A Survey on Internet of Things

Reshma Thomas[1]*, Somya Arya[2] & Dr. Kavita Khanna[3]

[1]Depart. of CSE, The Northcap Uni., Gurgaon, India,
*Corresponding Author E-mail: *reshma15csp013@ncuindia.edu*

[2]Depart. of CSE, The Northcap Uni., Gurgaon, India, E-mail: *somyaarya28@gmail.com*

[3]Assoc. Prof., CSE & IT, The Northcap Uni., Gurgaon, India, E-mail: *kavitakhanna@ncuindia.edu*

Abstract: One of the catchwords in the Information Technology is Internet of Things (IoT), wherein day-to-day objects having the capabilities of sensing, networking & processing would be interconnected & would communicate with different devices & services over the Internet [1,2]. Eventually, IoT devices will be able to sense their surroundings and adapt their behaviour accordingly or become responsive to the presence of people. Since IoT devices are being deployed increasingly, there are uncertainties about its security & privacy [5]. In this paper, an overview of IoT, architecture, different technologies used, mobile Crowdsensing applications, detailed analysis of IoT security issues, challenges, existing applications & future directions have been discussed.

Keywords*:* Internet of Things, RFID, Bluetooth, Wireless Sensor Networks, Security Challenges

I. INTRODUCTION

The Internet of Things (IoT) standard has become popular of late. The phrase "Internet of Things" also known as IoT is originated from the two words i.e. the first word is "Internet" and the second word is "Things" [1]. The word '*thing'* in the IoT means the thing's information. The connotation of the word IoT is "an Internet application sharing the thing's information in the whole world" [10]. IoT devices comprise personal computers, laptops, tablets, smart phones and other small size embedded devices. A Thing is an object of our everyday life placed in our everyday environment. It can be anything- from persons to animals to lights, table etc. The best definition for the IOT would be [1]:

"A network inclusive of smart objects that have the scope to share information, auto-arrange, reacting and acting when there is any change in the environment".

The core concepts of IoT are not new [2]. RFID, sensor networks have already been used in manufacturing and industrial context. Recently IoT has become evident as an enabling technology for the smart gird, smart health, smart transportation, and smart environment as well as for smart cities [8]. Smart home devices, distributed renewable energy resources and power substations come under the major smart grid devices. It's estimated that by the year 2020, IoT will have around 75 billion devices connected to it [3]. Therefore, to manage the huge amount of data generated by the IoT, data analytics will be required. Riggins and Wamba [3] have proposed a framework for analyzing the adoption, usage and impact of the Internet of Things enabled through the use of big data analytics. In [4], analysis of IoT attack surfaces, threat models, requirements, security issues, forensics, and challenges has been done in detail. Ennis et. al [5] have presented an intelligent doorbell system that has been designed to prevent doorstep crimes from happening. Existing Mobile Crowdsensing applications, their unique characteristics various research challenges and their solutions have been discussed in [6]. A conceptual model for the smart grid within the Internet of Things context has been proposed by Al-Ali and Aburukba [7], and also the smart grid existing

communication protocols have been explored. [8] surveys the middlewares that have already been designed for IoT and emphasizes on various technical challenges in this domain. Various security issues and challenges have been analyzed in [9].

II. ARCHITECTURE

Architectures help to represent, organize and structure the IoT in a way that it functions effectively [2]. It can be classified into hardware/network, software, and process.

A. Hardware or network architecture

To support the distributed processing environments that IoT needs, varied hardware or network architectures have been proposed. These include peer-to-peer (Andreini et al. 2010), EPC global (Yun and Yuxin 2010), and autonomic (Pujolle 2006).

B. Software architecture

IoT devices offer services, for which software architecture is necessary for its access and sharing.

