ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

Integration of WSN with IOT: A Review on Security Issues

Jagruthi H[1], Dr.Kavitha C[2]

Assistant Professor, Department of Information Science and Engineering, BNM Institute of Technology, Bengaluru, India[1]

Professor and HOD, Department of Computer Science and Engineering, Global Academy of Technology, R.R.Nagar, Bengaluru, India[2]

ABSTRACT: The advanced technology and the increasing computing power of processors, the use of wireless sensor networks have become largely distributed over wide areas. In recent years the wireless sensor networks is used in Agriculture, smart buildings, environmental, health and many other applications. WSN has the capability of sensing, actuating the environmental data the actual-time and favourable information can be collected using sensor systems. These WSNs can be combined with internet of things to allow association and extensive access to sensor data. In this paper we are presenting a review about combining of WSN with IOT, challenges faced by WSNs when integrating with IOT and how they can be explained from the aspects of security and privacy.

KEYWORDS: WSN. IOT, Security, Privacy

I. INTRODUCTION

Internet of Things (IoT) is nothing but information available everywhere, it allows objects and devices to collect and exchange data, and it is also a group of real objects, sensors, devices and software. IoT grants devices to be sensed and regulated in remote manner across current network framework creating space for more direct alliance of the natural world into computer-based systems that concludes in improved competence, certainty and budgetary benefit. when IoT is combined with actuator and sensor devices, the technology becomes an detail general class of cyber-physical systems, that also enclose the various other technologies like smart grids, home automation systems, intelligent transportation and smart cities [1]. Because of the use of internet of things spreaded extensively, computerized attacks are fairly to become a progressively physical threat.

The IOT was proposed by Kevin Ashton in 1982 .The main aim is giving a new and breakthrough communication between the numerous systems and devices as well as simplifying the interaction of humans with the practical environment, IoT has its application in almost many fields. But with all this using the internet framework for information exchange [2]. Security is one of the most important research issues on WSNs for internet of Things. IoT devices give a possibility of security hazards that could be abused to misuse consumers by: (1) misuse of private information and unofficial access to data (2) promoting attacks on other systems; and (3) generating safety hazards [3].

IOT has become important due to increase in use of sensor networks and radio frequency identification tags (RFID). RFID is nothing but a basic identification given to each individual device which plays as an identification mechanism for IOT.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

II. INTEGRATION OF INTERNET OF THINGS WITH WIRELESS SENSOR NETWORKS

A wireless sensor networks (WSN) are autonomous devices which monitors the real world and environmental conditions such as temperature, humidity using sensors. It also performs as a mainframe, which provides a virtual layer. The data about the real world can be accessed by network through main locations. The very important element in the IoT is wireless sensor networks (WSN). The main aim of connecting both wireless sensor network and IoT devices provides private access, as independent information systems will be able to combine and provide universal benifits [4].

Some of the applications of wireless sensor networks with IOT [5] [6] are Healthcare, Agriculture, Smart buildings (school, hospital, home), Supply chain management, Transportation, Defense , Intelligent home automation system, Smart city, Smart security management, Smart energy management, Logistics management.

III. SECURITY CHALLENGES IN WSN WITH IOT

The main objective is to investigate the security problems which arise when combining wireless sensor networks (WSN) and the internet. It is important to deal with the security of the IoT from a universal perspective and not as a set of confined problems related to distinct technologies. WSN plays an important role in collecting environmental information and concepts, integration of that with IOT can provide us with new perspectives. The various security demands that will arise in combining process are [7],

- Security
- Management
- Quality Of Service (Qos)
- Protection Of Information Privacy
- Protection Of Privacy

Here security plays a prime role when integrating WSN with IOT, many researchers addresses security challenges related to sensor networks. Some of the issues that are addressed are Node compromise, denial of service and unauthorized data access [9].

1) **Denial of service:** This is an attack that makes network resources unavailable to specific users. The attacks can be in any forms like transmitting malignant signals to sensor devices or sending unwanted information to sensors. Some of corrective measures have been introduced like authentication to avoid malignant signals from being processed by network [10].

