ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 6, PP 34-39

A Review on Internet of Things

Ashmita Shetty1, Varsha Salunkhe2, Komal Gothwal3, Dimple Bafna4
1(Assistant Professor, Information Technology, Atharva College of Engineering, Mumbai University , India)
2(Assistant Professor, Information Technology, Atharva College of Engineering, Mumbai University , India)
3(Assistant Professor, Information Technology, Atharva College of Engineering, Mumbai University , India)
4(Assistant Professor, Information Technology, Atharva College of Engineering, Mumbai University , India)

Abstract: *Internet, a progressive creation, is continually changing into some new sort of equipment and software making it unavoidable for anybody. The type of correspondence that we see now is either human-human or human-gadget, however the Internet of Things (IoT) guarantees an awesome future for the internet where the kind of communication is machine-machine (M2M).Internet of Things (IoT), which will make a tremendous system of billions or trillions of "Things" imparting with each other, are confronting numerous security issues.*

Keywords: *Internet of Things (IOT), Privacy, Security*

I. Introduction

Internet of Things (IoT) has pulled in extensive consideration amid the previous couple of years. The idea of IoT was initially proposed by Kevin Ashton in 1999. Because of quick advancements in mobile communication, Wireless Sensor Networks (WSN), Radio Frequency IDentification (RFID), and cloud computing, communications among IoT gadgets has progressed toward becoming more helpful than it was previously. IoT gadgets are proficient of co-working with each other. The World of IoT incorporates a gigantic assortment of gadgets that incorporate advanced mobile phones, individual PCs, PDAs, PCs, tablets, and other hand-held embed relations with gadgets. The IoT gadgets depend on financially savvy sensors and wireless communication systems to impart with each other and exchange important information to the concentrated system. The information from IoT gadgets is further prepared in the brought together system and conveyed to the expected goals. With the quick development of communication and internet innovation, our every day schedules are more concentrated on an anecdotal space of virtual world [1]. Individuals can work, shop, talk (keep pets and plants in the virtual world given by the system), though people live in the genuine world. Therefore, it is exceptionally hard to supplant all the human exercises with the completely robotized living. There is a bouncing farthest point of anecdotal space that confines the future improvement of internet for better administrations. The IoT has effectively integrated the anecdotal space and this present reality on the same stage. The real focuses of IoT are the arrangement of a savvy environment and hesitant autonomous gadgets for example, brilliant living, shrewd things, keen wellbeing, and savy urban communities among others [2]. Nowadays the adoption rate of the IoT gadgets is high, an ever increasing number of gadgets are associated through the internet. As indicated by examination [3], there are 30 billion associated things with rough 200 billion associations that will create income of around 700 billion euros by the year 2020. Presently in China, there are nine billion gadgets that are anticipated that would achieve 24 billion by the year 2020. In future, the IoT will totally change our living styles and plans of action. It will allow individuals and gadgets to convey whenever, wherever, with any gadget under perfect conditions utilizing any organize and any administration [4]. The principle objective of IoT is to make prevalent world for people in future. Fig. 1 demonstrates the idea of IoT with their abilities. Shockingly, the larger part of these gadgets and applications are not intended to handle the security and protection assaults and it expands a considerable measure of security and protection issues in the IoT networks, for example, privacy, authentication, information respectability, get to control, mystery, and so forth [5].

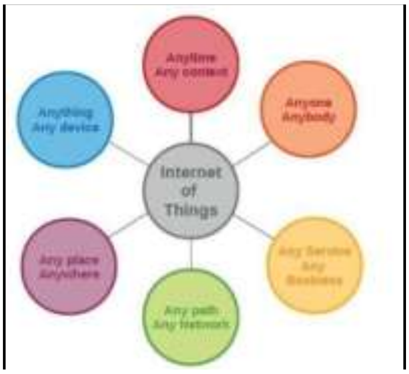

Fig 1. IoT

II. Iot Application

The main objectives of IoT are the configuration of a smart environment and self-conscious independent devices such as smart living, smart items, smart health, and smart cities among others [2]. The applications of IoT in industries, medical field, and in home automation are discussed in the following section.

