The Internet of Things (IoT): New age

[1]Prashant M. Adhao, [2]Rahul B. Mapari
[1]Assistant Professor, [2]Assistant Professor
[1]Department of Computer Science & Engineering, J N E College Aurangabad, MH, India

Abstract: **This paper addresses the Internet of Things. In 2008 the number of things connected to the Internet was greater than the people living on Earth.Within 2020 the number of things connected to the Internet will be about 50 billion. The internt has initially started with the Internet of Computers and file trasfer protocol , and noe its world wide web (WWW) and hence user communicate each other and exchaneg information. Now the internet not only used to commicate and exchngae the infromation by human but things can used intenet for commicate and exchngae and this term called internet fo things (IoT). In this paper we will present concpt of IoT and it's differnt applications and challenges.**

Keywords: **Internet of Things (IoT), Appliactions , challenges.**

I. Introduction :

The next wave in the era of computing will be outside the realmof the traditional desktop. In the Internet of Things (IoT) paradigm,many of the objects that surround us will be on the network in oneform or another. Radio Frequency Identification (RFID) and sensornetwork technologies will rise to meet this new challenge, in whichinformation and communication systems are invisibly embeddedin the environment around us. This results in the generation ofenormous amounts of data which have to be stored, processedand presented in a seamless, efficient, and easily interpretableform. This model will consist of services that are commodities anddelivered in a manner similar to traditional commodities.

Imagine a world where billions of objects can sense, communicate and share information, allinterconnected over public or private Internet Protocol (IP) networks. These interconnectedobjects have data regularly collected, analysed and used to initiate action, providing awealth of intelligence for planning, management and decision making. This is the world ofthe Internet of Things (IOT).The IOT concept was coined by a member of the Radio Frequency Identification (RFID)development community in 1999, and it has recently become more relevant to the practicalworld largely because of the growth of mobile devices, embedded and ubiquitouscommunication, cloud computing and data analytics.

IoT is a seamless connected network system of embedded objects/ devices, with identifiers, in which communication without any human intervention is possible using standard and interoperable communication protocolsThe term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention. The Internet of Things, also called The Internet of Objects, refers to a wireless network between objects, usually the network will be wireless and self-configuring, such as household appliances [1].

II. The Basic Concept:

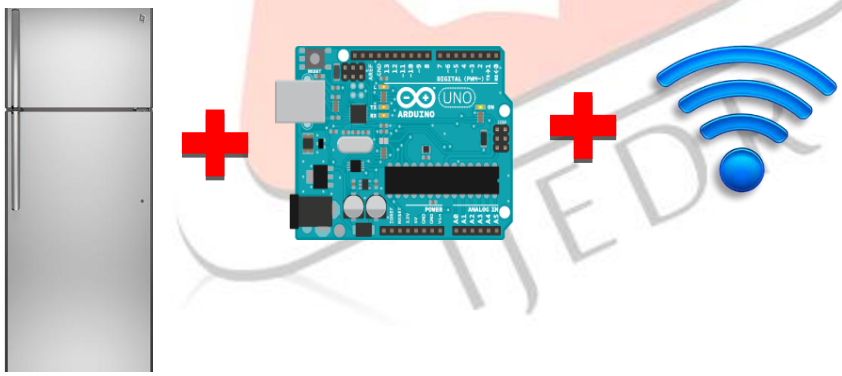
The IOT concept was coined by a member of the Radio Frequency Identification (RFID)[4] development community in 1999, and it has recently become more relevant to the

practical world largely because of the growth of mobile devices, embedded and ubiquitous communication, cloud computing and data analytics[2].

Since then, many visionaries have seized on the phrase "Internet of Things" to refer[3] to the general idea of things, especially everyday objects that are readable, recognisable, locatable, addressable, and/or controllable via the Internet, irrespective of the communication. Everyday objects include not only the electronic devices we encounter or the products of higher technological development such as vehicles and equipment but things that we do not ordinarily think of as electronic at all - such as food and clothing. When we talk about the "object" or "Things" it's include everyday objects from, small ones like bottle, wrist watches, tooth brush to really big objects like robot, vehicles, homes, etc. All such devices that interact with each other's and users and gathering and retrieve information about their environment change .IoT also contains different hardware to controlled different things or objects. Examples of "things" include:

- People
- Location (of objects)
- Time Information (of objects)
- Condition (of objects).

Start with a device (or *"things"*)– anything besides traditional computers which required intermediator to convey the instruction to things i.e. Computational Intelligence .Add Computational Intelligence to improve function of device. For example Arduino [5], Raspberry Pi[6], or any other. After that we need to connect the things which having the computational power to internet via connecting media like Wifi, LAN, WAN for global access. Bello fig. shows IoT enable refrigerator.



