IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-12, Dec 2018 E-ISSN: 2347-2693

Internet of Things: Security Issues and Countermeasures

Pradeep Kamboj[1*], Ajit Kumar Singh Yadav[2]

[1, 2]Department of Computer Science & Engineering, NERIST, Itanagar, India

[*]*Corresponding Author: pko@nerist.ac.in*

Available online at: www.ijcseonline.org

Accepted: 12/Dec/2018, Published: 31/Dec/2018

Abstract— Internet of Things (IOT) is an emanate trend, that exploits the vast number of inter-connected daily used smart-devices to provide numerous services. These devices may vary in size, computational power, capacity and their usability. Tremendous amount of data is transmitted and collected by these devices, there is a high risk of data theft, object manipulation, identity and network manipulation. Moreover, misuse of IOT devices can also lead to possibility of cyber-attack and to organize crime. While a tremendous rise has been seen in the usage of such devices, security vulnerabilities also rise accordingly. Therefore, it is necessary to identify the security issues and address them accordingly. In this paper we discuss the IoT reference model, some of its applications, security challenges, and their countermeasures. The primary goal of this research is to address security issues in IoT and discuss the countermeasures.

Keywords—IOT security, vulnerabilities, Data Encryption, DoS (Denial of Service), IDSs (Intrusion Detection Services).

I. INTRODUCTION

Today, we are living in a world of millions of smart devices with sensing, processing and actuating abilities and are capable of being connect to the Internet [1]. In the last decade, there is a tremendous growth in smart devices. Humans are facilitated with numerous services provided by these internet connected devices but on the other side society become susceptible to the vulnerabilities of the IoT environment [2]. The reasons for such security threats includes; lack of standards in the design of such devices and the exposure of IoT devices via heterogeneous technologies. Unfortunately enough research is not yet done to recognize the security needs. Hence the security and privacy issues in IoT are need to be addressed in depth that helps in the development of smart and secured IoT devices and enables superfluity of services for humans, ranging from energy management to smart vehicles [3].

IoT security is the area that attracts the attention of many academic and industrial researchers in recent times. Many organizations throughout the world are working in the security enhancement of IoT devices to primarily provide us the better services. In order to meet this requirement, researchers are putting efforts to discover potential threats and provide solutions against them. In this survey we summarize these threats and their solutions.

The main objective of this paper is to provide reader enough information regarding security threats in IoT and a way to deal with these security threats. The remaining paper is organized as follows. Section I contains the introduction of Internet of Things and security issues in them. In section II, we describe a system model for IoT. In section III, we discuss various IoT applications. Then in section IV, we address security threats in IoT. Discussion regarding their countermeasures is done in Section V. Finally, in section VI, we provide a conclusion and scope for future work.

II. IOT SYSTEM MODEL

Though there are several IoT system models, we discuss here a seven-level system model which was proposed by CISCO in 2014. Figure 1 shows this model [4]. The brief description of each level of this model is as under:

Level 1 Things: This level consists of smart devices, sensors, RFID readers, controllers etc. Data integrity and confidentiality needs attention from this level onwards.

Level 2-Connectivity/Edge computing: This level consists of all the components responsible for communication between devices. It also includes the edge computing, in which the data processing is done at device level to reduce the computational load at higher levels.

Level 3-Global Infrastructure: Data collected by the IoT devices need to be stored somewhere, as the devices are of limited processing capabilities and have a little storage capacity. This level consists of cloud infrastructure that is responsible for storage of data.

Level 4-Data Ingestion: Most of the applications need the historic data rather than the recently processed one. This may initiate the requirement of converting the data in motion to data at rest. This level consists of all the

functionalities that deals with the conversion of network packet data to database table data.

Level 5- Data Analysis: To make the data simpler and efficient for further processing, this level provides various means; ranging from normalization to indexing and data consolidation.

Level 6-Application: In this level the software cooperates with data ingestion and data analysis levels to provide information interpretation.

Level 7-People & Process: In this level, the end users exploit the analytical data through applications.

