International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org || PP. 32-37

A Pragmatic View on Internet of Things – The Current Scenario

* A.Lavanya[1], Dr.C.Bhuvaneswari[2]
[1](Assistant Professor & Head/ Computer Science / Kamban College of Arts and Science for women,)
[2] (Assistant Professor& Head/ Computer Science / Thiruvalluvar university model college of arts and science, Thirvennainallur.)

Abstract: *Internet of Things (IoT) is an important concept in internet world.IOT change the real world objects into intellectual virtual objects. The IoT aims to fuse everything in our world under a common infrastructure, giving us not only control of things around us, but also keeping us informed of the state of the things. This research article focuses on definitions, basic requirements, characteristics and aliases of Internet of Things. The main objective of this paper is to provide an overview of Internet of Things, architectures, and vital technologies and their usages in our daily life.*
Keywords: *Actuators, Bluetooth, EPC ,Internet of Things IoT, IPv6, RFID, Sensors ,Wi-Fi, Zigbee, ..*

I. Introduction

The Internet of Things is a novel paradigm in IT arena. The phrase "Internet of Things" which is also shortly well-known as IoT is coined from the two words i.e. the first word is "Internet" and the second word is "Things". The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billions of users worldwide. It is a interconnection of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies .

1.1 Definitions

There is no unique definition available for Internet of Things that is acceptable by the world community of users. The best definition for the Internet of Things would be: "An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment" Internet of Things is maturing and continues to be the latest, most hyped concept in the IT world. Over the last decade the term Internet of Things (IoT) has attracted attention by projecting the vision of a global infrastructure of networked physical objects, enabling anytime, anyplace connectivity for anything and not only for any one. The Internet of Things can also be considered as a global network which allows the communication between human-to-human, human-to-things and things-to-things, which is anything in the world by providing unique identity to each and every object. IoT describes a world where just about anything can be connected and communicates in an intelligent fashion that ever before. Most of us think about "being connected" in terms of electronic devices such as servers, computers, tablets, telephones and smart phones. In what's called the Internet of Things, sensors and actuators embedded in physical objects—from roadways to pacemakers—are linked through wired and wireless networks, often using the same Internet IP that connects the Internet. The "Internet of Things" refers to the coding and networking of everyday objects and things to render them individually machine-readable and traceable on the Internet.

1.2 The aliases of Internet of Things :

Includes Web of Things, Internet of Objects, Embedded Intelligence, Connected Devices and Technology Omnipotent, Omniscient and Omnipresent. In addition to these, it has also calling as counting (1) Cyber Physical Systems "Integrations of computation and physical processes", in which bringing the real and virtual worlds together (2) Pervasive Computing is a computer environment in which virtually every object has processing power with wireless or wired connections to a global network (3) Machine-to-Machine Interaction means no human intervention whilst devices are communicating end-to-end (4) Human Computer Interaction involves the study, planning, and design of interaction between people and computers

1.3 Requirements For successful implementation of Internet of Things:

*(IoT***)**, the prerequisites are (a) Dynamic resource demand (b) Real time needs (c) Exponential growth of demand (d) Availability of applications (e) Data protection and user privacy (f) Efficient power consumptions of applications (g) Execution of the applications near to end users (h) Access to an open and inter operable cloud system. According to another author, there are three components, which required for seamless Internet of Things

(IoT) computing (a) Hardware—composed of sensors, actuators, IP cameras, CCTV and embedded communication hardware (b) Middleware—on demand storage and computing tools for data analytics with cloud and Big Data Analytics (c) Presentation—easy to understand visualization and interpretation tools that can be designed for the different applications

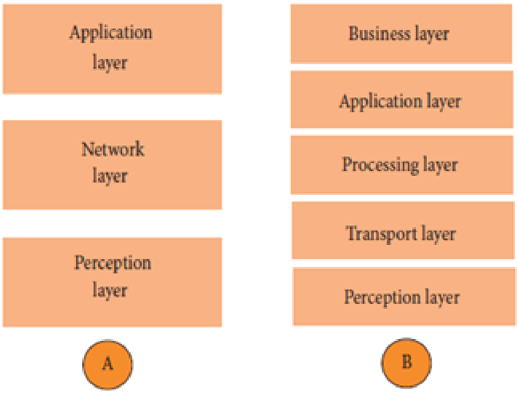

FIGURE 1: Architecture of IoT (A: three layers) (B: five layers).

II. Architecture Of Iot

There is no single consensus on architecture for IoT, which is agreed universally. Different architectures have been pro-posed by different researchers.

2.1. Three- and Five-Layer Architectures. The most basic architecture is a three-layer architecture [3–5] as shown in
Figure 1. It was introduced in the early stages of research in this area. It has three layers, namely, the perception, network, and application layers.

