International Journal of Latest Trends in Engineering and Technology
Vol.(12)Issue(4), pp.019-024
DOI: http://dx.doi.org/10.21172/1.124.05
e-ISSN:2278-621X

THE INTERNET OF THINGS:AN OVERVIEW OF THE AWARENESS, ARCHITECTURE & APPLICATION

Mayank Gupta[1], Sunil K. Singh[2]

Abstract- Internet of Things or IoT is the interconnection of smart devices that make use of sensors and actuators to perform highly specified tasks. It stands at the juncture of Embedded Systems and Transport and has gained quite a traction in the past few years due to the increased popularity of mobile devices and that coupled with efficient big data analytics that procures data and this data can be remotely monitored, as they are connected to a common network. This has allowed Internet of Things to delve into spaces such as Home Automation, Energy Optimization Healthcare etc. This Paper aims to summarize these by giving a brief introduction and thus acting as a Gateway into the world the world of IoT by discussing the architecture, uses as well as various prospects of the same. We also discuss the Security threats and vulnerabilities that it currently faces. The Section I deals with the Introduction and Goals, Section II covers the Architecture and Models and Section III covers the Application, Security and Future Prospects.

Keywords - Internet of Things, Smart Device, Device to Device Communication, IoT Challenges, Communication Model, Embedded Systems

1. INTRODUCTION

Internet of things can be classified as the interconnectivity of devices to perform specific tasks by making use of tools like computer software, mobile applications etc and executing these tasks through a variety of electronics devices like actuators, sensors, and motors. It lies at the juncture of Networking and Embedded Systems. The IIoT or the Industrial Internet of Things has also benefited from this as we are seeing the implementation of the Internet of Things which has led to optimizations well as increased efficiency in the industry. Each device may not individually possess an IP address, but the gateway through which they communicate will always possess one.

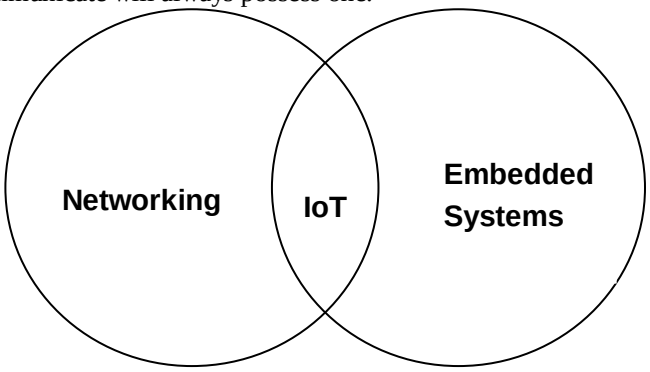

Fig 1.1: IoT at the juncture of Embedded Systems and Networking

1.1 Objectives of IoT

The primary objective of implementing the Internet of Things is to be able to connect devices that earlier used to be operated in isolation to achieve small-scale tasks and now utilizing their connectivity and databases to be able to automate, collect and share data and improve the efficiency and accuracy in our day to day life.

1.2 How to classify a device as an IoT?

A device may be connected to the internet and may still not be an IoT device. Here is a list of features that can be used to identify any such device.

The first and most fundamental trait is that these devices are either connected directly to a server on the internet or through interconnectivity on a local network.

These devices are controlled by either a small MCU or a CPU.

They may have data that is uploaded to a web server and is processed on the server itself.

[1] UG Scholar, Shiv Nadar University, Greater Noida, UP

[2] CSE Department, Chandigarh College of Engineering & Technology, Chandigarh

1.3 Impact of IoT

IoT has had an impact on the way that we have been interacting with our surroundings as it has improved efficiency by improving quality of life, bringing down wastage as well as helping us form demographics in areas earlier inaccessible. Also, this had led to an acceleration in the development of newer cost-effective MCU Units.

