Review paper: Internet of Things environment

[1]Hiteshkumar Parmar, [2]Dr. Shailesh. D. Panchal, [3]Deepak Upadhyay
[1]M.E cyber security, [2]Associate Professor, [3]Assistant Professor
[1]M.E cyber security
[1]GTU –School of Engineering and Technology, Gandhinagar, India

Abstract

When we are moving from traditional life style to smart life style, we use smart objects rather than the ordinary objects such as smart TV, smart AC, smart watch, smart mobile and what not. These smart devices either based on IoT or Not. It is not necessary that each and every smart devices are based on IoT. So differentiate the Smart devices are made with the IoT technology or not, this paper will help to identify the smart devices are made within the IoT. This survey paper also shows information of the IoT environment, IoT network, and Different parameter of IoT and security issue in IoT environment. Environment means whatever surrounding of us such as soil, trees, animals etc. IoT environment is a similar to ordinary Environment because how the different objects of environment are interrelated to each other like vise in IoT environment different object are interconnected to each other too. In this survey paper I also focus on role of cyber security in IoT environment.

Keywords: cyber security, vulnerability, attacks, Fog Computing, Cloud Computing

1. Introduction

When the term IoT(Internet of Things) comes in your mind then ,we have lots of thing running together like Hardware, software, sensors, actuators, Embedded system, Huge storage device (Cloud storage) etc. These all component are interconnected to each other to make IoT environment. In internet of things environment we have IoT network, IoT devices, Protocols for communications, IoT storage device and security module to protect this IoT environment. How all these component are communicate each other and how they all are interrelated to each other? We shall deeply study in this proposed work. Now a days term “smart” introduced itself everywhere. Smart means intelligent enough to analyze, computing and concluding. The smart devices has huge market share globally. Today we have wearable Smart devices, industrial smart devices, Health Care smart devices, Agriculture smart devices, Disaster Management smart devices etc. In this survey paper we focused on IoT environment and its different parameter.

Cyber Security play vital role to protect the IoT environment. Few past year ago we moved ourselves from offline to online, now our mostly work based on internet. We are buying, selling, auctioning, and doing the different business from our home or our office with the others globally. And we rapidly move ourselves from online to smart device users. Today we have smart TV, smart Fridge, and smartwashing machine. But are they belonging to IoT? The answer is “No”.

To justify the smart devices are based on IoT we should gone through the all parameter of IoT. We should study the IoT environment.If we make any smart devices then that device must have to intelligent enough to perform its functionality. While we are talking about the IoT devices, those devices are intelligent enough to perform its functionality. But security issue arise in very vast area in IoT. IoT suffered from different vulnerability, attacks, problem regarding physical security, energy management and privacy.To solve the problems regarding security and privacy done through the Cyber security. Cyber security is an art or science to protect or overcome damages against the cyber-attack such as credit card fraud, salami attack, DOS attack, DDOS attack, man in the middle attack etc. Cyber Security built platform for us to protect ourselves over the cyber spaces. Before going to justify the role of cyber security for IoT environment, we focused on IoT environment.

1.1 Internet of Things

IoT(Internet of Things), all devices interact, collaborate and share experiences and also reducing the human interference in their module. Internet of Things is the platform where intelligent device are connected to the internet. Kevin Ashton is the inventor of Internet of Things, who had invented IoT in 20 January, 1999.since the time IoT has solved a lot of problems such as disaster management, traffic nuisance, health care etc. With help of IoT we have smart villages, smart cities, smart health care devices, water quality monitor devices, smart farms.

1.1.1 Definition

- Internet mean inter connected network and Things mean the object which are smart enough to use the internet in very appropriate way.– Internet of Things, "Group of infrastructures interconnecting connected objects and allowing their management, data mining and the access to the data they generate."[1][2][3]

1.1.2 IoT Architecture

IoT architecture can be classified in following way

- Three layer architecture
- Five layer architecture
- Cloud based architecture
- Fog computing based architecture

- Three layer architecture

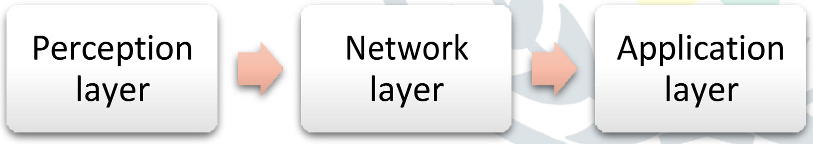

Figure 1: Three layer architecture

Application layer: delivering the application specific service to the users

Network layer: Connecting the smart things, network device and server. And also transmitting processing sensor data.

Perception layer: Sensors sense and gathered the information about appropriate subject. Senses physical parameter, identifies other objects in the environment.

