International Journal of Management, IT & Engineering
Vol. 9 Issue 10, October 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell’s Directories of Publishing Opportunities, U.S.A

Exploring the Security Issues in Internet of Things (IoT)

Dr. Subhash
Department of Computer Science Govt. PG College Naranul.Haryana
subh3105@gmail.com

Abstract

A revolutionary invention in the Information Technology is Internet of Things (IoT).Internet of Things (IoT) is a network of physical objects connected to internet.Physical objects embedded with Radio Frequency Identification (RFID), sensor and so on which allows object to communicate with each other.The future is Internet of Things, which will transform the real world objects into intelligent virtual objects. There is only either human to human or human to machine communication till now, but the Internet of Things (IoT) provides a great future for the internet where the type of communication is machine to machine (M2M).

The IoT is an intelligently connected device which comprised of smart machines interacting and communicating with other machines. IoT aims to connect everything in our real world in a common infrastructure, giving us controlof things around us as well as keeping us informed about the state of the things. Since the IoT is highly heterogeneous, security is a big challengein IoT.

Keywords— IoT, RFID, WSN, DoS, M2M

1. INTRODUCTION

The phrase “Internet of Things” which is also known as IoT is made from the two words i.e. the first word is “Internet” and the second word is “Things”. There is no unique definition available for Internet of Things.The Internet of Things (IoT) is a network of physical objects that describes a future where every day physical objects- devices, vehicles, buildings and other items—embedded with electronics, software, sensors can be connected to the Internetthat enables these objects to collect and exchange data and also be able to identify themselves to other devices [1]. IoT is closely identified with RFID, sensor technologies, wireless technologies. It allows objects to be sensed and controlled remotely across existing network infrastructure. Internet connects people across the world for emailing, conferencing, gaming, online trading and so on [2]. IoT includes, for example, Cameras connected to internetthat allow us to post pictures online with a single click, changing the lane while driving safely, locking the door, switching offthe lights and fansautomatically in a room when no one is around [2]. The Internet of Things can also be considered as a global network which allows the communication between human-to-human, human-to-things and things-to-things, which is anything in the world by providing unique identity to each and every object [3] Internet of things can be able to transfer data overthe network without human interaction and resulting in improved efficiency, accuracy and economic benefit. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities

2. IoT ARCHITECTURE

The existing architecture of Internetwith TCP/IP protocols, adopted in 1980 [4], cannot handle a networkas big as IoT which caused a need for a new open architecturethat could address various security and Quality of Service (QoS)issues as well as it could support the existing network applicationsusing open protocols [5].Without a proper privacy assurance, IoTis not likely to be adopted by many [6]. Therefore protection ofdata and privacy of users are key challenges for IoT [7]. For further development of IoT, a number of multi-layered securityarchitectures are proposed. [8] Described a three key level architectureof IoT while [9] described a four key level architecture.[10] Proposed a five layered architecture using the best features ofthe architectures of Internet and Telecommunication managementnetworks based on TCP/IP and TMN models respectively. Similarlya six-layered architecture was also proposed based on the networkhierarchical structure [11]. The IoT can be capable of interconnecting different kind of objects through the Internet, so there is a need for a flexible layered architecture. So generally it’s divided into six layers as shown in the Fig. 1.

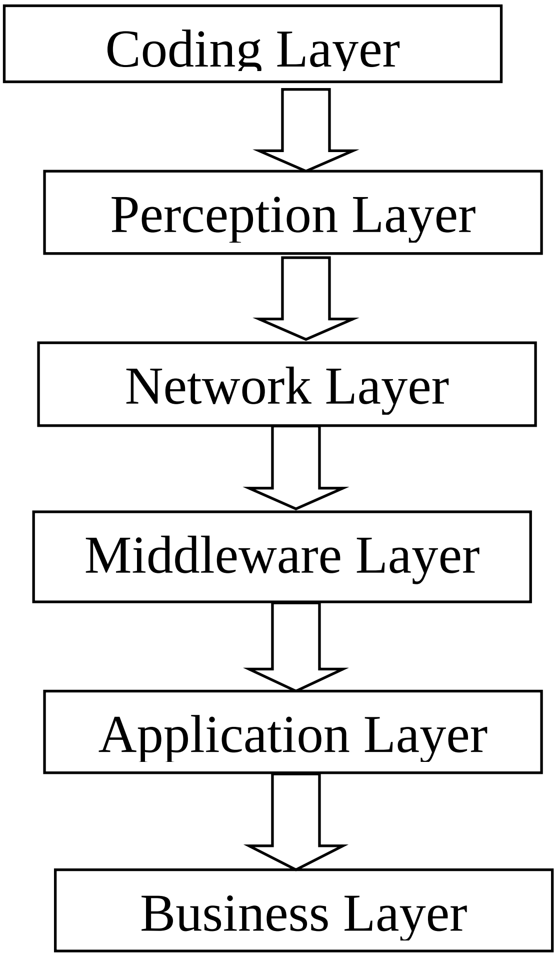

Fig. 1: Six-Layered Architecture of IoT

2.1 CODING LAYER

Coding layer is the foundation of IoT which provides identification to the objects of interest. In this layer, each object is assigned a unique ID which makes it easy to discern the objects [11].

