IOT AND SECURITY ISSUES FACED IN IOT

Gaurang Tandon [1] (MCA Student)

Dr.Devesh Katiyar[2] (Assistant Professor)

Dr.Shakuntala Misra National Rehabilitation University, Lucknow-226017

***Abstract* - Internet of Things (IoT) can be called as the collection of different types of devices, appliances and technologies connected with the availability to produce completely different services over net specially exchange of knowledge and data. Wireless communication networks are widely open to security threats. IoT permits a lots of devices, peoples, and services to connect and perform action or interchange information.Because of the exaggerated use of these devices, the IoT networks are very likely to be influenced by various number of attacks. In future, IoT will play a major role and may modification our living styles, standards, nonetheless as business models. The usage of IoT in many applications is expected to rise apace at intervals the returning years. Thus, security plays an awfully vital role to satisfy users and it includes of confidentiality, legitimacy, access managements in IoT, privacy nonetheless as trust between the users and the things. During this paper we'll study regarding IoT and also the totally different security issues in IoT system that occur, also as some ways and techniques which might be of help in solving those threats and issues.**

I. INTRODUCTION

The term internet of Things (IoT) is usually pictured as internet of Objects. Internet is that the most prestigious, prevailing and essential creation and after the introduction of IoT, internet got additional quality to form all aspects of life smarter. The elemental construct of IoT is to allow the freelance interchange of valuable data among unnoticeably embedded distinctively recognizable universe devices in our surroundings, that are supported by latest technologies e.g. RFID and WSNs within which sensing devices supported by totally different sensors.

IoT is novel method of assessing the web, with IoT, objects will acknowledges themselves and may adopt intelligent behaviour on the behalf selections creating talents, transfer data regarding themselves to different objects and access the dear and collective data by other IoT.

IoT is imbedding a network of heterogeneous detectors/sensors/devices in our each day's life. That it's creating further ways that to submit the gathered data and important information remotely in physical world. The utilizations of IoT is increasing on everyday basis. Because, it involves no human interaction and in step with a survey study in close to future the employment of IoT can considerably enhance. For swish communication among devices and transmission of information among devices while not human intervention numerous devices square measure connected to the web. Totally different fields of life wherever the IoT's applications will be used square measure as medication, producing industries, smart home, and sensible town yet as agriculture. A microchip that is named RFID will used for the transmission of information in IoT wirelessly but for secure communication in IoT it's essential to follow security mechanisms that totally different encoding algorithms will be used. By victimisation IoT services human will get tremendous advantages however with this they're imagined to pay heaps to keep up their privacy yet as security protection.

The main explanation for this is often that IoT devices have lack of a strong Security System. Thus, there's large potential risk as these devices are connected to the net which in very unsecure. In Oct 2016,users several websites together with Twitter, SoundCloud, Netflix and Reddit reportable that they're unable to access these websites as a result of the DDOS attack on network of IoT containing client devices so, these privacy and security problems on IoT devices results in the an entire novel online privacy security mechanism. DDOS could be a reasonably attack on network within which legitimate users' requests are disrupting from services by

causing the flood of fake requests on the targeted host server. It limits the bandwidth of legal users briefly.

II. IOT APPLICATIONS

The main objectives of IoT are - configuration of sensible surroundings and self-conscious independent devices which might help people in things like living, health, transportation. The applications of IoT in industries, medical field, and in home automation are mentioned within the following section

A. IoT in Industries

The IoT has given a good chance to create important industrial systems and applications, in an intelligent IoT transport industry, the licensed person will monitor the present location and movement of a vehicle. The licensed person may also predict its future location and road traffic. Earlier, IoT was only used in determining distinctive objects which had RFID tags. Later, scientists related it with different sensors such as GPS, phones, and actuators. The acceptance and services of latest IoT technologies principally rely upon the privacy of knowledge and security of data. The IoT permits several things to be connected, tracked and monitored therefore significant data and personal information is collected on its own. In IoT surroundings, the privacy protection may be a vital issue as compared to ancient networks as numbers of attacks on IoT are terribly high.