1. The perception layer is the physical layer, which has sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment.
2. The network layer is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data.
3. The application layer is responsible for delivering application specific services to the user. It defines various applications in which the Internet of Things can be deployed, for example, smart homes, smart cities, and smart health.

The three-layer architecture defines the main idea of the Internet of Things, but it is not sufficient for research on IoT because research often focuses on finer aspects of the Internet of Things. That is why, we have many more layered architectures proposed in the literature. One is the five-layer architecture, which additionally includes the processing and business layers [3–6]. T he five layers are perception, transport, processing, application, and business layers (see Figure 1). The role of the perception and application layers is the same as the architecture with three layers. We outline the function of the remaining three layers.

The transport layer transfers the sensor data from the perception layer to the processing layer and vice versa through networks such as wireless, 3G, LAN, Bluetooth, RFID, and NFC.The processing layer is also known as the middleware layer. It stores, analyzes, and processes huge amounts of data that comes from the transport layer. It can manage and provide a diverse set of services to the lower layers. It employs many technologies such as databases, cloud computing, and big data processing modules.The business layer manages the whole IoT system, including applications, business and profit models, and users' privacy. The business layer is out of the scope of this paper. Hence, we do not discuss it further.Another architecture proposed by Ning and Wang inspired by the layers of processing in the human brain. It is inspired by the intelligence and ability of human beings to think, feel, remember, make decisions, and react to the physical environment. It is constituted of three parts. First is the human brain, which is analogous to the processing and data management unit or the data center. Second is the spinal cord, which is analogous to the distributed network of data processing nodes and smart gateways. Third is the network of nerves, which corresponds to the networking components and sensors.

2.2. Cloud and Fog Based Architectures. Let us now discuss two kinds of systems architectures: cloud and fog computing. Note that this classification is different from the classification in Section 2.1, which was done on the basis of protocols

In particular, we have been slightly unclear about the nature of data generated by IoT devices, and the nature of data processing. In some system architectures the data processing is done in a large centralized fashion by cloud computers. Such a cloud centric architecture keeps the cloud at the center, applications above it, and the network of smart things below it..Cloud computing is given dominance because it provides great flexibility and scalability. It offers services such as the core infrastructure, platform, software, and storage. Developers can provide their storage tools, software tools, data mining, and machine learning tools, and visualization tools through the cloud.Lately, there is a move towards another system architecture, namely, *fog computing* where the sensors and network gateways do a part of the data processing and analytics. A fog architecture presents a layered approach as shown in Figure 2, which inserts monitoring, pre-processing, storage, and security layers between the physical and transport layers. The monitoring layer monitors power, resources, responses, and services. The pre-processing layer performs filtering, processing, and analytics of sensor data. The temporary storage layer provides storage functionalities such as data replication, distribution, and storage. Finally, the security layer performs encryption/decryption and ensures data integrity and privacy. Monitoring and pre-processing are done on the edge of the network before sending data to the cloud.Often the terms “fog computing” and “edge computing” are used interchangeably. The latter term predates the former and is construed to be more generic. *Fog computing* originally termed by Cisco refers to smart gateways and smart sensors, whereas *edge computing* is slightly more penetrative in nature. This paradigm envisions adding *smart data preprocessing capabilities* to physical devices such as motors, pumps, or lights. The aim is to do as much of preprocessing of data as possible in these devices, which are termed to be at the *edge* of the network. In terms of the system architecture, the architectural diagram is not appreciably different from Figure 2. As a result, we do not describe edge computing separately.

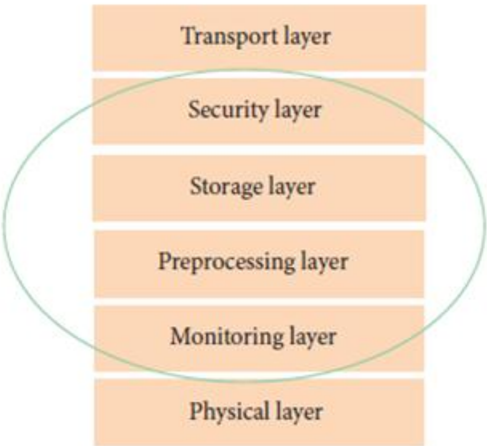

FIGURE 2: Fog architecture of a smart IoT gateway.

Finally, the distinction between protocol architectures and system architectures is not very crisp. Often the protocols and the system are code signed. We shall use the generic 5-layer IoT protocol stack (architectural diagram presented in Figure 2) for both the fog and cloud architectures.*2.3. Social IoT.* Let us now discuss a new paradigm: social IoT (SIoT). Here, we consider social relationships between objects the same way as humans form social relationships (see [14]). Here are the three main facets of an SIoT system:

1. The SIoT is navigable. We can start with one device and navigate through all the devices that are connected to it. It is easy to discover new devices and services using such a social network of IoT devices.
2. A need of trustworthiness (strength of the relation-ship) is present between devices (similar to friends on Facebook).
3. We can use models similar to studying human social networks to also study the social networks of IoT devices.