2.2 PERCEPTION LAYER

This is the device layer of IoT which gives a physical meaning to each object. It consists of data sensors in different forms like RFID tags, IR sensors or other sensor networks which could sense the temperature, humidity, speed and location etc of the objects. This layer gathers the useful information of the objects from the sensor devices linked with them and converts the information into digital signals which is then passed onto the Network Layer for further action.

2.3 NETWORK LAYER

The purpose of this layer is receive the useful information in the form of digital signals from the Perception Layer and transmit it to the processing systems in the Middleware Layer through the transmission mediums like WiFi, Bluetooth, WiMaX, Zigbee, GSM, 3G etc with protocols like IPv4, IPv6, MQTT, DDS et.

2.4 MIDDLEWARE LAYER

This layer processes the information received from the sensor devices. It includes the technologies like Cloud computing, Ubiquitous computing which ensures a direct access to the database to store all the necessary information in it. Using some Intelligent Processing Equipment, the information is processed and a fully automated action is taken based on the processed results of the information.

2.5 APPLIATION LAYER

This layer provides the services requested by customers. For example, it provides the temperature and air humidity measurements to customer. Application provides high quality smart services to meet customer needs [12]. Application layer is very helpful in the large scale development of IoT network .The IoT related applications could be smart homes, smart transportation, smart planet etc.

2.6 BUSINESS LAYER

This layer manages the overall IoT system services and activities. Business Layer builds a business model, graphs, flowcharts etc based on data received by Application Layer. The Business Layer also implements, design, monitor, analyze and develop the elements related to IoT. This layer supports decision making processes based on Big Data analysis. Business Layer also monitors and manages the underlying four layers. It also compares the output of each layer with expected output to enhance services [12]. For effective business strategies it generates different business models [13].

ENABLING TECNOLOGIES FOR THE IOT:

There are three types of technologies that enable the internet of things

A) NEAR-FIELD COMMUNICATION AND RADIO FREQUENCY IDENTIFICATION

In the 2000s, RFID was the dominant technology. After few years, NFC became dominant (NFC). NFC has become common in smart phones during the early 2010s, with uses such as reading NFC tags or for access to public transportation.

b) QUICK RESPONSE CODES AND OPTICAL TAGS

This is used for low cost tagging. Phone cameras decode QR code using image-processing techniques. In reality QR advertisement campaigns gives less aurnout as users need to have another application to read QR codes.

c) BLUETOOTH AND LOW ENERGY

This is one of the latest techniques. All newly releasing smartphones have BLE hardware in them. Tags based on BLE can signal their presence at a power budget that enables them to operate for up to one year on a lithium coin cell battery.

SECURITY ISSUES IN IoT

Internet is key infrastructure of IoT hence there is a possibility for some prominent security issues [14]. IoT is a collection of physical objects connected to internet; hence many security issues may occur. Some of the security issues are:

IoT makes everything and person locatable and addressable which will make our lives much easier than before; however without a lack of confidence about the security and privacy of the user's data, it's more unlikely to be adopted by many [15].

UNAUTHORIZED ACCESS TO RFID

An unauthorized access to tags that contains the identification data is a major issue of IoT which can gain any type of confidential or secure data about the user so it needs to be addressed. Not just the tag can be read by a miscreant reader but it can even be modified or possibly be damaged. In this context, [15] detailed some of the real life threats of RFID which includes RFID Virus, Side Channel Attack with a cell-phone and Speed Pass Hack.

CLOUD COMPUTING ABUSE

Computing is a big network of converged servers which allow sharing of resources between each other. These shared resources can face a lot of security threats like Man-in-the-middle attack (MITM), Phishing etc. Steps must be taken to ensure the complete security of the clouding platform. Cloud Security Alliance (CSA) proposed some possible threats among which few are Malicious Insider, Data Loss, Accounts Hijacking and Monstrous use of Shared Computers etc [16] which are summarized as followed:

- Malicious Insider is a threat that someone from the inside who has an access to the user's data could be involved in data manipulating.
- Data Loss is a threat in which any miscreant user who has an unauthorized access to the network can modify or delete the existing data.
- Man-in-the-middle (MITM) is a kind of Account Hijacking threat in which the attacker can alter or intercept messages in the communication between two parties.

