THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

A Brief Survey on Various Security Attacks In Iot

Umer Iqbal Wani[1], Gurpreet Singh[2], Mir Mohammad Yousuf[3], Mamoon Rashid[4], Bhanu Talwar[5]

[a, b, c, d, e]Assistant Professor, School of Computer Science & Engineering, Lovely Professional University, Jalandhar, India.

Abstract

Nowadays IoT is one of the most discussed-academic driven and industry driven topic.IoT is allowing millions and billions of devices to get connected and share valuable information.IoT has made an impact in almost every aspect of technology. From the concept of smart homes to health industry and many other fields, IoT is already making an impact and in future is expected to affect many more industries. With the generation of large amounts of data, data security is one of the priorities of every IOT environment. An efficient and market driven IoT environment has to provide high level of security to save data at a safer place. An IoT environment, apart from providing various data related services, has to assure data security to its users. In this article, a discussion on various IoT attacks has been presented, including their classification and various solutions to counter the attacks. Various attacks have been compared providing an overview about their damage levels.

Keywords-IoT, Attacks, Security, Encryption.

1.Introduction

A lot of development took place because of technological empowerment, in last twenty years. The computing power grew exponentially, giving rise to minute devices which are able to process data at a greater efficiency and within very less time. The number of devices getting connected to the internet is growing at a pace never seen before. With the availability of larger address space, currently,theiris no limit of adding devices to the internet and allowing them to share information. The objects are communicating and sharing information and this technically gave rise to a term known an Internet-of Things(IoT).

IoT has been defined as an interconnection of devices, such that devices exchange information without human intervention [1].IoT is impacting our life in a number of ways, in transportation, in healthcare industry, in education, in travel and tourism

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

industry etc. IoT is changing our life-style and allowing us to live a better and comfortable life by consuming resources judiciously and saving time as well as cost.IoT is providing new opportunities for growth and research.

IoT was introduced by Kevin Ashton in the year 1999[2].From then onwards, IoT evolved to a greater extent allowing sensors,electronic devices and other physical devices to get connected to the internet and exchange information. IoT has made the physical devices act in a smarter way[3].The physical devices communicate with other devices within a standard proximity. IoT provides a link between physical objects to the virtual world of information[4].Physical objects are able to identify and sense each other with the help of IoT.

In future, IoT is expected to have an important impact in home as well as business applications[5].The garages will get opened automatically, coffee will be prepared at the push of a button from a distance, appliances will be connected remotely.With such prominent future ahead, IoT is vulnerable to all sort of threats that come with internet. With the limited resource capability and sensitivity of the IoT devices, security is posing a bigger challenge than other prevalent challenges. As IoT is impacting our daily lives, so having a secure IoT based environment will guarantee a secure data driven successful life. The paper provides an overview about the security threats of IoT and their impact. A number of different IoT attacks and their solutions have been discussed. IoT attacks have been classified based on their vulnerability. The paper includes a section on literature survey, IoT architecture, various IoT attacks and finally a conclusion section has been involved as the end of the paper.

2. Literature Survey

The 3–layer architecture of IoT has been discussed in detail in [6][7][8].A 4-layer architecture has been discussed in [9][10], with the addition of one more layer – middle-ware layer.

A number of IoT vulnerabilities and attacks have been discussed in [9][11][12][13][14].Paper [15][16] discusses various attacks at the OSI layer. Security challenges have been addressed in [17][18][19].

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Currently a diverse group of solutions have been provided to the security threats present in IoT. A common solution should be identified for all the possible threats currently encountered. Also because of battery and computing power, implementing the solution is also very difficult. As IoT uses RFID and WSN technologies so security issues related to these have to be discussed, [20][21] discusses security related issues of RFID and WSN. Cryptography related attacks and various solutions to various attacks have been discussed in [22][23][24][25]. Paper[26] mentions various IoT applications and their benefit to the society.

3. IoT Architecture

In figure 1, a 3-layered architecture is shown. IoT technology works on 3 layers[4] – perception layer, network layer and application layer.