1.4 Literature Review

There have been many unique applications as well as advances in the sector in terms of innovation, newer models etc.For example, in the paper "Research on the architecture of Internet of things"1, the authors propose a new architecture model, a 5 level architecture that consists of the already existing Perception, Transport and Application Layer and in addition a Processing Layer, which deals with the storage and analyses of the data collected by the Perception Layer & the Business Layer, which includes the business model of the IoT device as well as the management of the same.Also, in the paper "Recent advancements in the Internet-of-Things related standards: A oneM2M perspective"2, there is a description of oneM2M that would enable devices that are from different vendors to interact with each other on a common network.

Artificial Intelligence has played a great role in the development of IoT devices. In "Application of Artificial Intelligence in Internet of Things"3, the authors make use of neural networks as well as fuzzy logic in place of already prevalent algorithms.In the Paper, "Smart Waste Management using Internet-of-Things" 4, the authors have a proposal model wherein the level of waste in a dustbin would be stored and sent to the server and according to the level of garbage, the route of the garbage trucks would be decided.

With respect to microcontrollers, in "Application for integrating microcontrollers to the Internet of Things", the authors propose a uniform model for a web application, compatible across all microcontroller which will allow the user to control them remotely using a UI that the user designs.5

2. AWARENESS AND TRENDS

2.1 Trends of IoT

IoT has been in existence since 1982. The first IoT device was conceived when Computer ScienceGraduate students in the Carnegie Mellon University decided to connect their local Coke machine to the APRANET, which enabled a user to check the temperature as well as the quantity of stocks left. Internet of Things has undergone a lot of changes since then, the chronology of which is as below in figure 2.1.

Gartner Technology Hype cycle, is a graphical representation of the acceptability, application and the growth of prospering technologies. Below is a the Gartner Technology Hype Cycle for IoT in comparison with recent technologies as shown in figure 2.2.

The introduction of IoT has inculcated a variety of trends in the market, some of these as follows:

Increase in no of Mobile devices- Due to these devices being applied in sectors such as healthcare there is increased no of MCU being used and this has led to an increase in no of active devices in these fields.

Development of Mobile Application- Since in many of these devices we see that they are connected to our Mobile Phones, there has been a bump in the no of Mobile Applications.

Security- Due to the security vulnerabilities, there is extensive research in the field of security to make the data as well as communication of these devices more secure.

Big Data Analytics-There is a generation of 2.5 Quintillions of Data everyday9, IoT is one of the many core contributors to that data being generated.

Automation-The automation sector too has gained a good boom by the introduction of various sensors, motors etc. Coupled with Machine Learning they are able to perform a variety of tasks in sectors such as Home Automation, Industrial Automation, and even Smart Cars.

3. ARCHITECTURE AND MODEL

3.1 Layers of IoT

Though there is no formally defined convention to be followed, but it is widely accepted that IoT is divided into 3 OSI Layers:

Perception Layer - We are already familiar with the Application Layer as well as the Network Layer, but with the addition of the newer input mechanisms like sensors and actuators we are introduced to a new category, the Perception layer. This Layer is used to define operations of the sensors, actuators as well as other devices that in conjunction are responsible for gathering information from the surroundings so that the data can be compared or processed.

Network Layer- Network Layer is the one that is responsible for transporting the data obtained from the Perception Layer and processing that data through the network. So it coordinates between the different network by providing a channel for the same.

Application Layer- The Application Layer is the one that interacts with the user directly which acts according to the demand of the industry. This includes application protocols like HTTP etc.

Communication Models for IoT10

3.2 Device to Device Communication Model

In this Model, these devices do not have an intermediary between them and have a direct communication link between them. Most of these devices do not possess a sophisticated communication equipment to support a direct link to the cloud and thus they are connected by simpler modes as shown in figure 3.1. Examples include Bluetooth modules, Zigbee, NFC Tags etc.The limitations of this kind of model are that the range of these devices are very limited and they only act in close proximity.