Figure 1. IoT System model

III. IOT APPLICATIONS

From its inception, the growth of IoT devices is exponential. According to a survey done by HP, connected devices in year 1990 were 0.3 million which grows to 9.0 billion in 2013 and expected to be 1.0 trillion by 2020 (shown in table 1). The reason for increasing demand of IoT devices is due to its immense applicability in real life [5]. We cannot limit the list of IOT applications as it is too long. Some of its applications, the major ones, are listed below:

Smart home: Smart homes has gained a vast popularity in recent times. The idea behind this concept is to save time, money and energy, and makes you feel better. With the help of IoT devices, one could think of switching on an AC before entering in house or unlocking the door for someone to temporary access even in your absence or switch off the home appliances remotely and so on [6].

Wearables: In order to cope with the fast moving life, everybody wants to keep themselves fit and updated. There are devices equipped with sensors and softwares that collect data and information about the user, which later on can be used to extract essential insight about the user. These devices mainly covers health, fitness and entertainment requirements.

Connected cars: A connected cars can be seen as a vehicle that is equipped with several sensors to optimize its operations, maintenance and comfort of passengers. Major brands like Tesla, BMW, Apple, Google are working on bringing the next revolution in automobiles.

Healthcare sector: The concept behind connected healthcare system and smart medical devices bears enormous potential not just for companies, but also for the well-being of people in general. In coming years IoT will going to play an important role in healthcare [7]. Smart wearable devices will collect the data to monitor the health of the user and provide tailored strategies to counter illness.

Smart retail: IoT has an immense potential in the retail sector. Retailers can use smart devices to make the customer's in-store experience better. One little example is to track consumers path using IoT devices. This trajectory later on can be utilized to deploy hoardings of their major products in high traffic areas.

Table 1. IoT device growth table

Year	Number of connected devices
1990	0.3 million
1999	90.0 million
2010	5.0 billion
2013	9.0 billion
2025	1.0 trillion

IV. Security threats in IoT and countermeasures

Security in IoT devices is often put on negligence and cheaper devices are made available in market in a short time. The devices that allow some protection usually employ at software or firmware level leaving the hardware vulnerable to attacks [8]. In this section we discuss about security goals, possible IOT attacks and their countermeasures.

A. Security Goals

Security can be achieved by exploiting three major areas which are: data Confidentiality, Integrity and Availability (CIA Security model shown in figure 2)

Data Confidentiality is the potential to provide the user an enough confidence about the secrecy of sensitive information by using different mechanisms to prevent its disclosure to an unauthorized user.

Data Integrity refers to the protection of user information against the malicious users who try to alter the data during its transit.

Data Availability ensures instantaneous availability of information to the authorized users even in the disastrous conditions. Best example of a vulnerability to availability is a DoS attack. Commonly used mechanism to protect availability includes: firewall, intrusion detection system and many more.

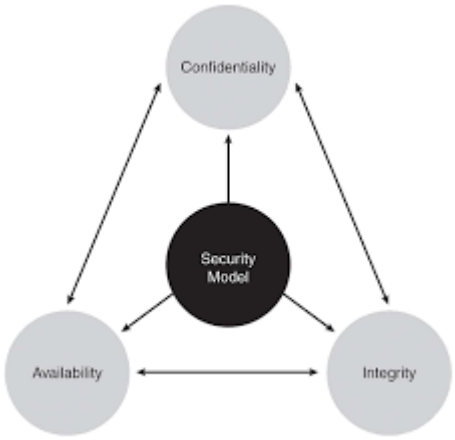

Figure 2. CIA Security model

B. IoT Attacks and countermeasures

In this section, we discuss attacks in first two levels of reference model and possible solutions to them.

1) IoT Attacks

Hardware Trojan: It is the malicious modification in the hardware of an IoT device with an intention to have an access on data or software running on it [9].