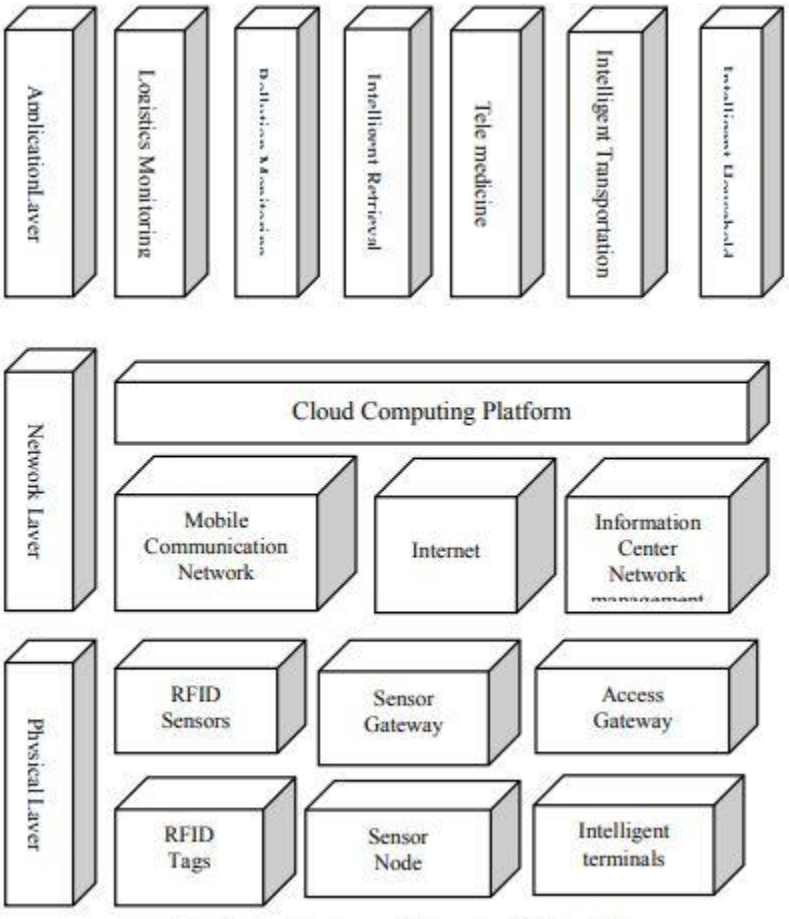


Fig.1: Architecture of Internet of Things [4]

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Perception Layer: This layer consists of various devices which gather data from the surroundings. Examples include sensors, RFID, Barcodes etc. The information collected in this layer is passed onto the network layer.Sensors and actuators are used to perform different functions such as querying location, vibration, temperature, weight motion, humidity, acceleration, etc.

*Network Layer:*This layer deals with transmission of data collected by perception layer.The various technologies used for data transfer are RFID, 3G, GSM, UMTS, Wi-Fi, Bluetooth Low Energy, infrared, ZigBee, etc. This layer is subdivided into two layers: routing layer and encapsulation layer. Routing layer deals with transmission of packets from source to destination and encapsulation layer deals with encapsulating or forming the packets.

*Application Layer:*This layer allows the users to use the IoT facilities and interact with the IoT system. Protocols for message passing are used in this layer.The application layer covers a large base of vertical markets such as smart transportation, smart building, industrial automation and smart healthcare.

4. Various security attacks in IoT

Security poses a big challenge in IoT because of heterogeneity and vast number of interconnected devices. Allowing large number of devices to transfer information in a secure manner is an issue of consideration in IoT. The attack can be carried out directly on the device, by tampering with the communication protocol, by attacking encryption policy, by using routing protocol faults.

The attacks can be classified into four categories based on various vulnerabilities: physical attack, network attack, software attack and encryption attack, as shown in figure 2.