B. IoT in Personal Medical Devices

The IoT devices also are wide utilized in healthcare industry for observation and assessment of patients. To observe the condition of a patient, Personal Medical Devices are either planted in the body or it might even be attach to the body externally. PMDs are tiny electronic devices that are getting quite common and common. They use a wireless interface to perform communication with a base station that's additional used to scan reading or status of the device, medical reports, and alter parameters of the device, or update reading on the device. Wireless interface causes plenty of security threats for the patient. The wireless interface of such devices is incredibly simple to cyber-attacks which may jeopardize the patient's security, privacy, and safety. In this industry, the first goal is to ensure the safety of network so as to stop the privacy of patient from malicious attacks. Once attackers attack mobile devices, they have their predefined goals. Generally, their aim is to get access to the patient's data, attack on devices to use their resources, or tamper with the working of applications which are observing patient's condition. There are numerous types of attacks on these medical IoT devices that eavesdrop in which privacy of the patient is leaked, integrity error due to which the message that is to be delivered is being altered, and accessibility errors that might even cause battery to exhaust.

C. IoT in Smart Home

The services for an IoT based smart home are increasing every day, electronic devices can effectively interact with one another using IP addresses. All smart devices are connected to the web in a smart home. Because the range of devices is increasing in these type of homes, the possibilities of harmful cyber-attacks is also increasing. If these devices are operated in a way that they are not interconnected then the probabilities of attacks will similarly decreases. Currently these devices are accessed via web at any place also irrespective of time. So, it means increased possibilities of attacks on these them. These home have 4 major components: service platform, smart devices, home gateway, and private network. Within the smart home, several devices are interconnected and they shares data through this private network. In a same way, there is a gateway that controls the flow of data among smart devices which are in connection with the external network. Service platform uses the services of service supplier that deliver completely different services to the home network.

III. SECURITY REQUIREMENTS

The devices and their users in an IoT based network are interconnected to make sure that the services are enjoyed irrespective of time and place. Most of the devices connected to the web don't seem to be equipped with appropriate security mechanisms and are at risk of numerous security problems e.g., integrity, confidentiality and credibility, etc. In IoT, some requirements are necessary for the security of the

data and to secure the network from harmful attacks. Here, some of the basic needed requirements of a secure network are discussed in short.

A. Resilience to attacks:

The system ought to be capable enough to recover itself just in case if it crashes at the time of information transmission. For an example, a server operating in a multiuser setting, it should be intelligent and robust enough to safeguard itself from intruders or an attacker trying to retrieve that data. Or if in case, the system is down it should recover itself without letting the users know that it was down.

B. Data Authentication:

Data and also the associated information should be genuine. A mechanism should be implied to authenticate and verify information transmission is from authentic devices only.

C. Access control:

Only licensed persons are provided access. There should be a supervisor who can controls the users and also access over them and who manages their usernames and passwords and gives users their access rights in order so that different users will only be allowed to read or modify relevant portion of the information or programs.

D. Client privacy:

This means that the information from the IoT devices supposed to be in secure hands. Personal information ought to only be accessed by licensed person to take care of the client privacy. It implies that any unauthenticated user from the system or a different client cannot have access to personal data of a client.

IV. IOT ARCHITECTURE AND FUNCTIONS

The most necessary challenge that has to be dealt very carefully with, while getting into the IoT in world is security. The design of IoT should be strong to take care of estimated range of users and their objects as not only users can communicate with one another but also these entities or objects also will interact with one another. There are 3 elementary policies of security that IoT follows that as follows;

1) Confidentiality: it implies that data or information should be safely hidden from all intermediate nodes and reach the destination in a very secure manner in IoT.

2) Integrity: this policy implies that information or data should reaching at the receiver point should be the same as it was sent from the sender site without any tampering.

3) Availability: for swift, easy, quick and uninterrupted communication over IoT, it's necessary for the service to be accessible all the time for constant operation of nodes.

To solve the security problems we will need to review regarding how IoT system works and what services are provided by it. There are 3 forms of layer in IoT. These layers vary from one another on the behalf of services they supply and also these layers have loose coupling and the flow of information is from lower to higher layer i.e. perception layer to lower layer i.e. application layer and network layer act as intermediate layer.