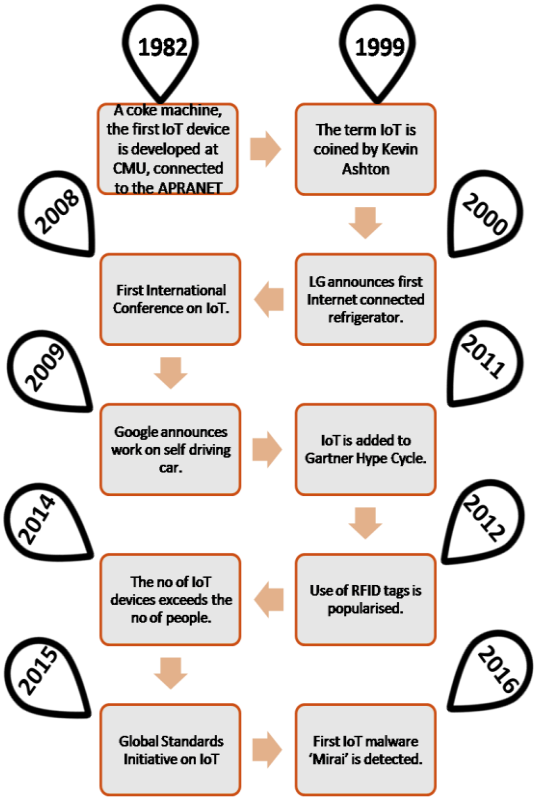

Fig 2.1 Timeline of the Internet of Things7

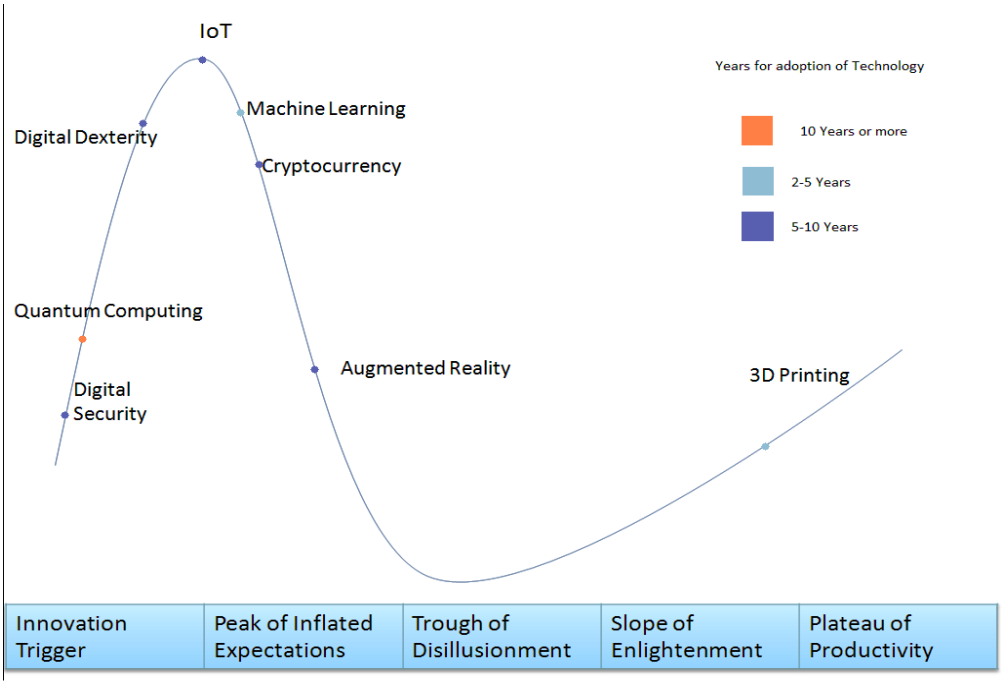

Fig 2.2 Gartner Technology Hype Cycle8

Fig 3.1 Device to Device Communication Model

3.3. Device to Cloud Communication Model

In this kind of Model, there is a parent server (a cloud server) that the device is connected to and continually sharesdata collected from the sensors, actuators etc over established means of data transfer namely Wi-Fi, LAN etc.The ASP by means of other communication protocols makes these contact with sensors and other output devices. Since it is connected to the internet, they can be remotely accessed by other network connections to the cloud server as shown in figure 3.2.

