Future Internet: The Internet of Things- A Literature Review

Kriti Chopra
Department of Computer Science and Engineering
ASET, Amity University
Noida, India
kchopra2111@gmail.com

Kunal Gupta
Department of Computer Science and Engineering
ASET, Amity University
Noida, India
kgupta@amity.edu

Annu Lambora
Department of Computer Science and Engineering
ASET, Amity University
Noida, India
lambora.annu@gmail.com

Abstract- **Internet today is the backbone of virtual communication worldwide. It is expanding its horizon with a fast pace. Internet is rightly defined as "network of networks". It is, in most simple terms, a means of establishing a connection between your computer and any other computer globally through servers and some dedicated routers. The major form of communication of current Internet is among humans (i.e. human-to-human). The next upcoming form of communication that uses Internet as the underlying technology is The Internet of Things (IoT). IoT extends the capabilities of Internet to enable machine-to-machine communication (M2M).Therefore, IoT can be said to provide communication among everyone and everything. IoT enables us to embed some sort of intelligence in the objects that are or can be connected to the Internet in order to exchange information, hence communicate, invoke certain actions based on inputs, take decisions and provide useful services. In this paper, the basic underlying workflow of IoT is discussed and the architecture of IoT is explained. The paper also highlights the most useful technologies of these days, which employ IoT for their functioning. Further, the applications and features of IoT are mentioned in the paper. Lastly, the issues and challenges in implementing the IoT are briefly discussed. The IoT today is gaining a lot of recognition due to its potential that is yet to be extracted by the industry, academia and government as well. These sectors can bring huge economic and professional benefits by employing IoT in the right manner.**

Keywords-IoT, Internet of Things, RFID, IoT architecture, Smart devices

I. INTRODUCTION

With the rapid advancement in technology, we are heading to a world in which everyone and everything will be able to communicate and be connected [1].Such technology that provides communication among anyone and at any place or any time is the Internet of Things (IoT). The IoT may be termed as the Internet of future that will enable machine-to-machine (M2M) learning [1]. The main idea behind IoT is to have independent, self-governing connection that is secure and allows exchanging of data among real world physical devices and real applications [2]. IoT enables a link between real life physical activities and virtual world [2].These days, numerous devices are connected to the Internet and the numbers of such devices are further increasing rapidly. Such devices can be PDAs, laptops, smart phones, personal computers (PCs), tablets and many other handheld embedded devices. Many of such smart phones these days have various sensors embedded in them which can sense, make informed decisions, compute, and transmit the accumulated information on the Internet [3]. By employing a network consisting of the devices having various types of sensors can further give rise to many services and applications which can be highly beneficial; personally, professionally and economically as well [2]. The IoT is an intelligent combination of sensor devices, processing unit which can also be placed on cloud, objects, communication infrastructure, action invoking system and a decision-making system [3]. Objects used in IoT systems have some features that uniquely identify them on the Internet. Smart sensor devices can sense these physical objects as the latter contain Radio-Frequency Identification Tags (RFIDs) or other barcodes for identification purposes [3]. After identification, these sensors pass on the object-specific information to the processing unit on the Internet. Various sensors may be used in combination for the purpose of designing smart applications. After the processing is done by the processing unit, the results are further forwarded to a system for making decisions and invoking suitable actions corresponding to the decisions. In this review, the basic workflow of IoT, its architecture, features and possible applications are addressed. The Internet of Things is a popular research area for industry, academia and government as well. Many international organizations in Europe and America are actively participating and contributing to the design and development of IoT in order to gain various beneficial and robust automated services [2]. The services built using IoT also have to undergo and surpass many security-related challenges. The flow of this review paper is as follows. Part II explains the basic workflow of IoT. Part III addresses the architecture employed in IoT. Part IV explains the technologies used in IoT. Part V depicts conceivable applications in the field IoT. Part VI describes the issues and challenges that arise in the design and implementation of IoT. Lastly, Part VII contains the conclusion of the paper.

