https://dx.doi.org/10.22161/ijaems.4.5.10 *ISSN: 2454-1311*

Security Issues & Threats in IoT Infrastructure

Archana Sahai

Assistant Professor, Amity University Lucknow, India
asahai @amity.edu

Abstract— *IoT (Internet of Things) expands the future Internet, and has drawn much attention. As more and more gadgets (i.e. Things) connected to the Internet, the huge amount of data exchanged has reached an unprecedented level.IoT today has a wide scope and researches say that IoT will definitely be a huge reason in the change of human lifestyle. But irrespective of the scope of IoT, we cannot be sure enough to implement it due to the security concerns. There is a genuine need to secure IoT, which has therefore resulted in a need to comprehensively understand the threats and attacks on IoT infrastructure. This paper discusses about the flaws in the security structure of IoT, it is a study about the various layers of IoT and how differentattacks are possible in those layers.*

Keywords— Internet of Thing (IoT), Denial of Service (DOS), Radio Frequency Identification (RFID), Data Distribution Services (DDS), Data Centre (DC).

I. INTRODUCTION

Internet can be defined as a bunch of connected items, network technologies, sensing and gateway devices, endpoints, data analysis systems/approaches, protocols and standards including the Internet Protocol (IP). Internet of Things can be defined as the Interconnectivity of devices which are physical. The Internet of Things enables a smarter bridging of digital, physical and human spheres by adding data capture and communication capacities to objects in a secure way to a networked environment. Internets of Things allow objects to be interconnected and are controlled on remote using networking.According to Gartner "The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment".

The IoT is comprised of the three core components: A collection of smart, connected products, product systems, and other Things connected through an Internet-like communication infrastructure to a computing infrastructure that are creating new forms of value. Data from the product condition, operation, and environment are delivered in real-time enabling capabilities to control, service, and upgrade the product and system performance. For manufacturers (i.e., those in the Things business), these innovations not only have the potential to generate incredible amounts of new value, but also to disrupt the status quo.

We live in a smart, connected world. The number of things connected to the Internet now exceeds the total number of humans on the planet, and we're accelerating to as many as 50 billion connected devices soon.

The rise of the IoT has been driven by the convergence of market forces and parallel innovation of enabling technologies. Products have evolved from purely physical components to complex systems combining processors, sensors, software, and digital user interfaces that are now connected to the Internet and each other. As their definition has evolved, product capabilities have multiplied, creating new forms of value and even doing things well beyond their primary function.

The impact is a fundamental transformation of how manufacturers create and exchange value with customers. This transformation is shifting the sources of value and differentiation to software, the cloud, and service, and spawning entirely new business models. To capture this great wave of value creation opportunity, manufacturers have an urgent need to rethink nearly everything — from how products are created, sold, operated, and serviced.

IoT incorporates everything in itself such as body sensor or cloud computing [2]. No matter its parking your vehicle, or it's a detail of a patient, or your wrist watch that reminds you to take your medicine, or a device that track you activity around [3]. We are today living in the ocean of IoT where every physical device is interrelated. The key element in IoT is the sensors.

1.1. *The major contributors of IOT are:*

- RFID (Radio Frequency Identification) : RFID tracks the data and helps to find the things and the related information.
- Sensors: In things when some physical change is detected, sensors collect that data and process it further.

https://dx.doi.org/10.22161/ijaems.4.5.10 *ISSN: 2454-1311*

- Smart technologies: The smart Technologies develop some of the processing capabilities and then it can also modify the capacity of networks.
- Nano technologies: Nano technologies are the smallest unit that can be used to interconnect the things using IoT.