C. Architecture for Processes

Business processes will surely be affected by the IoT. To productively structure the business processes, process architectures are needed. Normally, the four principal levels of IOT are as shown in fig.1, [3]:

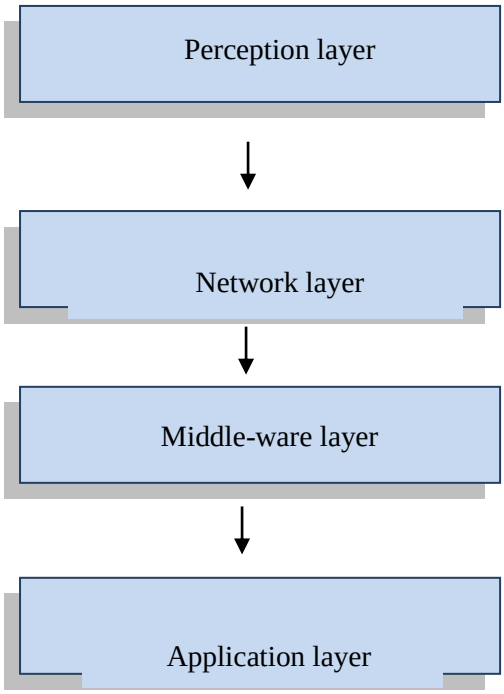

Figure 1. Four principal levels of IoT

I. Perception Layer

This layer comprises of different kinds of data sensors like RFID, Barcodes, or any other sensor network. Basically, it identifies the distinctive objects and deals with the data that has been collected from the real world by its respective sensor(s).

II. Network Layer

With the help of existing communication networks like Internet etc., the network layer transmits the information gathered, obtained from the above layer i.e. perception layer, to any data processing system.

III. Middle-ware Layer

Between the connected devices, the middle-ware layer ensures same service. In this layer, data processing systems are present that take actions automatically based on the results generated after data is processed and link the system with the database which provides storage capabilities to the collected data.

IV. Application Layer

This layer understands various practical IoT applications based on the user requirements and different type of industries such as Smart Home, Smart Environment, Smart Transportation and Smart Hospital etc.

III. TECHNOLOGIES

Originally, the RFID community members inspired the concept of IoT [1]. In [11], the key IoT technologies that have been included are RFID and UID/EPC.

A. Radio Frequency Identification(RFID)

RFID is a technique that helps in transmitting an object's or person's identity wirelessly using radio waves in the form of a serial number [1]. It has been used to track objects that have tags attached to them. Identification issues can be solved in a cost-effective way using RFID technology. The main RFID elements include tag, antenna, reader, access controller, server and software [10]. It is more reliable, effective, secured, low- priced and precise.

B. Internet Protocol (IP)

IP is the most important communications protocol in the IP suite for transmitting datagrams across network boundaries. IP has two versions: IPv4 and IPv6 [1]. Each of the two versions defines an IP address differently. IP address is basically a numerical label which is assigned to each device getting involved in a computer network that uses the IP for communication. The general term IP address usually still refers to the addresses that are defined by IPv4.

C. Electronic Product Code(EPC)

EPC is a distinct number used in a system where people, information, resources etc. involve moving of a product from supplier to customer to identify a specific item [1]. EPCs have varied representations, inclusive of binary forms that are suitable for use on RFID tags, and text forms that are suitable for sharing the data among organization data systems.

D. Bluetooth

Bluetooth is a wireless technology via which we can interchange data over short range from fixed and mobile devices. It banishes the need for exclusive wiring between devices such as handheld personal computers, printers etc. Bluetooth devices share a common channel for communication. A set of such devices is called Piconet [1]. At a time, 2-8 devices can be used for sharing the data in a Piconet, and that data may be anything from a text, picture to video and sound.

E. ZigBee

To enhance the structure of wireless sensor networks, one of the protocols, Zigbee, has been developed. It is inexpensive, of relatively short transmission range, is scalable, reliable, has a flexible protocol design [1]. It is broadly used in home automation, medical monitoring etc.

F. Near Filed Communication (NFC)

NFC is a wireless technology effective over short-distances. As making transactions and exchanging digital content becomes simpler, consumer's life becomes easier with NFC technology. When devices are touched together or brought near to one another, devices can become involved in radio communication with one another.

G. Actuators

An actuator is a machine's element that is accountable for controlling or moving a mechanism or system. It needs a control signal and a source of energy. The former is relatively low energy and may be electric voltage or current, pneumatic or hydraulic pressure, or even human power. Electric actuators are the most commonly used type.

H. Wireless Sensor Networks (WSN)

Sensors help in observing the features of the environment or other entities such as temperature, atmospheric moisture, motion, and quantity. When more than one sensor is used to interact, the network so formed is referred to as a WSN. A WSN is an important component in IoT model [1]. IoT based WSN has received phenomenal attention in many areas including security, military, health maintenance, precision agriculture monitoring and so on.