III. History

The Internet of Things (IoT) is the network of physical objects, devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.[7] The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more-direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit; when IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and

smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of almost 50 billion objects by 2020. British entrepreneur Kevin Ashton first coined the term in 1999 while working at Auto-ID Labs (originally called Auto- ID centres - referring to a global network of Radio-frequency identification (RFID) connected objects). Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications [8]. The interconnection of these embedded devices (including smart objects), is expected to usher in automation in nearly all fields, while also enablingadvanced applications like a Smart Grid, and expanding to the areas such as smart cities.

IV. Enabling technologies [9]

Implementation of the IoT concept into the real world with real time data processing ispossible through the integration of several technologies.In this section we discuss the some technologies. In this section will not provide a comprehensivesurvey of each technology. Our major aim is to provide apicture of the role they will likely play in the IoT. Interestedreaders will find references to technical publications foreach specific technology.

a) Identification, sensing and communication technologies:

‘‘Anytime, anywhere, anymedia” has been for a long time the vision pushing forward the advances in communication technologies. In this context, wireless technologies have played a key role and today the ratio between radios and humans is nearing the 1 to 1 value [10]. However, the reduction in terms of size, weight, energy consumption, and cost of the radio can take us to a new era where the above ratio increases of orders of magnitude. This will allow us to integrate radios in almost all objects and thus, to add the world ‘‘anything” to the above vision, which leads to the IoT concept. In this context, key components of the IoT will be RFID systems [11], which are composed of one or more reader(s) and several RFID tags. Tags are characterized by a unique identifier and are applied to objects (even persons or animals). Readers trigger the tag transmission by generating an appropriate signal, which represents a query for the possible presence of tags in the surrounding area and for the reception of their IDs. Accordingly, RFID systems can be used to monitor objects in real-time, without the need of being in line-of-sight; this allows for mapping the real world into the virtual world. Therefore, they can be used in an incredibly wide range of application scenarios, spanning from logistics to e-health and security. From a physical point of view a RFID tag is a small microchip1 attached to an antenna (that is used for both receiving the reader signal and transmitting the tag ID) in a package which usually is similar to an adhesive sticker [12]. Dimensions can be very low: Hitachi has developed a tag with dimensions 0.4 mm x 0.4 mm x 0.15 mm.

Sensor networks will also play a crucial role in the IoT. In fact, they can cooperate with RFID systems to better track the status of things, i.e., their location, temperature, movements, etc. As such, they can augment the awareness of a certain environment and, thus, act as a further bridge between physical and digital world. Usage of sensor networks has been proposed in several application scenarios, such as environmental monitoring, e-health, intelligent transportation systems, military, and industrial plant monitoring. Sensor networks consist of a certain number (which can be very high) of sensing nodes communicating in a wireless multi-hop fashion. Usually nodes report the results of their sensing to a small

number (in most cases, only one) of special nodes called sinks. A large scientific literature has been produced on sensor networks in the recent past, addressing several problems at all layers of the protocol stack [13]. Design objectives of the proposed solutions are energy efficiency (which is the scarcest resource in most of the scenarios involving sensor networks), scalability (the number of nodes can be very high), reliability (the network may be used to report urgent alarm events), and robustness (sensor nodes are likely to be subject to failures for several reasons). Today, most of commercial wireless sensor network solutions are based on the IEEE 802.15.4 standard, which defines the physical and MAC layers for low-power, low bit rate communications in wireless personal area networks (WPAN) [14]. IEEE 802.15.4 does not include specifications on the higher layers of the protocol stack, which is necessary for the seamless integration of sensor nodes into the Internet.

b) Middleware :

The middleware is a software layer or a set of sub-layers interposed between the technological and the application levels. Its feature of hiding the details of different technologies is fundamental to exempt the programmer from issues that are not directly pertinent to her/his focus, which is the development of the specific application enabled by the IoT infrastructures. The middleware is gaining more and more importance in the last years due to its major role in simplifying the development of new services and the integration of legacy technologies into new ones. This excepts the programmer from the exact knowledge of the variegate set of technologies adopted by the lower layers.

V. Applications:

Potentialities offered by the IoT make possible the development of a huge number of applications, of which only a very small part is currently available to our society. Many are the domains and the environments in which new applications would likely improve the quality of our lives: at home, while travelling, when sick, at work, when jogging and at the gym, just to cite a few. These environments are now equipped with objects with only primitive intelligence, most of times without any communication capabilities. Giving these objects the possibility to communicate with each other and to elaborate the information perceived from the surroundings imply having different environments where a very wide range of applications can be deployed.These can be grouped into the following domains:

_ Transportation and logistics domain.
_ Healthcare domain.
_ Smart environment (home, office, plant) domain.
_ Personal and social domain.