- Five layer architecture

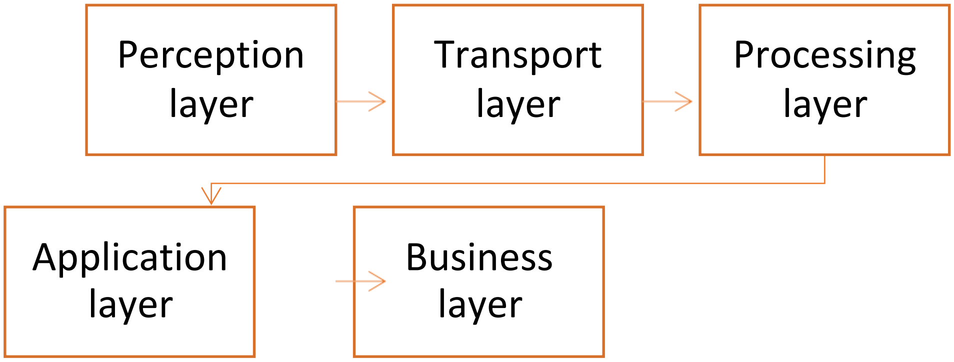

Figure 2: Five layer architecture

Business layer: It manage whole IoT system including application, business & profit module and user privacy.

Application layer: Delivering the application specific service to the users.

Processing layer: Store, analyses and process huge amount of data such as cloud computing.

Transport layer: Transport sensor data between layer through network like RFID, Bluetooth, and NFC.

Perception layer: Senses and gather information.

- Cloud based architecture

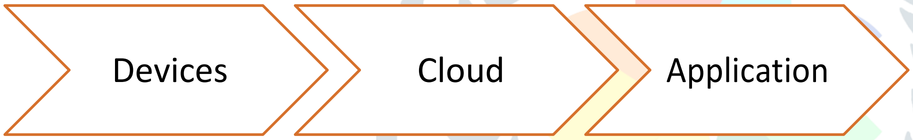

Figure 3: Cloud based architecture

Cloud – centric architecture keeps the cloud at the center application above it and the network of smart things below it. Data processing is done in large centralized method on cloud.

- Fog computing based architecture

Fog architecture present monitoring layer, pre-processing layer, storage layer and security layer between the physical layer and transport layers.

Transport layer
Security layer
Storage layer
Pre-processing layer
Monitoring layer
Physical layer

Monitoring layer: monitor layer monitors power, resources and the services

Pre-processing layer: Filtering, analyses and processing of sensor data take place here. Storage layer: Provide storage functionality.

Security: perform encryption/decryption to maintain integrity and privacy.

1.1.3 IoT Application

- Infrastructure application: Monitoring and controlling operation of sustainable urban and rural infrastructure.
- Agriculture application: water quality, soil quality, temperature etc. monitoring and controlling. Even automated farming techniques introduced itself.
- Environmental application: environmental protection by monitoring air or water quality, monitoring wild-life, prediction about earthquake or tsunami.
- Medical and health care application: remote health monitoring, emergency notification system. Even smart beds for patient, remotely measures heart rate or blood pressure.
- Energy management application: Power controlling and balancing. Remotely operate devices like AC, Fan, Lights even regulate them from remote place.

1.1.4 IoT Protocol

Messaging protocols: XMPP, CoAP, MQTT

Protocol	**MQTT**	**CoAP**	**XMPP**
XML based	No	No	Yes(Message oriented middleware)
TCP/UDP	TCP	UDP	TCP
IPV6/IPV4	Both	Both	Both
Messaging	Publish/Subscribe Request/Response	Request/Response	Publish/Subscribe Request/Response
Uses	From pervasive devices to a server/small message broker.	Simple electronic devices, Resource constrained devices.	Video, File transfer, gaming, IoT apps & social networking services.

Transport protocols: TCP- provide acknowledgment facilities across the network for TCP segment, and UDP-lightweight transport mechanism for connectionless communication.

Network protocols: 6LoWPAN-It provide wireless Internet connectivity at lower data rates. It is based on IPv6.

Data link and Physical protocols: IEEE 802.15.4-It is used for low-power or low-speed environment.

