Study of Security Challenges in Multilayered Structure and Various Attacks on IOT

Ms. Shilpa B. Sarvaiya Dr.Swati S.Sherekar Dr.V.M.Thakare

Abstract- **Internet of Things (IoT) is one of the most buzzing and discussed topic in research field today. Some of the researchers are also looking future of the world in this technology. Since then significant research and development have taken place on IoT, however various vulnerabilities are observed which shall keep IoT as a technology in danger. Internet of Things (IoT) has been a massive Advancement in the Information and Communication Technology (ICT) .It is projected that over 50 billion devices will become part of the IoT in the next few years. Security of the IoT network should be the fore most priority. In this paper, we evaluate the security challenges in the six layers of the IoT architecture. IoT has no uniform architecture and there are different kinds of attacks on the different layers of IOT such as unauthorized access to tags the malicious node injection attack, sinkhole attack, worm attack and side-channel attack. IoT devices are more vulnerable to attacks because it is simple and some security measure cannot be implemented furthermore, important security technologies like encryption are also analysed in the IoT context. Finally, as per the need of our conveniences the present study discusses about various security attacks on different layers of IoT, classify them and finding the most prominent attacks in IoT and highlight the future research directions within the IoT architecture and help to promote the development of IoT.**

***Keywords*- Internet of Things (IOT), layers architecture, Security, IOT Attacks**

I. INTRODUCTION

With the recent advancement in technology a potential innovation, Internet of Things is coming down the road which is growing as a global computing network where everyone and everything will be connected to the Internet [1]. Internet of Things is growing rapidly and the possibilities it can form are infinites. The number of machines requires internet services are increasing every day. The concept of allowing interaction between intelligent devices is a recent technology but the technologies composing the Internet of Things are goes back [2]. Internet of Thing is the approach of gaining data from different devices operated on different platform, and uniting them on any virtual platform existing [3].Internet of things ages back to 1982 when a modified coke machine was connected to the Internet. It has an ability to report the numbers of drinks contained within and that whether the drinks were cold or not [4]. In 1999, Bill Joy passed information about machine to machine communication [5]. In 1999, Kevin Ashton suggested the term "Internet of Things" to describe a communication between IoT comprises of a network of highly diverse digital objects interacted with each other and with humans too. It provides a sensor network with communication system, store and manage the information, provides access and also handles the privacy protection and data security problems [3]. Comparing the research aspects on security in IoT to security in Internet, former is the way complex than the later and therefore needs the significant attention of the researcher and a more precise research methodology and tools should been devices with the help of the internet [6].

II. Architecture of Internet of Things

More than 25,000,000,000 devices are expected to be interconnected by 2020 [9] which is a very large number so the current architecture of Internet with TCP/IP protocols, cannot manage a network as big as Internet of Things, hence to support that huge IoT network we need a new architecture that has an ability to handle various Quality of Service (QoS) and security issues in addition it has also capability of handling an existing network application. Without addressing suitable privacy promise, Internet of Things is not expected to be approved by many. Therefore security of data and isolation of users are crucial challenges for Internet of Things for advance growth of Internet of Things, a number of "*multilayered security architectures*" are proposed. Wang Chen has proposed a 3 level architecture of Internet of Things while Hui Suo proposed a 4 level architecture. Miao Wu has proposed a 5 layered architecture using Internet and telecommunication management networks architectures based on TCP/IP and TMN models individually. Similarly a 6 layered architecture was also projected based on the network hierarchical structure. So basically it has six layers as shown in the figure1

.

