Survey on Iot Security Issues And Solutions

Sangeeta Kol[1], Prof. Deepak Paranjpe[2]
[1]Dept of CSE
[2]Assistant Professor, Dept of CSE
[1, 2] Global Nature Care Sangathan Group of Institution, Jabalpur, Madhya Pradesh, India.

Abstract- *Internet of things (IOT) is a rising wireless technology that connects different things to the internet. Things can be "anything" that is around us. 'Over 50 billion one-of-a-kind gadgets can be related to the IoT through 2020 'said through Cisco. Contemporary security technologies are very constrained as they may be unable to fulfil safety requirements of IoT devices. As Cisco said, in coming years the growth of IoT can be progressive but at the equal time we need to offer a strong provision for security of user's data.*
In this paper, we can consciousness on specific vulnerabilities to the security of IoT devices and provide possible solution to them.

Keywords- WSN, RFID, IoT Architecture, protocol, Security, Privacy.

I. INTRODUCTION

The internet of things is simply an interconnection of various devices which might be merged in everyday items, allows them to do communication through the internet, said by means of the Oxford Dictionaries.' The idea of the internet of Things is first of all noted by Mr. Kevin Ashton, co-founder and executive director of the auto-ID center at MIT, in his presentation which is made to Procter & Gamble in 1999. [1]
The Artificial intelligence took the arena to a sure area in which the devices can talk with each other as a human does. This capability of devices delivers the development of "Internet of Things" (IoT) [2].The Internet of Things (IoT) has strong connectivity from "anyplace" to "anyone" at "anytime" for "anything" [3]. even though IoT has a greater future in coming years however security of information will be at utmost The Things in IoT, may be easily accessible to the crackers so that they will easily exploit the security of the objects. [4]

1.1 INTERNET OF THINGS

The architecture of IoT can be divided into three layers: Perception Layer, Network Layer and Application Layer as shown in Fig. 1.1. The figure shows the layered architecture of IoT, where each layer plays a very important role. Also, it shows the technologies and protocols they use to do their assigned work. The capability to implant the mobile networking and information processing functionality into today widest used computing devices transformed the world of IoT to new dimensions which use information and communication technology. [3] The main purpose of Internet of Things (IoT) is to enhance excellent of life, however, the interconnection among people and things and sensitive and critical data related to them can be eavesdropped by any individual via the internet. [2] [3] due to that so many issues have raised related to verification and access control [5].as a consequence, IoT is giving a brand new way of communication between humans, things and among things themselves. [6] The Internet of Things will rework the destiny of the internet and will make human life smooth such way that the things around us will interact with every other wirelessly and will manipulate and co-ordinate their assignment without our intervention. Now a day, those clever objects are targeted by some evil minded hacker which compromises the security of these devices subsequently IoT has the capacity to distribute these risks a long way more broadly than the internet has so far.

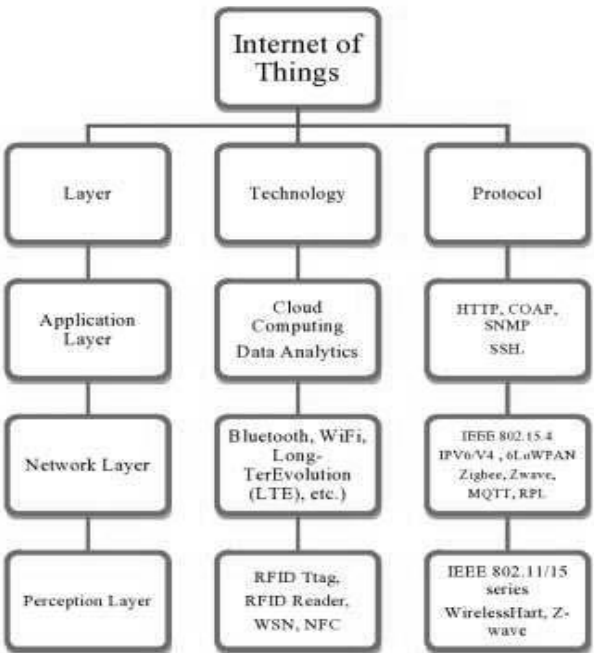

Fig. 1.1: IoT Architecture.

1.2 SECURITY CHALLENGES AND ISSUES

IoT has gained a lot of achievements in the research field from last few years but there are still some bids that need to be addressed for the presence of this technology. In this section, some of the threats in each architectural layer that needs special attention are discussed.

