International Journal of Engineering & Technology, 7 (2.32) (2018) 298-306

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Security Issues and Challenges in IOT: a Comprehensive Study

M.Bhargavi[1], Dr M.Nagabhushana Rao[2]

[1]Research Scholar, Department of CSE, K L University, Guntur, AP, India.
[2]Professor, Department of CSE, K L University, Guntur, AP, India.
**Corresponding author E-mail: bhargaviphd83@gmail.com*

Abstract

The Internet of Things (IoT) is a revolutionary model, with rising wireless sensor network technology. In IoT network devices are connected and communicated with each other or with human. IoT is extremely available to security assaults. In recent years, the internet of things has a continuous support in research. In the upcoming scenario, IoT will play an important role and changes our day-to-day life, principles as well as industry models. In this paper we provide ensuring security of data exchange, IoT architecture and IoT Security architecture, applications, drawbacks of IoT. We study about various security issues, Problems, normal and Denial of service attacks in different layers, issues and research defy in IoT are also discussed.

Keywords:*Internet of Things; Security; Challenges; Open Issues..*

1 Introduction

Computer technology will drastically change every aspect of human life which gave rise to the Internet of Things. It is the hot research topic in the real world scenario, which reduces the human intervention in performing the actions. It is also coined as IoT; it is a cutting-edge technology which provides the concept of communication between the intelligent objects. According to the Technology, IoT is not new for us by its name, it collects data from different things and converge it to any virtual platform works on infrastructure connected to internet.

The Carnegie Mellon coke Machine is the first machine that is connected to the internet of a computer which tracks on how many bottles were left and could measure the level and reports whether drinks were cold which gave rise to IoT in the year 1982. In 1999, Mark Weiser gave rise to the concept of ubiquitous computing; Bill joy gave a hint for device to device communication, IoT is projected by Kevin Ashton [1].

The fundamental initiative of IoT is to permit exchange of valuable and valid information between the real world entities or objects or things around the world. IoT can be developed by using the RFID and WSN technologies in sensing and decision making on the situation and automated action is to be performed.

1.1 What is Internet of Things?

The main motto of Internet of Things is to unite more and more devices to the Web and the Storing the data using cloud, where the devices converse themselves to gather the information and to interrelate with the environment around them. Internet is the vast area where many computers are located to exchange the information throughout the world. The things are objects or devices**.** Exact definition for IoT is not existed**; Internet of Things** is defined as the interconnected devices or objects which exchange the information to complete task in a smarter way. IoT is implemented in many areas like transportation, logistics, healthcare, agriculture and building smart homes.

1.2 Architecture of Internet of Things

There are many types of architectures three layers, four layers and six layers but figure1 represents five layered architecture consists of business, Application, Middleware, Network and Perception Layers[2]. Each Layer is discussed briefly:

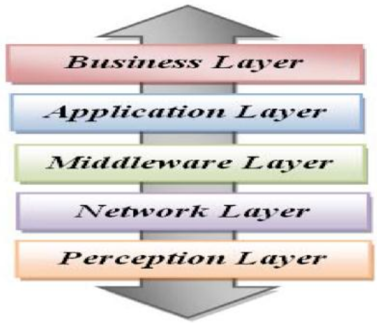


Figure 1: Five Layer IoT Architecture

Business Layer: Business layer is liable to improve research in IoT and support the services and applications of IoT. It builds different business strategies used in effective manner and business models.

Application Layer: This layer is used to develop applications for different industry sectors based on the data which is stored and processed. It promotes the increase of IoT in the large scale environment.

Middleware Layer: This layer works with the technologies like cloud computing, ubiquitous computing, which is used to store necessary information gathered from objects or devices into the database that can accessed directly. It receives the information from sensor nodes and from the intelligent processing equipment used to process and decision making is automatically done depending on the results [3].

Network Layer: This layer receives signals from the sensor layer and process them in the in the middleware layer through the communication channels.

Perception Layer: This layer is also called as sensor layer; it transforms the data into digital signals that are transferred to the network layer for future process. Devices or objects are connected and data in sensors could identify changes in the speed, environmental conditions and locations [4].

1.3 Applications

Smart Homes/Smart Buildings. We can monitor the resources and needs of the users and act accordingly by the sensors. The resources associated with the building is electricity and water that can be monitored by sensors and improve the satisfaction levels of human [5].

Smart Cities. In smart cities the communication between smart objects is more important. In road networks we can monitor the traffic congestion and control the road accidents by communicating them which improves the quality of life of citizens. Many sensor devices are allowed to monitor the space in the vehicle parking area, in case of availability and providing drivers with automated parking advice, it also provides the speed of the cars, pollution level data and smog information.

Smart Environment: IoT devices are used to sense (temperature, wind, rainfall, river height) environmental conditions. A strong architecture is needed to identify and monitor the human and animal life. In some situations like (volcanic areas, Tsunami, earthquakes) to be detected and a decision to be taken in such conditions. IoT has to develop in monitoring and decision support systems to find the solutions for real time problems. Fire detection is another important case for the environmental safety using temperature sensors by sending an alarm or message directly to the fire department to rescue the human life [5].

