A Study of Internet of Things (IoT) And Their Applications

Mrs. D.Suganthi[1], Mr. C.Jeyaganthan[2]
[1]Assistant Professor, Dept of Computer Science
[2]Senior Software Engineer
[1]Mahalashmi Women's College of Arts & Science,Paruthipattu, Avadi, Chennai – 71.
[2]Navis India Technologies, AscendasIntl.Tech Park, CSIR Road, Taramani, Chennai-113.

Abstract- *Internet of Things (IoT) making our life more easiest way and very simple to interconnect with all smart devices. Nowadays we have internet infrastructures are available anywhere and whenever we need. IoT is simply the network of interconnected things/devices, which are embedded with sensors, software, network connectivity and necessary electronical devices. IoT keeps establishing advanced connectivity (with the aid of internet) among the interconnected house hold devices or systems or services in order to make automation in all areas. It has a pack of important component. IoT provides lots of benefits to living society to improve the comfort living.*

Keywords- Sensor, Interconnection, Cloud, Data Processing, Protocols and Networks.

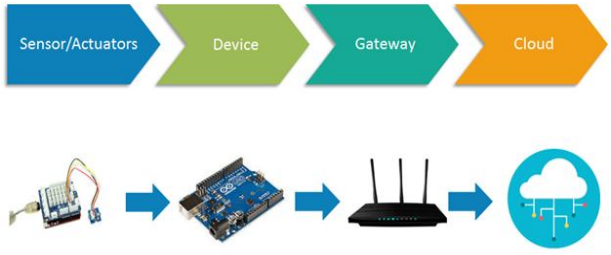
I. INTRODUCTION

In 20thCentuary, Internet has become universal, has touched every corner of the world, and its affect in ghuman life in unimaginable ways. Now we are entering an advanced technology world of even more extensive connectivity where a huge variety of devices will be connect through the web. It is a network of networks that consists of public, private, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet takes a vast range of information resources and services, such as the hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and file sharing.

We are in new generation world is "**Internet of Things**" (IoT). A global computer network provides the variety of information and communication facilities are interconnected with networks using standardized communication protocols. IoT is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer the data over a network without requiring human-to-human or human-to-computer interaction.

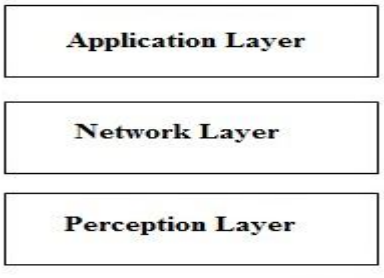
II. IoT ARCHITECTURE

A unique or standard consensus on the Internet of Things (IoT) architecture, which is universally defined. The IoT architecture differs from their functional area and their solutions. The IoT architecture technology mainly consists of four major components. There aresensors, protocols, actuators, cloud services, and layers. There exist 4 stages of IoT architecture. Such a number is chosen to steadily include these various types of components into a sophisticated and unified network.



Basically, there are three IoT architecture layers:

1. The client side (IoT Device Layer)
2. Operators on the server side (IoT Getaway Layer)
3. A pathway for connecting clients and operators (IoT Platform Layer)



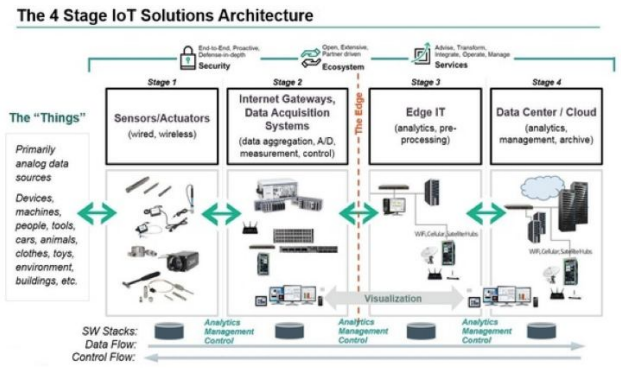
In fact, addressing the needs of all these layers is crucial on all the stages of IoT architecture. Being the basis of feasibility criterion, this consistency makes the result designed work. In addition, the fundamental features of sustainable IoT

architecture include functionality, scalability, availability, and maintainability. Without addressing these conditions, the result of IoT architecture is a failure.