Among the possible applications, we may distinguish between those either directly applicable or closer to our current living habitudes and those futuristic, which we can only fancy of at the moment, since the technologies and/or our societies are not ready for their deployment.

VI. Challenges in IoT

Security Concerns - With so many interconnected devices out there in market and plenty more to come in the near future, a security policy cannot be an afterthought. If the IOT devices are poorly secured, cyber attackers will use them as entry points to cause harm to other devices in the network. This will lead to loss of personal data out into the public and the entire trust factor between internet connected devices and people using them will deteriorate.In order to evade such scenarios, it's extremely critical to ensure the security, resilience and reliability of internet applications to promote use of internet enabled devices

among users across the world.Security constraints for IOT are so critical that even analyst firm Gartner came out with some astounding numbers. According to them, the worldwide spend for the IoT security market will reach $348 million in 2016, a rise of 23.7% from $281.5 million in 2015.

Privacy issues - The possibility of tracking and surveillance of people by government and private agencies increases as the devices are constantly connected to the internet. These devices collect user data without their permission, analyze them for purposes only known to the parent company. The social embrace of the IOT devices leads people to trust these devices with collection of their personal data without understanding the future implications.

Inter-operatability standard issues - In an ideal environment, information exchange should take place between all the interconnected IoT devices. But the actual scenario is inherently more complex and depends on various levels of communication protocols stacks between such devices.

The OEM's producing industry ready IoT devices will need to invest a lot of money and time to create standardized protocols common for all IoT devices or else it will delay product deployment across different verticals.

Legal Regulatory and Rights issues - There are no concrete laws present which encompasses the various layers of IoT across the world. The gamut of devices connected to each other raises many security issues and no existing legal laws address such exposures. The issues lie in whether current liability laws will extend their arm for devices which are connected to the internet all the time because such devices have complex accountability issues.

Emerging Economy and development issues - IoT provides a great platform for enablement of social development in varied societies across the world and with the proliferation of Internet across the various sections of the society in developing countries coupled with lowering costs of microprocessors and sensors will make IoT devices accessible to low income households.

But there are lot of shortcomings related to enablement of high speed internet and basic technology services architecture for commercial and business usage in developing countries. Until and unless, a basic infrastructure is in place, devices would be of no value to the users. While IoT brings about new opportunities; at the same time, it adds multiple layers of complexity. Such a new environment of devices will add a new dimension for policy makers in emerging economies who will need to chalk out a new blueprint for IoT related regulatory concerns.

VII. Conclusions:

The Internet has changed drastically the way we live, moving interactions between people at a virtual level in several contexts spanning from the professional life to social relationships. The IoT has the potential to add a new dimension to this process by enabling communications with and among smart objects, thus leading to the vision of ‘‘anytime, anywhere, any media, anything” communications. To this purpose, we observe that the IoT should be considered as part of the overall Internet of the future, which is likely to be dramatically different from the Internet we use today.

References:

[1]https://en.wikipedia.org/wiki/Internet_of_things.

[2]www.redbite.com/the-origin-of-the-internet-of-things/

[3] The Internet of Things :An Overview by the internet society.

[4] "Internet of Things (IoT): A vision, architectural elements, and future directions" by Jayavardhana Gubbia, Rajkumar Buyyab,∗, Slaven Marusic a, Marimuthu Palaniswami a

[5] https://www.arduino.cc/

[6] https://www.raspberrypi.org/

[7]Bo Y., Guangwen H., 2008. Application of RFID and Internet of Things in Monitoring and Anticounterfeiting for Products. International Seminar on Business and Information, Wuhan, Hubei, China, Pages: 392- 395.

[8] Zouganeli E., Einar Svinnset I., 2009. Connected Objects and the Internet of Things – a Paradigm Shift. International Conference on Photonics in Switching, Pisa, Italy, Pages: 1-4

[9]Luigi Atzori a, Antonio Iera b, Giacomo Morabito, "The Internet of Things: A survey" Computer Networks 54 (2010) 2787–2805

[10]L. Srivastava, Pervasive, ambient, ubiquitous: the magic of radio, in: European Commission Conference ''From RFID to the Internet of Things", Bruxelles, Belgium, March 2006.

[11] K. Finkenzeller, RFID Handbook, Wiley, 2003.

[12]A. Jules, RFID security and privacy:a research survey, IEEE Journal on Selected Arear is in 24 (2006) 381–394.

[13] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks 38 (4) (2002) 393– 422.

[14] <http://ieee802.org/15>.