# INTERNET OF THINGS (loT)

**[1]Ms. Yukta P. Mehta, [2]Mr. Vikas P. Dadhich , [3]Ms. Priya H. Pandey**

*Abstract*— **The Internet of Things (IoT) is the logical further developŵeŶt of todaǇ͛s IŶterŶet. Technological advancements lead to smart objects being capable of identifying, locating, sensing and connecting and thus leading to new forms of communication between people and things and things themselves. At the beginning we describe an overview of the Internet of Things. The Internet will continue to become ever more central to everyday life and work, but there is a new but complementary** ***vision for an Internet of Things (IoT), which will connect billions of objects – ͞thiŶgs͟ like sensors, monitors, and RFID devices – to the Internet at a scale that far outstrips use of the Internet as we know it. This paper studies the state-of-the-art of IoT and presents the key applications, challenges and future research areas in the domain of IoT. In addition to that we have added an idea about holographic camera with is related to security purpose in daily lifestyle.***

*Index terms*- **1.RFID 2.MEMS.**

## I. INTRODUCTION

THE INTERNET OF THINGS (IOT): "The Internet of Things" is a phrase coined by British technology pioneer Kevin Ashton who co-founded the Auto-ID Center at the Massachusetts Institute of Technology (MIT). The term describes a system where the Internet is connected to the physical world via ubiquitous sensors. It is now estimated by Cisco that by 2020 that as many as 50 billion devices of all types, shapes and sizes will be wirelessly connected to the internet.

The Internet of Things (IoT) is a computing concept that describes a future where every day physical objects will be connected to the Internet and be able to identify themselves to other devices. The term is closely identified with RFID as the method of communication, although it also may include other sensor technologies, wireless technologies or QR codes. The IoT is significant because an object that can represent itself digitally becomes something greater than the object by itself. No longer does the object relate just to you,

but is now connected to surrounding objects and database data. When many objects act in unison, they are known as having "ambient intelligence." "If we had computers that knew everything there was to know about things - using data they gathered without any help from us - we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best". Most of us think about being connected in terms of computers, tablets and smartphones. IoT describes a world where just about anything can be connected and communicate in an intelligent fashion. In other words, with the Internet of Things, the physical world is becoming one big information system.[2]The Internet of Things (IoT) is an environment in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to- computer interaction. IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS) and the Internet. The concept may also be referred to as the Internet of Everything. A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -- or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network. So far, the Internet of Things has been most closely associated with machine- to-machine (M2M) communication in manufacturing and power, oil and gas utilities.The first Internet appliance, for example, was a Coke machine at Carnegie Melon University in the early 1980s. The programmers could connect to the machine over the Internet, check the status of the machine and determine whether or not there would be a cold drink awaiting them, should they decide to make the trip down to the machine. [3]

## II. EXITING SYSTEM

### *A. Aims and objectives:-*

The aim of the Internet of Things Value

1.Creation Network is to:

2.Coordinate and help to increase and optimize the utilization of results and value creation in the area of IoT.

3.Identify research opportunities in IoT technology, applications and services.

4.Form a research and development community with cross disciplinary collaboration, including business, communication, nano electronics, microsystems, information systems, and software, with a focus on challenges in IoT issues. 5.Spawn continuing cross disciplinary collaboration among projects addressing the IoT at national and international level.[4]

Primary Objectives of IoT Platforms

- Data collection from various devices and data sources
- Storage of externally collected as well as internally generated data
- Stand-alone data processing and automatic decision taking
- Data visualization (developing an operator interface)
- Enterprise data integration (only for

Industrial IoT)

- Intelligent data exchange between devices [5]

Research the potential of IPv6 and related standards to support the future Internet of Things and to overcome its current fragmentation.

Develop a highly scalable IPv6-based Service-Oriented Architecture to achieve interoperability, mobility, cloud computing integration and intelligence distribution among heterogeneous smart things components, applications and services. Explore innovative forms of interactions with:

a) Multi-protocol integration & interoperability with heterogeneous devices.

b) Mobile & cellular networks. [6]

*B. Key Components of the IoT:-*

- Power of IoT comes from combination of:

– Faster & smaller microprocessors

–Smaller & better sensors (& cameras)

– More ubiquitous & robust wireless networks

– Expanding cloud storage capacity

– Enhanced “big data” capabilities

- It’s the miniaturization of everything that matters

– Both in terms of device size & cost[7]

*Security:-*

*C. Object-level security*

Security best practice has always indicated that the loss of physical security is tantamount to a logical breach, yet some early elements of the IoT incorporate that very flaw into their design. CISOs will need to be mindful, therefore, of the location and focus of the security provision.