I. Artificial Intelligence (AI)

AI is a field where machines can solve problems that are normally done by humans with their natural intelligence. In an electronic environment, devices become sensitive and responsive to the people's presence. This type of environment is referred to as ambient intelligence in a world of ambient intellect, these devices make it easier for the people to carry out their everyday life activities using Information and Intelligence. These devices can be context aware, recognizing you and your

situational context, can predict your desires without planned intervention. You can even customize them according to your needs.

IV. TECHNIQUE

Mobile Crowdsensing(MCS) that has been discussed in [7] is basically a technique where people having smartphones, wearables etc. collectively share data and extract information of common interest in order to survey, estimate or predict any processes. IoT applications can be categorized into two types- Personal sensing application, which is applicable to an individual, and, Community sensing, which involves monitoring of large scale phenomena [7]. For example, monitoring of a person's movement patterns would come under personal sensing whereas traffic congestion monitoring and air pollution level monitoring in intelligent transport system would fall under the second category. Further, the community sensing applications can be categorized into-Participatory sensing and Opportunistic sensing. When active participation of individuals is needed, it refers to as participatory sensing and when minimal involvement of user is required, it's known as opportunistic sensing.

Some unique characteristics of MCS are:

- Today's edge devices (smartphones etc) have more computing, communication and storage devices.

- Millions of these devices are already set up: People take these mobile devices wherever they go.

One of the complex problems that has come out is identifying the correct devices to generate the required data and also directing them to sense without proper frameworks in order to ensure the expected quality.

The smart grid devices which have been included in [8] include smart home devices, distributed renewable energy resources and power substations. NIST (National Institute of Standards and Technology) formed an abstract model for the smart grid for a better understanding. Smart home devices, renewable energy resources, substation devices will be assigned IPV6 address in order to represent the smart grid within the context of IoT [8].

V. EXISTING APPLICATIONS

MCS applications have been grouped into three categories [7] - environmental, infrastructure, and social.

- Environmental MCS applications: A prototype set up for monitoring the pollution is Common Sense. Mobiles communicate with various handheld air quality devices to measure air pollutants. Another example is CreekWatch, which combines reports from individuals to monitor the levels of water and quality in creeks.

- Infrastructure MCS applications: One of the examples of MCS implementations that has been done before that measured traffic congestion levels in cities is MIT's CarTel, which on using specialized devices can measure the car's location and speed and can even transmit the values it has measured to a central server using public Wi-Fi hotspots. Other examples include ParkNet, which on using ultrasonic devices installed on cars, can detect available parking spots, Nericell, which can determine the average speed of cars or traffic delays and detect the honking levels.

- Social MCS applications: In this category individuals share sensed information among themselves. Examples are BikeNet and DietSense. In BikeNet, people estimate location and the quality of the bike route, for example, how much C02 content is present on the route and compile the data to obtain the most suitable route for biking. In DietSense, individuals compare their eating habits by taking photographs of what they eat and share it within a community.

Other existing works include-

- TinyREST [9] is a framework for incorporating sensor networks into the internet. It basically gives us an idea on how we can combine sensors or actuators and sensor networks with the Internet through a system that sets up home services based on a middleware layer.

- Another project which is RFID based is the Fosstrak [9], whose focus is on the management of applications related to RFID. It is an open source RFID platform.

Ennis et. al [5] have designed an intelligent doorbell system solution which is targeted mainly at the older population to prevent them from doorstep crime. As soon as a person is in front of the door, his image will be captured and a notification would be sent to the older person. He can even seek assistance from a career and the carer can assist the old person whether or not to let the person in.

Middleware, which has been discussed in [9], is software that serves as a bridge between the infrastructure and the applications using it. [9] surveys the middlewares that have already been designed for IoT and emphasizes on different technical challenges in this domain.

VI. TECHNICAL CHALLENGES

A. Scalabity

Scalability looks like one of the big challenges that the middleware approaches faced since it's expected that IoT would support a wide range of devices. To effectively manage scalability issues, a dependable IoT middleware is required [9].

B. Interoperability

It's the ability to exchange and make use of information. This is also a very big challenge for the middleware approaches since a large number of devices are believed to integrate together in transmission and in exchange of information.

C. Unfixed Infrastructure

Each device in the IoT should not require a fixed infrastructure rather it should be efficient enough to announce its reality and the resources it provides.