Denial of Sevice (DoS) attack: Three possible types of DoS attacks are battery draining sleep deprivation and outage attack [10].

i) Battery draining: Generally IoT devices have limited battery. In this kind of attack a malicious user tries to engage an edge node in unnecessary computing, which leads the device running out of battery.

ii) Sleep deprivation: In this type of attack, an attacker tries to send undesired messages to the device that seems to be authorized. This attack was first described by Stajano [11].

iii) Outage attack: When a node stops its normal operation then node outage occurs. This may happen due to some error in manufacturing process, battery draining, sleep deprivation and code injection. One of the best example of this attack is the injection of Stuxnet [12] into Iran's nuclear plant's control chip and prevent it to detect abnormal behavior.

Physical tampering: The IoT devices are prone to physical attack due to their high availability and ease of access. The attacker can make changes to the circuit of the device with some predefined motive; may be to steal some cryptographic information for malicious use [13],[14].

Data Pollution Attack: As machine learning algorithms are used to train the data set at edge computing level, attacker can compromise the enough number of IoT devices as legitimate data source and mislead the learning algorithm to derive the conclusion as per attacker's expectations [15]. This kind of attack has been seen on social networking sites.

SQL injection: This attack is done by injecting malicious actor in the SQL query to process the unsecured part of the SQL database [16]. The main intention of the attacker is to escalate permissions and grant the unauthorized access to the system.

Data Transit Attack: This attack compromises the data confidentiality and integrity during the data transit period in network [17].

Routing Attack: the simplest of this attack is alter attack in which an attacker alters the routing table of nodes with the main intention to prevent the packet to reach the destination. Other types of routing attack includes Sybil[18], Grey Hole [19], Black Hole [20], Hello Flood[21] and Worm Hole [22].

2) Countermeasures

Trojan detection: To detect the Trojan attack, side-channel signals, including power [23],[24],[25], timing [26],[27] and spatial temperature [23],[28] can be used. Power and delay characteristics of wire or circuit are commonly affected by the hardware Trojan, which can be detected by comparing physical characteristics and heat distribution in the IC circuit.

Intrusion detection systems (DSs): In this system several policies are defined to measure the level of security in the IoT devices and continuous observation is made to keep track the violation of them. It is a promising approach to defend against battery-draining and sleep deprivation attacks. Several researches have been made to enhance the capabilities of IDSs [29]-[32].

Temper proofing: In this mechanism an extra hardware circuitry is augmented with the device to give protection against physical tempering. Some self-destruction mechanisms can also be used to give protection against temper attack [33].

Outlier detection: The basic principle behind the defense against the data pollution attack on learning environment is to reduce the effect of adding invalid data points in the result. These invalid data points are outliers in the training set. Rubinstein et al. [34] proposed a defense framework against this attack.

SQL injection protection: The best way to give protection against this attack is to validate all the data provided by the client before actually using it with a specific APIs. [11].

6LoWPAN: Most of the IoT devices are usually small in size and IP protocol cannot be used. Thus, 6LoWPAN protocol is used to connect the resource constrained IoT device to the outside world [12]. It also provide enough end-to-end security to defend against the attack on confidentiality and integrity of data.

Reliable routing: The major complication in implementation of the routing protocol is the access of messages by intermediate nodes. One way to handle this situation is to restrict intruders to alter the data packets by enforcing strong cryptographic schemes [35][36][37].

V. CONCLUSION AND FUTURE SCOPE

Security challenges emerge gradually along with the rapid development of IoT technology. In this paper we attempt to summarize some attacks possible on the first two levels of the IoT system model. The main motive of the paper is to give reader an opportunity to explore different attacks on IoT devices and their countermeasures. For future work some rigorous mechanisms need to be developed to deal with these issues effectively.

REFERENCES

[1] S. Karnouskos, P. J. Marrn, G. Fortino, L. Mottola, and J. R. Martinez deDios, "Applications and Markets for Cooperating Objects. Springer Briefs in Electrical and Computer Engineering," Springer, 2014, pp. i-xiv, 1-120.