HARDWARE ISSUEUS

a) COMPUTATIONAL AND ENERGY CONSTRAINT: Most of the strongest cryptographic algorithms needs a lots of computation and cannot be ported easily to devices that are battery driven and uses low-power CPU with low clock rate.

b) MEMORY CONSTRAINT: Traditional security algorithms were not designed according to limited memory space as these devices uses spacious RAM and hard drive. While IoT devices has limited memory (RAM and Flash memory) unlike the traditional devices like PC, Laptop, etc.. These devices use Real Time Operating System (RTOS) or General Purpose Operating System (GPOS) of lightweight version. Therefore, IoT security schemes should also be memory efficient as conventional security algorithms cannot be used directly for securing IoT devices.

SOFTWARE ISSUSES

a) **EMBEDDED SOFTWARE CONSTRAINT:** IoT devices use Real Time Operating Systems (RTOS), which are embedded with these devices hence these devices have very small network protocol stack and it results in lacking more security modules. So for IoT devices we need more robust and fault tolerant security module with small protocol stack.

b) **DYNAMIC SECURITY PATCH:** IoT devices are small and mobile in nature and has so many constrained. Therefore it might be very difficult to install a dynamic security patch as operating system or protocol stack might not support updated code and library

APPLICATIONS

Most of the daily life applications that we normally see are alreadysmart but they are unable to communicate with each otherand enabling them to communicate with each other and share usefulinformation with each other will create a wide range of innovativeapplications. These emerging applications with someautonomous capabilities would certainly improve the quality of ourlives. A few of such applications are already in the market, let'stake the example of the Google Car which is an initiative to providea self-driving car experience with real-time traffic, road conditions,weather and other information exchanges, In mall it is also used to control the humidity and temperature of mall via central AC by using temperature sensor, E-display system may be used to display Emergency message in Hospitals, all due to the conceptof IoT. There are a number of possible future applications thatcan be of great advantage. In this section, we present few of theseapplications.

SMART TRAFFIC SYSTEM

Traffic is an important part of a societytherefore all the related problems must be properly addressed.There is a need for a system that can improve the traffic situationbased on the traffic information obtained from objects using IoT technologies. For such an intelligent traffic monitoring system,realization of a proper system for automatic identification ofvehicles and other traffic factors is very important for which we need IoT technologies instead of using common image processingmethods. The intelligent traffic monitoring system will providea good transportation experience by easing the congestion. It willprovide features like theft-detection, reporting of traffic accidents,less environmental pollution. The roads of this smart city will givediversions with climatic changes or unexpected traffic jams due towhich driving and walking routes will be optimized. The trafficlighting system will be weather adaptive to save energy. Availabilityof parking spaces throughout the city will be accessible byeveryone.

SMART CITIES

To make the city as a smart city to engage with the data exhaust produced from your city and neighborhood.

- Monitoring of parking areas availability in the city.
- Monitoring of vibrations and material conditions in buildings, bridges and historical monuments.
- Detect Android devices, iPhone and in general any device which works with Bluetooth interfaces or WiFi.
- Measurement of the energy radiated by cell stations and and Wi-Fi routers.
- Monitoring of vehicles and pedestrian levels to optimize driving and walking routes.

•Detection of rubbish levels in containers to optimize the trash collection routes.
•Intelligent Highways with warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams.

SMART ENVIRONMENT

Prediction of natural disasters such as flood, fire, earthquakes etc will be possible due to innovative technologies of IoT. There will be a proper monitoring of air pollution in the environment.

SMART HOME

IoT will also provide DIY solutions for Home Automation with which we will be able to remotely control our appliances as per our needs. Proper monitoring of utility meters, energy and water supply will help saving resources and detecting unexpected overloading, water leaks etc. In home by using the iot system remotely monitors and manages our home appliances and cut down on your monthly bills and resource usage.

- **ENERGY AND WATER USE:** Energy and water supply consumption monitoring to obtain advice on how to save cost and resources.
- **REMOTE CONTROL APPLIANCES:** Switching on and off remotely appliances to avoid accidents and save energy.
- **INTRUSION DETECTION SYSTEM:** Detection of windows and doors openings and violations to prevent intruders.
- **ART AND GOODS PRESERVATION:** Monitoring of conditions inside museums and art warehouses.

MEDICAL FIELD

Hospitals will be fitted out with smart flexible wearable embedded with RFID tags which will be given to the patients on arrivals, through which not just doctors but nurses will also be able to monitor heart rate, blood pressure, temperature and other conditions of patients inside or outside the premises of hospital. There are many medical emergencies such as cardiac arrest but ambulances take some sort of time to reach the patient, Drone Ambulances are already in the market which can fly to that place with the emergency kit so due to proper monitoring, doctors will be able to lead the patients and can send in the drone to provide quick medical care until the ambulance arrive.