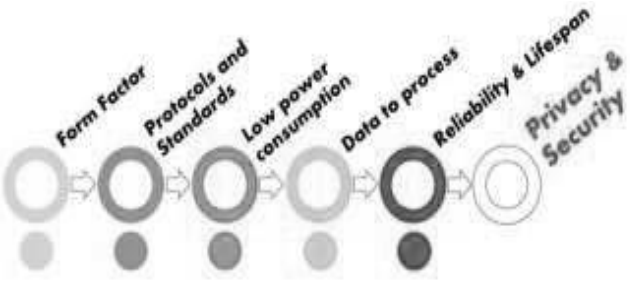

Fig1.3: Challenges for IoT.

Internet of Things safety issues is mainly manifested in the Following points:

- The very first step to secure IoT data is to provide physical security which includes sensor security; sensor interference and the signal intercepted by the sensor and it symbolizes the safety characteristic of IoT.
- The second is to maintain the operation of the various elements such as sensor operation, transmission systems and treatment systems to be safe. Related with traditional information systems security.
- The third is the information security additionally, exist in numerous factors, and it needs the data inside the sensor, the transmission system and the processing devices will no longer be stolen, tempered solid repudiation.

If those problems aren't handled nicely within the IoT, the country's monetary and security could be threatened. Therefore, it's far vital to in-intensity look at safety troubles that may be encountered within the utility of factors, to layout and enhances its security problems countermeasures. [5]

1.3 Perception Layer Challenges

1.3.1 Unauthorized Access to Tags:

Due to the lack of right authentication mechanism in a large variety of RFID systems, tags may be accessed through a person without authorization. The attacker can't simply examine the data but records can be changed or deleted additionally. [7]

1.3.2 Node Capture Attacks

In a node Capture attack, the adversary can seize and manage the node or tool in IoT by physically replacing the entire node, or tampering with the hardware of the node or device. This attack can also be known as node replication attack. It can incur a serious impact on the network. [8]

1.3.3 Tag Cloning:

Because tags are deployed on different objects which might be seen and their information may be examined and changed with a few hacking techniques. Consequently, they may be without difficulty captured by any cybercriminal who can create a reproduction of the tag and subsequently be compromising it in a manner that the reader cannot distinguish between the original and the compromised tag [7].

1.3.4 False Data Injection Attacks

With the captured node or device in IoT, the adversary can inject fake facts in the vicinity of regular facts measured by the captured node or tool, and transmit the false facts to IoT applications. After receiving the fake information, IoT applications can go back erroneous remarks instructions or offer incorrect offerings, which similarly influence the effectiveness of IoT applications and networks. [8]

1.4 Network Layer Challenges

As the main purpose of the network layer in IoT is to transmit accumulated data, the safety challenges in this layer focus on the effect of the availability of network resources. Network layer consists of the Wireless sensor network (WSN) which transmits the data from the sensor to its destination with reliability. [8]

The associated security problems are mentioned under:

1.4.1 Spoofing Attack:

The reason for spoofing attacks is for the adversary to benefit complete get right of entry to the IoT system, and send malicious records into the system. [9]. In IoT, examples of spoofing attacks include IP spoofing [24], RFID spoofing [10]. In an RFID spoofing attack, the adversary can spoof and record the facts of a valid RFID tag, and then send malicious information with this legitimate tag identification to the IoT system. [10]

1.4.2 Sinkhole Attack:

It is a type of attack in which the adversary makes the compromised node look attractive to the nearby nodes because of which all the data drift from any particular node is diverted closer to the compromised node resulting in packets drop i.e. all of the traffic is silenced while the machine is fooled to consider that the data has been obtained on the alternative facet. Furthermore, this attack results in extra energy consumption that may cause DoS attack [7].

1.4.3 Sleep Deprivation Attack:

The sensor nodes inside the Wi-Fi Sensor network are powered via way of batteries with not so longer proper lifetime. So the nodes are sure to comply with the sleep routines to boom their lifetime. Sleep Deprivation is the shape of attack which continues the nodes wakeful, resulting in extra battery intake and as a stop end result battery lifetime is minimized which reasons the nodes to close down. [11]

1.4.4 Denial of Service (DoS) Attack:

It is the form of attack in which the network is flooded with a vain lot of traffic with the aid of an attacker, ensuing in a useful resource exhaustion of the targeted system because of which the network will become unavailable to the customers. [12] Accordingly, DoS attack may be generated through attack schemes, including Ping of death, Tear Drop, UDP flood, SYN flood, Land attack, and so forth. To protect in opposition to DoS attacks, attacking schemes want to be carefully investigated first, and then the green protecting schemes to mitigate attacks need be developed to secure IoT systems.