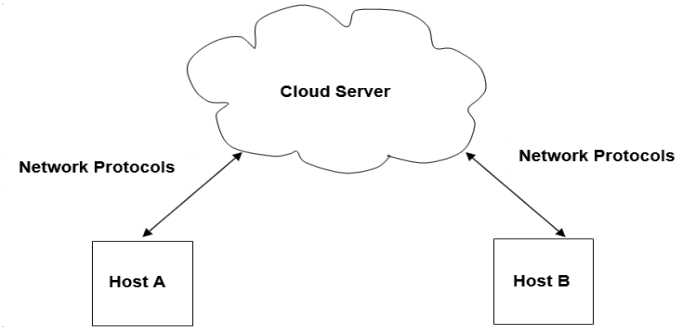

Fig 3.2 Device to Cloud Communication Model

3.4. Device to Gateway Model

In this Model, the device again needs to be connected to the Cloud Server but in this case, there is an application layer-gateway or an ALG between them. ALG uses TCP/UDP and allows for a more secure form of communication and allows the device individual access to the Server which would otherwise have been inaccessible to it. Also, the ALG helps to allow communication by translating protocols as the device and server may be communicating using different communication protocols at their endas shown in figure 3.3.

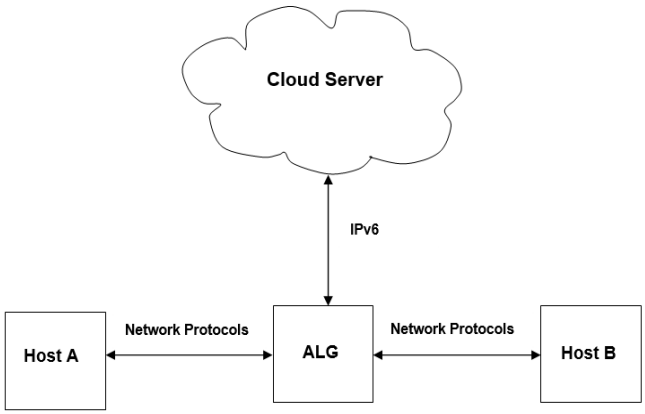

Fig 3.3 Device to Gateway Model

3.5. Back-End Data Sharing Model

As the name suggests, the Back-End Data Sharing Model is based on uploading the Data collected from the user to a third party or an external source to make an analysis on the data or for research purposes. It also allows for the data to be more accessible as well as transferableas shown in figure 3.4.