[2] H. Xiao, N. Sidhu, and B. Christianson, "Guarantor and reputation based trust model for Social Internet of Things," in Proc. International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, 2015, pp. 600-605.

[3] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The Internet of Things architecture, possible applications and key challenges," in Proc. IEEE 10th Int. Conf. Frontiers of Information Technology, 2012, pp. 257–260.

[4] "The Internet of Things reference model." CISCO, 2014. [Online] Available: http://cdn.iotwf.com/resources/71/IoT Reference Model White Paper June 4 2014.pdf

[5] Imen Ben Ida, Abderrazak Jemai and Adlen Loukil, A survey on security of IoT in the context of eHealth and clouds,2016 11th International Design Test Symposium (IDT), 18-20 Dec. 2016, Hammamet, Tunisia.

[6] I. Stojmenovic, ''Machine-to-machine communications with in-network data aggregation, processing and actuation for large scale cyber-physical systems,'' IEEE Internet Things J., vol. 1, no. 2, pp. 122–128, Apr. 2014.

[7] D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, "Internet of Things: Vision, Applications and Research Challenges". Volume 10, Issue 7, pp. 1497-1516, Ad Hoc Networks, (September 2012).

[8] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and Security inInternet of Things and Wearable Devices," IEEE Transactions on Multi-Scale Computing Systems, vol. 1, no. 2, pp. 99-109, April-June 1 2015.

[9] H. Salmani and M. M. Tehranipoor, "Vulnerability analysis of a circuit layout to hardware Trojan insertion," IEEE Trans. Information Forensics and Security, vol. 11, no. 6, pp. 1214–1225, 2016.

[10] A. Agah and S. K. Das, "Preventing DoS attacks in wireless sensor networks: A repeated game theory approach," Int. J. Network Security, vol. 5, no. 2, pp. 145–153, 2007.

[11] B. Dorsemaine, J. P. Gaulier, J. P. Wary, N. Kheir and P. Urien, "A new approach to investigate IoT threats based on a four layer model," 2016 13th International Conference on New Technologies for Distributed Systems (NOTERE), Paris, 2016, pp. 1-6.

[12] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals," RFC 4919, Aug. 2007.[13] X. Wang, S. Chellappan, W. Gu, W. Yu, and D. Xuan, "Search-based physical attacks in sensor networks," in Proc. IEEE 14th Int. Conf. Computer Communications and Networks, 2005, pp. 489–496.

[14] S. H. Weingart, "Physical security devices for computer subsystems: A survey of attacks and defenses," in Proc. Cryptographic Hardware and Embedded Systems. Springer, 2000, pp. 302–317.

[15] M. Mozaffari-Kermani, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "Systematic poisoning attacks on and defenses for machine learning in healthcare," IEEE J. Biomedical and Health Informatics, vol. 19, no. 6, pp. 1893–1905, Nov. 2015.

[16] V. Luong, "Intrusion detection and prevention system: SQL-injection attacks," Master's thesis, San Jose State University, 2010.

[17] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu and Dechao Qiu, "Security of the Internet of Things: perspectives and challenges", Wireless Netw ,2014.

[18] J. R. Douceur, "The Sybil attack," in Peer-to-peer Systems. Springer, 2002, pp. 251–260.

[19] B. Revathi and D. Geetha, "A survey of cooperative black and gray hole attack in MANET," Int. J. Computer Science and Management Research, vol. 1, no. 2, pp. 205–208, 2012.

[20] Z. Karakehayov, "Using REWARD to detect team black-hole attacks in wireless sensor networks," in Proc. Wkshp. Real-World Wireless Sensor Networks, 2005, pp. 20–21.

[21] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based Internet of Things," Int. J. Distributed Sensor Networks, vol. 2013, 2013.

[22] O. Garcia-Morchon, S. Kumar, R. Struik, S. Keoh, and R. Hummen, "Security considerations in the IP-based Internet of Things." [Online]. Available: https://tools.ietf.org/html/draft-garcia-core-security-04

[23] A. N. Nowroz, K. Hu, F. Koushanfar, and S. Reda, "Novel techniques for high-sensitivity hardware Trojan detection using thermal and power maps," IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems, vol. 33, no. 12, pp. 1792–1805, 2014.