A. IoT Perception Layer

IoT may be a system within which information is collected and also interchanged from the real world. For this numerous modules are used on perception layer that perform the gathering and management of information e.g. sound detector, temperature detector, movement detector etc. this layer are often divided more into 2 elements Perception node and Perception Network.

• Perception Node: this half is employed for the gathering and management of information.

• Perception Network: the information that's gathered and is forwarded to the gateways and management instructions that are sent to the controller are managed by this node.

It is a layer that's referred as the object layer. It uses sensors as detectors and actuators to spot and perform a particular action consequently. Jointly, these both become Wireless Sensor Network. Mainly, this layer gathers data from concrete objects, digitalize them then sends it to the

upper network layer. At this level 2 security problems arise one is security of sensing devices, another one is security of data that's collected from the objects.

When the abnormal behaviour of sensing devices/nodes is detected, it is often because of the physical attack like destroying the detector or cyber-attack by intruders. To produce the top quality services it's necessary to spot the faulty nodes and take corresponding actions to avoid such issues.

Another security issue that might arise on perception layer is that the algorithmic program used for cryptography and mechanism used for key management.

B. *IoT Network Layer*

An intermediate layer that's liable for controlling the process of data and collected information, aggregation of all information, and broadcast of that data etc. is termed Network layers. It functions as a middle ware between application layer and perception layer as a result it provides the source to destination directions/path to the information. The primary task associated on this layer is that the transmission of information in an economical means while no loss of information on heterogenic network and in original format.

An additional layer can be said to be in between application and network layer that's known as transport layer, it is liable for end to end communication by using of protocols TSP and UDP in accordance to whichever is needed. Security problems arise on this layer could also be concerning to the authentication, communication, encoding of information. Thus, it allows security by fulfilling the necessary requirements e.g. authentication of identity, secure communication, cryptography mechanisms. Sensors are safe and secure so as to guard the human privacy and objects from external world.

C. *IoT Application Layer*

The most topmost layer is application layer that encompasses the basic formulas, business logic and also as interface to the external users. There are different variety of application surroundings and therefore the security demand for such applications could vary from application to application, the one most basic characteristic is sharing of information. Traffic is managed via this layer. Solely those attacks are initiated at this layer that have path in Dos.

This layer is helpful if an oversized scale of IoT application is to be engineered. To make sure the protection at this layer criterion for the basic requirement has been predefined that has authentication, agreement on key, privacy security and protection, education concerning security and management of security. The protocols that are used at this layer are COAP that support UDP for transport and allows security via DTLS, MQIT support TSP for transport and allows security via TLS and SSL etc. on a daily basis there are new updates in technology completely different mobile applications are often connected to IoT that might have the ability of security management techniques in future era.

V. IOT ATTACKS CLASSIFICATION

There can be various attacks on IoT. They are divided as;

- Physical
- Network
- Software
- Encryption.

A. *Physical Attack*

When the physical gap between assaulter and device is so less, which means that they're close to one another then it's known as physical attack. On physical layer secure booting that's applied by exploitation of cryptographical algorithms of hash, for authentication use of digital signature, are the ways which make sure the integrity of code.

B. *Network Attack*

This kind of attack happens once attackers attack on the network system of IoT and harm it. It ought to be necessary for any device to confirm its authentication on IoT network before it transmits or receives information. On network layer a mechanism for authentication and point to point

cryptography can be used for maintaining the secrecy of information and guarantee security of rooting.

C. Software Attack

These attacks could occur if the IoT applications have some loop holes that simply are at risk of security that will offer possibility to attackers to attack the system in a very easy manner. At application layer to protect, security firewalls, control lists, antivirus package are often used that certify, encode also verify integrity.

D. Encryption Attack

The attack, which will occur to cause an interrupt in the cryptography system of IoT system are referred to as encryption attacks, the side channels, cryptanalysis and other people within the middleware are to be the sources of such attacks

Attacks on IoT can also be classified on the basis of the level of attack.