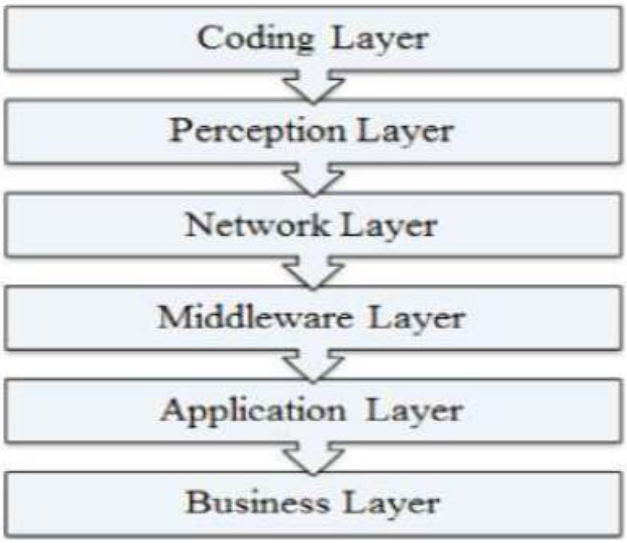

Figure-1 Six-Layered Architecture of Internet of Things

2.1 Coding Layer

Coding layer is the base of Internet of Things which gives essential identification to the devices that are part of Internet of Things. In this layer, each device is assigned with "*unique ID*" which makes it easy to distinguish the devices [2].

2.2 Perception Layer

Perception layer of Internet of Things, which provides a physical meaning to each device. It consists of data sensors in different forms which could sense the humidity, temperature, location and speed of the device. This layer collects the information of the device from the sensor connected with them and translates the information into digital signals which is then delivered onto the Network Layer for advance action.

2.3 Network Layer

The objective of Network Layer is accept the useful information in the form of digital signals from the Perception Layer and transfer it to the processing systems in the Middleware Layer through the trans-mission mediums like Bluetooth, WiFi, Zigbee, WiMaX, 3G, GSM, etc with protocols like IPv6, IPv4, DDS, MQTT, etc.

2.4 Middleware Layer

Middleware layer processes the data expected from Network Layer [2]. It contains the technologies like Ubiquitous computing, Cloud computing which provides a direct access to the database to record all the essential information in it. Using some Intelligent Processing Equipment, the information is processed and a fully automated action is taken based on the processed results of the information.

2.5 Application Layer

Application layer recognizes the applications of Internet of Things for all types of production, based on the administered data. Applications promote the advance development of Internet of Things so this layer is very useful in the huge scale development of Internet of Things network. The Internet of Things applications could be smart transportation, smart homes, smart planet etc.

2.6 Business Layer

Business Layer controls the services of Internet of Things and application and is liable for all the study related to Internet of Things. It makes different business models for different business strategies [1].

III. Different Security Attacks In IOT

In figure 1, a common IoT architecture is given. According to many researchers [4], IoT technology works on three layers perception layer, network layer and application layers as shown in Figure 1. Perception Layer involves various types of data sensors like RFID, Barcodes or any other sensor network. The aim of this layer is to obtain information from the environment by using sensors and then send it to the network layer. The aim of network layer is to transmit the data collected from the perception layer to any specific information processing system through internet, mobile network or any other kind of reliable network. The aim of the IoT of developing smart environment is accomplished at the application layer. The security of IoT is a big challenge because of complexity, heterogeneity and a large number of interconnected resources. The adversary can perform the attack on IoT system by damaging or tampering some node i.e. physical vulnerability, or from within its network by using faults in routing protocol and other network related protocol, or by using malicious program and by breaking encryption strategy i.e. encryption attack. Based on these vulnerabilities we classify the attack in four categories, as physical attack, network attack, software attack and encryption attack as shown in Figure 2. From each category, we considered one attack that is most dangerous from all the attack of that category. From physical attack, malicious node injection attack has been the dangerous attack. Since it is not only stopping the services but also modify the data. From network attack, sinkhole attack is the most risky attack. It not only attracts all the traffic towards the base station, but also the attacker can initiate other threats such as selective forwarding, altering or dropping the packets. From software attack, we select worm attack as most unsafe. Worms are probably the most destructive and dangerous form of malware on the internet. It is the self-replicating program which harms the computer by using security holes in networking software and hardware. It can delete the files in system, steals the information like passwords, they can also change the passwords without your notice, it causes the lockouts, etc.