In simple terms, the 4 Stages of IoT architecture consists of

1. Sensors and actuators
2. Internet getaways and Data Acquisition Systems
3. Edge IT
4. Data Center and Cloud.

An overview of the main stages in the IoT architecture diagram and the detailed presentation of these stages can be found on the diagram below.



III. IoT WORKS

IoT ecosystem consists of web-enabled smart devices that use embedded systems, such as processors, sensors and communication hardware, to collect, sends and receives the data they acquire from their environments. IoT devices share the sensor data when they collect by connecting to an IoT gateway. Sometimes, these devices are communicate with other related devices and act on the information they get from one another. The connectivity, networking and communication protocols used with these web-enabled devices largely depend on the specific IoT applications deployed.

IoT can also make use of artificial intelligence (AI) and machine learning to aid in making data collecting processes easier and more dynamic.

IV. MAJOR COMPONENTS on IoTWORKS

1. Gateway---Gateway enables to manage the data traffic flowing between protocols and networks. It is essential to configure it as the presence of TCP/IP protocol allows easy flow. And it also translates the network protocols and make sure the devices and sensors are connected properly.

2. Analytics---The analog data of devices and sensors are converted into an digital format that is easy to read and analyse. The main factor that influenced is security.

3. Connectivity Of Devices—Sensors collect the information and send it to the next layer where it is going to processed. The modern smart sensors and devices use various ways to be connected. The wireless networks like LORAWAN, Wi-Fi, and Bluetooth makes it easy for them to stay connected. The pros and cons that are classified in various forms like efficiency rate, data transfer, and power.

4. Cloud—The various tools are used for the purpose of collection of data that can collect, process, handle and store the data efficiently. This all is done by the one system i.e. IoT Cloud.

5. Integrating and Artificial Intelligence---IoT integrating the various models to improve the user experience and IoT makes things to act smart and enhances life through the use of data.

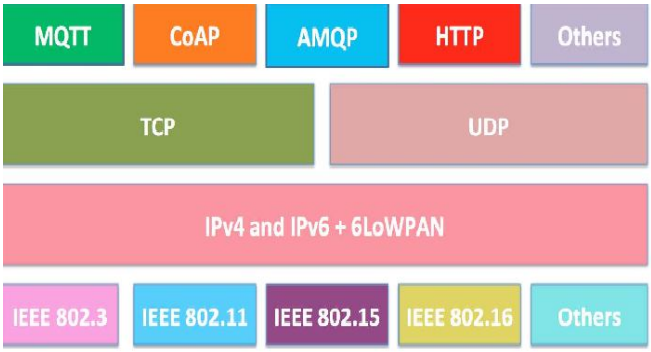
6. Sensing--- The sensor devices are used in IoT technologies, to detect and measure any change in the environment and report on their status. Active Engagement: IoT makes the connected technology, product, or services to active engagement between each other.

7. End point management and User Interface—It is very important that maintaining the end user points in IoT.This provides a visible and physical part that can be easily accessed by the user. With the help of advancement, there are various interactive designs that could be used easily and that can easily solve any complex query.

V. IoT PROTOCOLS

To fit all of the IoT Protocols on top of existing architecture models like OSI Model, have broken the protocols into the following layers to provide some level of organization:

- Infrastructure (ex: 6LowPAN, IPv4/IPv6, RPL)
- Identification (ex: EPC, uCode, IPv6, URIs)
- Comms / Transport (ex: Wifi, Bluetooth, LPWAN)
- Discovery (ex: Physical Web, mDNS, DNS-SD)
- Data Protocols (ex: MQTT, CoAP, AMQP, Websocket, Node)
- Device Management (ex: TR-069, OMA-DM)
- Semantic (ex: JSON-LD, Web Thing Model)
- Multi-layer Frameworks (ex: Alljoyn, IoTivity, Weave, Homekit)



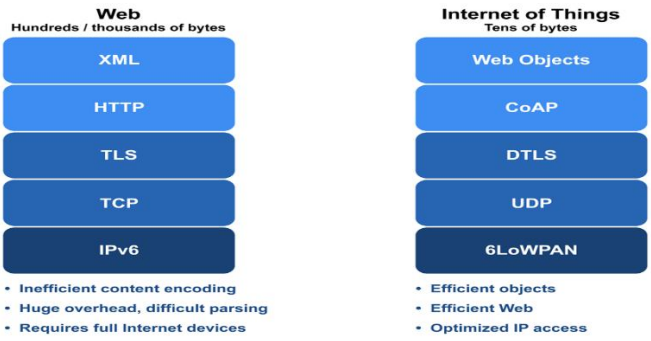
Some of the Specific Communication IoT Protocols are:

- MQTT – Message Queue Telemetry Transport Protocol
- DDS – Data Distribution Service
- AMQP – Advanced Message Queuing Protocol
- CoAP – Constrained Application Protocol

MQTT is widely accepted and emerging protocol for IoT also Facebook and Messenger using it for speed delivery of message is size of header is 2 Byte of length followed by 256 Byte size of Message.