Health-care: Another important application is healthcare IoT technology is to be developed in this sector to supervise the physical condition of the patients. Sensors are used to monitor the blood pressure, heart beat so if the patients need necessary medication in the remote areas they can get immediate medication which are sent by the doctors by communicating them.

Smart product and inventory Management. RFID technologies used in different sectors for inventory management. Inventory and product management is related to supply-chain, RFID is attached directly to the products or containers to monitor and manage the movement of the product until it is delivered [5].

Security and surveillance. Security supervision is important in every sector. Technologies of IoT have to increase the recital of the current solutions with cheaper and less insidious variety deployment of cameras and providing user privacy at the same time [5].

1.4 Drawbacks

Some of the limitations with evolution of IoT [6]:

1. **Privacy** – It involves exchanging valuable data concerning something. As everything is connected violates within the network would be easy by the hackers. By joining in a region of network would reveal everything concerning a personal or organization or each (may be). What if your workplace colleagues apprehend what medicines you are taking or wherever did you go last night?

2. **Safety** – If a scenario comes out of a disreputable hacker changes your medical prescription and you are provided expired medicines or those healthful medication to that you are allergic to, then there would be a health disaster. Since the buyer that point would be dependent entirely on the technology there would be least likelihood that he would hassle checking something. The verification today is completed manually by the buyer. However, nobody was aware of what's going to happen later.

3. **Compatibility** – At present there's no international customary for device compatibility. As an instance, home based appliances and equipments are also obtaining issues in connecting with laptops or mobile phones. Conjointly, Apple devices cannot connect with any other device. Likewise different makers got to agree upon this else folks can like shopping for only one brand and there would be a monopoly.

4. **Complexness** – If there's a bug all of a sudden electricity bangs, there would be downside since everybody are addicted to the IoT technology. The bugs can result in certain tasks incorrectly accomplished or not done in the least.

5. **Joblessness** – Since the innovation would do its errand independent from anyone else there is no need for any manpower, eventually prompting joblessness. Present PCs should be worked by somebody yet later the arrangements of undertakings would be finished by the machine itself.

6. **Being reliant totally** – Today's era kids are utilizing the cell phones, tablets, Internet, PCs, lifts, ventilation systems, and so on that they get exhausted without these things. Older generation can't envision the expression "getting exhausted" really exists since they figured out how to get occupied by accomplishing something profitable that really required manual work.

2 Security Architecture, Principles, Classification of Attacks

2.1 Security Architecture for IoT

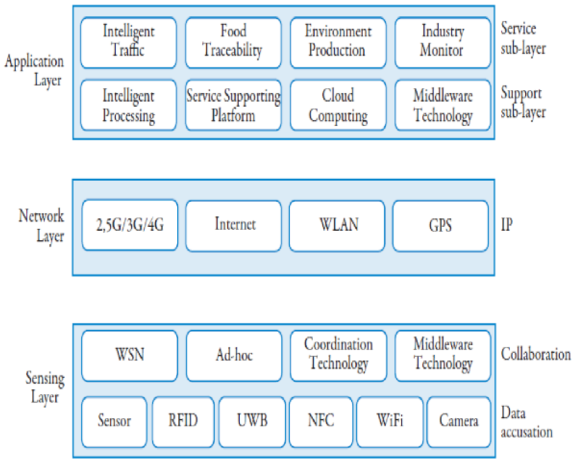


Figure 2: Security architecture

Figure2 represent the defence design of IoT and the sensor devices and technologies used to communicate with the above layers in perception layer [7]. It is also called sensing layer. Sensing layer uses sensor devices to gather the information. Network layer provides the IP technologies used for communication between the devices in the network [8]. Application Layer used to process the applications and technologies ued for the compatibility [9].

2.2 Security Principles for Internet of Things:

Following are the safety principles used to exchange the data in a secure way between the individuals, software, method and objects:

Confidentiality: Exchange of messages from the detector nodes should be secured in IoT. The data ought to be created obtainable solely to the approved users. An assailant should not understand the messages that are exchanged between the nodes [10].

Integrity: In [11], it verifies the accuracy of information. Receiver is ready to spot if the message is changed by the assailant and to spot whether or not it comes from the correct sender or not.

Authentication: The receiver ought to be able to establish the origin of changed messages. Whereas transmission of messages we want to see whether or not the node or person or factor is certified or not [12].

Authorization: IoT devices ought to be able to verify whether or not sure entities are approved to access their measured information. At the network layer solely approved objects ought to be able to access the IoT network. Unauthorized devices mustn't be able to route the messages in network as a result it's going to wipe out energy [10].

Freshness: This makes sure that no older messages to be replayed. This can be vital to secure communication from replay attacks [13].

Heterogeneity: IoT System ought to be dynamic and resilient as a result of it connects devices or nodes with totally different capabilities, complexities, software's and release versions [14].

Policies: Policies and standards are used for IoT networks for exchanging valuable information between the devices. Each and every node within the system is to be certified and approved, therefore the current policies for laptop and networks don't seem to be applicable so, it is essential to extend new policies and standards [15].