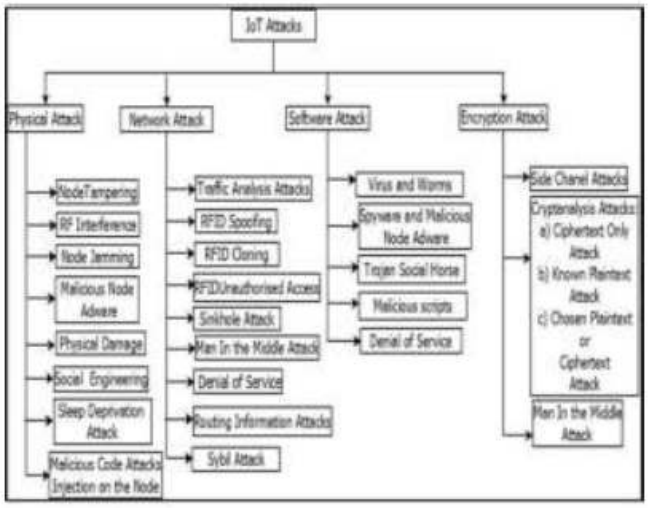

Fig. 2:IoT and its security attacks

From encryption attack, side channel attack is the most difficult to handle. It is very difficult to detect because attacker uses the side channel information to perform the attack [22].

IV. Classifications of IOT Attacks

4.1 Physical Attacks

Physical attacks are concentrated on hardware devices in the system.

4.1.1 Node Tampering: In this attack attacker physically alters the compromised node and can obtain sensitive information such as encryption key [21].

4.1.2 RF Interference on RFIDs: The attacker performs Denial of service attack by sending noise signals over radio frequency signals. These signals are used for RFID"s communication [22].

4.1.3 Node Jamming in WSNs: By using jammer the attacker can disturb the wireless communication. It causes Denial of service attack [21].

4.1.4Malicious Node Injection: In this attack, attacker physically injects a new malicious node between two or more nodes. It then modifies the data the passes the wrong Information to the other nodes. The attacker uses the multiple nodes to perform malicious node injection attack. The adversary first inserts a replica of the node B. After that, inserts other malicious nodes (node M1). Both these nodes work together to execute the attack. Thus collision is occurring at the victim node. Because of these, the attacked node cannot receive send any packet. Hence, the conclusion of watchdog nodes might be affected by incorrectly announcing the attacked node (the legitimate node) as acting maliciously. To prevent this attack, we use a monitoring verification (MOVE) scheme. It can check the monitoring node(s)" result and correctly identify any malicious behaviour. According to the acknowledgment, the verifier node will decide whether the node is malicious or not.

4.1.5 Physical Damage: The attacker physically harms components of IoT system and it results in Denial of service attack.

4.1.6 Social Engineering: The attacker physical interact and manipulates users of an IoT system. The attacker obtains sensitive information to achieve his goals.

4.1.7 Sleep Deprivation Attack: The aim of the attacker is to use more power that results in shutting down of nodes [23].

4.1.8 Malicious Code Injection: The adversary physically introduces a malicious code into the node of IoT system. The attacker can get full control of IoT system [23].

4.2 Network Attacks

These attacks are focused on the network of IoT system.

4.2.1 Traffic Analysis Attacks: The attacker intercepts and examines messages to obtain network information [21].

4.2.2 RFID Spoofing: An adversary spoofs RFID signals. Then it captures the information which is transmitted from a RFID tag. Spoofing attacks give wrong information which seems to be correct and that the system accepts [22].

4.2.3 RFID Cloning: In this attack, adversary copying data from pre-existing RFID tag to another RFID tag. It does not copy original ID of RFID tag. The attacker can insert wrong data or control the data passing via the cloned node [17].

4.2.4 RFID Unauthorized Access: If the correct authentication is not provided in the RFID systems, then the adversary can observe, alter or remove information on nodes.

4.2.5 Sinkhole Attack: In a sinkhole attack an adversary compromises a node inside the network and performs the attack by using this node. The compromised node sends the fake routing information to its neigh boring nodes that it has the minimum distance path to the base station and then attracts the traffic. It can then alter the data and also drop the packets[25].