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

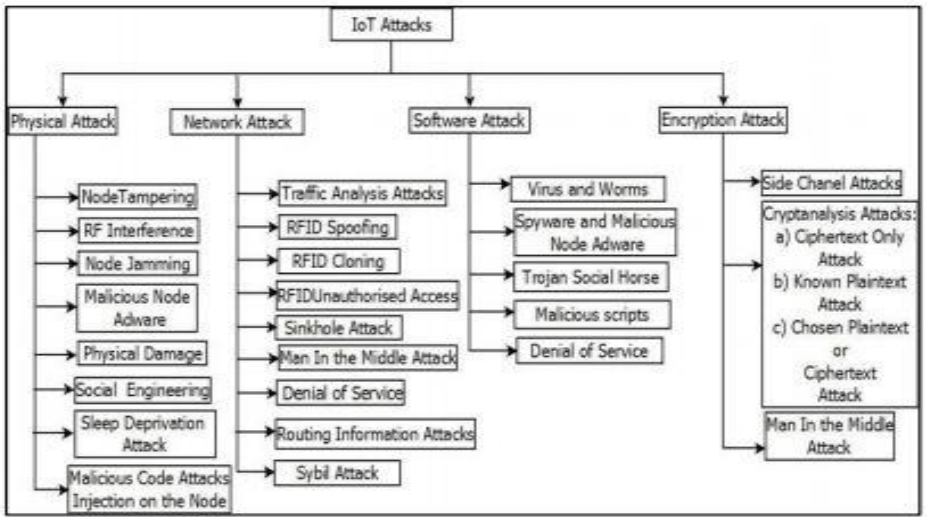


Fig. 2:IoT and its security attacks

A. *Physical attacks:*Physical attacks are more related to hardware devices of a system.

1)Node Tampering: The node is physically attacked and altered by the attacker. Sensitive information such as an encryption key can be obtained by the attacker [10].

2) Node Jamming in WSNs: This causes DoS or Denial of service attack. The attacker makes use of a jammer and affects a wireless network.

3) RF interference on RFIDs: The use of noise signals is made here. The attacker sends uses radio frequency signals to transport noise signals. The signals cause Denial of service attack using RFID technique.

4.) *Malicious Node Injection:*A new malicious and threat posing node is inserted in-between the normal nodes. The newly inserted node modifies the data so that wrong information is passed across the network. First a replica of a node is inserted (node B), then other malicious nodes are inserted. To prevent this attack, a scheme called as monitoring verification (MOVE) scheme is used. In this scheme, nodes are monitored and any abnormal behavior seen is reported at the appropriate time.

5.) *Social Engineering:*Theiris a physical interaction of the attacker with the users of the IoT system and finally manipulation of the system. Attacker gets hold of sensitive information from the system.

6.) *Sleep Deprivation Attack:*In this attack, the nodes are made to work more resulting in power loss and thus shutting down of the nodes.

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

B.Network Attacks

The attacks are related to the network of the IoT system.

1.) *Traffic Analysis Attacks:* In this attack,their is a simple interference in the message passing by the attacker. The attacker interrupts and tries to read out the messages to get information regarding the network.
2.) *RFID Cloning:* The attacker copies data from one RFID tag (previous) to another RFID tag. The original ID of the RFID tag isn't copied.
3.) *RFID Spoofing:* The attacker tries to recreate or imitate RFID signals. This attack passes on wrong information which seems correct and thus accepted by the system.
4.) *Sinkhole Attack:* In this attack, a node is made to send wrong routing information to other nodes. A wrong estimation of path to the base station through this node is sent to other parts of the network so that the traffic can be diverted from actual destination.
5.) *Man in the Middle Attacks:* In this attack, the attacker obtains sensitive information by eaves-dropping[8].
6.) *Denial of Service:* The attacker tries to deprive users from the actual services of the network by passing on large amounts of wrong information so that actual and true message is lost.

C. *Software Attacks:*

The use of malicious worms , malicious software , viruses is made by the attacker to cause the damage.

1.)Phishing Attacks: The attacker tries to obtain user sensitive information like username, password by making use of fake websites.

2.) *Malicious Scripts:* The attacker makes use of malicious scripts to steal informationand access the system.

3.) *Virus, Worms and Trojan Horse:*The attacker tries to damage the system by the use of malicious code. The code is circulated by downloading of attachments or through sending emails. The virus can be detected by the use of anti-virus software,firewalls and any other anti-intrusion system.

4) Denial of Service: The user is denied services at the application layer.

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

D. *Encryption Attacks:* These attacks try to obtain private keys by attacking encryption schemes.

1.) *Cryptanalysis Attacks:* The attacker makes use of plain-text or cipher-text to obtain the encryption key.

2.) *Ciphertext Only Attack:*The attacker gets access to the cipher-text and converts it into the corresponding plaintext.

3.) *Side-channel Attacks:* The information emitted by encrypting devices called as side-channel information is used to carry out the attack. The side-channel information may include power related, faults and frequency related information. Side-channel attack may include timing attacks,Simple and Differential Power Analysis, and Differential Fault Analysis Attacks.

4.) *Chosen Plaintext Attack:* The attacker makes a choice of encrypted plaintext and obtains the encryption key.