Key Management Schemes: Communication of IoT devices is ended with the exchange of messages. To acquire secure communication there is a necessity of encryption to keep up confidentiality of information between devices. To get secure communication, we want a mechanism of key management schemes to provide trust between totally different devices or things and share the keys amongst the devices [16].

Non-repudiation: In [13] Collection of resources and methods are used to prove the participation of an entity in exchanging of information.

Availability: Network services should be available to the nodes or devices. Attacks like denial of service may take the control of the services available as a result the entity is accountable to the measurement of the network [10].

Privacy: Privacy is the most important principle. The personal information revealed to the malicious devices is to be stopped [11].

2.3 Attack classification for IoT

Basically security attacks are divided into five types [17]. They are.

Physical attacks: The assaults work with the hardware parts of the system and it is more difficult to implement as they require costly material. For instances de-packaging of a chip, rebuilding formant and many others.

Side channel attacks: In this the communication is done between source and destination, so there is a necessity of encryption process to encrypt and decrypt data. This attack makes use of some information in encryption process to recover the device key which is victim and compromised.
Cryptanalysis attacks: These attacks are used to break the encryption process and to reveal the information in the IoT system.

Software attacks: Software attacks exploit the execution damages within the system through its interface. Virus programs inject unwanted code into the system and damages the system.

Network Attacks: these types of attacks focus on the devices or objects and communication channel in the network.

3 Layer Wise Security Problems in Iot

3.1 Perception Layer

Devices used in this layer are of different varieties of sensors. Popular devices are RFID, ZigBee and other sensor devices. When data was collected, the communication between devices or nodes is done through wireless communication. As the communication is done through wireless the source of transmission is in signals which are open in the public place. If protective measures are not taking in to consideration, then the signals will be observed, captured, and disconcerted simply. In sensing devices data access is controlled by attackers.

Universal types of attack are as follows [18]:

Node Capture: These types of attacks are physical attacks. Nodes in the network are compromised and reveal the information about the functionality of all the nodes and this may damage of the entire systems security.

Fake Node and Malicious Data: The attacker inserts a device to the network with forged set of instructions or information which may stop transmission of original data in the system. The snooze of node energy is limited and is denied by fake node. Fake node consumes high amount of energy of the nodes and it gain access or damage the entire system.

Denial of Service Attack: It is the reason for restricting the network services and avoid the services to be utilized.It is most regular attack that aroused in Wireless sensor Network and Internet.

Timing Attack: *K*ey information can be obtained, by executing encryption algorithm and analyzing the time required.

Routing Threats: As the network is wireless, routing is dynamic. These types of attacks are more because there is no fixed path between the source to destination. In the routing nodes may be inserted or deleted to extend or shorten the path, it can stop network transmission, tamper or resend routing information, creates a new error messages and increases the delay.

Replay Attack: It is also known as playback attack. Receiver receives a packet sent by the attacker to access trust of the system. Attacker message may damage the authenticated and verified certificate.

SCA (Side Channel Attack): In this type of attack is wicked nodes in the network can get accessed and the side channels of the node reveal the information and get access to devices in the network which performs encryption process.

Mass Node Authentication Problem*:* As all the nodes in the system or network are added and removed dynamically. So each node added to the network must be authenticated, if an attacker compromises then efficiency of the network is decreased.

3.2 Network Layer

Traditional Problems. Data communication between the nodes in the network will have certain security problems which will be a major problem to the data integrity and confidentiality. In old networks there are sufficient measures for providing security, but still there are some frequent threats like accessing the entire network system without permissions, stealing the information, integrity problems [18].

Compatibility problems. As the network is designed accordingly to the person's vision. So there may be compatibility problems in exchanging of information between two networks or devices in the same network. Existing security mechanisms are used to divide the coherent correlation between IoT machines. Diverseness in security creates interoperability and synchronization of network becoming shoddier.

Clustering Security Problems. In addition to network jamming, DoS attack is the problem of authentication etc. The network consists of many devices. If it uses the current technique to authenticate the devices, a large amount of data transfer will probably block the network. The current IP technology is not applicable to a huge number of node identification.

Privacy Disclosure. Hackers can simply accumulate huge amount of user's data privacy through the advancement of information retrieval technology and social engineering.

3.3 Application Layer

Security issues are different for industries or environment. In the designing of IoT, there are no common standards. Some industries work with the concept of device to device communication. It supports in medical sensing field. Some regular problems occur in this layer are [19-20]:

Data Access Permissions, Identity Authentication*:* Many users in the network use different applications. Single application may have many users. In order to avoid unauthorized user access to the application or network, effective technology for authentication is needed. Hostile and spam data is identified easily.

Data Protection and Recovery*:* Communication between the nodes requires user's privacy. Methods and algorithms that are defined and used for data processing and protection, which are not clear that leads to data loss and lamentable.

The Ability of Dealing with Mass-data: IoT is a WSN which consists of huge collection of nodes that are connected, where large amount of data transmission is done which leads to complex network environment. Processing of data and flexibility can't meet the network requirement, which leads to interruption in the network and chance of data loss

The Application Layer Software Exposures*:* while designing the software, trainer design nonstandard instructions that lead to difficulties and hacker can easily get access to the data and work with their purposes.