Frequency range	**915 MHZ**
Data rates	250 kb/s
Communication range	10 meters

1.1.4 IoT component

- Sensors
- Networks

- Standards
- Intelligent Analysis
- Intelligent Actions

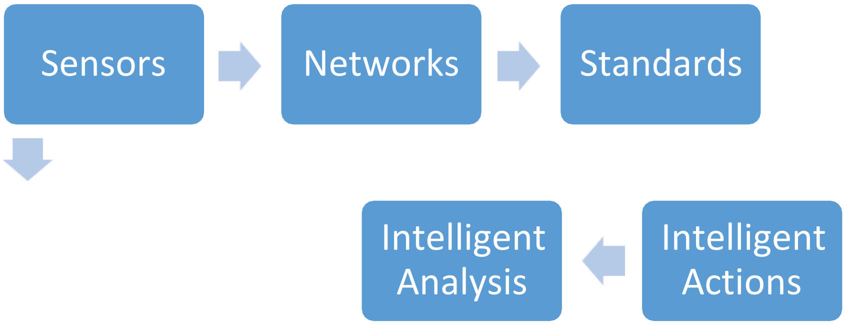

Figure 4: IoT component

- Sensors: According to (IEEE) sensors can be defined as: An electronic device that produces electrical, optical, or digital data derived from a physical condition or event. Sensor is intelligent electronic device which is used to take input the data of environment for further process and also used for giving output (information) as well. Sensor should be cheaper, smarter and smaller.
- Network: whatever the input getting from sensor further process take place in the network. The network can be classified as WAN, MAN & LAN. The network includes routers, bridge and topologies. The network connect different part of network to the sensors using different technologies such as Bluetooth, Wi-Fi and Ethernet.
- Standards:This is the third stage where the implementation process includes the sum of all activities of handling, processing and storing the data collected from the sensors.
- Intelligent Analysis: The analyses take place in the stage of implementation. The term artificial intelligent introduced itself for the computing.
- Intelligent Actions: In this stage different factor like deep learning, machine functionality improvement and machine influence to human action so on.

1.1.4 Issue of IoT

Instead of mobile and computer due to IoT now each and every devices are now free to connect itself to the internet. [1]We get smart devices but vulnerabilities also increase like below.[1] Device Cloning, Sensitive Data Exposure, Denial of Service and Unauthorized Access or Control.In IoT Network each and every node can communicate with each other, thus there will be probability for malicious node too. [8] Malicious node uses high bandwidth. [9] While we are talking about IoT Environment mainly we have three major problem we have to facedReal Time, Energy and Security.

1.1.5 Role of cyber security for IoT

Before going to take a look on role of cyber security we should understand the cyber security. The platform where the cyber spaces can be protected from its threat, overcome the weaknesses, exploit the vulnerability so on. To provide the security to any domain. We have to achieve security goal which is based on CIA model.

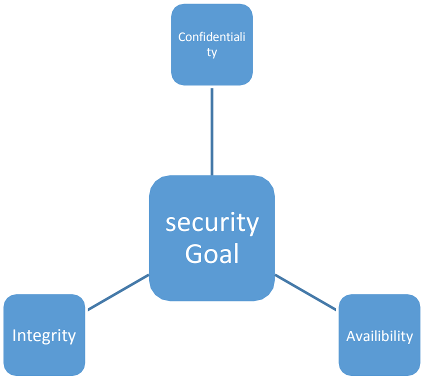

Figure 5: CIA Model

- Confidentiality: It is based on secrecy. Here message can be protected from the attacker.
- Integrity: It mean message can't be manipulate while travelling.
- Availability: It means resources should be available for all authorized person.

In cyber security ethical Hacker trying reach the security goal to provide security to various platform like IoT, Cloud computing and Data Mining. Some term should be understand as below when we are dealing with the cyber security.

- Vulnerability: A vulnerability is an exploitable weakness in system or in its design such as SQL injection, Buffer overflow, XSS (cross site scripting).
- Threat: A potential danger to an asset such as intrusion.
- Attack: To compromised system using vulnerability such as DOS attack.

Some important Tools for IoT

Contiki OS: It supports IPv6 and IPv4,CoAP, RPL and 6LOWPAN. Contiki is an open source, high portable and multi-tasking operating system. It is used for memory efficient, networked embedded systems and wireless sensor networks. Contiki has been used in a variety of projects from road tunnel fire monitoring, intrusion detection, network monitoring.

Cooja tool: Cooja is an emulator, emulator means a system that typically enables the host system to run software or use peripheral devices designed for the guest system: e.g.cooja enabling your laptop to run the RPL protocol, LIBP and/or other IoT protocol of interest.

Snort tool: Snort is an open-source, free and lightweight network intrusion detection system (NIDS) software for Linux and Windows to detect emerging threats. Snort multipurpose tool which is used for packet Logger, Sniffer, Forensic Data analysis tool and Network Intrusion Detection System.

Wireshark tool: It is packet analyzer tools. Wireshark monitor the network traffic.

