ISSN No. 0976-5697

Volume 8, No. 1, Jan-Feb 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Survey on Internet of Things [IoT]

A. Bhuvaneswari
Asst.Professor, Department of Computer Science,
Cauvery College for Women, Trichy, India

***Abstract*:** Today's communication technology supports humans to lead their life more sophisticatedly. The next step towards the sophistication is remotely controlling anything at anytime and anywhere without physical human intervention. This can be achieved by Internet of Things (IoT) which transforms the real world objects into intelligent virtual object. IoT integrates everything under a common infrastructure. This paper focuses to provide an overview of IoT, architecture, supporting protocols, applications and challenges

***Keywords*:** Internet of Things, RFID, Sensors, Actuators

I. INTRODUCTION

The Internet and Communication Technology grows rapidly with unimaginable advancement. Recent technological research mainly focuses on Internet of Things (IoT) which comes with two paradigms "Internet" and "Things". The basic idea of IoT is the presence of a variety of things or objects such as Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones etc. and interconnection of smart devices, buildings and others which are embedded with electronics, software, sensors, actuators and network connectivity enables these objects to collect and exchanges data. Communication between these things is achieved using routing protocols in a decentralized, self-organized and changing infrastructure. By giving each product a unique identifier and making it data available through the web, the IoT promises to enable product traceability throughout the product lifecycle. Technologies like RFID, Near Field Communication (NFC), Machine-to-Machine Communication (M2M) and Vehicular-to-Vehicular communication (V2V) are used to implement the current concept of IoT [1]. In future, Internet nodes may reside everyday things – food packages, furniture, paper documents and more. Hence everyday objects become information security risks. By providing high degree of smartness, interoperability of interconnected devices with autonomous behavior is possible [2]. IoT enabled things can be characterized by low resources in terms of both computation and energy capacity. Special attention is needed for resource efficiency and scalability problem.

The rest of this paper is organized as follows. Section 2 describes different definitions of IoT. Section 3 describes what technologies used for IoT. Section 4 describes the characteristics of IoT. Section 5 depicts the architecture of IoT. Section 6 discusses about routing protocols used for IoT. Section 7 provides the security and privacy concern of IoT and Section 8 lists the application of IoT. Section 9 outlines the challenges and future directions of IoT and Section 10 concludes the survey.

II. DEFINITIONS

Semantically "Internet of Things can be defined as, "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" [2][6]. Syntactically Internet of Things composed of two terms. The first one represents network oriented vision of IoT, while the second one focuses on "objects" to be integrated into a common framework. The common idea about the first version of the Internet was about data created by people, while the next version is about data created by things. Fig.1 depicts the different visions of IoT. The "Internet of Things" allows people and things to be connected Any1me, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service. Fig.2 shows the definition of Internet of Things.

- 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. **(Wikipedia)**
- The term "Internet of Things" has come to describe a number of technologies and research disciplines that enable the Internet to reach out into the real world of physical objects. **(IoT 2008)**
- "Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts". **(IoT in 2020)**

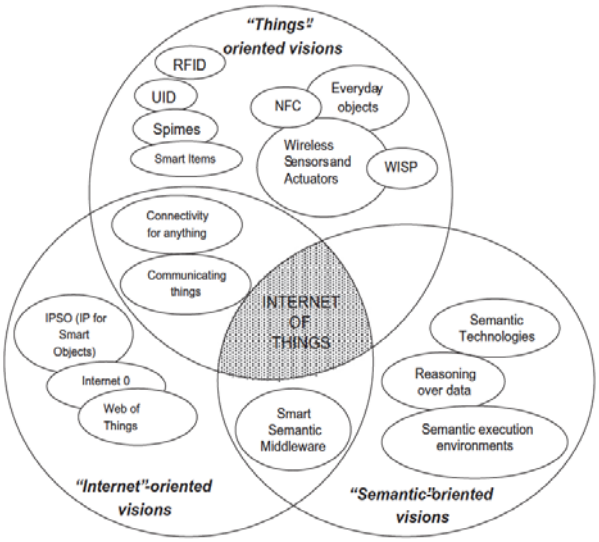

Fig.1. IoT as a result of the convergence of different visions [2]

Fig.2. Definition of Internet of Things **[S**ource: Perera et al. 2014]

III. TECHNOLOGIES INVOLVED

To implement the concept of Internet of Things, several technologies can be used such as,

- Radio Frequency Identification (RFID)
- Near Field Communication (NFC)
- Machine-to-Machine Communication (M2M)
- Vehicle-to-Vehicle Communication (V2V)

A. Radio Frequency Identification (RFID) [1][13]

RFID tag or label is a tiny microchip combined with an antenna. The antenna picks up the signals from an RFID reader and then returns the signal with additional information. The main aspect of RFID technology is item traceability and addressability. RFID is composed of one are more readers and several RFID tags. Each tag is provided with a specific address and is applied to the objects. Radio frequencies are used by the tags to transfer data attached to an objects. Information which is stored electronically in tags can be read by the RFID reader which monitor objects in real-time without the need of being in line-of-sight [1].