II. BASIC WORKFLOW OF IOT

Internet is evolving at a fast pace connecting zillions of things worldwide in the last few years; and such things are of varying processing capabilities, sizes, computational power with support to various kinds of applications [2].Therefore, there is a need to merge the conventional Internet with a smarter Internet of future, the Internet of Things. IoT lets the physical real objects to connect and also

equips them with intelligence in order to process the information specific to the object. This information is further used to make useful independent decisions [4]. Hence, IoT is capable of giving rise to numerous beneficial applications and also services which were unimaginable earlier [1]. The general IoT scenario is depicted in Fig. 1.

As the technology advanced, the storage capacities and processing power of the devices increased exponentially, in turn their sizes reduced. Such smart devices employ various types of actuator and sensor. These devices can also connect to the Internet and hence, can communicate. This in turn gives rise to a new set of opportunities [5].

Also, the real world objects are these days fitted with RFID tags or some other type of barcodes which can easily be scanned via smart devices like barcode readers, embedded RFID scanners and smart phones.

Fig. 1: The generic IoT scenario

Fig. 2 below depicts the basic IoT network implementing various types of applications and services. These things can be connected to other things with same service type.

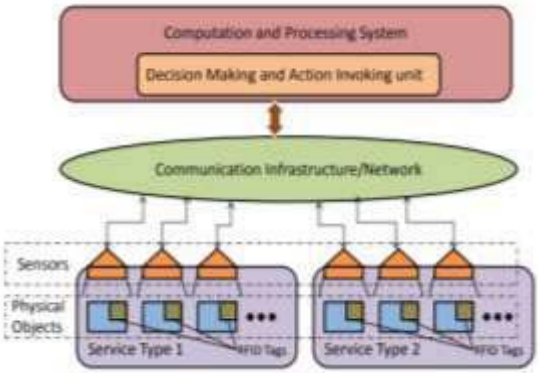

Fig. 2: The basic IoT network

The basic workflow for IoT is explained below:

1) ***Sensing of object, identifying and communicating object-specific information:*** This information may include sensed data including the motion, humidity, temperature, vibration, chemical composition of the air depending upon the different types of sensors. Varying types of sensors can be employed for designing and implementing smart applications.

2) ***Triggering of an action:*** Object-specific information that is received is then processed by a processing unit of the smart device. According to the processed information, an action that is to be invoked is determined.

3) The system or the smart device provides rich set of services and also provides with the mechanism of providing the feedback of the status of current system to the administrator. The results of the actions that were invoked are also sent to the administrator.

III. GENERIC ARCHITECTURE

Internet these days uses TCP/IP protocol for the purpose of communication among network hosts. With the advent of IoT, which will connect numerous objects to the Internet, traffic on the Internet will substantially increase and higher data storage requirements will arise [6]. Such huge network will also result in privacy and security issues [7]. Therefore, the proposed IoT architecture has to address various factors such as reliability, Quality of Service, scalability etc. As IoT lets everyone and everything to be connected and exchange information with each other, this gives rise to congestion and data storage requirements inside the network exponentially. Hence, the development of IoT is largely dependent upon the technological advancements and the design of different upcoming applications and underlying business models.

Basically, the IoT architecture comprises of five different layers as depicted in Fig. 3. All of these five layers have been described briefly:

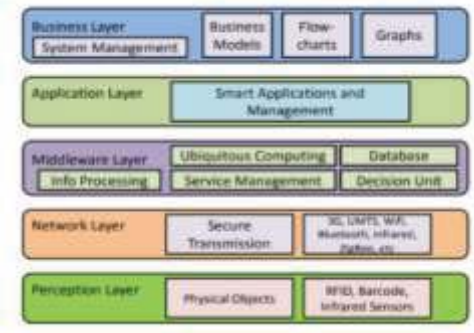

Fig.3: The IoT Architecture

1) ***Perception Layer:*** It is also referred to as 'Device Layer'. This layer constitutes of the real world objects and also the sensor devices. These sensors may be RFID tags, barcodes, or even infrared sensors based on the object's identification method used [8]. The main responsibility that lies with this layer is to identify the objects and collect their information with the help of sensor devices. Based on the type of sensor, this information may be regarding the object's location, orientation, humidity, motion, orientation etc. This information once collected is passed forward to the Network layer for transferring it securely to the processing unit.