2. Literature Review

1. Secure integration of IoT and Cloud computing 2016 Elsevier in this paper I learnt IoT problems from 2010 to 2016 , cloud computing and security issue in IoT and Cloud computing
2. Remote security management server for IoT Devices ICTC 2017, IEEE 2017 in this paper I learnt Device cloning attacks protection and Sensitive data exposure protection.
3. Block chain: A Game Changer for Securing IoT Data,I learnt from this paper about the block chain,and its

various component,about itspillars,and it's provide data security in IoT.Decentralize Autonomous Organization (DAO) the combination of AI and IoT environment.

4. Identifying Malicious Nodes in Multihop IoT Networks using Diversity and Unsupervised Learning,2018 IEEE,I learnt from this paper are In IoT Network each and every node can communicate with each other, thus there will be probability for malicious node too.

5. Malicious node detection system using hash chains approach in IoT based sensor networks. Malicious node uses high bandwidth, 2017.Journal of Advance Research in Dynamic & control Systems in this paper I got idea about attacks.There are mainly two types of attack using malicious nodePassive Attack & Active Attack.

6. Secure,Resilient, and Self configuring Fog Architecture for Untrustworthy IoT Environments, 20198 IEEE.In this paper I learnt about fog computing which provides security to the cloud.

7. Secure integration of IoT and Cloud Computing, Christosstergiou,Kostas E. psannis,Byung-GyyKim,Brij Gupta, future generation -2016.I learnt from this paper about IoT security Model.
8. Brain Russell, Drew van Duren, Practical internet of Things Security, 1st ed., Packt Publishing. I learnt from this book a lot from definition of IoT to all parameter of IoT and security parameter of IoT and cryptography technique.

3. Limitations

- In IoT Network each and every node can communicate with each other, thus there will be probability for malicious node too. [8]
- Malicious node uses high bandwidth. [9]
- Denial of Service attack is remain security issue.[1]
- Unauthorized Access or Control also remain security issue. [1]

4. Conclusions and possible future work

Internet of Things (IoT) is now in its initial stage. As we know each and every node in IoT environment are connected to each other for communication, the number of vulnerability take place to compromise the system of IoT environment. Till now IoT environment suffered from lots of attack such as Device Cloning, Sensitive Data Exposure, Denial of Service and Unauthorized Access or Control among these Device Cloning, Sensitive Data Exposure are mitigate other are still in working progress.

5. Acknowledgement

I am thankful to GTU PG school of Engineering and Technology, Gandhinagar to provide me great facilities, and my guide Prof. Deepak Upadhyay.

References

[1] Swapnil Naik, Vikas Maral(May 19-20, 2017)." Cyber Security – IoT." 2017 2nd IEEE International Conference on Recent Trends in Electronics Information & Communication Technology (RTEICT), India

[2] Madhusudan Singh, Abhiraj Singh, Shiho Kim ()." Block chain: A Game Changer for Securing IoT

Data.”

[3] Bruno Dorsemaine, Jean-Philippe Gaudier, Jean-Philippe Wary, Nizar Kheir, Pascal Urien(2015).” Internet of Things: a definition & taxonomy”, 978-1-4799-8660-6/15 $31.00
© 2015 IEEE DOI 10.1109/NGMAST.2015.71

[4] Mark S. Merkow, Jim Breithaupt (Jun 4, 2014). “Information Security: Principles and Practices, 2nd Edition. “

[5] Boheung Chung, Jeongyeo Kim, and Young sung Jeon. „On-demand security configuration for IoT devices”

[6] Mostafa Kahla, Mohamed Azab, Ahmed Mansour (2018). “Secure,Resilient,andSelf-configuringFogArchitectureforUntrustworthyIoT Environments”. 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering

[7] Seungyong yoon, JeongnyeoKim.”Remote security management server for IoT Devices”.TCTC-2017.Pade No.1162-1164

[8] Xin Liu, Mai Abdelhakim, Prashant Krishnamurthy , David Tipper “Identifying Malicious Nodes in Multihop IoT Networks using Diversity and Unsupervised Learning”. 978-1-5386-3180-5/18/$31.00 ©2018 IEEE

[9] Dr.T.Sasilatha, Balaji, P.Suresh Mohan Kumar(2017).” MALICIOUS NODE DETECTION SYSTEM USING HASH CHAINS APPROACH IN IOT BASED SENSOR NETWORKS”.Journal of Advance Research in Dynamic & control Systems.ISSN 1943- 023x Pages: 501 – 513

[10] Brain Russell, Drew van Duren, “Practical internet of Things Security”, 1st ed., Packt Publishing.

[11] Christos Stergious, Kosatas E. Psannis, Byung-Gyu Kim, Brij Gupta “Secure integration of IoT and Cloud computing” Elsevier 2016.