1) Different Configurations of RFID [1]:

Passive Reader Active Tag (PRAT) in which the reader is passive and receives signal from the battery operated active tags. The transmission range of RFID and the reader is from 1-2000 feet depending upon the architecture.

Active Reader Passive Tag (ARPT), which harvests the required energy to send data from the signal sent by the RFID reader because the tag does not have onboard power supplies. This is most commonly used.

Active Reader Active Tag (ARAT) in which both the reader and the tags are active, but the tags are only invoked by the reader when it comes in the proximity of the reader.

$$\text{Power Gain} = \frac{\text{Power of Signal Received by the Receiver}}{\text{Power of Signal transmitted by the same reader}}$$

2) Electronic Product Code (EPC) [1]

An Electronic Product Code (EPC) is a data stored tag of 96-bit wide. Out of 96-bit first 8 bits identifies the version of the protocol. The next 28 bits identify the organization that manages the data for this tag, the organization ID is assigned by the EPCGlobal consortium. The next 24-bits identify the kind of product; the last 36 bits are unique serial number for the tag. The last two fields are set by the organization that distributes the tag. The entire EPC number can be used as a key into global database to identify a particular product [1]. Fig.3 shows the structure of RFID code.

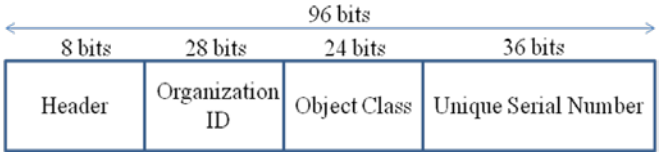

Fig.3. RFID Code

3) Near Field Communication (NFC) [1]:

NFC can be considered as an integration of RFID reader into a mobile phone. NFC operates within unlicensed Radio Frequency band. Operating range of NFC device is 20 cm, but it is directly depended on the size of the antenna in the device. NFC is a short range, low power wireless link and transfer small amount of data between two devices. No paring is required like Bluetooth before data transfer. This type of communication is safe because this cannot be done remotely.

4) Machine-to-Machine Communication (M2M) [1]:

M2M refers to the communication between computers, embedded processors, smart sensors, actuators and mobile devices. M2M is a five part structure. 1) M2M device capable of replying to request for data contained within that device. 2) M2M Area Network provides connectivity between M2M Devices and Gateways. 3) M2M Gateway ensures inter-working and inter-connection of communication networks of M2M Devices. 4) M2M Communication Networks enables the communication s between M2M Gateways and M2M Application. 5) M2M Applications contains the middleware layer where data goes through various application services.

3.5 Vehicle-to-Vehicle Communication (V2V) [1]:

V2V network doesn't have fixed topology as vehicles are moving from one place to another all the time. Vehicular networks can be applicable for safety and collision avoidance, traffic infrastructure and entertainment services. Vehicles communicate in two ways, which is vehicle-to-vehicle communication and vehicle with road side infrastructure.

IV. CHARACTERISTICS OF IOT

Characteristics of IoT can be categorized based on how intelligently it extracts knowledge from data, heterogeneous architecture to support many objects, complexity over dynamic changing of objects, scalability because of new things get into the network, parallel events, location identification and utilizing resources as a service.

- Intelligence – knowledge extraction from the generated data
- Architecture - A hybrid architecture supporting many objects
- Complex System - A diverse set of dynamically changing objects
- Size Considerations – Scalability
- Time Considerations – Billions of parallel and simultaneous events
- Space Considerations – Localization
- Everything-as-a-service – Consuming resources as a service

V. ARCHITECTURE

Until now IoT doesn't have proposed and uniform architecture. According to the recommendations of the International Telecommunication Union (ITU), the network, architecture of Internet of Things consists of,

A. Sensor, Connectivity and Network Layer:

This layer consists of RFID tags, sensors which are essential part of IoT. These are wireless devices which forms Wireless Sensor Network (WSN). Sensors collect real-time information and process it. This layer is also has the network connectivity which communicates the raw data to the next layer. WSN device have finite storage capacity, minimum bandwidth and low processing speed.

