which has good number of benefits to its users. It's an emerging technology where we connect daily objects to the internet for sending and receiving data. For an example home automation system, various durable goods, vehicles (cars and trucks) sensors. We can combine all these with internet. We can send and receive information as per user's requirement. IoT is facing security challenges as the devices are providing security to the personal properties like money or intellectual property via automated devices. IoT devices are connected with each other and share information during any haphazard situation. So there are equally more chances for hacking the systems or blocking the services in between transmission. Although fast information exchange is first and foremost requirement so it is not necessary to provide cosmplete security solutions for IoT. This paper contains various security challenges for internet of things and proposing solutions to overcome those security issues.**

Keywords— Central Power Station; EPC (Electronics product code); ONS (Object Name Service); RFID

I. INTRODUCTION

The EPC Technology called IoT was founded by MIT's Center of Auto-ID [1, 2] and analysis record was provided by ITU [3, 4]. While accepting a newly approached concept, there are two main points arises which are:

- By which human activity it is related to? Namely For the analysis of the similarities and the distinctness between it and human activities related with it, Which is required to be added with its some features which are completely distinct from others. It can be presented as a new supportive object[5].
- Which type of model should be described through this? A model, an objective that the human mind is the lack of a formal talk, is a deep perception. On the other hand, an explanatory model to a further extent theoretical model works on each element through which this technology provides the new things to the activities and engineering practices. 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, a 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. Product Code of Electronics (EPC)

With the help of the "things oriented", IoT derives are RFID (radio frequency identification) tags where things are considered as the things were very simple items.

- For several scenarios like EPC, ONS, AUTO-ID labs, the concept of IoT have target to design its architecture globally.
- EPC is mainly used to support use of RF identification and to spread it the globally network for the future of the networks and for standard global, it also makes the smart industry for global EPC network.
- The development of EPC code was done by the help of AUTO-ID of Massachusetts institute of technology for the purpose of data sharing in real world by inventing a specific identifier and the use of wireless communication, RFID technology through infrastructure of internet and its platform [6].

The size of EPC code is 96 bits which is divided in to 4 categories. The header is its first partition which is of 0-7 bits. It gives information about some parts like number, length and type. Manager is the second partition of 8-35 bits which describes the responsibility for maintaining the two cases (Object type code and Serial number) in their domain. The third partition is objective class which consists 36 - 59 bits. This is used for larger numbers or another grouping of objects developed by the manager of EPC. The fourth partition is Serial Number of 60-95 bits. This gives information about

978-1-5090-5434-3©2017 IEEE

encoding of a unique object identification number for all kinds. The number of unique identifiers is 2^{36} or 68,719,476,736 [7].

Encoding, tags, reader, savant, object name server (ONS), PML, EPC-IS are the different elements of EPC [8].

- EPC encoding has 4 fields of length 64 bits between 46 to 256 bit including EPC header, serial number, electronic product code manager, classification of objects. It is required to be a unique number for each good in the entire globe.
- Similar to RFID tags, EPC tag is very cheap and simple. These tags can be divided into two sub-categories (read/write tags & read-only tags).
- Reader is used to get necessary information from Electronic product code.
- EPC savant manages the information and it will deliver news that reaches the parts of reader.
- The address of host should get identify by acknowledge server named DNS. The aim of Domain Name Server is to give IP address for each host from a particular unique i/p name. ONS is completely dependent on EPC users and encoding for the identification that which data are kept in EPC-IS.
- PML (Physical Markup Language) is created from XML and it accepted a general standard arrangement to define natural objects.
- EPC-IS's target is collection. EPC-IS provides some distinct product info to electronic product code thus stored in PML format.

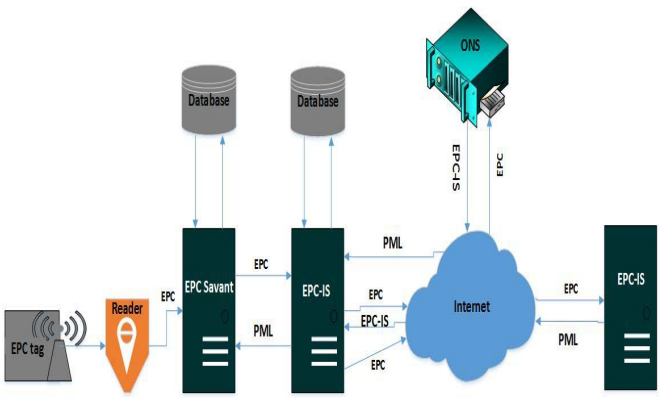

Fig. 1. Network architecture for EPC

For the working of EPC code system, the EPC reader read EPC data which is presented in tags and then sends it to EPC savant. After process and analysis, this data will move towards savant for complexity. EPC savant checks the data in EPC-IS.