2.3.1. Basic Components.

In a typical social IoT setting, we treat the devices and services as bots where they can set up relationships between them and modify them over time. This will allow us to seamlessly let the devices cooperate among each other and achieve a complex task.To make such a model work, we need to have many interoperating components. Let us look at some of the major components in such a system.

1. ID: we need a unique method of object identification. An ID can be assigned to an object based on traditional parameters such as the MAC ID, IPv6 ID, a universal product code, or some other custom method.
2. Meta information: along with an ID, we need some meta information about the device that describes its form and operation. This is required to establish appropriate relationships with the device and also appropriately place it in the universe of IoT devices.
3. Security controls: this is similar to "friend list" set-tings on Facebook. An owner of a device might place restrictions on the kinds of devices that can connect to it. These are typically referred to as *owner controls*.
4. Service discovery: such kind of a system is like a service cloud, where we need to have dedicated directories that store details of devices providing certain kinds of services. It becomes very important to keep these directories up to date such that devices can learn about other devices.
5. Relationship management: this module manages relationships with other devices. It also stores the types of devices that a given device should try to connect with based on the type of services provided. For example, it makes sense for a light controller to make a relationship with a light sensor.
6. Service composition: this module takes the social IoT model to a new level. The ultimate goal of having such a system is to provide better integrated services to users. For example, if a person has a power sensor with her air conditioner and this devicerelationship with an analytics engine, then it is possible for the ensemble to yield a lot of data about the usage patterns of the air conditioner. If the social model is more expansive, and there are many more devices, then it is possible to compare the data with the usage patterns of other users and come up with even more meaningful data. For example, users can be told that they are the largest energy consumers in their community or among their Facebook friends.

2.3.2. Representative Architecture.

Most architectures pro-posed for the SIoT have a server side architecture as well. The server connects to all the interconnected components, aggregates (composes) the services, and acts as a single point of service for users.The server side architecture typically has three layers. The first is the *base* layer that contains a database that stores details of all the devices, their attributes, meta information, and their relationships. The second layer (*Component* layer) contains code to interact with the devices, query their status, and use a subset of them to effect a service. T he topmost layer is the *application* layer, which provides services to the usersOn the device (object) side, we broadly have two layers. The first is the *object* layer, which allows a device to connect to other devices, talk to them (via standardized protocols), and exchange information. The *object* layer passes information to the *social* layer. The social layer manages the execution of users' applications, executes queries, and interacts with the application layer on the server.

Table 1: Comparison with other surveys on the basis of topics covered.

Survey Paper	Sensors	Architecture	Communication	Applications
" Internet of Things: A Survey," Atzori etal., 2010	RFID	Service Oriented Architecture	Communication Standards, IEEE 802.15.4, WSN,Zigbee, 6LoWPAN, NFC, Wireless Hart, M2M, EPC global, ROLL routing	Smart home, health, logistics, transport, agriculture, social, environment
"Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," Gubbi et al., 2013	RFID	Service Oriented Architecture	WSN, addressing schemes	Personal and home, enterprise, utilities, mobile
"The Internet of Things—A Survey of Topics and Trends," Whitmore et al., 2014	RFID	Semantic middleware	WSN, NFC, WSN	Smart infrastructure, health care, supply chains/logistics
Our survey	Covered various types of sensors: environmental, medical, neural, chemical, infrared, mobile phone sensors, RFID	Issues addressed by middleware, types of middleware: event based, service based, semantic, database, application specific	All layers of IP stack, protocols and standards of each layer, IEEE 802.15.4, 6LoWPAN, NFC, ROLL routing, COAP, MQTT, LPWAN, low energy wireless communication technologies: BLE, Zigbee, RFID-WSN integration	Smart home, health, logistics, transport, social, environment, agriculture, energy

III. Related Survey Papers

There have been many survey papers on the Internet of Things in the past. Table 1 shows how our survey is different from other highly cited surveys in the literature.Let us first consider our novel contributions. Our paper looks at each and every layer in the IoT stack, and as a result the presentation is also far more balanced. A novel addition in our survey is that we have discussed different IoT architectures. This has not been discussed in prior surveys on the Internet of Things. The architecture section also considers newer paradigms such as fog computing, which have also not been considered. Moreover, our survey nicely categorizes technologies based on the architectural layer that they belong to. We have also thoroughly categorized the network layer and tried to consolidate almost all the technologies that are used in IoT systems. Such kind of a thorough categorization and presentation of technologies is novel to the best of our knowledge.