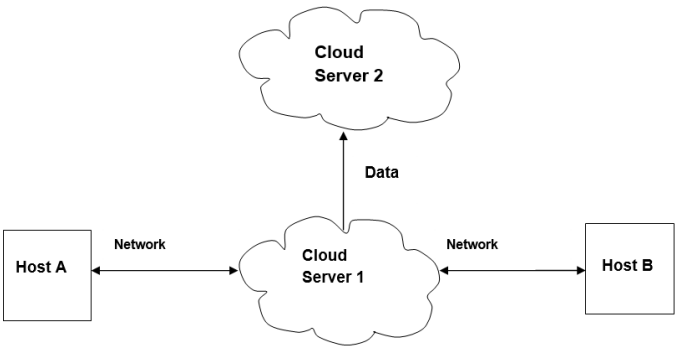

Fig 3.4 Back-End Data Sharing Model

4. APPLICATIONS, CHALLENGES AND SECURITY

4.1 Application of IoT

The use of IoT is spread to a lot of sectors where there is a need for data accumulation, automation, and monitoring.
But if we were to figuratively break it down to fundamental uses, some of those would be:-
Warehouse Management System - One of the key sectors that have benefited from the use of IoT have been warehouses. Warehouses used by Amazon have been able to completely eliminate the deployment of a human being on premises by maintaining an online database inventory system as well by using robotics to automate the same.11
Biomedical Monitoring and diagnosis- The shrinking size of microprocessors has enabled us to be able to deploy them in the field where we require these microchips to treat patients more effectively and also monitor their movements.
Wearable Technology- Wearable Technology is an ever-evolving sector which again makes use of microchips as well as data acquisition to increase the productivity of the user and increase usability.
Smart Grids- Considering the energy crisis we are facing in today's time, it has become increasingly important to have an integrated solution that would monitor and regulate our electricity usage and Smart Grid is a very optimum application for that. It makes use of wireless communication devices connected to a control unit to identify and distribute the optimum requirements, usage as minimizing electricity wastage.
Smart Homes- Home Automation is of the most upcoming fields and at the backbone of it is IoT. The Devices are able to control everything from security to automatic lighting and control of fans to more luxury tasks like mood lighting.
Driverless Vehicles- Considering the wide variety of sensors as well as data processing required to develop and run a driverless vehicle. IoT is propelling it forward by using the communication to actually improve driving in real time.
Agriculture and Farming- Considering the wide array of sensors at the disposal namely, moisture, soil, pH as well as other multispectral sensors farming and other agricultural activities have revolutionized. The monitoring and analysis have allowed for the replenishment of soil as well increase the crop yield.12

4.2 Challenges:

Security- The Primary Risk that these devices face is Security. Since due to the size as well as usability, these devices are powered by low power microcontrollers that do not have very sophisticated communication protocols and can easily be manipulated to shut down or malfunction or even account enumeration.
Data Risks-In addition to the security risk to the devices, since they collect and store a lot of data that is on the cloud is exposed if a cloud hack takes place, the data of several of millions of users can be disclosed.
Connectivity- In absence of a connection to a server, most of these devices may not be functional at their full capabilities and this may be tackled by establishing a local connection for these devices but then the data exchange and processing is not as effective.
Limited Processing Power -Since these devices have relatively limited capabilities we face trouble applying complex Machine Learning Algorithms or AI on these devices. Also, as we are currently edging towards physical limitations in terms of Semiconductors we are required to deploy AI to improve performance and accuracy.
Power- Since each is an individual unit, they need to have an individual power supply. Also, due to complex algorithms and high power processors, there is a need to have a sustainable energy supply for the same.13

4.3 Security:

Due to these devices being employed in limited capacities, they possess low computing power and memory and are not very high-end devices. These close the horizons of using most of the general protocols for security like anti-viruses, firewalls.15 Also, layered network security cannot be deployed due to the risk of the hardware being compromised. This turns these devices most vulnerable to security threats. In addition to that since these devices are continually accumulating data and storing them on servers, this data is also vulnerable to attacks. Figure 4.1 described the DCE Model as defined by the ITU.

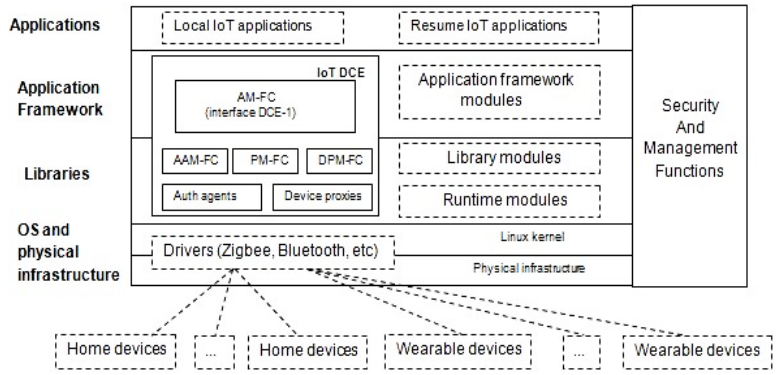

Figure 4.1 IoT DCE Model as mentioned in Rec. ITU-T Y.4115 (04/2017) Pg 18 14

4.4 Ways to counter security breaches

Password Protection- Always use password protection while connecting to an IoT device.

Authentication- In addition to password protection, using a multifactor authentication or an MFA as used by AWS is a good way to ensure security.

Updating the firmware- Updating the system to scan for new and enhanced threats is important to keep away.

Data Encryption- To secure data Secure Sockets Layer (SSL) protocol should be deployed in which only the receiver has a private key, with which they can access the data sent through the public key.