4 Security and Privacy Concerns in Internet of Things

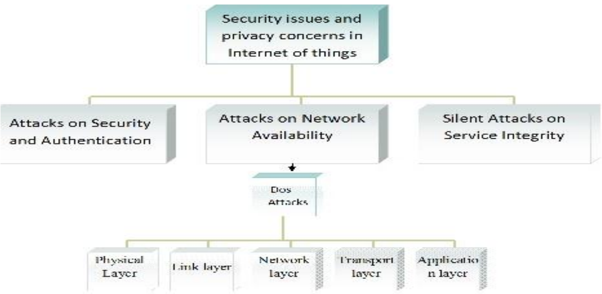

Security issues and privacy concerns in Internet of things
Attacks on Security and Authentication
Attacks on Network Availability
Silent Attacks on Service Integrity
Dos Attacks
Physical Layer
Link layer
Network layer
Transport layer
Applicatio n layer

Figure 3: Attack classification based on security and privacy

In figure 3 it gives the classification on security issues and privacy concerns in internet of things are classified into attacks on security and authentication, attacks on Network Availability and attacks on integrity. Dos Attacks arise based on the network availability in layers of IoT are listed and each layer attacks are discussed below:

4.1 Denial of Service Attacks on the Physical Layer:

Selecting and designing the communication frequency channel, modify and extract, encoding and decoding, scattering and gathering the information is done by physical layer. The attacks are [21]:

Jamming: In this type of attack, frequency channel is occupied by unwanted signals which prevent transmitting information between the nodes in the network.

Node tampering: Retrieving the sensible information from the node by substantial interfering.

4.2 Denial of Service Attacks on the Link Layer:

Different multiplexed information signals gives identification of information frame, fault access and medium access control. The DoS assaults occurred are [22]:

Collision: when two or more devices transmit the data packets on same frequency channel collision occurs. When collision occurs the original data is modified and mismatch at the receiver side which leads to retransmission of data [23].

Unfairness: In [23], an unfairness result in collision where rooted attack is very frequent .The other way to represent it is, exhaustion based attacks.

Battery Exhaustion: when uncommon huge traffic occurs, accessing of devices in a particular channel will be circumscribed.

4.3 Network Layer Denial of Service Attacks:

Routing is a dominant feature. The below list shows the classification of DoS attacks which occurs in this layer:

Spoofing: Spoofing refers to the misleading and repetition of traffic.

Hello flood attack: Huge traffic is occurred in a channel due to the blocking of the channel because of extremely large amount of messages results this hello flood attack. The attacker here receives a purposeless message from an unaccompanied harmful node which is repeated by the attacker for profuse traffic.

Homing: In this attack, cluster heads are explored in the traffic and Security key managers manage to turn off the entire system.

Selective forwarding: This attack itself refers that, an accommodated node only chooses some nodes rather than picking up all the nodes .The basic condition to select a node is the harmful material is accomplished by the attacker resulting in the nodes which do not transfer packets of data.

Sybil: In this case of attack, duplication of an individual node is done by the attacker and many identities to additional nodes is presented.

Wormhole: Dislocation of bits of data is occurred in the network in this DoS attack .This dislocation of data frame is transferred through extracting the data bits above a minimal latency.

Acknowledgement flooding: Whenever the routing procedures are utilized in the sensor networks and acknowledgements are needed. The preordained adjacent nodes receives the acknowledgements which is imitated by harmful node possess erroneous data.

4.4 Denial of Service Attacks on the Transport Layer:

This layer results in the genuine data transmission and evades the surfeit traffic in the routers due to obstruction. The following gives the list of attacks:

Flooding: Flooding cite to deliberate obstruction of interaction medium through broadcast of redundant messages and huge transfer.

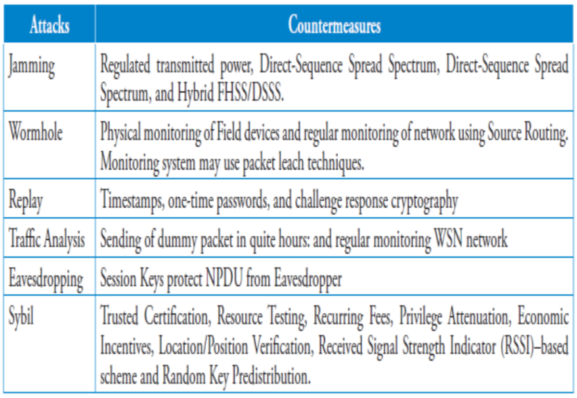
De-synchronization: In this type of assaults, fabricated data is generated at single end or at both the ends appealing retransformation for the rectification of hypothetical fault. While carrying out the imitated instructions the depravation of energy occurs in one or both the end points is caused due to this.

4.5 Denial of Service Attacks on the Application Layer:

Traffic management is done by this application layer. Other responsibility is it also serves as software providerto present the translation of data into accessible form for various applications or assists in gathering of data by requesting queries. A Route-based DoS attack is introduced to generate heavy traffic in the path heading to base station by provoking the sensor nodes [22-24].