IV. Applications of Iot

There are a diverse set of areas in which intelligent applications have been developed. All of these applications are not yet readily available; however, preliminary research indicates the potential of IoT in improving the quality of life in our society. Some uses of Io applications are in home automation, fitness tracking, health monitoring, environment protection, smart cities, and industrial settings1.Home Automation. Smart homes are becoming more popular today because of two reasons. First, the sensor and actuation technologies along with wireless sensor net-works have significantly matured. Second, people today trust technology to address their concerns about their quality of life and security of their homes.In smart homes, various sensors are deployed, which provide intelligent and automated services to the user. T hey help in automating daily tasks and help in maintaining a routine for individuals who tend to be forgetful. They help in energy conservation by turning off lights and electronic gadgets automatically. We typically use motion sensors for this purpose. Motion sensors can be additionally used for security also.

4.1 Smart Cities

2.1. Smart Transport. Smart transport applications can manage daily traffic in cities using sensors and intelligent information processing systems. The main aim of intelligent transport systems is to minimize traffic congestion, ensure easy and hassle-free parking, and avoid accidents by properly routing traffic and spotting drunk drivers. The sensor technologies governing these types of applications are GPS sensors for location, accelerometers for speed, gyroscopes for direction, RFIDs for vehicle identification, infrared sensors for counting passengers and vehicles, and cameras for record-ing vehicle movement and traffic.

4. **Smart Water Systems**. Given the prevailing amount of water scarcity in most parts of the world, it is very important to manage our water resources efficiently. As a result most cities are opting for smart solutions that place a lot of meters on water supply lines and storm drains.

These meters can be used to measure the degree of water inf low and outflow and to identify possible leaks. Smart water metering systems are also used in conjunction with data from weather satellites and river water sensors. They can also help us predict flooding.

5. **Health and Fitness**. .

IoT appliances have proven really beneficial in the health and wellness domains. Many wearable devices are being developed, which monitor a person's health condition.Health applications make independent living possible for the elderly and patients with serious health conditions. Currently, IoT sensors are being used to continuously monitor and record their health conditions and transmit warnings in case any abnormal indicators are found. If there is a minor problem, the IoT application itself may suggest a prescription to the patient.IoT applications can be used in creating an Electronic Health Record (EHR), which is a record of all the medical details of a person. It is maintained by the health system. An EHR can be used to record allergies, surges in blood sugar and blood pressure.Smart Environment and Agriculture. Environmental parameters such as temperature and humidity are important for agricultural production. Sensors are used by farmers in the field to measure such parameters and this data can be used for efficient production. One application is automated irrigation according to weather conditions.Production using greenhouses [99] is one of the main applications of IoT in agriculture. Environmental parameters measured in terms of temperature, soil information, and humidity are measured in real time and sent to a server for analysis. T he results are then used to improve crop quality and yield.

6. **Social Life and Entertainment.**

Social life and entertain-ment play an important role in an individual's life. Many applications have been developed, which keep track of such human activities. The term "opportunistic IoT" refers to information sharing among opportunistic devices (devices that seek to make contact with other devices) based on movement and availability of contacts in the vicinity. Personal devices such as tablets, wearables, and mobile phones have sensing and short range communication capabilities. People can find and interact with each other when there is a common purpose.Circle Sense is an application, which detects social activities of a person with the help of various types of sensor data. It identifies the social circle of a person by analyzing the patterns of social activities and the people present in those activities. Various types of social activities and the set of people participating in those activities are identified. It uses location sensors to find out where the person is and uses Bluetooth for searching people around her. The system has built in machine learning algorithms, and it gradually improves its behavior with learning.

V. Conclusion

In this survey paper we presented a survey of the current technologies used in the IoT domain as of 2017. Currently, this field is in a very nascent stage. The technologies in the core infrastructure layers are showing signs of maturity. However, a lot more needs to happen in the areas of IoT applications and communication technologies. These fields will definitely mature and impact human life in inconceivable ways over the next decade.

References

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

[2]. I. Pena˜-Lopez,´ Itu Internet Report 2005: The Internet of Things, 2005.

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

[4]. 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.

[5]. 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.

[6]. 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

[7]. 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.

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

[9]. 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.

[10]. 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.

[11]. 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.

[12]. 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 (Fed-CSIS ’14), pp. 1–8, IEEE, Warsaw, Poland, September 2014.

[13]. 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.

[14]. L. Atzori, A. Iera, and G. Morabito, “SIoT: giving a social struc-ture to the internet of things,” IEEE Communications Letters, vol. 15, no. 11, pp. 1193–1195, 2011.

[15]. M. Swan, “Sensor mania! The internet of things, wearable computing, objective metrics, and the quantified self 2.0,” Jour-nal of Sensor and Actuator Networks, vol. 1, no. 3, pp. 217–253, 2012.