2) **unauthorized data access :** This is also one of the security issue for smart wireless sensor networks , a large amount of information is generated by sensors where this information are easily seen and it is prone to attack if security measures are not taken. Some encryption schemes have been proposed because of complexity of data encryption, faster encryption schemes need to be developed [11].

3) Node compromise: A wireless sensor networks consists of thousand of nodes working altogether, each node will be prone to attack if the nodes are not properly monitored [10]. A false node can be introduced in to network which can send false information to other nodes. Since the energy constraints are more it is impossible to introduce the security measures [12]. If the internet is connected to sensor network, the sensor nodes can be adjusted remotely which edges to fresh attacks and virus received to network connection that can exploit many other nodes of network [13].

.

IV. SECURITY ISSUES IN IOT LAYERS

With the high use of internet of things many devices are connected to internet, this devices leads to many information security risks. The four layers of IOT Application layer, Perception layer, Network layer and Physical layer plays a most important role in making IOT more secure and reliable. So we need to make sure that these four basic layers are secured .The fig 1 indicates the survey of security issues in various Layers designed for IOT [14]:

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

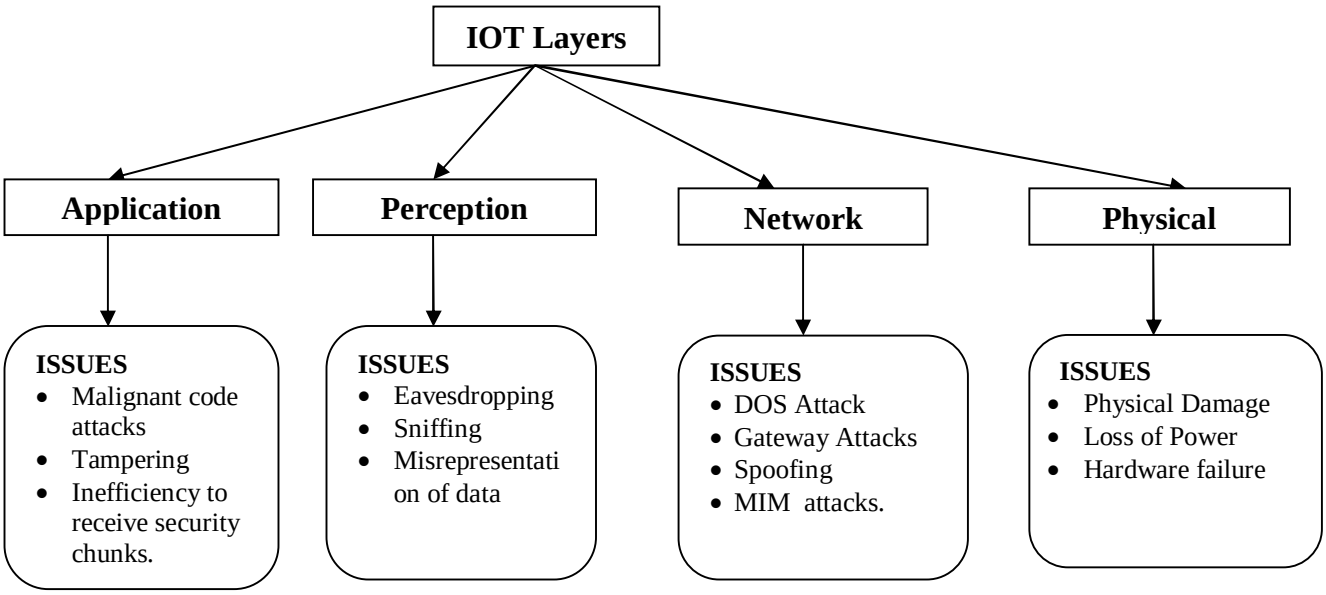

Fig 1: IOT layered Architecture

Perception layer:

It is a physical layer that has sensor technology that senses and gathers information about the environment, temperature, humidity, pressure and RFID. Perception layer senses a few real parameters or analyzes other smart objects in the environment. The security attack in perception layer will be at node level and these are made up of sensors, the nodes are the prime targets for hackers because all the information is collected from sensors. Some of the common threats are sniffing, eavesdropping and misrepresentation of data.