- **PATIENT SURVEILLANCE:** Monitoring of conditions of patients inside hospitals and in old people's home.
- **ULTRAVOILET RADIATION:** Measurement of UV sun rays to warn people not to be exposed in certain hours.

SMART AGRICULTURE

It will monitor Soil nutrition, Light, Humidity etc and enhancing the green housing experience by automatically adjustment of temperature to maximize the production. Accurate watering and fertilization will help improving the water quality and redeeming the fertilizers respectively.

- **WINE QUALITY ENHANCING:** Monitoring soil moisture and trunk diameter in vineyards to control the amount of sugar in grapes and grapevine health.
- **GREEN HOUSES:** Control micro-climate conditions to maximize the production of fruits and vegetables and its quality.

- **GOLF COURSES:** Selective irrigation in dry zones to reduce the water resources required in the green.

INDUSTRIAL CONTROL

- **MACHINE TO MACHINE APPLICATIONS:** Machine auto-diagnosis the problem and control.
- **INDOOR AIR QUALITY:** Monitoring of oxygen levels and toxic gas inside chemical plants to ensure workers and goods safety.
- **TEMPRETURE MONITORING:** Monitor the temperature inside the industry.
- **OZONE PRESENCE**: In food factories monitoring of ozone levels during the drying meat process.
- **VEHICLE AUTO-DIAGNOSIS:** Information collection from Can Bus to send real time alarms to emergencies or provide instructions to drivers.

CONCLUSION AND FUTURE WORK

In this paper we have discussed the current state of internet of things and presented a well-defined architecture, analyzed the various security issues in IoT and application of IoT. In future, a framework to detect Denial of Service (DoS) attack in IoT will be proposed and its effectiveness will be measured.

REFERENCES

[1] Jun Wei Chuah ―The Internet of Things: An Overview and New Perspectives in Systems Design‖ 2014 International Symposium on Integrated Circuits 978-1-4799-4833-8/14.

[2] Sarita Agrawal, Manik Lal Das ―Internet of Things – A Paradigm Shift of Future Internet Applications‖ Institute of technology, nirma university, ahmedabad – 382 481, 08-10 december, 2011.

[3] Aggarwal, R. and Lal Das, M. (2012) RFID Security in the Context of "Internet of Things". First International Conference On Security of Internet of Things, Kerala,17-19 August 2012, 51-56. http://dx.doi.org/10.1145/2490428.2490435

[4] "From the ARPANET to the Internet" by Ronda Hauben -TCP Digest (UUCP). Retrieved 2007-07-05 It can be accessed at:http://www.columbia.edu/ rh120/other/tcpdigest paper.txt

[5] Jian An, Xiao-Lin Gui, Xin He, "Study on the Architecture and Key Technologies for Internet of Things," in Advances in Biomedical Engineering, Vol.11, IERI-2012, pp. 329-335

[6] Lan Li, "Study of Security Architecture in the Internet of Things," in Measurement, Information and Control (MIC), 2012, Volume: 1, pp. 374-377

[7] "The Internet of Things," ITU Report, Nov 2005

[8] Wang Chen, "AN IBE BASED SECURITY SCHEME OF INTERNET OF THINGS," in Cloud Computing and Intelligent Systems (CCIS), 2012, pp. 1046, 1049

[9] Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi Liu, "Security in the Internet of Things: A Review," in Computer Science and Electronics Engineering (ICCSEE), 2012, pp. 648-651

[10] MiaoWu, Ting-lie Lu, Fei-Yang Ling, ling Sun, Hui-Ying Du, "Research on the architecture of Internet of things," in Advanced Computer Theory and Engineering (ICACTE), 2010, pp. 484-487

[11] Xu Cheng, Minghui Zhang, Fuquan Sun, "Architecture of internet of things and its key technology integration based-on RFID," in Fifth International Symposium on Computational Intelligence and Design, pp. 294-297, 2012

[12] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash ―Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications‖ ieee communication surveys & tutorials, vol. 17, no. 4, fourth quarter 2015.

[13] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi and Talha Kamal ―A Review on Internet of Things (IoT)‖ International Journal of Computer Applications (0975 8887) Volume 113 - No. 1, March 2015.

[14] Tuhin Borgohain, Uday Kumar and Sugata Sanyal ―Survey of Security and Privacy Issues of Internet of Things‖

[15] "RFID Security Issues - Generation2 Security". It can be accessed at: http://www.thingmagic.com/index.php/rfid-security-issues

[16] V. Ashktorab, S.R.Taghizadeh, "Security Threats and Countermeasures in Cloud Computing," in International Journal of Application or Innovation in Engineering and management (IJAIEM), Volume 1, Issue 2, Oct'12.