4.6 Common Attacks Countermeasures

Table1 provides existing countermeasures to improve the IoT security communication Technologies. Some of the countermeasures for the frequent attacks that are occurred [37]:



Attacks	Countermeasures
Jamming	Regulated transmitted power, Direct-Sequence Spread Spectrum, Direct-Sequence Spread Spectrum, and Hybrid FHSS/DSSS.
Wormhole	Physical monitoring of Field devices and regular monitoring of network using Source Routing. Monitoring system may use packet leach techniques.
Replay	Timestamps, one-time passwords, and challenge response cryptography
Traffic Analysis	Sending of dummy packet in quite hours: and regular monitoring WSN network
Eavesdropping	Session Keys protect NPDU from Eavesdropper
Sybil	Trusted Certification, Resource Testing, Recurring Fees, Privilege Attenuation, Economic Incentives, Location/Position Verification, Received Signal Strength Indicator (RSSI)–based scheme and Random Key Predistribution.

Table1. Countermeasures of layer wise attacks

4.7 Taxonomy of Attacks on IoT

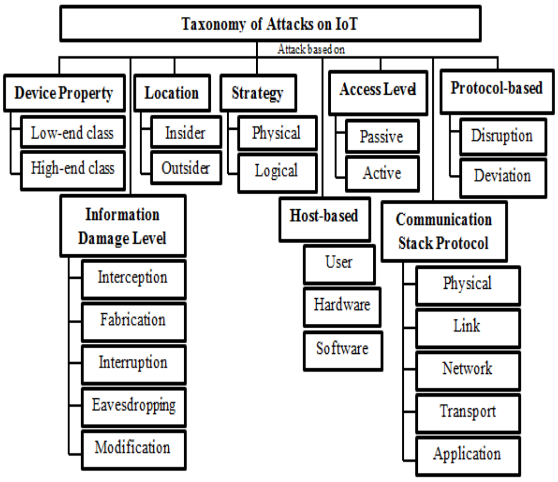


Figure 4: Attacks based on different criteria

Figure 4 represents attacks on IoT depends on several factors. They are based on device property, location, strategy, information damage level, host-based, access level, communication stack and finally based on protocol- based.

A. Spoofed, Alter, Replay Routing information

Spoofing, altering, and replay routing are mutual direct attacks target on routing information when the data transmitted between two nodes. Spoofing refers fraud or deceiving computers or its users and can be detectable by IoT devices. Generating false messages and designing routing loop are the attacks generated. Attackers just listen to the transmitter. When the sender stops sending signals to the receiver then the attacker starts sending the untrustworthy signal [25].

B. Sybil Attack

Because of rise in IoT systems, it exposes to Sybil attacks, one node can act in multiple locations at a time with multiple identities. It reduces the secured data integrity and utilization of resources.

C. Denial of Service (DoS)

Numbers of request packets are transmitted from one node to another node in the network to interrupt the services to other nodes which results in the network capacity. It may crash the system or it is forced to restarted is the capability of common DoS attack. Distributed denial of service prevents accessibility in large networks.

D. Device based Attacks

These attacks results in abnormal behavior of the devices in the piece of the system might act unusual behavior due to the power of the device [25]. These classified into two:

E. Bottom-end device class attack

In this it involves devices which consume low power to attack the system; it is low cost because of using radio link for connecting the system to outside environment.

F. Top - end device class attack

Complete devices are used for the attacks on IoT System. These attacks uses Internet, so it can be accessed from anywhere, anytime.

G. Attacks Based On Access Level

Availability of the IoT systems is affected by access level. They are of

Passive attacks: These attacks do not disturb the transmission between IoT devices or users. But, it just watch and learn how to use the data from system is called passive attack.

Active attacks: Active attacks break the security feature of the data by disturbing the network communication.

H. Attacks Based On Adversary Location

A challenger commenced from anywhere to assaults the IoT system. Insider or outsider Attackers are attacks based on adversary location [25].

Internal attacks: Attacker tries to execute an internal program that damage or destroy the working of IoT devices. These are called as internal or insider attack.

External attacks: It is also called as an outsider attacker. It is a trial and error method, used to access the IoT network. As they attack from external they don't know about IoT architecture and it is public.

G. Attacks based on Attacks Strategy

Assaults have their own strategies in damaging the IoT system. It runs their own program which damage the system. There are two strategies:

Physical attacks: Attacks on Physical devices i.e. infrastructure or hardware components.

Logical attacks: A logical attack on IoT system can be defined as an attack on the communication channel of an IoT system. Here the physical devices of the system are not harmed by the attackers.

H. Attacks Based On Information Damage Level

Sensor nodes in IoT are used to monitor variable parameters of the given environment. Any open information can be easily modified and tampered by an opponent. Attacks based on information level damage can be classified into six types[25]:

Interruption: Interruption is the process of depriving the accessibility of the network. Resource fatigue occurs during an interruption and can send even send the IoT device into push to close the system.

Eavesdropping : An eavesdropping incident occurs when an opponent or a malicious outsider blocks the receiver of an IoT device from picking up a transmitted packet. Radio frequency identification devices (RFID) usually encounter this problem. Confidentiality of the system takes a hit when this occurs.