D. Spontaneous Interaction

Since the movement of things cause sudden interactions, unplanned events are generated. Due to this, there is a need of middleware to manage events.

VII. SECURITY GOALS

The major security goals include data confidentiality, data integrity and data availability.

A. Data Confidentiality [5]

It is the ability to allow authorized users to access sensitive and protected data. There are many security mechanisms to provide data confidentiality- Data Encryption: a way in which the data can be converted into a form which is not readable (ciphertext), the Two-step verification: a process which involves two authentication methods and allows the access only if the two dependent components pass the authentication test and the most common Biometric Verification, by means which every person cab be uniquely identified [12].

B. Data Integrity [5]

It's quite possible that while the communication is happening, cybercriminals could alter the data or the data could be affected by various other factors. Data Integrity aims to protect the useful information from the cybercriminals, so that the data cannot be interfered without the system catching the threat [13].

C. Data Availability [5]

IoT security's one of the main goals is to make data available to its users, whenever required. This goal ensures that the IoT services are available to the authorized parties when needed. It's quite possible that the availability of data is denied at the user-end due to DoS attack. So to countermeasure the attacks on the services, it is essential to provide firewalls.

VIII. SECURITY, CHALLENGES AND ISSUES

Few threats that are present in the architectural layer and need special attention are discussed below:

A. Unauthorized Access to the Tags

Since every RFID system doesn't have a proper mechanism for authentication, someone without having authorization also can accessed the tag.

B. Radio Frequency Jamming

RF Jammers can disturb the communication happening via RF signals by compromising the RFID tags.

C. Malicious code injection

In this kind of attack, an attacker can inject a malicious code into the system by compromising a node. Because of this, the whole network can even shutdown or in the worst case, a full control of the network can be obtained by the attacker.

D. Man-in-the-Middle Attack

In this attack, the communication channel is affected allowing any unauthorized party to monitor all the private communications between the two parties hideously.

E. Malicious Insider

Whenever an insider succeeds in extracting the data and later on alters it on purpose, this kind of attack is known to occur.

Some of the approaches that have been discussed in [3] for preserving privacy are:

a) Anonymization

Before sharing any information with a third party, this approach would remove any identifying information from the sensor data.

b) Secure multiparty computation

Many cryptographic techniques are available. It uses these techniques to transform the data.

c) Data perturbation

This is one of the appropriate approaches that adds noise to the sensor data and helps in preserving privacy.

- Resource constraints need to be addressed in a holistic manner [4].

IX. FUTURE WORK AND CONCLUSION

In this literature review, we have provided a survey on IoT architecture, technologies, existing applications in designing middleware systems. In addition to this, we have discussed about the technical and security challenges and what are the issues that require further research. It also gives light onto the future scope. An integrated architecture is currently being explored at a societal scale for collecting and processing sensor data from the mobile sensing devices. Additionally, we need to explore the open issues like data storage, security and privacy, and propose possible methods to resolve them.

Conflict of interest: The authors declare that they have no conflict of interest.

Ethical statement: The authors declare that they have followed ethical responsibilities

REFERENCES

[1] Madakam et. Al(2015).Internet of Things(IoT):A Literature Review.Journal of Computer and Communications
[2] Whitmore et. al (2015).The Internet of Things—A survey of topics and trends. Inf Syst Front (2015).
[3] Riggins and Wamba(2015).Research Directions on the Adoption, Usage and Impact of the Internet of Things through the Use of Big Data Analytics.The 48 Hawaii International Conferences on System Sciences.
[4] Farooq et. Al(February 2015). A Critical Analysis on the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications Volume 111 - No. 7.
[5] Ennis et. al "Doorstep: A doorbell security system for the prevention of doorstep crime", IEEE 2016.
[6] K. Ganti et. Al(November 2011).Mobile Crowdsensing: Current State and Future Challenges.IEEE Communications Magazine.
[7] Al-Ali and Aburukba(2015).Role of Internet of Things in the Smart Grid Technology.Journal of Computer and Communications.

[8] Chaqfeh and Mohamed(2012).Challenges in Middleware Solutions for the Internet of Things.In Proc. of The 2012 International Conference on Collaboration Technologies and Systems.
[9] Yinghui Huang et. Al(2010).Descriptive Models for IoT. International Conference on Intelligent Control and Information Processing.

