DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5687

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

# LITERATURE REVIEW ON SECURITY ASPECTS OF IOT

Rohit Malik
Student, CSE Department
UIET, M.D University
Rohtak, India

Kamna Solanki
Assistant Professor, CSE Department
UIET, M.D University
Rohtak, India

Sandeep Dalal
Assistant Professor, DCSA
M.D University
Rohtak, India

***Abstract:*** This Review paper sheds light on the very approach of Internet of Things. The whole conception of having all the gadgets to be interconnected is a landmark of our technological advancements. The wonders that IoT has provided us have redefined what communication and efficiency means to us. Accessibility has become a more refined privilege, all because of IoT. However it seems all that glitter isn't gold, IoT being a technological wonder it still attaches some limitations to it, foremost of it being the issue of security where data privacy is a very crucial issue that goes in various spheres of social and technological systems, it is something that IoT has to be developed to overcome. Also, the second aspect is the number of devices connected. This research paper also discusses the design aspects of the IoT architecture, its components and various security issues of IoT which can be developed to achieve better efficiency.

***Keywords:*** IoT, M2M, IoT Architecture, IoT Components, Utilization in IoT, Weakness of IoT, Security of IoT.

## I. INTRODUCTION

The concept of Internet of Things is contemplated from the idea that through a wired of wireless network an enormous number of devices are interconnected. Rather a fact of tremendous amusement that the devices linked to the web exceeded the number of humans on the planet. The whole concept of Internet of Things have provided a transition of the technology sphere to the modern age in the true sense. The whole idea that it holds the self-ability to configure and adapt a wireless network with the aim to inter-link everything is itself astonishing. The idea of IoT is to collude a network whose sphere covers many devices merely.

Internet of Things has worked and assisted us to gain the very crucial and rewarding ability to be interconnected. It has become such a great aspect of the modern age tech that IT Giants such as Samsung has claimed that almost all their devices are connected to the internet as of 2017. Even Apple proudly promotes its iOS devices to be connected to the iCloud. This also compiles individual tech like the following:

- Geographical Information System
- Radio Frequency Identification Detection
- Smart Objects
- Global Positioning System

Internet of things requires a canny handling framework and dependable transmission inside a system.

Internet has 3 noteworthy performing actors as client, device and server.

IoT gadgets are isolated into 2 essential gatherings -

***Edge Devices*** – These are low asset gadgets containing sensors/actuators.

***Gateway Devices*** - These are high asset gadgets which will total the information from edge gadgets. They are in charge of mingling edge gadgets to the web.

### *IoT ARCHITECTURE*

IoT engineering has 4 distinct layers:

#### *A. Application layer*

It is the top most layer in IoT architecture and legitimate connection between the client and web which is responsible for delivery of all services to the users in various fields. Technique utilized by the application layer are Machine Learning, information mining, information preparing and different investigation to process the data from framework.

#### *B. Middleware Layer*

Mediated between application and network layer. Its main point is to shield the hardware particulars from unauthorized access and grant the testers to mainly limelight on the evolution stage rather than other. It authenticates clients to furnish a more secure environment alongside proficient conveyance of administrations.

#### *C. Network Layer*

Secures information exchange over sensor and is responsible of totaling the data from different sources and directing it to adjust goal. This layer use technology like WSN, Bluetooth,

Infrared, 3G network. In this layer our aim is to properly allocate unique address for each object. Ipv6 is the best protocol used in this manner.

*D.* ***Perception Layer***

The utilization of creative sensors facilitate the relatedness among gadgets besides promoting the swap of data between them. It contains integrated hardware for discernment and securing of information. Example - RFID is a technique in which chips are installed into the gadgets for automated recognition.

## *IoT COMPONENTS*

### *A. Identification*

Decisive for the internet of things to name and match assistance with their request. Recognizable proof techniques in IoT architecture are Electronic product codes (EPC) and Ubiquitous codes (u Code). Here consign the Internet of things gadgets is analytical to distinguish between item ID and its determinant address. For example for a selective temperature sensor its name will be the object ID and it also have an address within that communication protocol in which it is performing. What's more, ipv6 is used an addressing method for IoT gadgets.

### *B. Sensing*

It means aggregation of data from familiar access inside a system network and direct it back to data directory, data hub or storage drive then composed information is explored to proceed for explicit action in regard to decisive assistance.

### *C. Communication*

Interface heterogeneous items together to convey particular keen administrations. Examples of transmission protocols used for the Internet of things includes Wi-Fi network, Bluetooth, Z-Wave & LTE-Advanced.

### *D. Computation*

Processing units like micro-controllers, micro-processors and other software applications together represents the computing ability of the IoT gadgets.

### *E. Services*

Internet of things assistance will be typecast in four divisions -

1. Integrity related
2. Data augmentation
3. Cooperative aware
4. Ubiquitous

### *F. Semantics*

It refers to the competency of elicitation knowledge stylishly for essential services.