If in case savant found any data then this will quickly transfer to savant and if it does not find the data then EPC-IS would ask for query which helps in EPC codes for taking keyword to the ONS.

When object name server comes to the internet protocol address of remote product code IS, the local product code IS will threw it backward by query to request of electronic product code IS. Its purpose is to take product data and pass to savant and then wait for cache of PML. Hence EPC savant is a main position.

B. *Radio frequency Identification Technology*

In the embedded communication, RFID is the most important factor which consist a very simple designing for the wireless data communication technology. It can help in positioning the Auto-ID of the object. RFID is used in electronic bar-coding. This concept is for automatically detect an object for store and retrieve the remote data by the help of radio signals. In General, RFID components are made by the help of Tag-Reader Database, Antenna, Tags and software for Information management. The Data transferred between sender and receiver device in the form of radio waves [7]. The sender information named as tags while receiving information as reader or tag reader. Generally, tags are placed on the objects. If tags would be placed on the basis of category on the supply power then it would be of mainly three types:

1. Semi-active tags
2. Active tags
3. Passive tag

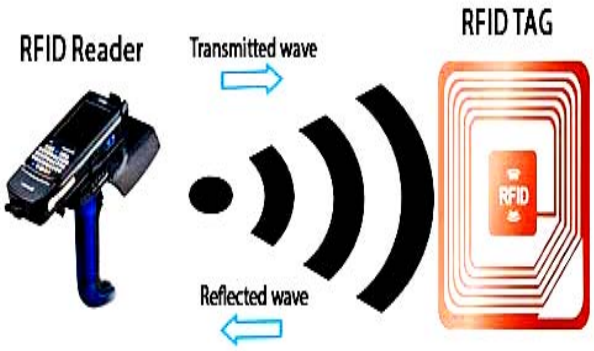

Fig. 2. RFID Reader

Active and passive tags are somewhere different, but in general, it is assumed that active tags take the required energy from mobile battery, while passive tags have scope and range reading than the active tags by using EM radiation power emitted from the reader and there is no power supplied by

978-1-5090-5434-3©2017 IEEE

them. Passive tags are small in dimensions and having less cost and long duration life. Semi-Active tag is other kind of tag which can use the energy from reader which gets emitted by the battery. By the help of Antenna, it is possible to transmit the radio signals in between reader and tag. There is software available for data processing and its collection. But in case if required, this software can permit the data that may required to interchange from tag reader being accept, store and retrieve in data base. For electronic barcodes, this RFID technology can get substituted. A barcode is nothing before RFID technology because RFID technology has an automatic scanner system. Both of these two technologies are having major differences. One of the key differences is that for handling a big data volume which is important for data collection by tag reader [9].

III. CHALLENGES FACED 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? It is 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 [10]. To narration in this section, we will draw a few key challenge areas:

- Access control, Security, Privacy, Management of identity.
- Standardization and Interoperability.
- Data deluge.

IV. ATTACKS IN IOT

In real time devices, there are so many chances of attack on the network so probability of attacks may be reduced if IoT is applied in the real world. It will help in making our device more reliable to the internet which is neither reliable nor trustful network. As the technology is developing rapidly, so our life is becoming easier than before but there are many people who are technically sound and uses their skills in wrong manner. So, If IoT is applied in any network then security threats presented in any network may get reduced. There are some areas where network may get affected:

Unauthorized person exploit security vulnerabilities, like by creating risks to physical safety in certain cases. A participant reveled that how he was able to disturb remotely into two differently connected insulin pumps and he able to change their settings as well, so that no longer delivered medicine. One other participant reviles that attacker can intrude into car's internal computer network without touching the car. The attacker may get access anything in the car such as built-in technology, telemetric unit and it can control the vehicle's engine and breaking as well.

Prone area of attack for IoT devices is where the security may be impossible for the respective person such as public place where attacker may easily get direct physical access inside the IoT devices. Anti-Temper features and other design innovations will need to be considering security.

Many IoT devices do not having capability to update itself so the chances of attack are raised. The upgrade process is cumbersome or impractical.

