March - April 2020
ISSN: 0193-4120 Page No. 11209 - 11214

IOT Applications and Techniques to Solve Its Security issue

[1] Sayan Nath, [2] Avijit Mondal , [3] Radha Tamal Goswami , [4] Arnab Das
[1,2,3,4] *Computer Science & Engineering,*
[1] *Techno International Batanagar, West Bengal, India (sayan.nath@tib.edu.in)*
[2] *Research Scholar MAKAUT, West Bengal, India (avijit.mondal@tib.edu.in)*
[3]*Techno International New Town, Kolkata, West Bengal, India (rtgoswami@tict.edu.in)*
[4] *Jis University Kolkata (arnabdaspaper@gmail.com)*

Article Info
Volume 83
Page Number: 11209 - 11214
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 15 April 2020*

Abstract:
The term Internet of Things for the most part alludes to situations where arrange availability and processing capacity stretches out to articles, sensors and ordinary things not typically thought about PCs, permitting these gadgets to create trade and expend information with insignificant human mediation [1]. In this paper we have discussed different communications model and applications of IOT in day to day life. We have also discussed different security challenges of IOT devices and its probable solutions using network security and Endpoint security.

Keywords: *IOT, Sensor, Network security, Endpoint security.*

Introduction:

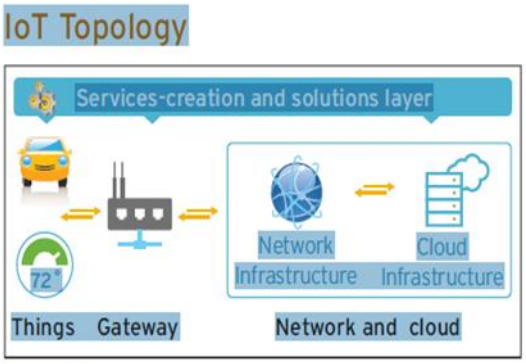


Figure 1

1.**Things:** These are defined as uniquely identifiable nodes, primarily sensors that communicate without human interaction using IP connectivity. There
are millions of IP addressable “things” around us already – from RFID tags to fitness bands – and their numbers are expected to rise exponentially
as sensors become cheaper, smaller and more power-efficient. Morgan Stanley estimates that this number could be as high as 50 billion by 2020, which translates to approximately 6.4 devices for every one of the 8 billion human beings who are expected to be on the Earth at that time[2].

March - April 2020
ISSN: 0193-4120 Page No. 11209 - 11214

2.**Gateways:** These act as intermediaries between things and the cloud to provide the needed Internet connectivity and security.

3.**Network infrastructure:** This is comprised of routers, gateways, repeaters and other devices that control data flow. They also connect to the telecom and cable networks (3G, 4G/LTE) operated by service providers.

4.**Cloud infrastructure:** Cloud infrastructure contains large pools of virtualized servers and storage that are networked together[3]. Supporting the IoT, this infrastructure runs applications that analyze data from devices and sensors in order to generate actionable information used for services and decision-making.

The idea of connecting object to each other and internet is not new, but till IOT is very popular because of the following causes:

Cellular Connectivity— Current 4G LTE innovation offers high transmission capacity of up to 100 megabytes for each second and an enormous scope of in excess of ten kilometers. Unwavering quality and accessibility are likewise acceptable. On the drawback, 4G LTE innovation is related with significant expenses—a few dollars or more for a module contrasted with not exactly a dollar for Wi-Fi. Cell network additionally has high force utilization necessities, making it not exactly perfect for IoT applications, where battery life ought to stretch out over numerous years.

Extraterrestrial Connectivity- This network choice incorporates satellite and other microwave advances. IoT partners by and large use it just when cell and fiber choices are not plausible, since it has the greatest expenses. For example, associations inside national safeguard may utilize satellite network for unmanned automatons. Extraterrestrial alternatives have low-to-medium transfer speed, high range, and medium-to-high unwavering quality and accessibility. Just a couple of businesses depend on extraterrestrial network for IoT applications.

Advances in Data Analytics— IoT examination is the use of information investigation devices and techniques to acknowledge an incentive from the enormous volumes of information created by associated Internet of Things gadgets. ... IoT examination offers comparable advantages for the administration of server farms and different offices, just as retail and social insurance applications.

Ascent of Cloud Computing– for Large Scale IoT Solutions. Web of Things (IoT) produce a tremendous measure of information or enormous information. ... Distributed computing additionally permits information move and capacity through the web or with an immediate connection that empowers continuous information move between gadgets, applications, and cloud.