B. Gateway and Network Layer:

Gateways are responsible for routing the data coming from the Sensor, connectivity and network layer and pass it to the Management Service Layer. This layer having large storage capacity to store the data collected by the sensors, RFID tags etc. This layer is responsible for integrating various network protocols.

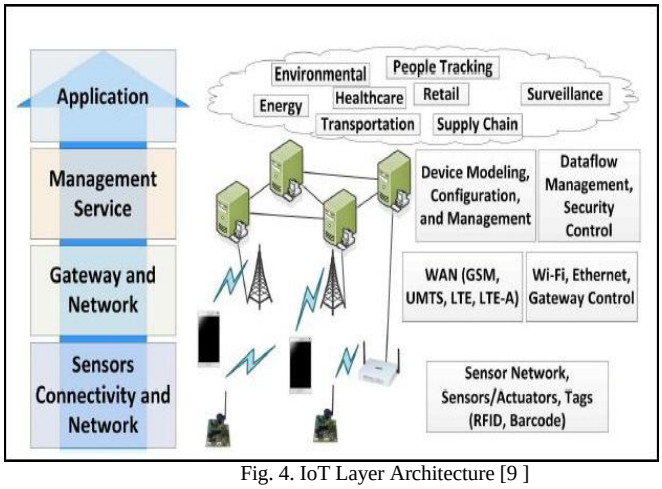

Fig. 4. IoT Layer Architecture [9]

C. Management Service Layer

This layer is responsible for Securing Analysis of IoT devices, Analysis of Information and Device Management. Data management is extracting the necessary information from the raw data collected by sensors and provides a valuable result. For immediate request this layer provides abstract data, extract information and manage the data flow. This layer is responsible for data mining, text mining, service analytics etc.

D. Application Layer

Application layer forms the topmost layer of IoT architecture which are responsible for effective utilization of the data collected. Various IoT applications include Home Automation, E-health, E-Government etc.

VI. ROUTING PROTOCOLS

Routing protocols of IoT can be categorized based on the layer in which it is used [3][9]. Like computer network's OSI Reference model, IoT also has same layers like datalink, network and transport/session layers. The datalink layer connects two IoT elements which can be two sensors or the sensor and gateway that connects a set of sensors to the Internet.

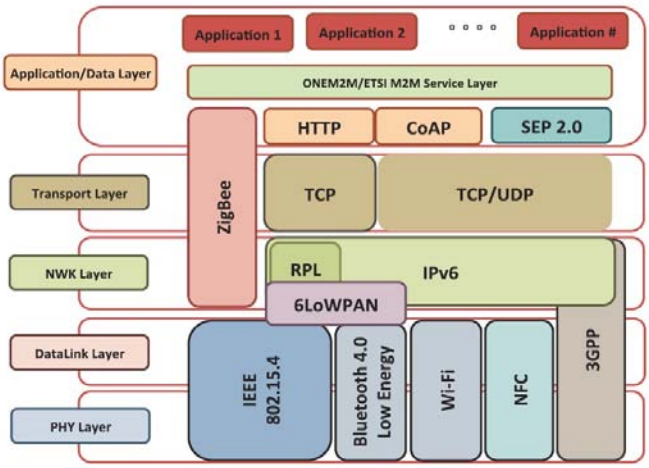

Fig.5 Protocols used in IoT Layers [8]

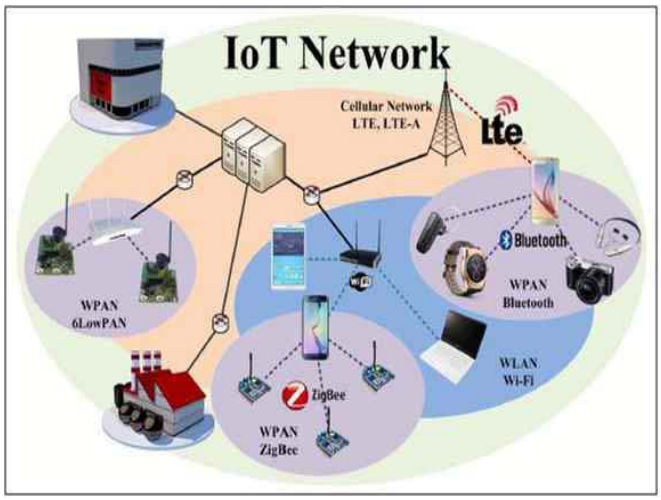

Fig.6 Elements and Protocols used in IoT Network [9]

A. IoT Data Link Protocol [3]

In this section, physical (PHY) and MAC layer protocols are discussed which are mostly combined.