IoT is not only unsecured with an attacker or a hacker but also unsecured with environment such as some IoT devices may get moisture in the rainy season, the higher temperature is also not goods, and it creates so much damage to the IoT devices.

V. CURRENT AVAILABLE SOLUTIONS

As the IoT is the solution of comfort, technology, get smart, solution on click of smart phone or many other important things as if a person if driving so the car is being automatically controlling console is observing the mental level of the driver and according to its blood pressure and heart beat car will be able to control itself or pacemaker inserted in a patient heart and if it a smart device and it is connected to the network or if somebody is doing some work in which it loose it live and it is totally depending on the IoT device and if it is hacked so there might be possibility it may lose its life or if car's IoT devices would get hack then all the person who are in the car may gets into trouble. So there is a big question the how we can secure the IoT devices without losing life of somebody or may put into trouble. If we talk in broad way that how we can secure the IoT devices so the solution is that we have to find an alternative of internet because the root of the security vulnerability is internet whatever the big crime is

978-1-5090-5434-3©2017 IEEE

going on is occurring with the help of internet number of intellectual has said the world is in the cyber war fare. Classified information of government can be got with the help of internet there are various examples of classified information being theft by the intelligent hackers around the world. Number of powerful countries is intruding other countries to know the information. Highly secure areas are not secure today, if talk about internet noting in impossible, anything could happen in the world so to say that IoT can be secure is not be meaningful. For the current solution to the security of IoT device is to find the way which if alternative of internet.

Software updating of IoT devices is very important, if the software is not updated then it may be easily vulnerable. Timely it requires software updated to secure these devices. Every device which is connected to internet needs to be updated whether it may be personal computer, smart phone or any other device such as IoT. But the problem is IoT devices are huge in number and it quite difficult to update these devices one by one.

Prevent unauthorized accessing by using the high security codes. After a certain amount of time these security code must be reviewed. Virus defense mechanism should be very good. Sign codes are the good option for the code security so that malicious code can not affect the system.

Energy consumption is the major issue for IoT because every device related to IoT works in electronic mode and connected to network, in case if these IoT devise get cut off to its power source then it may be serious issue for the security of the IoT devices. So, all IoT devices should be connected to the central power station which provides power support to these devices as backup. But it might be a possibility if this central power station reach at its empty level then in that condition what will happen with these IoT devices. In that condition a particular IoT device will be applied on that central power station which will examine the central power station power level so that if the power level reaches at minimum level, in that condition user may be intimate by this IoT device which is connected to the central power station.

VI. CONCLUSION & FUTURE WORK

The reason of introducing the IoT is to connect world with the internet by using Sensors and RFID technology so that human life can be more easy and comfortable but still there are many issues which are affecting the technology. The future of IoT is so bright. Everything is about to depend upon IoT devices, the tendency of human being is going to grow itself and make its life more comfortable without any stress. If we want solution on our finger, then these types of facilities are going to be provided by the IoT. So whatever the security measures are discussed in this paper can be implemented in future to strengthening to the IoT devices. Ultimately these devices are providing good facilities to its user.

REFERENCES

[1] Wikimedia Foundation Lnc., “Electronic product code: from Wikipedia, the free encryclopedia”.
[2] MIT Auto-ID Center, “The Auto-ID Savant specification1”.
[3] International Telecommunication Union, “ITU internet reports 2005: the internet of things”.
[4] International Telecommunication Union, “The internet of things 2009: Executive summary”.
[5] Yinghui Huang “Descriptive models for Internet of Thing” International confrencenin Intelligent control and Information Processing, August 2010.
[6] Asghar, Mohsen Hallaj, Atul Negi, and Nasibeh Mohammadzadeh. “Principle application and vision in Internet of Things(IoT)”, International Conference on Computing Communication and Automation, 2015.
[7] David L. Brock, “Integrating the Electronic Product Code (EPC) and the Global Trade Item Number (GTIN)”, Updated edition published November 1, 2001.
[8] Luigi Atzori, Antanio Lera, Giacomo Morabiti “The Internet of Things: Survey”, ScienceDirect , July 2010.
[9] Lu Yan, Yan Zhang, Laurence T., Yang Huansheng Ning, “The internet of things - from RFID to the next-generation Pervasive network system”, 2008.
[10] Asghar, Mohsen Hallaj, Atul Negi, Nasibeh "Principle application and vision in Internet of Things (IoT)", International Conference on Computing Communication & Automation, 2015.

978-1-5090-5434-3©2017 IEEE