Settings for IOT Appplications:

Setting	Description	Examples
Factories	Standardized production environments	Operating efficiencies ,optimizing equipment use, inventory
Retail Environments	Spaces where consumer engage in commerce	Store, Bank, Restaurant ,arenas-anywhere consumer consider and buy

March - April 2020
ISSN: 0193-4120 Page No. 11209 - 11214

Vehicles	System inside moving vehicles	Car, trucks, ships, aircraft, Train; Condition based maintenance ,Usage based Design
Cities	Urban Environments	Public spaces and infrastructure in urban settings: adaptive traffic control, smart meters, resource management

Internet of Things Communications Models:

IoT has 4 communication Models:

D-to-D Communications

The D to D correspondence model speaks to at least two devices that can associate and communicate between each other[4]. these gadgets use conventions like Bluetooth, Z-Wave or ZigBee to build up direct gadget to-gadget correspondences, as appeared in Figure 2.

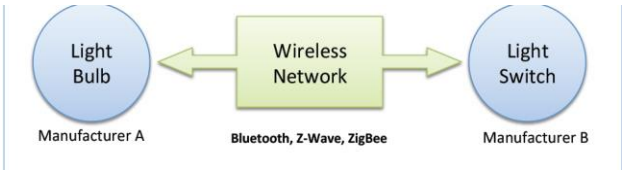


Figure 2

D to-C Communications

In a D to C correspondence version, the Internet of things machine associates directly to an Internet based cloud management(ICM) like an software specialist company to alternate records . This technique plenty of the time exploits existing interchanges structures like normal IEEE802.3 or IEEE802.11 institutions with combined with electronic media with IP address to put connectivity with cloud, which in the end interfaces with the cloud authority in figure 3.

Figure 3

D to-G Model

In the D to G model, Internet of things gadgets fundamentally interface with a middle person gadget to get to a cloud administration. This model regularly includes application based programming working on a neighbourhood passage devices (like a cell phone or a "centre point") that goes about as a delegate between an IoT gadget and a cloud administration. The model is showed up in Figure 4.

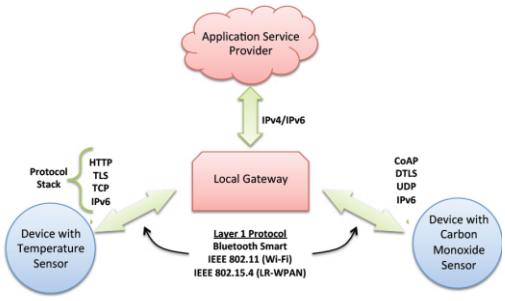


Figure 4

Issues are raised by the Internet of Things :

March - April 2020
ISSN: 0193-4120 Page No. 11209 - 11214

Security cases

Attack Name	Story	Resource	Date
Car recall	Chrysler recalled 1.4 million hackable cars in July, 2015	CNN News	July 24, 2015
Lizard Stressor	An attack online service hosted in Bosnia. It can convert homes and commercial routers into a zombie horde.	An online article	Jan 2015
	First wide-scale hack involving television sets and at least one refrigerator ☺. 750,000 spams were sent.	Proofpoint	Jan,2014
Linux.Darlloz	Discovered a worm for devices running Linux .	Symantec	Nov, 2013
Hacked Camera	A hacker was able to shout abuse at a two-year-old child by exploiting a vulnerability in a camera advertised as an ideal "baby monitor".	ABC News	Aug, 2013

Figure 5
Unique Security Challenges of IoT Devices

1. Secure constrained devices
2. Authorize and authenticate devices
3. Manage device updates
4. Secure communication
5. Ensure data privacy and integrity
6. Secure web, mobile, and cloud applications
7. Ensure high availability
8. Prevent incidents by detecting vulnerabilities
9. Manage vulnerabilities
10. Predict and preempt security issues

Various IoT contraptions are intentionally organized with no ability to be overhauled, or the update methodology is counter-intuitive.

Various IoT contraptions work in a manner where the customer has a long side zero certified detectable quality into within the elements of the device or the specific data streams they produce. This makes a security frailty when a customer acknowledges an IoT device is playing out explicit limits, when truth be told it might be performing unwanted limits or assembling a bigger number of data than the customer plans.

Some IoT devices, similarly as other biological sensors, are proposed to be straightforwardly embedded in the earth, where a customer doesn't adequately observe the device nor screen its working status. A security break may drive forward for a long time before being seen and cured if update or balance is even possible or down to business. So additionally, the customer presumably won't realize that a sensor exists in his/her condition, conceivably allowing a security break to proceed for broad stretches without distinguishing proof.

IOT Security Solution:

In IoT we have two types of security.

1. Endpoint security

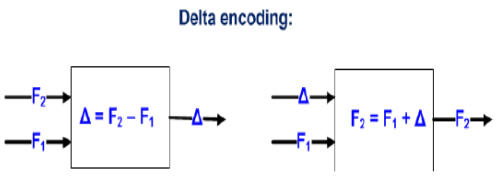
2. Network security

1. Endpoint security:-

Endpoint security includes vulnerability and patch management.