In paper [22] gives the simple technique to identify sinkhole nodes. In proposed technique, when a node send a packet to its neigh boring node it creates the entry of hop distances and ID in its database. It then computes the average hop-count except minimum hop-count and compares average and minimum value. If this minimum value is too small as compared to the average hopcount, then it is vulnerable to sinkhole attack.

4.2.6 Man in the Middle Attacks: The attacker over the internet intercepts the communication between the two nodes. They obtain the sensitive information by eavesdropping.

4.2.7 Denial of Service: An attacker floods the network with large traffic so that services are unavailable to its intended users.

4.2.8 Routing Information Attacks: In this attack, the attacker can make the network complex by spoofing, modifying or sending routing information. It results in allowing or dropping packets, forwarding wrong data or partitioning the network.

4.2.9 Sybil Attack: In this attack, malicious node that takes the identities of multiple nodes and acts as them. For e.g. in Wireless Sensor Network, voting system single node can vote many times.

4.3 Software Attacks

The attacker performs the attack by using virus, worm, spyware, adware etc. to steal data, deny the services, etc.

4.3.1 *Phishing Attacks:* The attacker obtains the private information like username, passwords by email spoofing and by using fake websites.

4.3.2 *Virus, Worms, Trojan horse, Spyware and Aware:* An adversary can damage the system by using malicious code. These codes are spreads through email attachments, downloading files from the Internet. The worm has the ability to replicate itself without any human action. We can use worm detector, anti-virus, firewalls, intrusion detection system to detect the virus.

The paper [17] combines anomaly and signature detection with honeypot to protect the system from worms. This hybrid scheme takes the advantage of honeypot and anomaly signature detection and provides the protection against worms.

4.3.3 Malicious Scripts: By injecting malicious script the attacker can gain access to the system.

4.3.4 Denial of Service: The attacker blocks the users from the application layer by denying services[10].

4.4 Encryption Attacks

These attacks depend on destroying encryption technique and obtain the private key.

4.4.1 *Side-channel Attacks:* The attacker uses the side channel information that is emitted by encrypting devices. It is neither the plaintext nor the cipher text, it contains information about power, the time required to perform the operation, faults frequency, etc. Attacker uses this information to detect the encryption key. There are different types of side channel attack such as timing attacks, Simple and Differential Power Analysis, and Differential Fault Analysis Attacks [21]. Here, we consider timing attack. Timing attacks are dependent on the time require for executing operations. It gives the information of the secret keys. By using this information an attacker can find fixed Diffie-Hellman exponents, factor RSA keys, and break other cryptosystems [21]. Cryptosystems process different inputs in different time. Because of branching and conditional statements, RAM cache hits, processor instructions that run in non-fixed time, etc. Timing computations are providing to a statistical model. It provides the guessed key bit to a certain extent of assurance.

Cryptanalysis of a Simple Modular Exponentiation:

Diffie-Hellman and RSA operations involve calculation of R = y mod n, where n is public and y can be obtained by a listener. The adversary wants to search the secret key x. To perform the attack, the victim must calculate yx mod n for many values of y, where y, n, and the estimation time are known to the adversary and x remains the same. The needed data and timing computation might be gained by secretly listening on an interactive protocol. Hence, an adversary could see the messages received by the target and calculate the time required to respond to each y. A common method to stop timing attacks is to perform all operations in such a way that they take absolutely the same amount of time by adding delay. Sometimes this is difficult.

4.4.2 Cryptanalysis Attacks: In this attack, the adversary obtains the encryption key by using either plaintext or cipher text. Based on methodology used, there are different types of cryptanalysis attacks.

4.4.2.1Cipher text Only Attack:

In this the attacker can access the cipher text and determine the corresponding plaintext.

4.4.2.2 Known Plaintext Attack: In this method, the attacker knows the plaintext for some parts of the cipher text. The aim is to decrypt the remaining part of the cipher text utilizing this information.

4.4.2.3. Chosen Plaintext Attack:

The attacker gets to choose what plaintext is encrypted and find the encryption key.