1.4.5 Unsecured Protocols:

The protocols presently working at the physical level of interactive devices consist of proprietary non-IP solutions inclusive of Bluetooth, IR, ZigBee, Z-wave, and so on. These protocols work flawlessly best at small scale and within a restrained geographical place. Given that IoT intends to connect the things at a huge scale and covering a large location, by using IP based solutions, as a result, IoT poses a chance of revealing regular things to the world of internet and permitting them to interconnect with any other speaking node.

1.5 Application Layer Challenges

The primary reason of the Application layer is to help offerings requested by customers. For this reason, challenges within the application layer consciousness on the software attack. Right here, several viable challenges inside the application layer of IoT are supplied below. [8]

1.5.1 Phishing Attack:

In a phishing attack, the adversary can reap the private information of users, such as identity and passwords, by means of spoofing the authentication credentials of users via the inflamed e-mails and phishing websites [13].

1.5.2 Malicious Virus/worm:

A malicious virus/worm is a few other undertakings to IoT applications [13].The adversary can infect the IoT application with malicious self-propagation attacks (worms, malicious program, and so on.), after which achieve or tamper with private data.

1.5.3 Sniffing Attack:

An attacker can force an attack on the machine by introducing a sniffer utility into the device, which can benefit network facts resulting in corruption of the system.

1.5.4 Malicious Scripts:

Malicious scripts constitute the scripts which can be introduced to the software, modified in a software program, and deleted from software program with the motive of harming the device capabilities of IoT [13].

II. SECURITY AT DIFFERENT LAYERS

2.1 Perception Layer

- At first node authentication is important to save you unlawful node get right of entry to; Authentication is achieved through Cryptographic Hash Algorithms which offers digital signatures to the terminals that would withstand all of the viable recognized attacks like side-channel attack, Brute force attack and Collision attack.[14]
- Privateness of the information is guaranteed with the aid of symmetric and asymmetric encryption algorithms including RSA, DSA, BLOWFISH and DES and so forth. This prevents an unauthorized get entry to the sensor data while being accrued or forwarded to the following layer. Due to their low energy consumption benefit, they may be without problems achieved by the sensors. [14]
- As for hiding the sensitive information, the anonymity of the region and identity is received using the k-Anonymity technique which ensures the protection of the information like identification and place and many others of the user.[6]

- Physical strategies or code mechanisms or a mixture of each the strategies are used for supplying the RFID safety. Data encryptions, blocker tag, tag frequency modification, jamming, kill order policy, and so on. Are the commonly used physical strategies while the code mechanisms encompass the format of protocols for RFID node safety? Hash Lock protocol, LCAP, Hash Chain and re-encryption protocol are the RFID safety protocols. Strategies like key distribution policies, intrusion detection mechanisms, relaxed routing protocols, and so forth. Also, are employed to acquire the protection. [6]

2.2 Network Layer

The network layer which might be both wired or wireless is exposed to numerous kinds of attacks. Due to the openness of the wireless channels, communications may be monitored effortlessly by a few hackers. [7]

- With the assist of a proper authentication process and point to point encryption, illegal entry to the sensor nodes to unfold fake data could be avoided [7].
- After the Authentication process, routing algorithms are applied to make sure the privateness of data exchange among the sensor nodes and the processing systems. The safety of routing is ensured by using imparting more than one path for the data routing which improves the potential of the system to stumble on a mistake and keep performing upon any sort of failure inside the system. [7]
- IPV6 over Low power wireless personal area networks(6LoWPAN), Routing Over Low-power and Lossy Networks (RPL), Datagram transport Layer security (DTLS), Constrained Application Protocol (COAP) have surfaced as authorized lightweight variants to IPV6, IP routing protocol, TLS and HTTP respectively. With the creation of IP equivalent protocols for the IoT, the IoT devices are in a position to communicate with distinct net devices each with their network and past that with lesser safety threats.
- MQTT is the more preferred IoT protocol above the transport tier. It is simple and rapid with low code footprint. MQTT comes with its very own set of security features. But, these measures nevertheless leave the network vulnerable. So the trend in securing the transport layer is to at ease the MQTT protocol with Secure Socket Level (SSL) certification.