[24] T. Iwase, Y. Nozaki, M. Yoshikawa, and T. Kumaki, "Detection technique for hardware Trojans using machine learning in frequency domain," in Proc. IEEE 4th Global Conf. Consumer Electronics. IEEE, 2015, pp. 185–186.

[25] M. Tehranipoor, H. Salmani, and X. Zhang, "Hardware Trojan detection: Untrusted manufactured integrated circuits," in Integrated Circuit Authentication. Springer, 2014, pp. 31–38.

[26] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," IEEE Design and Test of Computers, vol. 27, no. 1, pp. 10–25, 2010.

[27] A. Nejat, S. M. H. Shekarian, and M. S. Zamani, "A study on the efficiency of hardware Trojan detection based on path-delay fingerprinting," Microprocessors and Microsystems, vol. 38, no. 3, pp. 246–252, 2014.

[28] K. Hu, A. N. Nowroz, S. Reda, and F. Koushanfar, "High-sensitivity hardware Trojan detection using multimodal characterization," in Proc. IEEE Design, Automation & Test in Europe Conference & Exhibition, 2013, pp. 1271–1276.

[29] S. S. Doumit and D. P. Agrawal, "Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks," in Proc. IEEE Conf. Military Communications, vol. 1, 2003, pp. 609–614.

[30] C.-C. Su, K.-M. Chang, Y.-H. Kuo, and M.-F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks [wireless sensor networks]," in Proc. IEEE Conf. Wireless Communications and Networking, vol. 4, 2005, pp. 1927– 1932.

[31] A. Agah, S. K. Das, K. Basu, and M. Asadi, "Intrusion detection in sensor networks: A non-cooperative game approach," in Proc. IEEE 3rd Int. Symp. Network Computing and Applications, pp. 343–346.

[32] A. P. R. da Silva, M. H. Martins, B. P. Rocha, A. A. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in Proc. ACM 1st Int. Wkshp. Quality of Service & Security in Wireless and Mobile Networks, 2005, pp. 16–23.

[33] A. D. Wood and J. Stankovic, "Denial of service in sensor networks," IEEE Computer, vol. 35, no. 10, pp. 54–62, 2002.

[34] B. I. Rubinstein, B. Nelson, L. Huang, A. D. Joseph, S.-H. Lau, S. Rao, N. Taft, and J. Tygar, "ANTIDOTE: Understanding and defending against poisoning of anomaly detectors," in Proc. ACM 9th SIGCOMM Conf. Internet Measurement, 2009, pp. 1–14.

[35] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, and M. Rossi, "Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples," in Proc. IEEE Int. Symp. World of Wireless, Mobile and Multimedia Networks, 2012, pp. 1–7.

[36] P. Bhatt, B. Thaker, N. Shah, "A Survey on deploying secure IoT Products", Int. J. Scientific Research in Computer Science and Engineering, vol. 6, issue. 5, Oct 2018, pp. 41-44.

[37] A. Sebastian, S. Sivagurunathan, "A Survey on Load Balancing Schemes in RPL based Internet of Things", Int. J. Scientific Research in Network Security and Communication, vol. 6, issue. 3, Jun 2018, pp. 43-49.

Authors Profile

Mr. Pradeep Kamboj is an Assistant Professor in the Department of Computer Science & Engineering at NERIST, Itanagar, Arunachal Pradesh, India. He has more than 16 years of research and teaching experience. His major research area includes VANET, Artificial Intelligence, datamining, Theory of computer science etc. He has several research papers in international journals.

Mr. Ajit Kumar Singh Yadav is an Assistant Professor in the Department of Computer Science & Engineering at NERIST, Itanagar, Arunachal Pradesh, India. He has more than 17 years of research and teaching experience. His major research area includes datamining, image processing,machine learning etc. He has several research papers in international journals.