2.1. IoT in Industries

The IoT has provided a fair opportunity to build significant industrial systems and applications [1], in an intelligent IoT transportation system, the authorized person can monitor the existing location and movement of a vehicle. The authorized person can also predict its future location and road traffic. In earlier stage, the term IoT was used to identify unique objects with RFID. Latterly, the researchers relate the term IoT with sensors, Global Positioning System (GPS) devices, mobile devices, and actuators. The acceptance and services of new IoT technologies mainly depend upon the privacy of data and security of information. The IoT permits many things to be connected, tracked and monitored so meaningful information and private data collected automatically. In IoT environment, the privacy protection is more critical issue as compared to traditional networks because numbers of attacks on IoT are very high.

2.2. IoT in Personal Medical Devices

The IoT devices are also widely used in healthcare systems for monitoring and assessment of patients [3]. To monitor the medical condition of a patient, Personal Medical Devices (PMDs) are either planted in patient's body or it may attach to patients body externally. PMDs are small electronic devices that are becoming very common and popular. The market value of these devices is projected to be around 17 billion dollars by 2019 [5]. These devices use a wireless interface to perform communication with a base station that is further used to read status of the gadget, medical reports, and change parameters of the gadget, or refresh status on the gadget. Wireless interface causes a considerable measure of security and protection dangers for the patient. The wireless interface of such devices is anything but difficult to digital assaults that may endanger the patients security, protection, and wellbeing. For the situation of medicinal services, the essential objective is to guarantee the security of system keeping in mind the end goal to keep the protection of patient from vindictive assaults. At the point when assailants assault mobile devices, they have their predefined objectives. For the most part, their point is to take the information, assault on devices to use their assets, or may close down a few applications that are monitoring patients condition. There are numerous sorts of assaults on medical devices that include eavesdropping in which protection of the patient is spilled, integrity blunder in which the message is being modified, and accessibility issues which include battery draining assaults. A few digital security dangers identified with security, protection, and wellbeing of medical information of patient are talked about as takes after:

1. PMDs are basic to any errand that utilizations battery control. Subsequently these devices must help a constrained encryption. In the event that the gadget is a piece of various networks then classification, accessibility, security, and integrity will be at high hazard.
2. As PMDs have no authentication component for wireless communication. So the information put away in the gadget might be effortlessly gotten to by unapproved people.
3. Absence of secure authentication additionally reveals the devices to numerous other security dangers that may leads to malevolent assaults. A threatening may dispatch Denial of Administration (DoS) assaults.
4. The information of patient is sent over transmission medium which might be adjusted by unapproved parties, as a result security of a patient may misfortune.

2.3. IoT in Smart Homes

The IoT smart home services are increasing step by step [5], advanced gadgets can adequately speak with each other using Internet Protocol (IP) addresses. All smart home gadgets are associated with the internet in a smart home environment. As the number of gadgets increases in the smart home environment, the odds of malevolent assaults likewise increase. In the event that smart home gadgets are operated independently the odds of malevolent assaults likewise decreases. Presently smart home gadgets can be gotten to through the internet everywhere whenever. Along these lines, it increases the odds of malignant assaults on these gadgets. A smart home comprises of four parts: service platform, smart gadgets, home passage, and home network as appeared in Fig. 2. In the smart home, numerous gadgets are associated furthermore, smartly shares information using a home network. Consequently, there exists a home door that controls the stream of information among smart gadgets associated with the external network. Service platform utilizes the services of service provider that deliver different services to the home network.

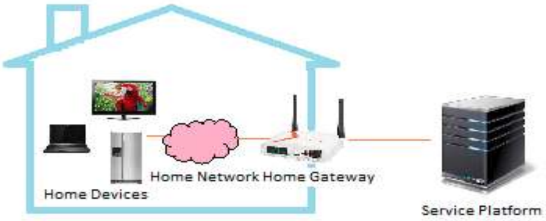

Fig 2. Elements of a smart home in IoTs.

III. Security Requirements

In IoT, every one of the gadgets and individuals are associated with each other to provide services whenever and at wherever. Most of the gadgets associated with the internet are not outfitted with productive security systems and are vulnerable to various privacy and security issues e.g., classification, integrity, and credibility, and so forth. For the IoT, some security requirements must be satisfied to prevent the network from noxious attacks. Here, probably the most required capacities of a secure network are briefly examined.