2.3 Middleware and Application Layer

This layer integrates the Middle-ware and Application layer to shape a blanketed security mechanism. The security categorization is stated underneath: [7]

- Symmetric key cryptosystem, public key cryptosystem and certification transfer technology are used to gain authentication and key settlement inside the heterogeneous network. Fingerprint technology, digital watermarking, anonymous authentication, threshold cryptography, and so on are used to obtain the security of private data.
- Data security is ensured via diverse encryption technology which saves from data-stealing threats. Furthermore, to prevent other malicious activities from the miscreant customers, Anti-Dos firewalls and updated spyware and malware are introduced.
- Intrusion detection techniques offer answers for diverse security threats by generating an alarm at the prevalence of any suspicious activity in the system due to the continuous monitoring and preserving a log of the intruder's activities that may help to trace the intruder. There are unique current intrusion detection strategies which include the information mining method and anomaly detection.
- In IoT surroundings, middleware may be used as a platform that supports interoperability, and it may provide safety for devices and information. Consequently, even as we layout middleware structure, protection, privacy, and use of multi-communication medium have to be taken into consideration.
- The essential security services in IoT are confidentiality, Data integrity, source integrity or authentication, availability and replay safety. Encryption/decryption strategies assist in achieving confidentiality. Data integrity is executed through message integrity codes (MIC). Availability is ensured through the use of IDS and firewalls. Integrity protected timestamps, sequence numbers, nonces, and so on are used for replay protection.
- IoT systems are incorporating biometric authentication method to enhance the security measures. some of the newer bio-authentication method includes facial scan and eye scan like Smartphone, IoT devices may even put in force fingerprint sensor, so that handiest a certified person might be able to get entry to the IoT device.

III. CONCLUSION

In spite of the fact that IoT is one of the strength eras which is utilized in each region from domestic Automation to

a protracted manner-flung hospital manage and from clever town to industrial enterprise Plant. As we apprehend each coin has sides. Further, IoT has such masses of merits in addition to demerits too. i.e. Security and Privacy.

REFERENCE

[1] http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things.

[2] Surapan Krajik and Panwit Tuwanut," A survey on internet of things architecture, protocols, possible application, security, privacy, real-world implementations and future trends", proceedings f ICCT, 2015,pg 26 to 31.

[3] Rolf H.Weber, "Internet of Things - New security and privacy challenges," in Computer Law and Security Review (CLSR),2010, pp.23-30

[4] Rodrigo Roman, Pablo Najera and Javier Lopez, "Securing the Internet of Things," in IEEE Computer, Volume 44, Number 9, 2011, pp. 51-58

[5] Chen Qiang , Guang-ri Quan , Bai Yu and Liu Yang, "Research on Security Issues of the Internet of Things", International Journal of Future Generation Communication and Networking, Vol.6, No.6 , pp.1-10, 2013.

[6] Mike Burmester and Breno de Medeiros, "RFID Security: Attacks, Countermeasures and Challenges."

[7] M.U. Farooq, Muhammad Waseem, Anjum Khairi, Sadia Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)", International Journal of Computer Applications (0975 8887) Volume 111 - No. 7, February 2015.

[8] Jie Lin, Wei Yu, Nan Zang, Xinyu Yang, Hanlin Zhang, Wei Zhao, " A survey on Internet of Things: Architecture, Enabling Technologies, security and Privacy, and Applications", IEEE Internet of Things Journal.

[9] Aikaterini Mitrokotsa, Melanie R. Rieback and Andrew S.Tanenbaum, "Classification of RFID Attacks."

[10] Nadeem AHmed, Salil S. Kanhere and Sanjay Jha, "The Holes Problem in Wireless Sensor Network: A Survey," in Mobile Computing and Communications Review, Volume 1,Number 2

[11] I. Andrea, C. Chrysostomou, and G. Hadjichristofi. Internet of things: Security vulnerabilities and challenges. In Proc. of 2015 IEEE Symposium on Computers and Communication (ISCC), July 2015.

[12] A. Mukaddam, I. Elhajj, A. Kayssi, and A. Chehab. Ip spoofing detection using modified hop count. In Proc. of 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, May 2014.

[13] X. Wang, W. Yu, A. Champion, X. Fu, and D. Xuan. Detecting worms via mining dynamic program execution. In Proc. of Third International Conference on Security and Privacy in Communications Networks, 2007.

[14] Yassine MALEH and Abdellah Ezzati, "A Review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks," in International Journal of Wireless & Mobile Networks (IJWMN),Volume 5, Number 6, 2013