### *IoT VS M2M*

By the definition both IoT and M2M systems may not be advertised as identical. A mutual property of IoT and M2M is remote access to gadgets. Despite there are some fundamental variation between them. The classical M2M refers to transmission between two or more gadgets by aid of a mobile or fixed line network. We call it steep point to point communication. M2M utilization usually subsist of a hardware module installed into a device on the user subordinate which transmits through a mobile or fixed line network with the comparable application usually on the side of service worker. Here main objective is to reduce management and maintain amount. M2M associate things with system but IoT associates system with things. IoT is positioned on the IP network for parallel network of gadgets to a storage drive of a user. IoT usually associates neural data with big data analytic system for enhancement of productivity, increment of manufacturing and stake on market, enhancement of utility. As M2M which only hold gadgets but IoT supports passive sensors, low durability sensors and low amount devices which are not supported by M2M machines. IoT devices broadcast through IP networks which are usually linked to a storage drive which makes it an extensible and flexible solution but M2M are adapted towards installation of sim cards of fixed line network. It is must to specify that M2M associate with IP is a component of IoT. Internet of things is an immense perception than M2M because it may be unified into the global company business while M2M is more align close to maintenance. Despite IoT facilitate a broad spectrum of utilization in usual life, its ongoing application is finite and symbolic changes are expected in the coming time.

### *IoT UTILIZATION*

A. ***Home & Office*** - It has become radical ratio of success in the residential area. Example- You can switch ‘off’ your home lights when you are not at home, you can switch ‘on’ your air conditioner before reaching home.

B. ***Manufacturing*** – Industrial internet is creating a new buzz in the manufacturing sector with sensors, software and big intelligence data to create dazzling machines. Example- You can track your goods whether it reached the location or not, you can keep track of manufacturing figures more accurately and efficiently.

C. ***Transportation*** – It includes engine off your car from your phone, get details of mileage, sensors automatically detect the temperature and allows air conditioner to start automatically.

D. ***Health care*** – It will provide actualize analysis of an individual’s health and provide game plan to combat illness.

E. ***Energy*** – It will collect data in a programmed fashion of electricity consumers and suppliers which will increase efficiency as well as economics.

F. ***Agriculture*** - In India, approximately 70% of the people are dependent upon agriculture as it is their only source of income. IoT has also helped the farmers in reducing their efforts as sensors installed in an agricultural field detects automatically temperature, humidity and accordingly starts irrigating the fields.

This becomes possible only because of IoT as all devices and tools are interconnected to the internet.

### *IoT WEAKNESS*

#### *A. Robustness In Connectivity*

Not firmly established internet connectivity available therefore combination of human and sensors via the internet connectivity is a large scale challenge.

#### *B. Interoperability & Standardization*

Devices produced by different merchants vary in innovation and administrations in this way making them incongruent. Standardization should be re-routed to give interoperability among different items and sensor hubs inside WSN.

#### *C. Naming & Identity Management*

As many/boundless objects are associated, each must have extraordinary recognizable proof. In introduce situation deficiency of address space is a noteworthy task.

#### *D. Safety & Security Of Objects*

Access to data by vindictive/unapproved individual should be anticipated to make preparations for physical harm or modification in characterized usefulness.

#### *E. Data Confidentiality & Encryption*

Usage of encryption to keep up information respectability at layer of data preparing.

#### *F. Big Data*

As we know infinite number of devices are interconnected to each other and each must have data associated with it. We will have data intelligence concept here so that only competent data must be extracted from a gigantic database.

## II. RELATED STUDIES

**Canedo and Skjellum, "Using ML to secure IoT systems" (2016).**

The authors have discussed several security challenges which are heterogeneity in system and number of devices increasing day by day. In the paper, the authors have proposed the idea of machine learning technique and testbed creation method to face the security challenges in an IoT framework [1].

**Khoo, "RFID as an Enabler of the IoT: Issues of Security and Privacy" (2011).**

The authors have discussed enabling technology RFID which has the potential of identifying gadgets, be aware of their position then exchange information and take precautions if necessary. They have also discussed various challenges in the RFID system which are security and privacy issues. In this paper, the authors have proposed a technique which is a feasible solution by putting a tag to sleep position to face the security issues [2].

**Ayyash et al. "IoT: A Survey on Enabling Technologies, Protocols and Applications" (2015).**

The authors have discussed buzz technology IoT which is the combination of internet, sensors and M2M technologies. They have also discussed various use-cases of different

protocols associated with IoT. In this paper, the authors have discussed the alliance between IoT and prominent automation like big data intelligence, cloud computing and fog computing [3].

