International Journal of Engineering & Technology, 7 (2.7) (2018) 163-167

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Critical review attacks and countermeasures in internet of things enabled environments

Mohan Kumar Ch[1]* , M Kameswara Rao[2]

[1]Department of Computer Science and Engineering, [2]Department of Electronic Computer Science and Engineering
Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India – 522502.
**Corresponding author E-mail: mail2mohan.ch@gmail.com*

Abstract

Internet of Things (IoT) generally referred as Industry 4.0, Now a day's Application Areas are everywhere like Smart Transportation, Smart Construction, Fitness monitoring, Energy Supervision, Construction managing, Environmental Supervise, Groceries supply chain. IoT has a compound network of smart nodes; information sending and receiving of nodes are through the Internet. In this process, it is vulnerable to attacks. In This paper, we review the possible attacks with respect to Cisco- Seven Layer model.

Keywords: *IoT, thing, Security Attack, Industry 4.0, Countermeasures, lightweight protocols.*

1. Introduction

Internet of Things (IoT) generally referred as Industry 4.0[11] does not fit to any common definition by any experts; Furthermore IoT provides administration effects over the traditional-net by focusing on person-things, or things-things, communication between things. IoT provides a medium of interconnection of varied things, where the word thing resembles a human being, or potentially any device that can request a service or provide a service [1].

The development of the IoT worldview is a standout amongst the most amazing wonders of the most recent decade. The improvement of different protocols for communication, alongside the scaling down of handsets, gives the chance to change a confined gadget into a conveying thing. Additionally, processing power, energy capacity, and capacity abilities of little-registering gadgets have significantly enhanced while their sizes have reduced totally.

2. The IoT paradigm

In this segment, we initially talk about one of the IoT reference models depicted in the writing. At that point, we portray the extent of IoT applications. From there on, we clarify what security implies in the extent of IoT. We take Cisco – Seven Layer model for my research purpose this model observed in educational and business publications.

CISCO's Seven-Layer model can possibly be standardized and in this way make a broadly acknowledged reference model for the Internet of Things [2]. In this model, information stream is typically bi-directional. Be that as it may, the overwhelming heading of information stream relies upon the user application. With a specific end goal to outline Attacks on IoT Infrastructure and their countermeasures in each Layer.

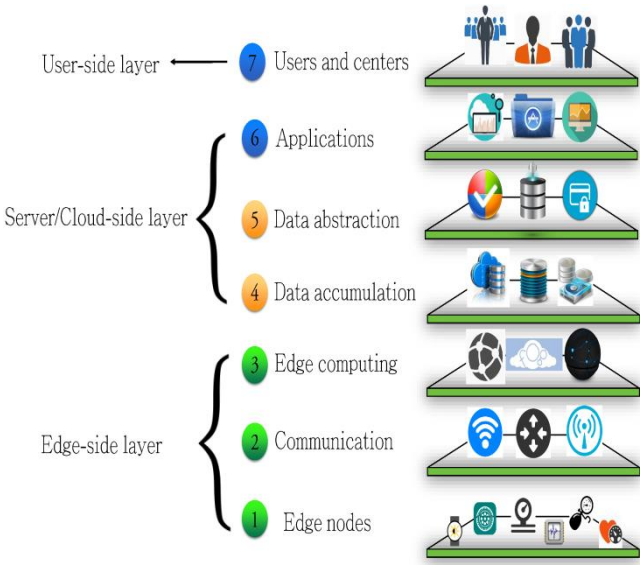


Fig. 2. 1 Cisco-Seven Layer Model [6].

Edge devices (Layer 1): The principal layer of this reference display regularly comprises of computing hubs, e.g., RFID reader, sensors, controllers, and distinctive adaptations of RFID labels. Information integrity and confidentiality must be considered from this layer upwards.

Communication (Layer 2): This layer consists of the considerable number of segments that are responsible to transmission of data or instructions: (i) transmission between gadgets in the primary layer, (ii) transmission between the segments in the second layer, and (iii) transmission of data between the 1st and 3rd layers.