Network layer

Network layer is responsible for connecting to other network devices, and servers. Its features are also used for transmitting and processing sensor data. The original network layer architecture is almost same to the architecture open in traditional networks. To provide roadway to carry, exchange data and network information between multiple sub-networks, network layers plays an important role. Generally at the main network the security services provide the IoT system as a full, and has been toughened to protect against hazards are like as follows:

- The attack where the attacker secretly broadcasts the information and establishes a connection between sender and receiver and eavesdrops into their conversation by sending the messages it hears from sender to receiver, which is called man in the middle attack.
- Spoofing is an attack by where the attacker compromises an identity and can send malignant information to receiver end nodes on the network.
- Confidentiality is nothing but the information that is exchanged between the sender and receiver can be modified by an attacker.
- Replay attack is nothing but the attack where original information is resent by an unknown person to gain access to an pre-existing connection by spoofing their own identity [14].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

Application layer

Application layer delivers application specific services to the user. It defines various applications like smart homes, smart cities, smart transportation and smart health. In application layer the malicious attacker can inject bugs/faults in the application program that makes the application to be malfunctioned.

Physical layer

Physical layer consists of physical components, power supplies, and physical security. The issues that occur in physical layer are hardware failure, physical damage, and loss of power.

V. SECURITY MEASURES TO PROTECT IOT

Some of the security measures have been proposed by various authors, here are a few listed proposed security measures because of the high use of internet of things many devices are connected to internet, this devices leads to many information security risks. Since internet plays an important role here the main focus is on network layer.
A.Sardana and S. Horrow proposed identity management Framework, it addresses problems related to authentication of data between the cloud and device using identity manger and service manager, where the identity manager authenticates the data and sends information to service manager to validate the instructions of the service to be performed [15].
Zhao, Walker and Wang proposed intelligent transportation system security methods, it addresses issues regarding risk analysis where a public key infrastructure is used in that certificate authority is used for monitoring and managing security authorization for the network nodes on ITS to devices to avoid data from being discontinued [16].
Lui, Xiao, Chen proposed authentication and access control, it addresses on fixing loopholes in device security and data integrity, where the user requests authentication to access a device and asks permission from a registration authority (RA), RA in turn send user a question , if response is OK, the user is authenticated to access the device[17].
Li You-guo, Jiang and Ming-fu proposed security middleware, it addresses on providing security to intelligent home systems and communication devices, where it uses entity identification, security storage, security audit, data encryption and decryption, digital signature to secure communication between devices [18].

SECURITY REQUIREMENTS FOR IOTS

- Data Authentication is required for creating a connection between two devices and exchanging private and public keys through sensor nodes to avoid data theft.
- Data Confidentiality assures the end to end security of messages exchanged between IOT devices.
- Data integrity avoids man-in-the middle modification of data by assuring that the data receiving at the receiver node is in unaltered form and remains as transmitted by the sender.
- Data confidentiality is the fundamental issue in IoT scenario, illustrating the guarantee that only authorized persons can access and modify data [8].
- Access control is regulating the access to resources by granting or denying according to rules.