**Khorshed et al. "Integrating IoT with the power of Cloud Computing and the Intelligence of Big Data Analytics – A Three Layered Approach" (2015).**

The authors have discussed blend IoT with emerging technologies like big data analytics and cloud computing. They have also discussed sequence of lab observations done on distinct hardware products. In this paper, the authors have proposed that the random forest algorithm achieved the highest success rate by performing on 18 different cyber-attacks. In this paper, the authors have challenged that no one has performed such operation on hardware objects so far in the IoT complex environment [4].

**Granjal et al. "Security for the IoT: A Survey of Existing Protocols and Open Research issues" (2015).**

The authors have discussed the next generation internet where user, sensors and internet connectivity are associated with each other. In this paper, the authors have proposed the use of ipv6 for better connectivity [5].

**Zhu et al. "Green IoT for Smart World" (2015).**

The authors have discussed a technology green IoT which diminishes the energy utilization. They have also performed overview architecture of IoT and Green IoT. In this paper, the authors have explained sensor cloud which is an innovative ideal in green IoT conception [6].

**Stampar and Fertalj, "Artificial Intelligence (AI) in Network Intrusion Detection" (2015).**

The authors have discussed that in past disclosure of network attacks is identified by human operators as with mounting growth in the network bandwidth sector we need a system with high efficient security and privacy perspective system. In this paper, the authors have prospective a way by using artificial intelligence which is in turn a branch of machine learning where primary intention is gaining knowledge from data [7].

**Weber and Boban, "Security challenges of the IoT" (2016).**

The authors have discussed security challenges of IoT exclusively in the area of privacy and confidentiality among heterogeneity and limitation in managing the devices as they are increasing every second. In this paper, the authors have compared the two technology which are IoT and M2M [8].

**Gupta and Shukla, "IoT: Security Challenges for Next Generation Networks" (2016).**

The authors have discussed that IoT is an aging and have clear issues which are related to security concern. . In this

paper, the authors have discovered that IoT devices have low computational power and low memory management which are a serious issue in the networking field [9].

### Chaudhary et al. "The IoT: Challenges & Security Issues" (2014).

The authors have discussed have discussed general layer architecture of IoT, its future aspects and limitations. In this paper, the authors have provided a guarded development of the IoT building by dealing with security concerns at each layer of the IoT framework [10].

## III. CONCLUSION

In the present era, IoT has become an important tool for interconnection of various networks. The importance is evident from the fact that in the year 2008, the number of gadgets connected to internet were more than the then population of the world. In the fast moving world, machines have reduced manual labor and efforts as a man can do anything which he can possibly think of by the click of a button. Few limitations such as lack of standardization of sensors which is a potential privacy issue and the increasing number of devices are causing problems in functioning of the system, IoT has become an integral part of human life as its aspirations to boost the essence of life by connecting various smart devices and applications

## IV. REFERENCES

[1] Janice Canedo and Anthony Skjellum, "Using Machine Learning to Secure IoT Systems", Auburn University, doi:10.1109/PST.2016.7906930, pp.219-222, December 2016.

[2] Benjamin Khoo, "RFID as an Enabler of the Internet of things: Issues of Security and Privacy", doi: 10.1109/iThings/CPSCom.2011.83, pp.709-712, October 2011.

[3] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols and Applications", doi:10.1109/comst.2015.2444095, vol. 1553-8777X(p), June 2015.

[4] MD Tanzim, Neeraj Anand Sharma, Kunal Kumar, A B M Shawkat Ali and Yang Xiang, "Integrating Internet-of-things with the power of cloud computing and the intelligence of big data analytics- A Three Layered Approach", doi: 10.1109/APWCCSE.2015.7476124, Deakin University, Australia, December 2015.

[5] Jorge Granjal, EdMundo Monteiro and Jorge Sa Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues", doi: 10.1109/comst.2015.2388550, vol. 1553-877X(p), January 2015.

[6] CHUNSHENG ZHU, VICTOR C. M. LEUNG, LEI SHU and EDITH C.-H. NGAI, "Green Internet of Things for Smart World", doi: 10.1109/ACCESS.2015.2497312, vol. 3, pp. 2151-2162, November 2015.

[7] M. Stampar and K. Fertalj, "Artificial Intelligence in Network Intrusion Detection", doi: 10.1109/mipro.2015.7160479, pp. 1318-1323, July 2015.

[8] Mario Weber and Marija Boban, "Security challenges of the Internet of things", doi: 10.1109/MIPRO.2016.7522219, pp. 638-643, June 2016.

[9] KrishnaKanth Gupta and Sapna Shukla, "Internet of things: Security Challenges for Next Generation Networks", doi: 10.1109/ICICCS.2016.7542301, pp. 315-318, February 2016.

[10] Gurpreet Singh Matharu, Priyanka Upadhyay and Lalita Chaudhary, "The Internet of things: Challenges & Security Issues, doi: 10.1109/ICET.2014.7021016, pp. 54-59, December 2014.