5.) *Chosen Ciphertext Attack:*The attacker converts the chosen cipher-text into plain-text and finds the encryption key.

6.) *Man in the Middle Attacks:* The attacker obtains the key by intercepting communication between the two entities.

5.Conclusion

As IoT is based on traditional network architecture so the flaws associated with the traditional architecture will be found in the IoT environment as well. Some new attacks have also been devised to affect only the IoT environment. A number of solutions for IoT related attacks have been researched and devised. However, while devising any solution for possible IoT security threats, the computation as well as the battery power of the devices is always a challenge. The need of an efficient security mechanism which takes into consideration the device constraints is required. The different attacks that have been discussed above can be avoided, in some cases, by simply taking care of normal security precautions.While as,at a larger scale, an efficient and powerful security mechanism has to be devised for secure future IoT applications.

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

6.References

[1] T. Yousuf, R. Mahmoud, F. Aloul, I. Zualkernan, "Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures", International Journal for Information Security Research (IJISR), Volume 5, Issue 4, December 2015.

[2] K. Ashton, "That 'internet of things' thing.", RFID Journal 22, no. 7, 2009, pp.97-114.

[3] "The Internet of Things", International Telecommunication Union. ITU Internet Reports 2005.

[4] 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,.

[5] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp.336-341,London, 2015,

[6] I. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," 2015 IEEE Symposium on Computers and Communication (ISCC), pp.180-187,Larnaca, 2015. [7] L. Patra and U. P. Rao, "Internet of Things — Architecture, applications, security and other major challenges," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp.1201-1206, New Delhi, India, 2016,.

[8] M.U. Farooq, M. Waseem, A. Khairi and 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.

[9] Wahid, Abdul, P. Kumar, "A Survey on attacks, Challenges and Security Mechanism In wireless Sensor Network", JIRST- International Journal for Research in Science & Technology, Volume 1, Issue 8, pp. 189-196,January 2015.

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[10] 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.

[11] 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.

[12] Kandah, Farah, Y. Singh, and C. Wang, "Colluding injected attack in mobile ad-hoc networks", IEEE Conference on Computer Communication Workshops (INFOCOM WKSHPS), 2011.

[13] Kaur, Damandeep, and P. Singh, "Various OSI Layer Attacks and Countermeasure to Enhance the Performance of WSNs during Wormhole Attack",International Journal on Network Security 5.1 (2014): 62. [14] Reed, Damon, "Applying the OSI seven layernetwork model to information security", SANS GIAC GSEC Practical Assignment Version 1.4 b Option One 2003.

[14] Reed, Damon, "Applying the OSI seven layernetwork model to information security", SANS GIAC GSEC Practical Assignment Version 1.4 b Option One 2003.

[15] D. Singh, G. Tripathi, and A.J. Jara, "A survey of Internet of-things: Future vision, architecture, challenges and services," 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 287-292, IEEE, 2014. [16] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), vol. 3, IEEE, pp. 648-651,2012.

[17] 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.

[18] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classification of RFID attacks" Gen 15693 (2010). [19] H. Li, Y. Chen and Z. He, "The Survey of RFID Attacks and Defenses," 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), Shanghai, 2012.

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[20] Kocher, Paul, et al. "Introduction to differential power analysis." Journal of Cryptographic Engineering 1.1 , pp.5-27 ,(2011).

[21] Kelsey, John, et al. "Side channel cryptanalysis of product ciphers." European Symposium on Research in Computer Security. Springer Berlin Heidelberg, 1998.

[22] Kocher, Paul C. "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems." Annual International Cryptology Conference. Springer Berlin Heidelberg, 1996.

[23] Zulkifli, M. Zaid W. Mohd, "Attack on Cryptography, 2008.

[24] F. Kandah, Y. Singh, W. Zhang and C. Wang, "Mitigating colluding injected attack using monitoring verification in mobile ad-hoc networks", Security and Communication Networks, pp.1939-0122,2013.

[25] 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.

[26] Jain, Pragya and Sardana, Anjali, "Defending against Internet Worms Using Honeyfarm", Proceedings of the CUBE International Information Technology Conference, pp.795-800,2012.

[27] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of Things for Smart Cities," in IEEE Internet of Things Journal, vol. 1, no. 1, pp.22-32,Feb. 2014,.

Copyright © 2019Authors