2) ***Network Layer:*** It can also be called 'Transmission Layer'. The main responsibility of this layer is to securely

transmit the information which is collected from sensor devices to the processing unit of the system. The medium to transmit this information can either be wired or wireless. The technology that can be used may be infrared, WiFi, 3G, Bluetooth etc based on the sensor devices. Hence, in simpler terms, the job of network layer is to transfer the information from Perception layer to Middleware layer.

3) ***Middleware Layer:*** IoT objects and devices implement various types of services. Every device can connect and communicate to only those devices that implement the similar type of service. The main responsibility of this layer is service management. It can also communicate with the database. Middleware layer picks up the information coming from the Network layer and then saves the same in the database. This layer processes the information and performs ubiquitous computations. Finally, it takes automatic decisions by analysing the outcomes.

4) ***Application Layer:*** It is the responsibility of this layer to provide global management of the entire application depending upon the information of the object processed at the Middleware layer. Various applications can be implemented by using IoT such as smart homes, smart manufacturing, smart health, intelligent transportation and more.

5) ***Business Layer:*** The business layer coordinates with the entire IoT system comprising of various applications and also the services. This layer creates graphs, flowcharts and business models based on the data extracted from Application layer. Business model plays a crucial role in the success of IoT technology. After the result analysis, this layer helps in determining future actions and strategies for business.

IV. TECHNOLOGIES USED IN IOT

The Internet of Things employs some key technologies like RFID, 2D barcodes, NFC etc. These technologies enabled physical real world objects to be referred and to be uniquely identified over the Internet [8]. Some of the majorly used technologies in IoT are explained below:

1) ***Radio Frequency Identification (RFID)***

It is a technology that transfers the object's or a person's identity by a serial number using some radio waves [8].RFID technology is highly important in IoT in order to resolve issues related to object identification in an economic manner [9]. RFID tags can be categorized in three different categories on the basis of power supply method used in tags. These categories can be referred to as Active RFID, Passive RFID and Semi Passive RFID. RFID Tags mainly constitute of a reader, an access controller, software, an antenna, a tag and a server. RFID Tags can be used in applications such as patient monitoring, distribution, military applications and so on.

2) ***Internet Protocol (IP)***

The Internet Protocol is a major primary network protocol which is employed on Internet. IP is responsible for the transmission of datagram over the network boundaries. IP has two versions in operation currently: IPv4 and IPv6. Although, IPv4 is still being majorly used over the Internet. IPv4 can be classified over a range of 5 classes- A, B, C, D and E. A, B and C are used for normal use of the Internet users. IPv6 has the capability to cater to a large number of IP addresses.

3) ***Barcode***

A Barcode can be described as a method of encoding characters and digits by the use of the combination of white spaces and vertical bars of different widths. They are the optical codes which are readable by machines. Each item having a barcode label attached to it, has its information stored on the barcode. QR Code systems are gaining huge popularity in automotive industry because of their ability to read fastly and store a large amount of data in comparison to the old standard systems. Usually, barcodes are interpreted using laser scanners and cameras.

4) ***Wireless Fidelity (Wi-Fi)***

Wi-Fi is a wireless technology used for networking allowing the computers or other devices to establish communication over a signal. Vic Hayes has developed Wireless Fidelity. These days, Wi-Fi is used to deliver very high speed WLANs (Wireless Local Area Network) in order to connect millions of public locations like hospitals, cafes, airports etc., organizations and houses. Today, Wi-Fi is also being integrated in handheld devices, tablets, notebooks and Consumer Electronics (CE) devices [8].

5) ***Bluetooth***

Bluetooth is a technology that operates wirelessly for small distances. It is an economical alternative to other wireless technologies. Bluetooth eradicates the need for physical cabling among the connected devices like PDAs, notebooks, printers, tablets etc. It works in the range of 10 to 100 meters and communicates at a speed of less than 1 Mbps. Bluetooth technology can also be used to create Personal Area Networks (PANs). It generally can be connected using two topologies; Piconet and Scatternet. Piconet connects up to 8 devices at a same time for the purpose of sharing data.

6) ***ZigBee***

This technology was created to enhance the functioning of wireless sensor networks (WSN). It is created by ZigBee Alliance which came into existence in 2001. ZigBee is a technology that operates for short transmission ranges, has low cost, and is reliable and scalable. Its data transmission rates are lesser and its protocol design is highly flexible. ZigBee is developed on IEEE 802.15.4 standard and it consumes less power [9].It works on the topologies such as mesh, clustered tree and star. ZigBee is majorly used in automation of homes, medical monitoring, digital agriculture etc.