1.2. ***IoT requires five phases:***

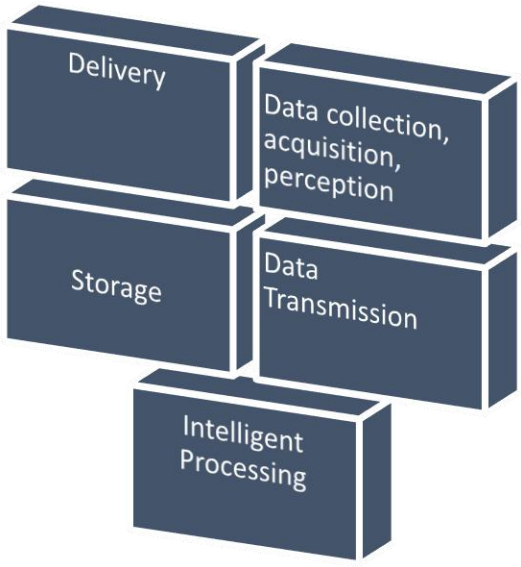

Fig.1: Five phases of IoT

Phase 1: Data collection, acquisition, perception
Firstly, we assemble and retrieve various kind of Information from things or devices. After this some of the important factors are examined and is preceded by the collection of data. The things that can be used in the data collection can be a static body or it can also be a dynamic vehicle.
Phase 2: Storage
All the data that has been collected in phase 1 is allocated to the memory locations and as we know that generally all the components of IoT are stored in small memories and usesthe cloud computing. Due to the low memory all kinds of data storage in the stateless devices is done in the form of cloud.
Phase 3: Intelligent processing.
The data stored in the cloud is analyzed and is provided with the intelligent processing for real time. And then IoT becomes capable of controlling things
Phase 4: Data Transmission.
We can say that data transmission is a part in all of the above phases;Data is transmitted from various kinds of sensors, and the different RFID tags or chips to the DCs. And then the data is transmitted from DCs to the processing unit.From processors the data is transmitted to the controllers and the end users.
Phase 5: Delivery.
All the delivery of information and data from the processors, processors to controllers and end user is completed in the delivery phase.

II. THREATS & ATTACKS IN IoT

Cyber threats could be launched against any IoT assets and facilities, potentially causing damage or disabling system operation, endangering the general populace or causing severe economic damage to owners and users [9, 10]. Examples include attacks on home automation systems and taking control of heating systems, air conditioning, lighting and physical security systems. The information collected from sensors embedded in heating or lighting systems could inform the intruder when somebody is at home or out. Among other things, cyber-attacks could be launched against any public infrastructure like utility systems (power systems or water treatment plants) [11] to stop water or electricity supply to inhabitants.
Security and privacy issues are a growing concern for users and suppliers in their shift towards the IoT [12]. Data Integrity, Data vulnerability & Data confidentiality must be kept in mind when we study anything related to the security issues of internet. A Threat can be defined as a possible danger that might exploit a vulnerability to beach security & therefore cause problem. Thus we can say that due to the evolution of threats security needs to be increased and steps must be taken to prevent various threats & attacks[1].
The attacks can be classified into three parts

2.1. ***Phase attack***

- Phase attack Phase attack deals with the variety of attacks that are on the layers that we have already discussed.
- Data Leakage is an activity done by a dishonest person; it can be internal i.e. within the organization or external.
- Data leakage is international & may be authorized or malicious.
- Data Sovereignty says that all the information should be a part of the laws of the country
- Data Loss can also be one of the attacks of phase attack, Data loss or loss of information or data due to a failure in the software or hardware.
- Data Authentication provides integrity & originality to our data.
- Modification of Sensitive Data During transmission of data this may happen that the data is modified and sent to the end node

https://dx.doi.org/10.22161/ijaems.4.5.10 *ISSN: 2454-1311*

2.2. Attacks as per architecture

Well defined IoT architecture is not established properly yet. However, a three-layerhigh level architecture is commonly accepted [13]. This architecture consists ofthree layers:

Perception Layer
Network Layer
Application layer

A brief description of each layer is given[14]:

2.2.1. **Perception Layer**: the main task of the perception layer is to perceive the physical properties of things around us that are part of the IoT. This processof perception is based on several sensing technologies (e.g. RFID, WSN, GPS,NFC, etc.). In addition, this layer is in charge of converting the information todigital signals, which are more convenient for network transmission.