Comparing Web and IoTProtocols :

The following figure shown below to provide the performance benefit that these protocols bring to IoT.



By comparison, IoT protocols are optimized for constrained devices and networks, and produce a much smaller data overhead of tens of bytes.

VI. TYPES OF IoT

IoT networks can be categorized by the distance.

1. **Nano network**: Applied in the military and biometrical sphere, Nano networks typically consist of a group of a few extremely small devices, which carry out simple jobs such as actuation, storage, computing and sensing.
2. **Body Area Network**: This network is designed to connect devices that are worn on the body or in some cases, inside the body when talking about embedded electronic equipment like pacemakers.
3. **Near Field Communication Network**: NFC is a low-speed network that connects devices together over a small distance of around 4cm.
4. **Personal Area Network**: This kind of network would usually span one or two rooms.
5. **Local Area Network**: It describes a network that covers an entire building, be it a residential or business property.
6. **Wide Area Network**: This network is typicallyemployed over a large geographical area and is the larger building block that links LANs together.
7. **Wireless Mesh Network**: A more complex type of network you may encounter is a WMN which is often an ad hoc network of wireless devices that connect directly together and typically consists of gateways, mesh routers and mesh clients.

VII. ADVANTAGES of IoT

- Ability to access information from anywhere at any time on any device;
- Improved communication between connected electronic devices;
- Transferring data packets over a connected network saving time and money; and
- Automating tasks helping to improve the quality of a business's services and reducing the need for human intervention.

VIII. DISADVANTAGES of IoT

- The number of connected devices increases and more information are shared between devices.
- Enterprises may eventually have to deal with massive number of IoT devices, collecting and managing the data from all those devices will be challenging.

IX. APPLICATIONS of IoT

There are a many set of areas in which intelligent applications have been developed.Some uses of IoT applications are, home automation, smart cities, smart water systems, Energy Conservation, fitness tracking, health monitoring, environment protection, smart environment and Agriculture, and industrial settings.

X. RISKS at IOT

Understand the convolution

Understanding the complexity of vulnerabilities, and how serious of a threat they pose is going to become a huge challenge.

Susceptibility management

Another big challenge for enterprises in an IoT environment will be learning how to quickly patch IoT device vulnerabilities and how to prioritize them. Upgrading custom firmware often requires extra time and effort.

Identifying refuge controls

In the IT world, redundancy is critical. If one product fails, another is there to take over. The concept of layered security works similarly, but we still have to see how well enterprises can layer security and redundancy to manage IoT risk.

Interruption and denial-of-service attacks

If thousands of IoT devices try to access a corporate website or data service feed that isn't available, a company's happy customers will become frustrated, resulting in revenue loss, customer dissatisfaction and potentially poor reception in the market.

Security analytics competence

The variety of new devices connecting to the Internet will create a flood of data for enterprises to collect process and analyse. While certainly organizations will identify new business opportunities based on this data, new risks emerge as well.

XI. IoT SECURITY

IoT can drive huge economic opportunities for industries and enable exciting innovations that reach across all the fields. Diverse IoTsolutions, everything from remote monitoring, predictive maintenance and smart spaces to connected products and customer-facing technologies like mobile apps, can reduce operational complexity, lower costs and speed up time to market.