- **Resilience to attacks:** The framework ought to be skilled enough to recover itself on the off chance that on the off chance that it crashes during data transmission. For an illustration, a server working in a multiuser environment, it must be intelligent and sufficiently strong to protect itself from intruders or an eavesdropper. For the situation, in the event that it is down it would recover itself without intimation the users of its down status.
- **Data Authentication:** The data and the related information must be confirmed. An authentication instrument is utilized to permit data transmission from just bonafide gadgets.
- **Access control:** Only authorized persons are provided access control. The framework administrator must control access to the users by managing their usernames and passwords and by defining their access rights so that different users can access just relevant portion of the database or programs.Threats in smart home in IoTs.
- **Client privacy:** The data and information ought to be in safe hands. Personal data should just be accessed by authorized person to maintain the client privacy. It implies that no irrelevant verified user from the framework or some other sort of client can't approach to the private information of the client.

IV. Security Challenges With Iot Application

4.1. Devices Lack Fundamental Security Features

In a recent survey issued by PwC, it is said that around 70% of associated IoT devices lack fundamental security safeguards. The lack of inherent security features makes the IoT arrangements vulnerable to a variety of emerging and targeted security attacks. However, IoT application advancement and usage is still in an incipient stage. Every enterprise must form custom IoT arrangements with robust security features to execute and utilize them securely.

4.2. Specially Designed Malware

Some cyber criminals have already started creating and distributing malware by targeting both small and large IoT arrangements. Symantec, the security software firm, has in a recent report expressed that its researchers have discovered another, malignant "worm" that is spreading on the Internet. This has been adjusted to assault installed devices running the Linux operating system, including numerous devices that are part of the Internet of Things". The rapidly growing popularity and appropriation rate of IoT will encourage more and more cyber criminals to engineer malware by targeting IoT devices, applications, and arrangement environments. The developers must explore approaches to eliminate the escape clauses that will make the IoT arrangement vulnerable to targeted malware attacks. Similarly, the enterprises must monitor the security of infrastructure, network and devices. This will keep the IoT application useful in spite of targeted malware attacks.

4.3. Need to Keep All Components of IoT System Secure

To keep the IoT application secure over a period of time, the enterprise need to center around the security of its key components including implanted software, communication channels, data stored inside and various devices. Likewise, it need to ensure that the tools utilized for data aggregation and data centers utilized for sensor data examination must not be vulnerable to security attacks.

Subsequently, an enterprise needs to execute a variety of system level authentication and authorization while deploying the IoT application. Additionally, it needs to execute the most recent protocol to keep the data secure, and install firewall to keep the network secure. Subsequently, an enterprise needs to execute a custom security strategy by focusing on all parts of each IoT application.

4.4. Variations in Quality of IoT Devices

Numerous organizations will offer full stack IoT services to deliver faster and top notch service to customers. In any case, the quality of IoT devices utilized by individual customers differs. A few customers utilize costly IoT devices designed with powerful sensor and processors, whereas others utilize inexpensive or expendable IoT devices. The cyber criminals may utilize the expendable IoT devices as a tool to access and assault enterprise IoT applications.

The cyber criminals can even execute targeted malware attacks. These can occur through smart washing machines, air-conditioners, refrigerators, heating devices and other ordinarily utilized accessories associated with the internet. Henceforth, the enterprise users need to evaluate both quality and security of IoT devices utilized by customers. Additionally, they should utilize secure protocols and sweep the data received from the customers' devices. This would help them to protect the IoT application from targeted malware attacks.

4.5. Keeping Communication between Device and Server Secure

A number of studies have featured that the concerns related to data privacy will influence the selection rate of IoT arrangements. Both individual and enterprise users will look of IoT applications that gather, store, break down and trade data proficiently without compromising privacy and security. While building IoT arrangements, the developers must eliminate the data privacy issues by adopting end-to-end encryption and implementing token- based authentication.

However, a number of studies have featured the vulnerability of data traded between the IoT device and server. At the point when communications between the IoT device and server isn't encrypted completely, it turns out to be simple for the cyber criminals to send malevolent information/commands to the IoT application. By doing so they can access the data stored in the server. Henceforth, enterprises make utilization of the most exceptional encryption procedures to ensure that the all communication between the devices and server is encrypted.