2.2.2. **Network Layer:** the network layer is responsible for processing the received data from the Perception Layer. In addition, it is in charge of transmitting data to the application layer through various network technologies, suchas wireless/wired networks and Local Area Networks (LAN). The main mediafor transmission include FTTx, 3G/4G, Wifi, bluetooth, Zigbee, UMB, infrared technology, and so on. Huge quantities of data will be carried by the network.Hence, it is crucial to provide a sound middleware to store and process thismassive amount of data. To reach this goal, cloud computing is the primarytechnology in this layer.

2.2.3. **Application Layer:** the application layer uses the processed data by the previous Layer. In fact, this layer constitutes the front end of the whole IoTarchitecture through which IoT potential will be exploited. Moreover, this layerprovides the required tools (e.g. actuating devices) for developpers to realize theIoT vision. The range of possible applications is intelligent transportation, logistics management, identity authentication, location based services, safety, etc.

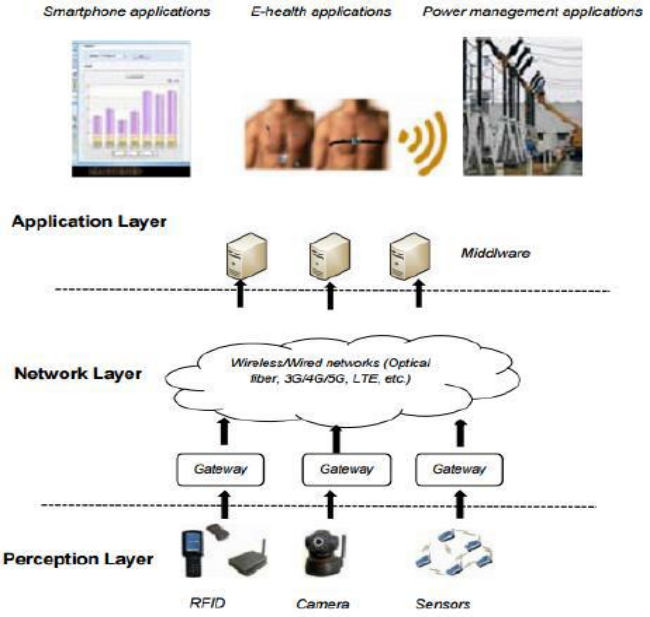

Fig.2: IoT layers

The possible threats that can be in these layers are.-

- **External attack:**These external terrifying attacks come from experienced & trained hackers. These external hackers can find vulnerable network or socially manipulate insiders to get past outer network defenses.
- **Wormhole attack:** In the wormhole attack the intruder does not capture the data, instead the intruder forwards this data in another node and then he retransmits the data from that node [8].
- **Selective forwarding attacks**: In this attack the intruder chooses some selective packets and drop them: i.e. , they select some packets and allow the rest.
- **Sinkhole attack**: In Sinkhole attack, for long durations the sensors are not attended. Therefore the intruder attacks the information and post attacks like selective forward, fabrication, & modification.
- **Sewage Pool attack:** In this malicious user select a particulars region and now the intruder changes the selected base station node so that the selective attacks becomes less successful.
- **Hello flood attack**: In this a Hello message will be introduce to all the neighbor of the reachable area at a certain frequency level. And then, this malicious node converts itself into a neighbor for all the selected nodes of that region and starts to broadcast. And hence a flooding attack cause unavailability of the records by sending huge number of unwanted messages.
- A**ddressing** All Things in Iot: In this the malicious users implements the malicious machine to attack the virtual machine of the user. Using this, a person can hack all the confidential data and use the data for malicious purpose.