Security must be addressed throughout the device lifecycle, from the initial design to the operational environment: 1. Secure booting: When power is first introduced to the device, the authenticity and integrity of the software on the device is verified using cryptographically generated digital signatures. The foundation of trust has been established, but the device still needs protection from various run-time threats and malicious intentions. 2. Access control:

Next, different forms of resource and access control are applied. Mandatory or role-based access controls built into the operating system limit the privileges of device components and applications so they access only the resources they need to do their jobs. If any component is compromised, access control ensures that the intruder has as minimal access to other parts of the system as possible.. The principle of least privilege dictates that only the minimal access required to perform a function should be authorized in order to minimize the effectiveness of any breach of security. 3. Device authentication: Authentication allows a user to access a corporate network based on user name and password, machine authentication allows a device to access a network based on a similar set of credentials stored in a secure storage area. 4. Firewalling and IPS: The device also needs a firewall or deep packet inspection capability to control traffic that is destined to terminate at the device. The device needn’t concern itself with filtering higher-level, common Internet traffic—the network appliances should take care of that—but it does need to filter the specific data destined to terminate on that device in a way that makes optimal use of the limited computational resources available.

5. Updates and patches: Once the device is in operation, it will start receiving hot

patches and software updates. Software updates and security patches must be delivered in a way that conserves the limited bandwidth and intermittent connectivity of an embedded device and absolutely eliminates the possibility of compromising functional safety[10]

*D. Basic precautions*

Secure the wireless network: The old Wired Equivalent Privacy (WEP) protocol is still widely used, but it is weak and easily compromised. Make sure the home wireless network is instead protected by the Wi-Fi Protected Access II (WPA2) protocol and a strong, complex password.

Give your Wi-Fi network an obscure name,: or SSID, that doesn't give attackers personal information they can use in social- engineering attempts. For instance, don't call it "[Your Name] House." Instead, call it something random, such as "FBI Surveillance Van."

Disable guest network access entirely, and to be strict about who — or what — can get on the network.

Create two different Wi-Fi networks: if your router can handle multiple SSIDs. Trey Ford, global security strategist at security company Rapid7, suggests one network for computers, tablets and smartphones used for online banking shopping and general Web activity; another network can be for smart devices.

Good password management is essential. Neither network equipment (such as routers and switches) nor newfangled gadgets (such as smart TVs) should use default factory-set administrator passwords. Change each admin password to something suitably strong and complex, and regularly change them going forward. When possible, usernames should be also changed to make it even harder for attackers to brute-force their way in.[11]

CHALLENGES

1.DATACOLLECTION, PROTECTION AND PRIVACY:The vision for the IoT is to make our everyday lives easier and boost the efficiency and productivity of businesses and employees. The data collected will help us make smarter decisions. But this will also have an impact on privacy expectations. If data collected by connected devices is compromised it will undermine trust in the IoT. We are already seeing consumers place higher expectations on businesses and governments to safeguard their personal information.[11]

2. MINIATURIZATION

Electronic miniaturization is not simply a process of making everything smaller. Miniaturization of one phase of a product usually reveals limitations and obstacles in other parts of the overall design and manufacturing process. So progress often comes in uneven spurts, as advances in a specific technology—semiconductor fab, pc board, power, manufacturing, and packaging—leapfrog other technologies. Developments in several areas other than integrated-circuit dies are proving critical to the continued progress of miniaturization.[12]

3.SEMANTIC TECHNOLOGIES

The main description models for the Semantic Web include the Resource Description Framework (RDF)\, and the Web Ontology Language (OWL) is based on description logic and facilitates construction of ontologies for different domains. Semantic data can be accessed by software agents for query, reasoning and analysis purposes to derive additional knowledge from the represented data. There are also common software tools and open libraries such as Jena [and Sesame to work with semantic data.[13]

## III. FEATURES

*A. ADVANTAGES:-*

1.Minimize Cost and Area

Because many IoT devices will have to be very inexpensive and small, it is important to minimize the silicon area of these devices. In addition, silicon IP embedded in these chips, such as memory, should not only be as small as possible, but should

minimize any additional wafer processing cost due to extra masks or processing steps.

2.Field Programmability

To perform such tasks as setting user preferences or updating keys, embedded non-volatile memory will need to be programmable not only during chip manufacturing and test but also in the field with the chip installed in end-user equipment.

3. Low Voltage, Low Power

Many devices that will be connected in

the IoT ecosystem will run on small where battery replacement may be difficult or even impossible, power for wireless sensors may come from energy harvesting, either used directly or for recharging a small battery. These devices would convert the energy from motion, light, heat or an electromagnetic field into the electrical energy needed to power the sensor and, in some cases, an integrated processor. In these situations, the sensor, processor and any embedded memory would have to have low standby and operating power dissipation.