Table 1. A Summary Of Different Types Of Attacks And Their Threat Levels Their Nature And Suggested Solutions

Type	Threat Level	Behaviour	Suggested Solution
Passive	Low	Usually breach data confidentiality. Examples are passive eavesdropping and traffic analysis. Hostile silently listen the communication for his own benefits without altering the data	Ensure confidentiality of data and do not allow an attacker to fetch information using symmetric encryption techniques.
Man in the middle	Low to Medium	Alteration and eavesdropping are the examples of this attack.An eavesdropper can silently sense the transmission medium and can modify the data if encryption is not applied and steal the information that is being transmitted. Hostile may also manipulate the data.	Apply data confidentiality and proper integration on data to ensure integrity. Encryption can be also applied so that no one can steal the information or modify the information or encode the information before transmission.
Eavesdropping	Low to Medium	The information content may be lost by an eavesdropper that silently senses the medium. For example in medical environment, privacy of a patient may be	Apply encryption on all the devices that perform communication.

		leaked.	
Gathering	Medium to High	Occurs when data is gathered from different wireless or wired medium. Examples are skimming, tampering and eavesdropping. Data is being collected to detect messages. Messages may also be altered.	Encryption can be applied to prevent this kind of attack. Identity based method and message authentication code can also be applied in order to prevent the network from such malicious attacks
Active	High	Effects confidentiality and integrity of data. Hostile can alter the integrity of messages, block messages, or may reroute the messages. It could be an internal attacker.	Ensure both confidentiality and integrity of data. To maintain data confidentiality, symmetric encryption can be applied. An authentication mechanism may be applied to allow data access to only authorized person.
Imitation	High	It impersonate for an unauthorized access. Spoofing and cloning are the examples of this attack. In spoofing attack a malicious node impersonate any other device and launch attacks to steal data or to spread malware. Cloning can rewrite or duplicate data	To avoid from spoofing and cloning attacks, apply identity based authentication protocols. Physically unclonable function is a countermeasure for cloning attack.
Privacy	High	Sensitive information of an individual or group may be disclosed. Such attacks may be correlated to gathering attack or may cause an imitation attack that can further lead to exposure of privacy.	Apply anonymous data transmission. Transmit sample data instead of actual data. Can also apply techniques like ring signature and blind signature.
Interruption	High	Affects availability of data. This makes the network unavailable.	Applying authorization, only authorized users are allowed to access specific information to perform certain operation.
Routing diversion	High	Only the route is diverted showing the huge traffic and the response time increased.	Ensure connectivity based approach so no route will be diverted.
Blocking	Extremely High	It is type of DoS, jamming, or malware attacks. It sends huge streams of data which may leads to jamming of network, similarly different types of viruses like Trojan horses, worms, and other programs can disturb the network.	Turn on the firewall, apply packet filtering, anti-jamming, active jamming, and updated antivirus programs in order to protect the network from such attacks.
`Fabrication	Extremely High	Affects the authenticity of information. Hostile can inject false data and can destroy the authenticity of information.	Data authenticity can be applied to ensure that no information is changed during the transmission of data.
DoS	Extremely High	Malicious user may modify the packets or resend a packet again and again on network. User can also send bulk messages to devices in order to disturb the normal functionalities of devices.	Apply cryptographic techniques to ensure security of network. Apply authenticity to detect the malicious user and block them permanently. In this way, the network is prevented from damage.

V. Conclusion

The main accentuation of this paper was to feature major security issues of IoT particularly, focusing the security attacks and their countermeasures. Because of lack of security component in IoT devices, numerous IoT devices turn out to be soft targets and indeed, even this isn't in the casualty's learning of being infected. In this paper, the security requirements are examined such as privacy, integrity, and authentication, and so on. In this survey, twelve different kinds of attacks are categorized as low-level attacks, medium-level attacks, abnormal state attacks, and extremely abnormal state attacks alongside their nature/behavior and additionally recommended answers for encounter these attacks are examined. Considering the importance of security in IoT applications, it is really important to install security system in IoT devices and communication networks. Moreover, to protect from any intruders or security threat, it is likewise recommended not to utilize default passwords for the devices and read the security requirements for the devices before using it for the first time. Disabling the features that are not utilized may decrease the odds of security attacks. Moreover, it is important to ponder different security protocols utilized as a part of IoT devices and networks.

References

[1] J. S. Kumar and D. R. Patel, “A survey on internet of things: Security and privacy issues,” International Journal of Computer Applications, vol. 90, no. 11, 2014.

[2] M. Abomhara and G. M. Køien, “Security and privacy in the internet of things: Current status and open issues,” in Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE, 2014, pp. 1–8.

[3] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct 2010.

[4] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, “A vision of iot: Applications, challenges, and opportunities with china perspective,” IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014.

[5] M. Abdur Razzaq, R. A. Sheikh, A. Baig, and A. Ahmad, “Digital image security: Fusion of encryption, steganography and watermarking,” International Journal of Advanced Computer Science and Applications (IJACSA), vol. 8, no. 5, 2017.