IoT is facing varied forms of attacks and also active attacks and passive attacks which simply disturb the functionality and get rid of the advantages of its services. In an exceedingly passive attack, an attacker simply senses the node or might steal the data however it doesn't attacks physically. However, the active attacks disturb the performance physically. These attacks are divided into 2 more classes that are external and internal attacks. Such vulnerable attacks forestall the devices to interact properly. Thus the safety constraints should be applied to secure devices from malicious attacks. Levels of attacks can also be divided into four varieties

1. Low-level attack: If an attacker's attack on a network is unsuccessful.

2. Medium-level attack: If an intruder is just listening to the information but doesn't change it.

3. High-level attack: If the attack is made on a network and also the data is tampered with.

4. Extremely High-level attack: When the attack is on a network by gaining access by unauthorized means and he performs some malicious operation like sending bulk messages, or jamming the network.

VI. DISCUSSION

IoT is the means of assessing the web, with IoT, objects will acknowledges themselves and may adopt intelligent behaviour on the behalf decisions making skills, transfer data concerning themselves to different objects and access the valuable and aggregate data by other IoT. The utilization of IoT is increasing daily. Because, it doesn't require human interaction. If by exploitation IoT services many benefits are often gained alongside we are required to pay attention in terms of maintaining the privacy of it.

There is large potential risk as these IoT devices are unsecure and are connected to the web. To deal with the safety problems we should study about how IoT system works and what services are provided by them. During this paper various IoT layers are mentioned and the way every layer is different in services. IoT network has 3 layers, Perception, Network and Application layer. After that it also discusses various type of IoT attacks. The aim of this discussion was to know properly how IoT works, what are threats there, what few security mechanisms are there which might be taken in use to improve security.

VII. CRITICAL ANALYSIS

The term internet of Things (IoT) often described as internet of Objects and in the future the use of IoT can considerably enhance. For easy communication and transferring of information among devices without human assistance numerous devices are connected to the web. IoT devices have lack of a strong Security System. There are 3 IoT Security policies which have to be followed - confidentiality, availability and integrity. IoT network has Application Layer, Network and Perception Layer, every layer is totally different from one another and uses numerous protocols that are different from internet protocol to cope with security problems. Perception layer is liable for gathering and transmission of information to outer world

therefore security of sensing devices is a problem on this layer. Second layer is Network layer that's liable for processing, aggregation, and broadcasting an additional layer is also thought of on this Network layer is transport layer for end to end communication. The uppermost layer is Application layer that gives an interface to the external users, it deals with security problems by providing authentication agreement on key, security and protection, education concerning security and management of security. To avoid different security issues some customary policies are to be followed. For this policy to work properly security services are often used that are authentication, encryption, firewall antiviruses.

VIII. CONCLUSION AND PERSONAL OPINION

As day by day the popularity of IoT is growing in every field of life and is helping the life more easy and simple. Now, mobile applications are also connected with it to enhance the performance. As in future it is expected that the use of IoT will massively increase thus it may arise many security issues specially related to the privacy of personal information of people. Hence in this paper is been written to highlight the use of IoT devices, there working, functionality, architecture which help in understanding the issues about the IoT applications. IoT devices are great to use for easy daily life of human beings, but they also hold a great risk of exposure of personal information as well as risk of misuse or tampering of the data and information from these devices. Therefore before using such devices people should know about this topic very well and thoroughly understand the risks as well as take measures for proper security for their own good. Because cybercrime is also increasing day by day, without proper knowledge of this topic, if any of these devices is attacked by any hacker, people can experience losses and even have risk to their health. So I would recommend my readers to initially go through my paper and also read other papers about measure that they can take to safeguard themselves from these security risks and privacy issues of using IoT devices.

IX. REFERENCES

1) "An overview of Security Issues in Internet of Things" -Muqaddas Bano and Saira Sakhawat, Virtual University of Pakistan.

2) "Security Issues in the Internet of Things (IoT)"- Ayushman Chhapariya , Neetu Sikarwar, Institute of Engineering Jiwaji University, Gwalior.