Edge computing (Layer 3): also referred as fog computing, is the 3rd layer of the model in which basic information handling is started. This layer is fundamental for minimize load while processing

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

time. And the quick transfer of data to above layers. In Real-Time computation need to perform at the edge. The processing amount depends on a provider of service, a node for computing. Regularly, basic signal handling and some algorithms are used at this point.

Data accumulation (Layer 4): The superior part of the appliance cannot require instant processing of data. This layer enables change of information in the movement to information very still, i.e., it enables us to store the information for further examination or to impart to abnormal state processing servers. The primary errands of this layer are converting the packet format to database set of structured tables, lessening information through separating and specific putting away, and deciding if the information is important to higher layers.

Data abstraction (Layer 5): This layer gives the chance to render and store information with the end goal that further preparing ends up plainly easier or more proficient. The regular assignments of elements at this layer incorporate standardization, de-standardization, ordering and combining information place into one area and giving privileges to various information storage areas.

Applications (Layer 6): major functionality of application layer is an interpretation of information or data understanding, where programming collaborates with layer 4 and layer 5. The uses of IoT are various and may fluctuate essentially crosswise over business sectors and modern needs.

Users and centers (Layer 7): The main layer of the IoT is the place the clients. Clients make utilization of the appliance and their expository information.

2.1. The scope of The Internet of Things Applications:

We initially talk about the scope of major Application Areas: Smart Transportation, Smart Construction, Fitness monitoring, Energy Supervision, Construction managing, Environmental Supervise, Manufacture, and assembly line management, Groceries supply chain [10].

Figure 2.2: Applications Area of IoT [13]

2.2 Security in the scope of IoT:

Next, we characterize two of the most generally utilized terms in the extent of IoT: a secure thing and an Attack on security. When characterizing what a secure thing is, it is vital to comprehend the attributes that characterize security. Generally security requirements we refereed as **CIA**. Means **Confidentiality, Integrity, and Availability**. We listed from the various literature of security to provide security with CI3ATNRP extension to Basic CIA [14].

- **Secure object**: An object that has the majority of the listed point out security prerequisites.

•**An attack on Security**: An action that compromises at least one of the previous points out security prerequisites.

Table 2.1: Security requirements [14]

Requirement	Definition	Abbreviations
Confidentiality	Ensuring that only authorized user access the information	C
Integrity	Ensuring completeness, accuracy, and absence of unauthorized data manipulation	I
Availability	Ensuring that all system services are available, when requested by an authorized user	A
Accountability	An ability of a system to hold users responsible for their actions	AC
Auditability	An ability of a system to conduct persistent monitoring of all actions	AU
Trustworthiness	An ability of a system to verify identity and establish trust in a third party	TW
Non-repudiation	An ability of a system to confirm occurrence/non-occurrence of an action	NR
Privacy	Ensuring that the system obeys privacy policies and enabling users to control their data	P

3. Vulnerabilities of IoT and their countermeasures

In this section, we examine diverse attacks at the layer of edge-side in Cisco IoT Model and depict conceivable countermeasures against them.

3.1 Edge Nodes:

Next, we talk about different possible attacks with Respective to the First Layer of the Cisco model. In this layer contains processing node, sensors, and small controlling nodes.

		Threat	Against
Edge Nodes	Computing Nodes	Hardware Trojans	All
		Side-channel attacks	C,AU,NR,P
		DoS	A,AC,AU,NR,P
		Physical attacks	All
		Node replication attacks	All
		Camouflage	All
		Corrupted Node	All
	RFID Tags	Tracking	P,NR
		Inventorying	P,NR
		Tag Cloning	All
		Counterfeiting	All
		Eavesdropping	C,NR,P

3.1.1. Computing nodes: We start with possible actions in opposition to the edge processing hubs, e.g., RF readers, sensors, and smaller nodes to compromise security.