Alteration: Information in IoT devices is the process where the information sent to the Iot device in question is modified by the attacker.

Fabrication: Fabrication is the process where imitation data is sent over the network to the IoT device. It compromises the authentication of IoT systems due to the damage to the information in the system.

Message Replay: Here the attackers hold the present conversation in the gathering that is to be played again. The intention for message replay is that it intercepts the new message and modifies it to confuse the IoT end device and cause harm to the system. The system believes that they are communicating with each other unaware of a third party

Man-in-the-middle: Transmission between two devices is secretly relayed and alters the transmission by the attacker where the two parties think that they are directly communicating. The attacker wants to steal information in "Y" and places two other nodes in between X and Y. When X completed transmitting of data to Y, if Y is still getting the messages then Y think that it is truly from X but not from attacker. Let us consider the case of a phone conversation between a representative of a bank and a customer. A malicious outsider can intercept the call and steal sensitive information such as account numbers, ATM pin numbers etc.,

I. Host-Based Attacks

Hosts are those devices such as users, software and hardware. In host based attacks the embedded systems containing operating system and system software are the main targets.

User-compromise

A person may extract sensitive data such as security information including passwords, login IDs among others. For example the building passwords can be accessed authenticative individual.

Software-compromise

Here the assailant pushes the IoT device to the limits of its capability. It does so by overflowing the resource buffer. The system can be made to be inoperable and unresponsive to the users. The system can many time s be placed in sleep mode.

Hardware-compromise: Here the adversary directly interferes with the hardware of the IoT device in question by tampering with the hardware directly. They do it in a myriad number of ways. They insert malicious code or also replace the device drivers. A possible scenario is that a smartphone can be exploited by using the I/O port as its target.

J. Attacks based on Protocol

There are two ways where the protocol of IoT systems can be compromised and can threaten the security mechanism and availability of the device. It is illustrated below [25]

Deviation from protocol: An outsider does not follow protocol and tend to violate them because of application and network protocol and there are standard protocols that are not followed by the attackers.

Protocol disruption: In the context of IoT devices, availability is one of the security attributes. But the system is still not foolproof and attackers can disrupt the protocol by disrupting the inside or the outside of the network and can severely compromise the availability of the IoT device.

4.8 Study of various Types of Attacks and Possible Solutions

There are various kinds of attacks; based on the nature and behavior of attack and threat level of attacks are discussed in this section. Attacks are categorized into four types based on the levels. And possible solutions to threats/attacks [26].

Low-level attack: The efforts of the intruder to attack the network are not successful.

Medium-level attack: The integrity of the data transmitted over the network is not compromised by the intruder is able to intercept the messages and eavesdrop.

High-level attack: The integrity of the data is compromised if the attacker so wishes to do so.

Extremely High-level attack: The attacker gains complete control over the network by gaining unauthorized access and perform illegal operations like jamming the network making it unavailable and sending bulk messages.

5 IOT Challenges

Providing security for IoT is the biggest challenge. The application data in an IoT device can be of many types and of various backgrounds like enterprise, consumer or personal. The data that is generally stored in IoT devices are sensitive in nature need to be guarded carefully. We can take the example of the health record of a patient among many others. While IoT devices improve communication drastically there are still some issues that are needed to be worked on such as scalability availability and response time. Security remains a huge concern while transmitting data over a network especially over large distances and crossing international borders [27].

Data Privacy: some manufactures of smart televisions gathers the information on the viewing habits of its customers to utilize that information to their commercial gain. So data privacy remains a concern.

Data Security: It remains a daunting task to protect transmitted data over the internet and from observing devices.

Insurance Concern: the companies selling IoT devices collect sensitive data about the health and driving status of the user in order to use this information to decide about the coverage.

Lack of Common Standard: Each device in IoT system has different standards. But there are no common standards for all the devices that are manufactured and are permitted and non permitted devices that are connected to the internet.

Technical Concerns: It has been a growth spurt of IoT devices. The consequence of this is that more traffic is being generated and hence there is a need to increase the network bandwidth to accommodate these devices. There is also additional need to store the data collected for further analysis.

Attack Security and System Vulnerabilities: the attack vulnerabilities are listed below [27].

System Security: Focuses on entire IoT system to identify challenges in security, framework designed for providing proper guidelines to maintain network security.

Application security: It is specific to each application and works according to each application to handle the scenario requirements.

Network security: It deals with the security issues between different IoT devices and ensuring impenetrable transmission

5.1 Issues and Challenges:

Security related challenges and issues in IoT are: [28, 29]

1. Security of the IoT devices can be time consuming because of various reasons such as the low computing power due to which the processing of the security algorithms becomes slow and cumbersome. There is also the problem of battery capacity being severely limited and related the the quantity of computation and resource demand. Then there is also the question of storage.
2. IoT comprises of many devices. Communication is done between the devices or nodes. Keep it mind that providing security for the nodes is important. Cryptography is the solution for providing security. But, it is not feasible on constrained devices that is optimized and demand in fewer resources.
3. The complexity and length of some protocols and procedures used are more expensive.
4. There is no correct solution to all of the IoT device problems. The dependency is strictly on the basis of application to application.
5. In IoT, devices are freely available and can be easily accessed by the attacker as it does not have a fixed structure. Security has to be provided for both the software and hardware access by external and unauthorized agents.
6. Devices in the network are different, the applications run on different devices is difficult so it is needed to have standards and policies for interoperability.