Protecting employees, customers, valuable operational technologies and business investments with secure. Experienced IoT security companies recommend a three-pronged approach to protect data, devices and connections:Secure provisioning of devices.Secure connectivity between devices and the cloud. Securing data in the cloud during processing and storage. Security concerns with IoT are also driven by:

- Device heterogeneity or fragmentation
- Connection to valuable operational technology
- Challenges with the security of legacy devices

XII. SECURITY LIMITATIONS

Limitations based on the Network:

- Multi-Protocol Networking
- Dynamic network topology and Mobility

Limitations based on the Software:

- Dynamic security patch
- Embedded software constraint

Limitations based on the Hardware:

- Tamper resistant packaging
- Memory constraint

Limitations based on IoT Communication Devices:

Devices of the IoT are resources constrained, and therefore, traditional security mechanisms are not precise in smart things. Security limitations related to the IoT communication devices are:

- Memory Capacity
- Energy Capacity
- Processing Capacity

XIII. COMPLICATIONS OF USING IoT

As the Internet of things facilitates a set of benefits, it also creates a significant set of challenges. Some of the IoT challenges are given below:

Security: As the IoT systems are interconnected and communicate over networks. The system offers little control despite any security measures, and it can be lead the various kinds of network attacks.

Privacy: Even without the active participation on the user, the IoT system provides substantial personal data in maximum detail.

Complexity: The designing, developing, and maintaining and enabling the large technology to IoT system is quite complicated.

XIV. CONCLUSION

IoT keeps establishing advanced connectivity (with the aid of internet) among the internet connected devices or systems or services in order to make automation in all areas. It has a pack of important component. IoT provides lots of benefits to living society to improve the comfort living.

These systems allow greater transparency, control, and performance when applied to any industry or system. The future of IoT is virtually unlimited due to advances in technology and consumers' desire to integrate devices such as smart phones with household machines. Wi-Fi has made it possible to connect people and machines on land.

REFERENCES

[1] O. Vermesan, P. Friess, P. Guillemin et al., "Internet of things strategic research roadmap," in Internet of Things: Global Technological and Societal Trends, vol. 1, pp. 9–52, 2011.

[2] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal, "Choices for interaction with things on Internet and underlying issues," Ad Hoc Networks, vol. 28, pp. 68–90, 2015.

[3] O. Said and M. Masud, "Towards internet of things: survey and future vision," International Journal of Computer Networks, vol. 5, no. 1, pp. 1–17, 2013.

[4] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of internet of things," in Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10), vol. 5, pp. V5-484–V5-487, IEEE, Chengdu, China, August 2010.

[5] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT '12), pp. 257–260, December 2012.

[6] H. Ning and Z. Wang, "Future internet of things architecture: like mankind neural system or social organization framework?" IEEE Communications Letters, vol. 15, no. 4, pp. 461–463, 2011.

[7] M. Weyrich and C. Ebert, "Reference architectures for the internet of things," IEEE Software, vol. 33, no. 1, pp. 112–116, 2016.

[8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): a vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[9] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, "Fog computing: a platform for internet of things and analytics," in Big Data and Internet of Things: A Road Map for Smart Environments, pp. 169–186, Springer, Berlin, Germany, 2014.

[10] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proceedings of the 1st ACM MCC Workshop on Mobile Cloud Computing, pp. 13–16, 2012.

[11] I. Stojmenovic and S. Wen, "The fog computing paradigm: scenarios and security issues," in Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS '14), pp. 1–8, IEEE, Warsaw, Poland, September 2014.

[12] M. Aazam and E.-N. Huh, "Fog computing and smart gateway based communication for cloud of things," in Proceedings of the 2nd IEEE International Conference on Future Internet of Things and Cloud (FiCloud '14), pp. 464–470, Barcelona, Spain, August 2014.

[13] L. Atzori, A. Iera, and G. Morabito, "SIoT: giving a social structure to the internet of things," IEEE Communications Letters, vol. 15, no. 11, pp. 1193–1195, 2011.

[14] M. Swan, "Sensor mania! The internet of things, wearable computing, objective metrics, and the quantified self 2.0," Journal of Sensor and Actuator Networks, vol. 1, no. 3, pp. 217–253, 2012.

[15] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell, "A survey of mobile phone sensing," IEEE Communications Magazine, vol. 48, no. 9, pp. 140–150, 2010.

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

[17] A. Whitmore, A. Agarwal, and L. Da Xu, "The internet of things—a survey of topics and trends," Information Systems Frontiers, vol. 17, no. 2, pp. 261–274, 2015.

[18] D. Zeng, S. Guo, and Z. Cheng, "The web of things: a survey," Journal of Communications, vol. 6, no. 6, pp. 424–438, 2011.

[19] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "Role of middleware for internet of things: a study," International Journal of Computer Science & Engineering Survey, vol. 2, no. 3, pp. 94–105, 2011.