4.4.2.4 Chosen Cipher text Attack:

By using the plaintext of chosen cipher text the attacker can find the encryption key.

4.4.2.5 *Man in the Middle Attacks:*

When two users are interchanging the key the attacker intercepts the communication and obtains the key [25].

V. Analysis of Different IOT Attacks:

Table1: Comparison of IOT Attacks[13][25]

Classifications Types/parameters	Malicious Node Injection Attacks	Sinkhole Attacks	Worm Attack	Side-channel Attack
OSI Layer	Physical[11]	Network[12]	Application[12]	Application, physical[1]
Attack Type	Active –As the attacker compromise the node[16]	Active -As it provides the wrong information those results in packet dropping [15].	Active -As it modifies the files [13].	Passive-As the attacker can find encryption key by using the side channel information [1].
Attacker Location	External, Internal	External	Both	Internal
Attack Threat	Availability -due to collision at the victim node it cannot Transmit the packet [18].	Availability, Confidentiality -As all the data is attracted to the Compromised node [5].	Availability, Integrity, Authenticity -As it can delete, modify the data	Confidentiality, Integrity-by using side channel information it can find the encryption key [1].
Damage Level	High -As it can modify the data and pass the wrong info to other nodes [15].	High -As all data is flowing through Compromised node the attacker can do anything with packet [15].	High -As it can delete files, mail Documents [14].	High-As the attacker can obtains the secret key without detecting [1].
Detection Chances	Low -As it is replica (clone) of legitimate node [18].	Difficult -To detect when it is near to base Station [25].	Anti-virus can identify it [13].	Negligible because adversary uses side channel information [19].
Possibility of Prevention	Yes - If we could avoid replication attack [21].	Yes -if node authentication is provided [14].	Yes -by avoiding suspicious sites, files [13].	Yes –By using preventive methods [19].
Attacks Based on	Inserting Malicious Node [21].	Routing [19].	Malicious Code [13].	Side-channel information[19]

Vulnerability	Wireless Nature and Hidden Node Problem [21].	Node Authentication is not provided [14].	Not following Security Policies [13].	Side-channel information[19]
Existing solutions and their limitations	Not Possible to detect if more than two nodes are malicious, Consumes power because of over hearing [21]	When Malicious Node near to The base station (1 or 2 hop distance), Algorithm cannot accurately detect sinkhole node[18]	New worms are created everyday [13]	Affect the performance of the system [20].

VI. Conclusion

IoT has been a hot research topic for the last few years and like other revolutionary technologies, it also faces many challenges, most significant of which are the security and privacy threats. In this paper, we described the working of six layers of IoT (Coding layer, Perception Layer, Network Layer, Middleware (Processing) Layer, Application Layer, and Business Layer) and then we explored the security loopholes that can be exploited in these layers. 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. Researchers have proposed different solutions on these attacks to tackle it. However implementation of all these security measures and techniques together consumes computation as well as battery power of devices which is not acceptable for IoT technology and its devices. There is a need of a security mechanism which handles maximum security. Problems but it should be light weight and robust for fit for IoT technology. Many of the attacks on IoT have been discussed and classified above. Some of these attacks can be avoided by just keeping some security precaution while the development of any application like checking node identity while communication or using devices which are difficult to tamper. However some attacks which are known,which are difficult to detect or prevent, there has been a need to find asecure and efficient solution. IoT is an extension of Internet, which brings new security challenges in multi-layered structure. The proposed IoT architectures are under various attacks on different layers, such as Physical attack, Network attack, software attack and encryption attack. There should be universal standards in architecture and security challenges. They can be helpful to promote the development and adoption of IoT .only in this way, can IoT develop better and can we achieve more benefits from the technology.

7.