Provide Secure Data Storage

Many applications involving the exchange of sensitive data, such as point-of-sale and financial transactions, will require high code, key and data security. The memory that stores this information thus must have

a high level of physical security and be extremely difficult to reverse engineer.[14]

## IV. SCOPE

The Internet of Things (IoT) is transforming the everyday physical objects that surround us into an ecosystem of information that will enrich our lives. From refrigerators to parking spaces to houses, the IoT is bringing more and more things into the digital fold every day, which will likely make the IoT a multi-trillion dollar industry in the near future. While the IoT represents the convergence of advances in miniaturization, wireless connectivity, increased data storage capacity and batteries, the IoT wouldn't be possible without sensors. Sensors detect and measure changes in position, temperature, light, etc. and they are necessary to turn billions of objects into data-generating "things" that can report on their status, and in some cases, interact with their environment. Because sensor endpoints fundamentally enable the IoT, sensor investments are an early indicator of the IoT's progress. And, according to PwC's.

THE FUTURE OF THINGS
Forecasts For Future Developments in The Global High Tech Economy: 2014-2020

6th Annual Digital IQ survey of nearly

1,500 business and technology executives, the IoT movement is underway.[15]

Aerospace and aviation (systems status monitoring, green operations)

Automotive (systems status monitoring, V2V and V2I communication) Telecommunications

Intelligent Buildings (automatic energy metering/ home automation/ wireless monitoring)

Medical Technology, Healthcare, (personal area networks, monitoring of parameters, positioning, real time location systems) Independent Living (wellness, mobility, monitoring of an aging population) Pharmaceutical, Retail, Logistics, Supply Chain Management, Manufacturing, Product Lifecycle Management, Processing industries - Oil and Gas, Safety, Security and Privacy, Environment Monitoring People and Goods Transportation, Food traceability, Agriculture and Breeding Media, entertainment and Ticketing, Recycling.

The IoT connects things such as manufacturing facilities and transportation systems to the internet. These devices make valuable data available in real-time. IoT enabled units are available in road, railway, and automotive sensors, advanced medical devices, factory automation sensors,

industrial robotics, agricultural sensors, and electrical transmission sensors. In fact, IoT devices can be found in virtually any area which involves tracking and tracing of information. The huge volumes of data collected via the Internet of Things in laboratories or manufacturing facilities would benefit from the storage and organizational capacity of a Laboratory Information

Management System (LIMS). Those organizations that capture and analyze this wealth data efficiently will reap tremendous benefits from the Internet of Things. LIMS are used in clinical, biological and chemical laboratories for instrument management and analytical activities. They can help track information in the production process and supply chain for businesses across a variety of industries. Data Management systems which offer the ability to marry the online data captured from IoT sensors with offline analytical results provide a huge value proposition for engineers looking to track and trend production operations. The Internet of Things is an evolving technology which will work hand-in-hand with next-generation LIMS installations.[16] We all are aware of the high number of uncertainty takes place around us. Its one of the important issues we need to handle and make our life safer. As IoT is making itself wider and more advance it may solve our problems .As we already know IoT is going to make art of holography possible. It gives us idea about holographic 3D camera this holographic 3D camera will create virtual camera image of main camera in 'n' direction we need. Take an assumption that uncertainty occurs and someone tries to enter the security surveillance area and try to shatter camera it may be or may not be the original camera because the camera are image of each other it will be difficult to guess the original camera if poacher shatter the anyone of this camera it will break the laser security and siren will be activated and all the gates of the society or building will be closed which will prevent the uncertainty and may also save our life.

## References

1. http://www.ttiinc.com/object/me- zogbi-20140109.html
2. https://www.techopedia.com/defini tion/28247/internet-of-things-iot
3. http://internetofthingsagenda.techtarget.com/definition/IoT-security- Internet-of-Things-security
4. http://www.internet-of- things.no/objectives.html
5. http://www.slideshare.net/AggreGa te1/internet-of-things-anatomy
6. http://googleweblight.com/?lite_url

=http://iot6.eu/aims_and_objective s&ei=MS0lbCXA&lc=en- IN&s=1&m=45&ts=1452167045&

sig=ALL1Aj5djxPTbsjzWW_AqhJ CvZ0DOkiYeg
7. http://www.slideshare.net/athierer/i nternet-of-things-wearable- technology-sept-2014

8. https://www.slideshare.net/mobile/TheMarketingDistillery/iot- presentation
9. http://www.windriver.com/whitepa pers/security-in-the-internet-of- things/wr_security-in-the-internet- of-things.pdf
10. http://www.anypresence.com/blog/

2015/07/20/key-components-iot- application-platform/
11. http://www.securingtomorrow.com

/blog/knowledge/3-key-security- challenges-internet-things/
12. http://electronicdesign.com/boards/ many-technologies-contribute- miniaturization
13. http://senzations.net/wp-content/uploads/2014/08/SenZation s_Semantic_PB.pdf
14. https://www.silabs.com/iot/Pages/i ot-applications.aspx
15. https://www.pwc.com/us/en/increa sing-it-effectiveness/assets/future- of-the-internet-of-things.pdf
16. http://www.corelims.com/the- future-of-the-internet-of-things-iot/