https://dx.doi.org/10.22161/ijaems.4.5.10 *ISSN: 2454-1311*

- **DDS**: Thousands of attackers grouped together to initiate such attacks. In this type of attack some unwanted traffic size of huge size are populated so that they could deplete the memory resources. And, now the some important request is not allowed to reach the DC & thus it depletes the bandwidth of DC. In Denial of service, the authorized user in banished from the usage of such services.
- **IP Spoof Attack**: In spoofing the intruder pretends to be someone else so that he could access some confidential information IP spoof attacks, can be IP address attacks, in which the attacker impersonates the IP address of the authorized user.
  There are various kinds of Spoof attack
  - Hiding attack
  - Refraction attack
  - Impersonation attack
- **GoodPut**: GoodPut is the rate at which the data can be transferred from one node to another. We can also say that GoodPut is the ratio between the total data we are receiving and the delivery time.
- **Data Center (DC's)** : A DC can be said to be a centralized for storage purpose as well an management purpose. A DC can be used in house computer system as well as in large storage system.

2.3. Attacks based on Component

As we know that IOT connects everything from the internet. Data can not only be attended, theft loss, breach or disaster data can also be modified by some compromised sensors. Due to this reason it is mandatory for the end user to verify the received information.

III. SECURITY ISSUES & PRIVACY CONCERN

As we discussed from the threats we know that with the vast use of IOT in our day to day environment, we need to find measures for security so that we could own an IOT network that will be effective and the one that could manage security risk. There is immense potential in IOT but it all becomes flamed when we see it from the security point of view, There are some most common security issues that flaws the entire IOT systems.

3.1. Security issues in the wireless sensor networks-

As we study about the attack on network availability we learn that the DOS attack can affect all five layers which are physical layer, link layer, network layer, transport layer & application layer[6].

3.2. The DOS attacks the physical layer by-

1**. Jamming**- In this the intruder creates a jam between the communicating nodes and thus prevent nodes from communication.

2. Node Tampering - Tampering the node physically so that some sensitive information may be tampered.

3.3. DOS (denial of service) attack at the link Layer

The data link layer in WSN multiplexes the data stream; it detects the data frame and checks the error control. The denial of service attack in link layer are-

1) **Collision**- When two data nodes transfer packets of data at equal frequency and at the same time then this type of DOS attack ,i.e. collision can be initiated . Due to the collision attack small amount of data changes that result in the mismatch of result in the end node. Due to which the whole set of data needs to be re-transmitted.
2) **Unfairness**- In unfairness, the collision attack is repeated again and again and the data needs to be transmitted for every collision attack.
3) **Battery Exhaustion-** It is similar to jamming but battery Exhaustion attack creates high traffic due to which end nodes become incapable of communicating to one-another. This occurs when there are large numbers of requests in the system.

3.4 DOS attack on the network layer

The main and the most important usage of network layer are routing. The main DOS attack that takes place in the network layer are-

1) **Spoofing**- In spoofing the intruder gains an unauthorized access, i.e., the confidential information is at a risk of leakage. The main reason to spoofing can be to gain vulnerability to someone else's confidential data
2) **Hello flood attack-** In Hello flood attack, as we have already discussed, a large amount of messages are sent that are useless, but these messages occupy the resources due to which two or more nodes are unable to communicate and hence the traffic or a Jam is created in the system.
3) **Hamming**- In this kind of network attack traffic is created of cluster heads these cluster heads have a capability to shut down the whole system and thus the entire network.
4) **Selective Forwarding**- In this type of a DOS attack only few selected nodes are send rather than all the nodes. And the criteria of selection of node are done as per the requirement of attacker so that this

https://dx.doi.org/10.22161/ijaems.4.5.10 *ISSN: 2454-1311*

malicious motive is achieved and the data packets are not forwarded.

3.5 DOS attack on the transport layer

In this a reliable data transmission comes into action i.e. all the congestion is avoided and all the high traffic jams and floods are prevented[5].