Hardware Trojan: HT is a malevolent change the built-in circuit; it leads possible actions against original functionality in the integrated circuits (ICs) [4]. Trojans are for the most part partitioned into two classes in view of their activating systems [3],[4]: **(i) Trojans activated by externally**, these type of actions are happening with connected devices **(ii) Trojans activated by internally** these type of actions happens within node state changes or internal software changes are met inside the incorporated circuit.

Side-channel Non-network attacks: Every device may omit the data into network even we are not using any communication network. Normally in this layer happens non- network side effects raises due to manufacturing defects.

DoS attacks: we summarize majorly 3 types of Denial **of Service** attacks.

Physical Attack (or) Tampering: All are working in the environment of hostile to access the gadgets might be conceivable, hence they exceptionally possible of attacks to software as well as

hardware. In this case, the attacker gets physical device accessing and separates the important cryptographic or coded data. And change the program or change the working framework.

Node replication attacks: This type of attack, the assailant or opponent incorporates another new hub, e.g., a malignant node, to existing hubs of the network by duplicating one hub's ID. This attack as leads to decrease their performance of Network. Besides, the attacker can without much of knowledge can create packets or change the direction or route of the existing packet. This attack ordinarily makes serious harm the framework and attacker get access share secret keys [5].

Camouflage: In this kind of attack, the assailant embeds a fake edge hub or assaults an approved hub with a specific end goal to cover up at the edge level. A short time later, the modified/counterfeit hub can work as an ordinary hub to acquire, process, send, or divert packets [5, 6]. Besides, such a hub can work in an inactive mode in which it just directs traffic analysis.

Corrupted/malicious node: The principal objective of corrupting nodes is to increase unapproved access to the system they have a place with. Malicious hubs infused into a system can acquire access to different hubs, conceivably controlling the system for the attacker [5]. A malignant node can likewise be utilized by the attacker to infuse false information into the framework or forestall conveyance of genuine messages [6].

3.1.2 Radio Frequency Identification Tags:

Tracking: Undisclosed analysis is a major possible attack on RFID tags. Regrettably, approximately all tags give a distinctive identification number. As an effect, a near-illegal reader can simply and efficiently interpret a tag that is attached to an artifact or an entity. Those type of reading a possible attack on the sequence of RFID tags. Some time tags are named with personal profiles like manufacturing company name.

Inventorying: When tags having information about attached the devices. Specifically, electronic item code (EIC) labels have custom fields of two: code of a producer and code of an item. Thus, a person who having EIC tag is liable to reviewing [7], a label reader can analyze the item individually. This risk shows the way to privacy.

Tag cloning: like spoofing or masquerade of RFID tags may want to stay entirely profitable to hackers, and extremely hazardous because of loose recognition of the company. When tag cloning happens entire damage to sensitive areas like banking sector data as well as cards.

Counterfeiting: In this type of attack, the opponent changes item identification or tag modification. Normally, this type of attacks with basic information is enough to do a partial modification of tag ID [8].

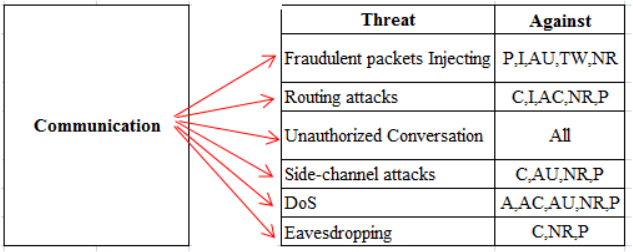
Eavesdropping: The attacker capture, analyze and stores the data in the network for further action. The captured statistics may be used as the key to attack, which includes cloning of tags.