7) ***Near Filed Communication (NFC)***

NFC is a wireless technology that operates in short ranges. It works on the frequency of 13.56 MHz, needing a distance

of up to 4 cm. This technology is convenient and allows consumers worldwide to interchange digital information, make simple transactions, and connect to the electronic devices by the use of a touch. NFC can also operate smoothly in dusty environment, it does not need line of sight communication and hence it is an easy and convenient connection method.

8) ***Actuators***

Actuators convert the energy into motion. They take up some source of power in the form of hydraulic liquid or electric current. They can create a rotary motion, linear motion or oscillatory motion as well. Actuators operate at limited ranges, generally till 30 feet and exchange data at less than 1 Mbps. Actuators generally are employed in the field of manufacturing and in industrial applications. The actuators can be classified into three categories: (1) Electrical: solenoids, ac and dc motors and stepper motors (2) Hydraulic: which employ hydraulic liquid for the purpose of actuating motion (3) Pneumatic: which employ compressed air for the purpose of actuating motion. These three categories are widely used these days although electric actuators are the most popular.

9) ***Wireless Sensor Networks (WSN)***

Wireless Sensor Network consists of autonomous and independent devices which are spatially distributed. WSN uses certain sensors in order to monitor and analyze environmental and physical conditions like sound, vibration, pressure, temperature, motion and different pollutants, present at varying locations. WSN is formed by thousands of nodes that can communicate with one another and can transmit data to each other. WSN in IoT has gained huge popularity in many fields like security, manufacturing, flood detection, military, healthcare forest fire etc. [9].

10) ***Artificial Intelligence (AI)***

Artificial Intelligence can be termed as a technology that consists of electronic and virtual environments which are in turn responsive to the surroundings and people. In an intelligent world, the devices work in direction to help people in order to carry out their routine life activities in an easy and natural manner with the use of Information or Intelligence which is fed in the connected devices in the network. Artificial Intelligence is characterized by: (i) Embedded: Multiple devices are networked in the environment (ii) Context Aware: Such devices are able to recognize you and the context of your situation (iii) Personalized: Such networks are customized according to your needs (iv) Adaptive: These can easily change or adapt in response (v) Anticipatory: These can perceive your desires without mediation.

V. POSSIBLE FUTURE APPLICATIONS

The Internet of Things has its applications in various aspects of our everyday life. Fig.4 depicts various major applications of IoT in almost every sphere of life. Some of the important and possible futuristic applications of IoT are given below:

1) ***Design of smart cities:*** Internet of Things can assist in the designing of smart cities. It can be helpful in monitoring the air quality, economical lighting up of city, finding emergency routes, watering gardens etc.

Fig.4: Major Applications of IoT

2) ***Predicting natural disasters*****:** Natural disasters can be predicted by using a combination of some sensors with their independent simulation and coordination. This will help to take suitable actions prior to the occurrence of disaster.

3) ***Design of smart homes***: Internet of Things can help in designing smart homes. This will enable the user to monitor the consumption of energy, detect emergencies, searching things in the home with ease, security etc.

4) ***Design of efficient transport system:*** The intelligent system of transportation shall provide the users with an efficient and manageable transportation control by the use of sensors, and information [9]. This automated and intelligent system will have exciting features like transport law enforcement, mitigating pollution, reducing jams in traffic, reducing arrival delays etc.

5) ***Industrial applications:*** The Internet of Things is beneficial in industries as well. It can help in managing numerous automobiles for an organization. IoT can also help to analyze the environmental performance of these automobiles and select the ones that require maintenance [8].

6) ***Medical applications:*** The Internet of Things is highly employed in medical sector also [8]. It can help in the proper monitoring of patients' health, their activities, their medicine intake etc.

These are some of the major applications of IoT which are yet to be fully explored in future.

VI. KEY ISSUES IN IMPLEMENTING IOT

IoT has a wide range of benefits and has its applications in almost every field these days. On the other hand, it also goes through many issues and challenges during and after its implementation [7], [9]. Some of these issues are explained here briefly:

*1) **Interoperability and need for Standardization**:* Almost all the manufacturers build devices using their own underlying technologies which may not be available to others. Therefore, it is highly important to standardize IoT in order to render interoperability between objects.