VI. CONCLUSION

Internet of things is spreaded widely across many areas with the use of internet, it is nothing but information available everywhere, anytime. A wireless sensor network plays an important role when integrating with IOT, the use of sensors in the network devices when connected to internet plays a major role. When the IOT is combined with wireless sensor networks, security is a major challenge, when the data is sent from one end to other end the information should be in a secured form. Here we have discussed about various security problems that occur in different layers and the survey on security measures proposed by various authors and its limitations. Here more research has to be done in the field of secured communication of messages through sensor devices and internet.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

REFERENCES

[1] Ala Al-Fuqaha, Senior Member, IEEE, Mohsen Guizani, Fellow, IEEE, Mehdi Mohammadi, Student Member, IEEE, Mohammed Aledhari, Student Member, IEEE, and Moussa Ayyash, Senior Member, IEEE," Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", IEEE communication surveys & tutorials, vol. 17, no. 4, fourth quarter 2015, pp.2347-2376.

[2] Mahesh Patil et al. / International Journal of Computer Science & Engineering Technology (IJCSET) ," Survey on energy consumption in wireless IOT " Vol. 7 No. 01 , ISSN : 2229-3345,Jan 2016.

[3] C. Alcaraz, P. Najera, J. Lopez, and R. Roman, "Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?" 1st International Workshop on the Security of the Internet of Things (SecIoT10), Tokyo Japan 2010.

[4] Deeksha Jain, P. Venkata Krishna and V. Saritha," A Study on Internet of Things based Applications", School of Computing Science and Engineering VIT University, Vellore, TN, India.

[5] Dhananjay singh,gaurav tripathi,Antonio jara,"secure layers based architecture for internet of things",IEEE,2015.

[6] Hamed Sabbagh Gol," Integration of Wireless Sensor Network (WSN) and Internet of Things (IOT), Investigation of Its Security Challenges and Risks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 1, pp 37-40, January 2016.

[7] Daniele Miorandi a, ⇑, Sabrina Sicari b, Francesco De Pellegrini a, Imrich Chlamtac a," Internet of things: Vision, applications and research challenges", Contents lists available at SciVerse Science Direct Ad Hoc Networks journal homepage: www.elsevier.com/locate/adhoc Ad Hoc Networks 10 (2012) 1497–1516.

[8] Dan Partynski, Simon G. M. Koo, "Integration of smart sensor networks into internet of Things: Challenges and Applications", IEEE international conference on Green Computing and Communications and IEEE internet of things and IEEE cyber, physical and social computing, 2013.

[9] H. Chan and A. perrig, "Security and privacy in sensor networks," Computer, vol. 6, no. 10, pp. 103-105, 2003.

[10] A. Perrig, J. Stankovic, and D. Wagner, "security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53-57, 2004.

[11] J. Undercoffer, S. Avancha, A. Joshi, and J. Pinkston, "Security for sensor networks," in *CADIP Research symposium*, 2002, pp, 1-11.

[12] D. Christin, A. Reinhardt, P. Mogre and R. Steinmetz, "Wireless sensor networks and the internet of things: Selected challenges," in *Proceedings of the 8th Fachgesprach drahtlose sensornetze*. IEEE, 2009, PP. 54-57.

[13] Sathish Alampalayam Kumar 1 Tyler Vealey1 Harshit Srivastava," Security in Internet of Things: Challenges, Solutions and Future Directions", 49th Hawaii International Conference on System Sciences, IEEE Computer Society, 2016.

[14] http://www.cisco.com/c/en/us/about/security-center/secure-iotproposedframework.html. "Securing the Internet of Things: A Proposed Framework", available online, accessed on June 2016.

[15] A. Sardana and S. Horrow, "Identity management framework for cloud based internet of things", Proceedings of the First International Conference on Security of Internet of Things, pp. 200-203, 2012.

[16] Zhao, Walker and Wang. "Security Challenges for the Intelligent Transportation System", Proceedings of the First International Conference on Security of Internet of Things, pp. 107-115, 2012.

[17] Lui, Xiao, Chen. "Authentication and Access Control in the Internet of things" 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW), pp.588 – 592, 2012.

[18] Li You-guo, Jiang Ming-fu. "The Reinforcement of Communication Security of the Internet of Things in the Field of Intelligent Home Through the Use Of Middleware", Fourth International Symposium on Knowledge Acquisition and Modeling (KAM), pp. 254 - 257 2011.