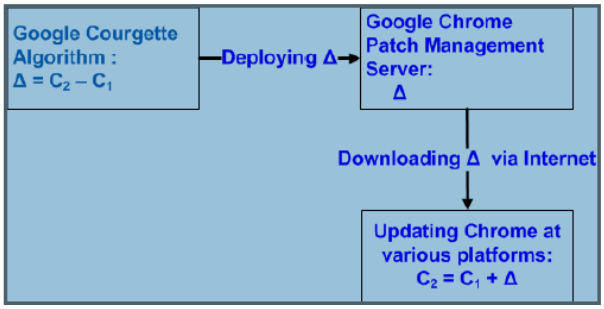
Vulnerability and patch management with FOTA(Firmware Over The Air)-

FOTA is a technology developed for updating the firmware of mobile phones due to software bug fixes. It uses delta encoding technique to reduce the patch size. Delta encoding can be shown as fig 6.



Delta encoding is used for software vulnerability management. A significant example is Google Chrome software updating powered by an efficient delta coding algorithm Courgette. Here we can use the same concept for IoT device security also.

March - April 2020
ISSN: 0193-4120 Page No. 11209 - 11214



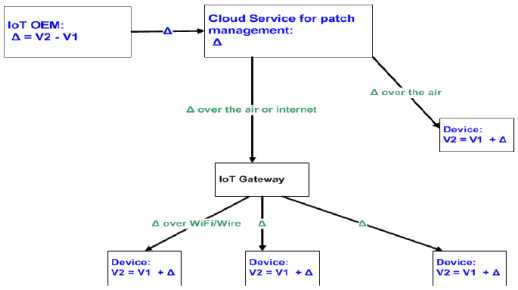
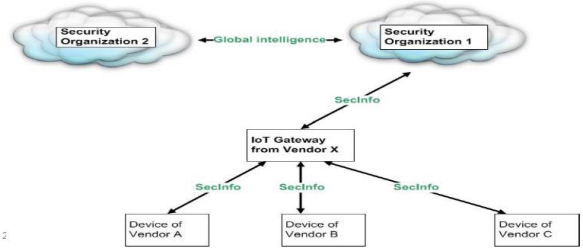


Figure 7 **FOTA for IoT security for general devices**

2**. Network security:-**

To provide network security we need some protocol like OpenIOC, CybOX, IODEF[7].OpenIOC is used by an Organization to exchange security information. Security information is a piece of information that can be used to search for or identify potentially compromised systems. Examples are IP address/domain name,URL, Email Address,HTTP user agent etc. These 3 protocol can be more useful in the era of IoT security if we connect the network in the following order.



Conclusion:

IoT addresses a developing bit of how individuals and establishments are apparently going to cooperate with and join the Internet and structure sort out into their own, social, and money related lives. Answers for expanding the upsides of IoT while confining the dangers won't be found by participating in a pleased discussion that pits the affirmations of IoT against its idle limit dangers. Or then again maybe, it will take showed obligation, talk, and cooperation over a degree of accessories to plot the best ways forward.

References:

1. 1 For more information on IoT as it relates with those with disabilities see for example: Valerio, Pablo. “Google: IoT Can Help The Disabled.” *InformationWeek*, March 10, 2015. http://www.informationweek.com/mobile/mobile-devices/google-iot-can-help-thedisabled/ a/d-id/1319404; and, Domingo, Mari Carmen. “An Overview of the Internet of Things for People with Disabilities.” *Journal of Network and Computer Applications* 35, no. 2 (March 2012): 584–96. doi:10.1016/j.jnca.2011.10.015.
2. 44 “Meet the Nest Thermostat | Nest.” Nest Labs. Web. 31 Aug. 2015. https://nest.com/thermostat/meet-nest-thermostat/
3. “Samsung Privacy Policy--SmartTV Supplement.” Samsung Corp. Web. 29 Sept. 2015. http://www.samsung.com/sg/info/privacy/smarttv.html
4. Thierer, Adam, and Andrea Castillo. “Projecting the Growth and Economic Impact of The Internet of Things.” George Mason University, Mercatus Center, June 15, 2015. http://mercatus.org/sites/default/files/IoT-EP-v3.pdf

March - April 2020
ISSN: 0193-4120 Page No. 11209 - 11214

5. Greenberg, Andy. “Hackers Remotely Kill a Jeep on the Highway—With Me in It.” *WIRED*, July 21, 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
6. “Samsung Smart TV’s Voice Recognition Creates Privacy Concerns.” *CBS This Morning*. CBS News, February 10, 2015.
7. http://www.cbsnews.com/videos/samsung-smart-tvs-voice-recognition-creates-privacy-concerns/
8. 7. Bradbury, Danny. “How Can Privacy Survive in the Era of the Internet of Things?” *The Guardian*, April 7, 2015, sec. Technology.
9. http://www.theguardian.com/technology/2015/apr/07/how-can-privacy-survive-the-internet-of-things