6 Defending DDoS in the IOT Age

IoT is changing the way we do business, opening up many new avenues, the opportunities that lie before us, and the security threats we face. At the RSA 2015, IDC analyst Chris Christiansen argued that there is no money in security and embedded security in consumer IoT devices is minimal. Although enterprises, researchers and vendors are constantly working on solutions to protect IoT devices, there is always a difficult choice to make regarding tradeoff between device security and market profits. Manufacturers eager to get their products to the market are presented the choice of security and profit and profit is obviously their option [30-34].

We can classify the DDoS attack defense strategies into are classified into two types:

i. Precautionary defense strategies to prevent serious attacks on the devices. This is also known as proactive measures.

ii. Reactive attack defense strategies work in two ways, either they try to mitigate the source of the attacks or to try and identify the source of the attacks on the devices

Proactive DDoS defense measures in the security framework design protocols such that there is a strong interlinking between the security protocol and the devices themselves both are equally protected. Some of such proactive measures are:

a. Hardening the IoT device for secure boot and leveraging hardware security features like the Trusted Platform Module/Trusted Execution Environment (TPM/TEE), Trust zone, crypto acceleration and so on.
b. Deploying Intrusion Detection and Prevention System (IDS/IPS) and adoption of robust encryption mechanisms.
c. Segment IoT device in its own network and deploy firewalls for network access.
d. Ensuring strong authentication passwords for proper login.
e. Enabling visibility, accessibility and audit reporting of IoT devices to enterprise management offering them greater level of control.
f. Deploy smart gateway devices to enhance security of the network perimeter.
g. Managing vulnerabilities and ensuring regular and secure firmware updates

7. Open Issues for the Iot Security

Instead of concentrating on a specific part or device or region, the entire systems is considered as a unit and plan how to create solutions, architectures for the security issues and proceed to combine heterogeneous devices across the networks.

7.1 Overall Security Architecture for the Entire Iot System

In IoT system security differs from application to application and their solutions. With different application paradigms we can provide appropriate and customized solutions to each and every problem according to their contexts. [35] This means IoT security architecture has the intrinsic quality that multiple frameworks cannot be solved by a specific framework. Some ideas can be borrowed from software engineering; we can extract the similarities among the application. So the designing of the final security architecture that is common to provide basic solutions for security which is similar application in IoT.

7.2 Lightweight Security Solutions

As there are specific features in IoT, our future research direction is to provide lightweight solutions. These solutions have to meet the specific requirements of our applications. Application computational and security requirements are classified into different levels[36].

7.3 Efficient Solutions for Massive Heterogeneous Data

In IoT network, the devices generated huge amount of different type of data for every minute. It is efficient to identify the path to work with massive amount of different data.

8 Conclusions

IoT gives tremendous changes in the usage of internet and also provides many number of research opportunities in real-world. Current days' providing security and privacy for the networks is a challenging task for the researchers. This paper discusses on security architecture, problems, applications, various attacks, normal and Denial of service attacks in each layer, taxonomy of attacks, various security, open issues and challenges for the IoT Security. It is proven that in IoT, security is no way concern in many areas. To resolve many issues, more research should be done.

References

[1] Evans, D. (2011). The Internet of Things:Howthe next evolution of the internet is changing everything. CISCO White Paper, 1(2011), 1–11.

[2] Khan, R., Khan, S.U., Zaheer, R. and Khan, S. (2012) Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. 10th International Conference on Frontiers of Information Technology, December 2012, 257-260. http://dx.doi.org/10.1109/fit.2012.53

[3] Tan, N. and Wang, N. (2010) Future Internet: The Internet of Things. 3rd International Conference onAdvanced Computer Theory and Engineering, August 2010.

[4] Wu, M., Lu, T., Ling, F., Sun, J. and Du, H. (2010) Research on the Architecture of Internet of Things.3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), August 2010.

[5] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, Imrich Chlamtac (2012)

[6] " Internet of things: Vision, applications and research challenges", in Adhoc networks. ScienceDirect, 2012, pp 1497-1516.

[7] Soumyalatha, Shruti G Hegde, "Study of IoT: Understanding IoT Architecture, Applications, Issues and Challenges", in international journal of advanced networking and applications.

[8] Sundmaeker, H., Guillemin, P., Friess, P., & Woelffle, S. (2010). Vision and challenges for realising the Internet of Things. Cluster of European Research Projects on the Internet of Things, European Commision.

[9] Mitchell, S., Villa, N., Stewart-Weeks, M., & Lange, A. (2013). The Internet of everything for cities: connecting people, process, data and things to improve the livability of cities and communities.

[10] Zheng, L., Zhang, H., Han, W., Zhou, X., He, J., Zhang, Z., & Wang, J. (2011). Technologies, applications,and governance in the internet of things. Internet of Things-Global technological and societal trends. From smart environments and spaces to green ICT.