Limited Control- By allowing the IoT to device access to only a limited no of resources that it requires to complete its function, and in an event of an external attack they do not have complete control over the device.16

5. CONCLUSION

According to a Research by Statista 6, we can expect to have around 75 Billion IoT Devices installed worldwide by 2025. This will include sectors already having IoT like healthcare, automation, and agriculture to sectors such as administration, marketplaces as well as business processes.

Also, with the recent advancements in the sectors of Machine Learning and AI, which will provide integrated solutions to minimize operation costs, improve accuracy and give a more personalized experience.

The recent introduction of LiFi17 which relies on a light source for it to transfer data at a higher bandwidth compared to a Wi-Fi is also gaining steam in this progress as it may allow for a quantum leap in the ever-evolving fields of IoT.

6. REFERENCES

[1] Miao Wu, Ting-lie Lu, Fei-Yang Ling, ling Sun, Hui-Ying Du,"Research on the architecture of Internet of things". 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE),2010

[2] HyuncheolPark,Hoichang,KimHotaekJoo,JaeSeungSong,"Recent advancements in the Internet-of-Things related standards: A oneM2M perspective",ICT Express Volume 2, Issue 3, September 2016, Pages 126-129

[3] AbdulhafisAbdulazeezOsuwa,Esosa Blessing Ekhoragbon,Lai Tian Fat,"Application of Artificial Intelligence in Internet of Things",9th International Conference on Computational Intelligence and Communication Networks 2017.

[4] Gopal KirshnaShyam, Sunilkumar S. Manvi, Priyanka Bharti,Smart Waste Management using Internet-of-Things (IoT),Second International Conference On Computing and Communications Technologies, 2017.

[5] Syed MarufulHuq,M.Ashikur Rahman, Sabbir M. Saleh,"Application for Integrating Microcontrollers to Internet of Things",2017 20th International Conference on Computer and Information Technology (ICCIT), 22-24 December, 2017

[6] https://www.statista.com/topics/2637/internet-of-things/, October 2018

[7] https://hqsoftwarelab.com/about-us/blog/the-history-of-iot-a-comprehensive-timeline-of-major-events-infographic, September 2018

[8] Heather Pemberton Levy,https://www.gartner.com/smarterwithgartner/whats-new-in-gartners-hype-cycle-for-emerging-technologies-2015/, October 2018

[9] Bernard Marrhttps://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#6654514060ba, September 2018

[10] "Internet of Things Global Standards Initiative".ITU. Retrieved 1 June 2016.

[11] Evan Ackerman,https://spectrum.ieee.org/automaton/robotics/industrial-robots/interview-brad-porter-vp-of-robotics-at-amazon ,October 2018

[12] Jerry Lee,https://blogs.microsoft.com/iot/2018/01/23/farmers-improve-management-crop-yields-iot/ ,October 2018

[13] FriedemannMattern and Christian Floerkemeier,"From the Internet of Computers to the Internet of Things",Distributed Systems Group, Institute for Pervasive Computing.

[14] ITU-T Rec. Y.4115 (04/2017) Reference architecture for IoT device capability exposure.

[15] Yunjung Lee, Yongjoon Park, DoHyeun Kim 2, "Security Threats Analysis and Considerations for Internet of Things"

[16] Elisa Bertino , Kim-Kwang Raymond Choo , DimitriosGeorgakopolous , Surya Nepal, Internet of Things (IoT): Smart and Secure Service Delivery, ACM Transactions on Internet Technology (TOIT), v.16 n.4, December 2016

[17] Peggy Smedley,https://connectedworld.com/li-fi-takes-on-the-iot/, October 2018

[18] K. Asha Rani, A. V. R. Mayuri, "Paper on Basics of Internet of Things", International Journal of Emerging Trends in Science and Technology.

[19] JayavardhanaGubbi, RajkumarBuyya, SlavenMarusic,MarimuthuPalaniswamia,"Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions", 2015 8th International Conference on Security Technology.

[20] SomayyaMadakam, R. Ramaswamy, SiddharthTripathi,Internet of Things (IoT): A Literature Review,Journal of Computer and Communications, 2015, 3, 164-173.