References

1. Mr. Vishal Kansagara, Mr. Darshan Thoria, and Ms. Drashti Hirani „" OVERVIEW ON INTERNATE OF THINGS (IoT)" International Journal of Advance Research in Engineering, Science & Technology *e ISSN: 2393-9877, p-ISSN: 2394-2444 (Special Issue for ITECE 2016)*
2. Guicheng Shen and Bingwu Liu,"The visions, technologies, applications and security issues of Internet of Things," in *EBusiness and E-Government (ICEE), 2011* pp. 1-4
3. Ling-yuan Zeng,"A Security Framework for Internet of Things Based on 4G Communication," in *Computer Science and Network Technology (ICCSNT), 2012*, pp. 1715-1718
4. Jason Pontin,"Bill Joy"s Six Webs," *MIT Technology Review, 29 September 2005*
5. Kevin Ashton,"That "Internet of Things" Thing", *RFID Journal, 22 June 200*
6. H.D. Ma,"Internet of things: Objectives and scientific challenge," in *Journal of Computer Science and Technology, 2011*, pp. 919-924
7. QuandengGOU, Lianshan YAN, Yihe LIU and Yao LI ―Construction and Strategies in IoT Security System‖ 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing.
8. Suchitra.C1, Vandana C.P2 "International Journal of Computer Science and Mobile Computing", *IJCSMC, Vol. 5, Issue. 1 January 2016*
9. Ibrahim R.Waz,Mohamed Ali sobh,Ayman M.Bahaa-Eldin,"Internet of Things(IOT) Security Platforms" ,2017 IEEE
10. Mian Muhammad Ahemd,Munam Ali Shah,Abdul Wahid,"IOT Security: A Layered Approach For Attacks & Defenses" 2017 Internation conference on communication Technologies(Com Tech).
11. Pavan Pongle,Gurunath Chavan,"A Survey:Attacks on RPL and 6LowPAN in IOT",2015 International Conference on Pervasive Computing(ICPC).
12. Jyoti Deogirikar, Amarsinh Vidhate"Security Attacks in IoT:A Survey", International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) ISMAC 2017)
13. L. Li, "Study on security architecture in the Internet of Things," International Conference on Measurement, Information and Control (MIC), pp. 374-377, Harbin, China, 2012.
14. I. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," 2015 IEEE Symposium on Computers and Communication (ISCC), pp.180-87, Larnaca, 2015.
15. Wahid, Abdul, P. Kumar, "A Survey on attacks, Challenges and Security Mechanism In wireless Sensor Network", JIRSTInternational Journal for Research in Science & Technology, Volume 1, Issue 8, pp.189-196,January 2015.
16. S.N Uke, A.R Mahajan, R.C Thool "UML Modeling of Physical and Data Link Layer Security Attacks in WSN", International Journal of Computer Applications, Volume 70– No.11, May 2013.
17. Li, Hong, Y. Chen, and Z. He. "The

Survey of RFID Attacks and Defenses." 8th International Conference on IEEE Wireless Communications, Networking and Mobile Computing (WiCOM), 2012.

18. M.U. Farooq, M. Waseem, A. Khairi, S. 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
19. Zulkifli, M. Zaid W. Mohd, "Attack on Cryptography", (2008).
20. Md. I. Abdullah,M. M. Rahman and M. C. Roy, "Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count" I. J. Computer Network and Information Security, pp.50-56, 2015.
21. S. Issues, "A Survey of RFID Deployment and Security Issues |Korea Science A Survey of RFID Deployment and Security Issues A Survey of RFID Deployment and Security Issues | Korea Science," *J. Inf. Process. Syst.*, vol. 7, no. 4, pp. 16–17, 2011.
22. R. Uttarkar and P. R. Kulkarni, "Internet of Things□: Architecture and Security," *Int. J. Comput. Appl.*, vol. 3, no. 4, pp. 12–19, 2014.
24. V. Soni, P. Modi, and V. Chaudhri, "Detecting Sinkhole Attack in Wireless Sensor Network," *Int. J. Appl. or Innov. Eng. Manag.*, vol. 2, no. 2, pp. 29–32, 2013.
25. Zejun Ren,Xiangang Liu,Runguo Ye,Tao Zhang,"Security and Privacy on Internet of Things"vol.5,2017 IEEE.date 5/1/2017.