[11] S. Capkun, L. Buttyan, and J. P. Hubaux. Self-organized public-key management for mobile ad hoc networks. IEEE Transactions on Mobile Computing, 2(1):52–64, January 2003.

[12] M. C. Chuang and J. F. Lee. Team: Trust-extended authentication mechanism for vehicular ad hoc networks. IEEE Systems Journal, 8(3):749–758, September 2014.

[13] S. U. Maheswari, N. S. Usha, E. A. M. Anita, and K. R. Devi. A novel robust routing protocol raeed to avoid dos attacks in wsn. In Proc. of 2016 International Conference on Information Communication and Embedded Systems (ICICES), February 2016.

[14] X. Yang, J. Lin, W. Yu, P. M. Moulema, X. Fu, and W. Zhao. A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems. IEEE Transactions on Computers, 64(1):4–18, January 2015.

[15] Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of security and privacy issues of internet of things. arXiv preprint arXiv:1501.02211.

[16] Garcia-Morchon, O., Kumar, S., Struik, R., Keoh, S., & Hummen, R. (2013). Security Considerations in the IPbased Internet of Things.

[17] Verissimo, P., & Rodrigues, L. (2001). Fundamental security concepts. InDistributed Systems for System Architects, Springer US. (pp. 377-393).

[18] Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). Proposed embedded security framework for internet of things (iot). In Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on (pp. 1-5). IEEE.

[19] Shancang Li, Kewang Zhang. : Principle and application of wireless sensor network. M. Beijing: China Machine Press (2008)

[20] Xueguang Yang, Fengjiao Li, Xiangyong Mu, etc.: Design of security and defense system for home based on Internet of things. J. computer application. 30(12):300-318 (2010)

[21] Antonio J. Jara, Miguel A. Zamora, Antonio F. G. Skarmeta. : HWSN6 Hospital Wireless Sensor Networks Based on 6LoWPAN Technology: Mobility and Fault Tolerance Management. C. In:International Conference on Computational Science and Engineering, 879-884 (2009)

[22] http://sensors-and-networks.blogspot.in/2011/08 /physical-layer-for-wireless-sensor.html

[23] Ahmad Abed Alhameed Alkhatib, and Gurvinder Singh Baicher. "Wireless sensor network architecture." International conference on computer networks and communication systems (CNCS 2012) IPCSIT. Vol. 35. 2012, pp. 11-15.

[24] Sunil Ghildiyal, Amit Kumar Mishra, Ashish Gupta, Neha Garg, "Analysis of Denial of Service (DoS) Attacks in Wireless Sensor Networks" IJRET: International Journal of Research in Engineering and Technology; eISSN: 2319-1163 | pISSN: 2321-7308

[25] Al-Sakib Khan Pathan, "Denial of Service in Wireless Sensor Networks: Issues and Challenges", Advances in Communications and Media Research, Vol. 6 (Edited by Anthony V. Stavros), ISBN: 978-1-60876-576-8, Nova Science Publishers, Inc., USA, 2010.

[26] Mukrimah Nawir , Amiza Amir , Naimah Yaakob , Ong Bi Lynn, "Internet of Things (IoT): Taxonomy of Security Attacks", 2016 3rd International Conference on Electronic Design (ICED), August 11-12, 2016, Phuket, Thailand.

[27] Mirza Abdur Razzaq, Muhammad Ali Qureshi, Sajid Habib Gill, Saleem Ullah, "Security Issues in the Internet of Things (IoT): AComprehensive Study", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017, pp 383-389

[28] Ning, H. Liu, and L. T. Yang, "Cyberentity security in the internet of things," Computer, vol. 46, no. 4, pp. 46–53, 2013.

[29] Christof paar,ndre weimerskirch,"embedded security in a pervasive world", information security technical report,2007- Elsevier, volume 12,issue 3, 2007,pages 155-161.

[30] Matthew eby, jan Werner,gabor karsai, akos ledeczi,"embedded systems security co-design", april 2007, SIGBED Review,volume4 issue 2, publisher: ACM

[31] Stankovic, J.A.: Research Directions for the Internet of Things. IEEE Internet of Things Journal. 1, 3-9 (2014)

[32] Internet of things Top Ten, https://www.owasp.org/images/7/71/Internet_of_Things_ Top_Ten_2014-OWASP.pdf

[33] Granjal, J., Monterio, E., Silva, J. S.: Security for the internet of things: A survey of existing protocols and open research issues. IEEE Commun. Surv. Tutorials. 17, 1294-1312 (2015)

[34] European Union Agency for Network and Information Security.: Major DDoS attacks involving IoT devices. (2016)

[35] Sonar, K., Upadhyay, H.: A Survey: DDoS Attack on Internet of Things. Int. J. Engg. Research and Development. 10,58-63. (2014)

[36] Qi Jing,Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, Dechao Qiu, "Security of the Internet of Things: perspectives and challenges", wireless networks (2014) published:springer

[37] Otmane El Mouaatamid, Mohammed Lahmer, Mostafa Belkasmi "Internet of Things Security: Layered classification of attacks and possible Countermeasures" e-TI – Numéro 9 – 2016 – http://www.revue-eti.net – ISSN 1114-8802