The main DOS attacks on the transport layer are:-

1) **Flooding:** In this DOS attack a huge amount of unnecessary message are sent so that the attackers can successfully create congestion.
2) **De Synchronization:** In this DOS attack, a fake message is created either at one or both nodes of the system so that the retransmission can be requested for the correction of an error that not even exists. Due to which energy is lost at both ends and the attacker can be successful in his malicious motive.

3.6 DOS attack on the application layer

In this the traffic management is monitored. This layer also provides the software for application that translates data into different forms and sends queries. In application layer a path is based, denial of service attack is initiated so that the sensor node can create heavy traffic and congestion is created.

IV. CONCLUSION AND FUTURE DIRECTIONS

It is a challenge to secure IoT network. IoT networks have to worry about sophisticated attackers from both nation-states and competitors, and the misuse from employees, and vendors. As IoT uses network architecture which is similar to traditional network architecture for communication among different devices, flaws of traditional network architecture is also inherited in it. With the development of IoT, many kinds of attacks also have been invented to breach the security of IoT devices. This paper discusses about the possible threats and attacks which can arise from the application of IoT. This paper will be of much use for researchers in the field of securities; it will helpto identify the major problems in IoT security and will provide better knowledge of the threats, increase in the ethical issue, theft, and misuse of information and privacy issues.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, (2010), *"The internet of things: A survey*," http://citeseerx.ist.psu.edu.

[2] Shen, Guicheng, and Bingwu Liu., (2011), *"The visions, technologies, applications and security issues of Internet of Things."* E-Business and E-Government (ICEE), International Conference on. IEEE, 2011.

[3] Brussels, (29 September 2008), *Future networks and the internet: Early Challenges regarding the "Internet of Things,"*, Commission Staff Working Document, SEC (2008)2516.

[4] Pawel Rotter, (2008), *A Framework for Assessing RFID System Security and Privacy Risks*. IEEE Pervasive Computing, 7(2):70–77, June 2008.

[5] D. Eastlake,(2011), *Transport Layer Security (TLS) Extensions: Extension Definitions*, RFC 6066, 2011.

[6] J. M. Kizza, (2013), *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations* Guide to Computer Network Security. Springer, 2013.

[7] J. Lopez, R. Roman, and C. Alcaraz, (2009), *"Analysis of security threats, requirements, technologies and standards in wireless sensor networks*," in Foundations of Security Analysis and Design V. Springer.

[8] D. Jiang and C. ShiWei, (2010), "*A study of information security for m2m of iot,"* in Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference.

[9] Y. Cheng, M. Naslund, G. Selander, and E. Fogelstrom, (2012), *"Privacy in machine-to-machine communications a state-of-the-art survey*," in Communication Systems (ICCS), 2012 IEEE International Conference on. IEEE, 2012, pp. 75–79.

[10] M. Rudner, (2013), *"Cyber-threats to critical national infrastructure: An intelligence challenge,"* International Journal of Intelligence and CounterIntelligence, vol. 26, no. 3, pp. 453–481, 2013.

[11] R. Kozik and M. Choras, (2013), *"Current cyber security threats and challenges in critical infrastructures protection,*" in Informatics and Applications (ICIA), 2013 Second International Conference on. IEEE, 2013, pp. 93–97.

[12] P. N. Mahalle, N. R. Prasad, and R. Prasad, (2013) "*]Cyber Security and the Internet of Things - River Publishers" in* International Journal of Computer Applications, vol. 63, no. 12, pp. 1–6. *https://www.riverpublishers.com/journaldownload.php?file=RP_Journal_2245-1439.*.

[13] Wu, M., Lu, T., Ling, F., Sun, J., Du, H., (2010), *Research on the architecture of internet of things.* In: 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), IEEE (2010).

[14] Romdhani, Imed & Abdmeziem, Riad & Tandjaoui, D. (2015). *Architecting the Internet of Things: State of the Art.*