3.1.3 Countermeasures for Threats at Edge Nodes Layer

	Threat	Countermeasures
Computing Nodes	Hardware Trojans	Side-Channel signal Analysis
		Trojan Activation methods
		Circuit/Design Modification
	Side-channel attacks	Circuit/Design Modification
		Kill/Sleep Command
		Isolation
		Blocking
	DoS	IDSs
		Secure Firmware update
		Personal Firewall
		Cryptographic Schemes
	Physical attacks	Circuit/Design Modification
	Node replication attacks	Cryptographic Schemes
	Camouflage	Cryptographic Schemes
		Secure Firmware update
	Corrupted Node	Side-Channel signal Analysis
		IDSs
		Secure Firmware update
		Cryptographic Schemes

3.2 Communication Layer:

Next, we discuss attacks with respective communication layer .



Fraudulent packets injecting: In this action, opponent inserts false packets into a communication channel. Opponent uses 3 types of techniques to attack communication layer: (i) inserting false or fake packets, (ii) control the packet or modifies the route of packet, and (iii) replications of packets [5].

Routing attack: in this type of action route is altered by Attacker. Possible attacks are: (i). **Black Hole:** in this mode packets are drop by the node with an intersection of a malicious node within the shortest path of packet routing and packet. (ii). **Gray Hole**: The nodes specifically drop few packets. (iii). **Worm Hole**: this type happens even channel having authentication and confidentiality. Opponent a set of actions in the different location of packets, while traveling one network to other networks. (iv). **Hello Flood**: malicious nodes sending "HELLO PACKETS" to each hub an existing network and claim to be next or near the node. (v). **Sybil**: the attacker adds fake identities to nodes.

Unauthorized conversation: every application of IoT conversation between the nodes happens to fulfill the task, but some nodes are not secure so that time attacks are possible.

Side-channel attacks: These are powerful attacks against encryption. This attack signifies an actual danger to the security and dependability of secrecy usage. As said before, attacks on a side

channel. They just concentrate data that is regularly unexpectedly leaked.

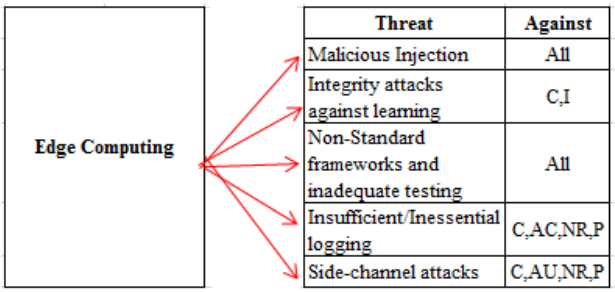
DoS attacks: The attacker may embed a hub/switch that deliberately disregards the communication convention with a specific end goal to create impacts or jam the signals [5]. A harmful switch/hub may likewise decline to the path of messages.

Eavesdropping: Attacker intentionally listen to the private data in the communication channel. It can give significant data to the assailant when the information is decoded. In this circumstance, usernames and additionally passwords are regularly simple to separate. At the point when packets likewise convey get to control data, for example, hub setup, shared system secret key, and hub identifiers, spying can give basic data. The attacker can utilize and process this caught data to plan other custom-made attacks [15].

3.2.1 Countermeasures for Threats at Communication Layer:

	Threat	Countermeasures	
Communication Layer	Fraudulent packets Injecting	IDSs	Cryptographic Schemes
	Routing attacks	Reliable Routing	
	Unauthorized Conversation	Role-Based Authorization	
	Side-channel attacks	Circuit/Design Modification	Isolation
		Kill/Sleep Command	Blocking
	DoS	IDSs	Personal Firewall
		Secure Firmware update	Cryptographic Schemes
	Eavesdropping	Cryptographic Schemes	Kill/Sleep Command
		Isolation	Blocking
		Personal Firewall	

3.3 Edge computing Layer (Fog): We mainly look into on feasible threats to the sensor networks.



Malicious injection: In addition to the side channel attacks mentioned earlier, the information disclosed to the attacker through additional components such as service providers, servers etc. are also considered as side channel attacks.