3) "A STUDY ON SECURITY ISSUES AND CHALLENGES IN IoT"- A.Vithya Vijayalakshmi , Dr. L. Arockiam Ph.D. Scholar, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli - 2, Associate Professor, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli – 2.

4) "Security Issues & Threats in IoT Infrastructure" - Archana Sahai Assistant Professor, Amity University Lucknow, India.

5)" IOT SECURITY ISSUES" - De Gruyter, United States, 2017.

6) " IoT: Smart Vehicle Management System for Effective Traffic Control and Collision Avoidance" - Rohini Temkar; Vishal Asrani; Pavitra Kannan.

7) " Developing Patterns in Security Challenges for Coordination of IOT, Bigdata, Network Security: A Survey" - M. Aruna; Vadduri V S N S A D Bhavani; Sanapathi Anusha.

8) " IoT for Healthcare" - B. Sobhan Babu; K. Srikanth; T. Ramanjaneyulu; I. Lakshmi Narayana.

9) " Disease Prediction Using Heart rate Variability Analysis – IoT" - Dharmik Jampala; Venkat Naidu Mittapalle; Sitanshu Nandan.

10) " Smart Security & Home Automation Using Internet of Things (IoT)" - Pranay Pratim Das, Indranil Bhattacharjee.

11) " IOT Based Industrial Automation" - Rohan Jacob; Akash Patil; Sheetal Patil; Rupa Patta.

12) " A Health Care Monitoring System with Wireless Body Area Network using IOT" - M. Rathika.

13) " Internet of Things: Smart Home Automation System using Raspberry Pi" - Smita Mahindrakar; Ravi K. Biradar.

14)"Home Automation Device Protocol (HADP): A Protocol Standard for Unified Device Interactions" - Thomas Gonnot, Won-Jae Yi, Ehsan Monsef, Jafar Saniie - Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL, USA.

15)"Internet of Things: Services and Applications Categorization" - Matthew Gigli, Simon Koo - Department

of Mathematics and Computer Science University of San Diego San Diego, USA.

16)"Research of Intelligent Transportation System Based on the Internet of Things Frame" - Yuqi Wang, Hui Qi - Department of Electronic Information and Control Engineering, Beijing University of Technology, Beijing, China.

17)"Improving the Patient Discharge Planning Process through Knowledge Management by Using the Internet of Things" - Nitya Ahilandam Kamalanathan, Alan Eardley, Caroline Chibelushi, Tim Collins - Faculty of Computing Engineering and Sciences, Staffordshire University, Stafford, UK.

18)"Modeling Secure Home Area Network Based on IoT for Resource Constraints Environment" - Minsu Park1, Mwawi Kayuni, Tiwonge Manda1, Hyunsung Kim - Department of Computer Science, Chancellor College, University of Malawi, Zomba, Malawi Mathematical Sciences Department, Chancellor College, University of Malawi, Zomba, Malawi Department of Cyber Security, Kyungil University, Kyungbuk, Korea.

19)"Internet of Things (IoT): A Literature Review" - Somayya Madakam, R. Ramaswamy, Siddharth Tripathi - IT Applications Group, National Institute of Industrial Engineering (NITIE), Vihar Lake, Mumbai, India.

20)"Hybrid Security Techniques for Internet of Things Healthcare Applications" - Lobna Yehia1, Ayman Khedr2, Ashraf Darwish - Computer Science Department, Faculty of Science, Helwan University, Cairo, Egypt Information Systems Department, Faculty of Computers & Information, Helwan University, Cairo, Egypt.

21)"The Internet of Things and Next-generation Public Health Information Systems" - Robert Steele, Andrew Clarke - Discipline of Health Informatics, the University of Sydney, Sydney, Australia.

22)"A Review of Security Concerns in Internet of Things" - Engin Leloglu - R&D Department, Vestel Electronic Inc., Manisa, Turkey.

23)"Personal Perspectives: Individual Privacy in the IOT" - Johanna Virkki , Liquan Chen - Department of Electronics and Communications Engineering, Tampere University of Technology, Tampere, Finland, School of Information Science and Engineering, Southeast University, Nanjing, China.