*2) **Naming and Identity Management:*** IoT is a huge network connecting billions of devices and objects, each of which needs to be uniquely identifiable on the Internet. Hence, we need a robust and efficient naming mechanism to dynamically assign and monitor each object's identity.

*3) **Confidentiality of Information:*** IoT employs various types of identification technologies to identify objects such as 2D Barcodes, RFID Tags and so on. Since these tags are embedded in daily use objects, which carry their information, it becomes mandatory to ensure safety and confidentiality to such data [9]. It is also important to prevent unauthorized access to this information.

*4) **Network security:*** Sensor devices in the IoT network send the data over the transmission channel, which can be wired or wireless. The entire transmission system must be robust and able to manage data coming from numerous sensor devices, also ensuring that no data is lost because of congestion in network. The system must also ensure efficient security measures for the data that is transmitted preventing it from any form of external interference.

*5) **Objects security and safety:*** IoT network constitutes of large number of objects which are spread geographically, therefore it becomes highly important to monitor and prevent any unauthorized access to these objects which may damage them physically or alter their operation.

*6) **Greening of IoT:*** The energy consumed by the network is increasing rapidly because of high data rates, large number of Internet-enabled applications and huge growth rate of edge-devices connected to the Internet. This network energy consumption will increase significantly with the IoT in future. Therefore, there is a need to make these network devices energy efficient with the use of green technologies.

VII. CONCLUSIONS

The paper reviewed the upcoming future of the Internet known as "Internet of Things" which will let everything and everyone connect. IoT works with intelligent sensor devices in order to communicate independently, exchange important information and make informed decisions. In simple terms, IoT transforms the current mode of communication that is majorly human to human into human to machine and machine to machine. The paper briefly explained the workflow of IoT, proposed generic architecture for IoT, described probable applications for future, mentioned some of the most important technologies used in IoT and lastly addressed some of the key issues linked with the implementation of IoT. IoT is still a new field in its infant stage and needs a lot of research to tackle the challenges for its successful implementation. But once successfully implemented, it has the ability to render numerous benefits personally, professionally and economically.

REFERENCES

[1] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, Wei Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications", in IEEE Internet of Things Journal (Volume: 4, Issue: 5, Oct 2017), March 2017.

[2] Khan, R., Khan, S. U., Zaheer, R., & Khan, S., "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in 10th International Conference on Frontiers of Information Technology (FIT), 2012.

[3] Joshua E. Siegel, Sumeet Kumar, Sanjay E. Sarma, "The Future Internet of Things: Secure, Efficient, and Model-Based", in IEEE Internet of Things Journal (Volume: 5, Issue: 4 , Aug. 2018), Oct 2017

[4] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li and Hongbin Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things", IEEE Internet of Things Journal (Volume: 4 , Issue: 5 , Oct. 2017), April 2017.

[5] John A. Stankovic, "Research Directions for the Internet of Things", IEEE Internet of Things Journal (Volume: 1, Issue: 1 , Feb. 2014), March 2014.

[6] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi and Talha Kamal, "A Review on Internet of Things (IoT)",in International Journal of Computer Applications, Volume 113-No.1, March 2015

[7] Borgia, E., Special Issue on "Ïnternet of Things: Research Challenges and Solutions (editorial)". *Computer Communications*, Volumes 89–90, 1 September 2016, Pages 1-4.

[8] Anne H. Ngu, Mario Gutierrez, Vangelis Metsis, Surya Nepal, Quan Z. Sheng, "IoT Middleware: A Survey on Issues and Enabling Technologies" in IEEE Internet of Things Journal (Volume: 4 , Issue: 1 , Feb. 2017) 1-20, Oct 2016.

[9] J. Zheng, D. Simplot-Ryl, C. Bisdikian, & H. Mouftah, "The Internet of Things," in IEEE Communications Magazine, Volume: 49, Issue: 11, pp: 30-31, 2011.

[10] Feng Wang, Liang Hu, Jiejun Hu, Jin Zhou, Kuo Zhao, "Recent Advances in the Internet of Things: Multiple Perspective" in IETE Tech. Rev. 2016