Integrity attacks against machine learning: IoT uses a verity of machine learning techniques that are vulnerable to attacks. Two important types of these attacks are Causative and Exploratory. Causative attacks may make changes to both training and testing data, or only training data, but exploratory attacks will make changes to testing data only

Side-channel attacks: In addition to the side channel attacks mentioned earlier, the information disclosed to the attacker through additional components such as service providers, servers etc. are also considered as side channel attacks.

Non-standard frameworks and inadequate testing: Non-standard coding defects may augment the privacy and security issues and may turn up because IoT integrates a variety of devices into networks and no standard framework or policies to detect these defects.

Insufficient/inessential logging: Logging helps to identify intrusion or a hacking attempt in real time and keeps the information safe. The edge computing based frameworks might be harmed because of deficient logging [9]. It is additionally required that the log documents be encoded.

3.3.1 Countermeasures for Threats at the Edge Computing Layer:

	Threat	Countermeasures
Edge Computing	Malicious Injection	Pre-Testing
	Integrity attacks against learning	Outlier Detection
	Non-Standard frameworks and inadequate testing	Pre-Testing
	Insufficient/Inessential logging	Pre-Testing
	Side-channel attacks	Circuit/Design Modification
		Kill/Sleep Command
		Isolation
		Blocking

4. Conclusion

we observed possible attacks and countermeasures for threats in IoT Infrastructure with the respective standard model of Cisco devices. We need security for each environment those are enabled with the Internet of Things. And also normal Protocols and Cryptographic Techniques are not suitable due to devices are low processing and low power consumption. So we require lightweight protocols to provide security at each layer in IoT.

References

[1] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787-2805, 2010.

[2] “The Internet of Things reference model," http://cdn.iotwf.com/resources/71/IoT Reference Model White Paper June 4 2014.pdf, accessed: 10-1-2016.

[3] D. M. Shila and V. Venugopal, “Design, implementation and security analysis of hardware Trojan threats in FPGA," in Proc. IEEE Int. Conf. Communications, 2014, pp. 719-724.

[4] 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.

[5] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, “ Wireless sensor network security: A survey," Security in Distributed, Grid, Mobile, and Pervasive Computing, vol. 1, p. 367, 2007.

[6] G. Padmavathi and D. Shanmugapriya, “A survey of attacks, security mechanisms and challenges in wireless sensor networks," arXiv preprint arXiv: 0909.0576, 2009.

[7] A.Juels, “RFID security and privacy: A research survey," IEEE J. Selected Areas in Communications, vol. 24, no. 2, pp. 381-394, 2006.

[8] J. Westhues, “Hacking the prox card," RFID: Applications, Security, and Privacy,pp. 291-300, 2005.
[9] B. Grobauer, T. Walloschek, and E. Stocker, “ Understanding cloud computing vulnerabilities," IEEE Security Privacy, vol. 9, no. 2, pp. 50-57, Mar. 2011.
[10] Dr. Ch. Ramesh Kumar, Dr. Chalasani Srinivas, "`IOT Home Mechanization Frame work" International Journal of Civil Engineering and Technology, ISSN: 0976-6308 (Print) ISSN: 0976-6316 (Online) JAN 2018, Volume 9, Issue 1, pp. 929-936
[11] Industry 4.0, http://www.bitkom.org/74733.aspx.
[12] Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems (River Publishers Series in Communications) by Ovidiu Vermesan, Petter Friess
[13] A.Mosenia and N. K. Jha, “A comprehensive study of security of Internet of Things," IEEE Trans. Emerging Topics in Computing, DOI:10.1109/TETC.2016.2606384, 7 Sept., 2016.
[14] Y. Cherdantseva and J. Hilton, “A reference model of information assurance & security," in Proc. IEEE Int. Conf. Availability, Reliability and Security, 2013, pp. 546-555.
[15] M.Tanooj Kumar, S.L.Narayana Reddy, B.Katyayini, Sk.Shabana Azmi,” Optimized and secured storage approach for IoT based applications,”, International Journal of Mechanical Engineering and Technology, ISSN 0976-6340, 8(12), (2017).