1) IEEE 802.15.4e: IEEE 802.15.4e is the commonly used IoT standards for MAC which is the extension of IEEE 802.15.4. It defines the frame format; header includes source and destination addresses, and the communication between nodes. It support low power communication. It uses time synchronization and channel hopping to enable high reliability, low cost.

2) IEEE 802.11 AH: This protocol is a low energy version of the IEEE 802.11 (Wi-Fi) wireless medium which is used for all digital devices like laptops, tablets, and digital TVs. IEEE 802.11 ah includes synchronization of frames, bidirectional packet exchange, short MAC frame of about 12 bytes, null data packet with a tiny signal and increase sleep time and waking up occasionally to exchange data only.

3) Wireless HART: WirelessHART protocol operates pn the top of IEEE 802.15.4 PHY and adopts Time Division Multiple Access (TDMA) in its MAC. It is a secure and reliable protocol used for advanced encryption and calculates the integrity to offer reliability.

4) Z-Wave: Z-Wave is a low-power MAC protocol designed for home automation and used for IoT communication for smart home and small commercial domains. It covers upto 30 meter point-to-point communication. It uses CSMA/CA for collision detection and ACK message for reliable transmission. . It follows master/slave architecture

5) Bluetooth Low Energy: Bluetooth low energy or Bluetooth smart is a short range communication protocol with PHY and MAC layer and widely used for in-vehicle networking. It provides low latency and fast transmission. It follows master/slave architecture with two types of frames: adverting and data frames.

6) ZigBee: ZigBee supports a wide range of network topologies including star, peer-to-peer, or cluster-tree. ZigBee standard defines two stack profiles: ZigBee and ZigBee Pro. These stack profiles support full mesh networking and work with different applications allowing implementations with low memory and processing power. ZigBee Pro offers more features including security using symmetric-key exchange, scalability using stochastic address assignment, and better performance using efficient many-to-one routing mechanisms.

7) DASH7: DASH7 is a wireless communication protocol for active RFID that operates using Industrial Scientific Medical (ISM) band. It is designed for scalable, long range outdoor coverage with higher data rate comparing with Zigbee. Low cost, supports encryption and IPv6 addressing.

8) HomePlug: HomePlug GreenPHY (HomePlugGP) is developed by HomePlug Powerline Alliance that is used in home automation applications. It covers both PHY and MAC layers and has three versions. HomePlug-AV is the basic power line communication protocol which uses TDMA and CSMA/CA as MAC layer protocol. HomePlugGP uses Robust OFDM coding to support low rate and high reliability transmission. Moreover, HomePlugGP has a power-save mode that allows nodes to sleep much more than Home Plug by synchronizing their sleep time and waking up only when necessary.

9) LTE-A: Long-Term Evolution Advanced (LTE-A) is a set of standards designed to fit M2M communication and IoT applications in cellular networks. LTE-A is a scalable, lower-cost protocol compared to other cellular protocols. LTE-A uses OFDMA (Orthogonal Frequency Division Multiple Access) as a MAC layer access technology. The architecture of LTE-A consists of a core network (CN), a radio access network (RAN), and the mobile nodes. The CN is responsible for controlling mobile devices and to keep track of their IPs. RAN is responsible for establishing the control and data planes and handling the wireless connectivity and radio-access control.

*10)*LoRaWAN: LoRaWAN is a newly arising wireless technology designed for low-power WAN networks with low cost, mobility, security, and bi- directional communication for IoT applications. It supports redundant operation, location free, low cost, low power and energy harvesting technologies.

11) Weightless: Weightless is another wireless WAN technology for IoT applications designed by the Weightless Special Interest Group (SIG) - a non-profit global organization. It has two sets of standards: Weightless-N and Weightless-W. Weightless-N was first developed to support low cost, low power M2M communication using time division multiple access with frequency hopping to minimize the interference. It uses ultra- narrow bands in the sub-1GHz ISM frequency band. On the other hand, Weightless-W provides the same features but uses television band frequencies.

12) DECT/ULE: DECT (Digital Enhanced Cordless Telecommunications) is a universal European standard for cordless phones. In their latest extension DECT/ULE (Ultra Low Energy), they have specified a low-power and low-cost air interface technology that can be used for IoT applications.

Due to its dedicated channel assignment, DECT does not suffer from congestion and interference. DECT/ULE supports FDMA, TDMA and time division multiplexing which were not supported in the original DECT protocol.

B. Network Layer Protocols[3]

Network Layer have been partitioned into two sublayers: routing layer which handles packet transfer from source to destination and encapsulation layer that forms packets.

1) RPL: Routing Protocol for Low-Power and Lossy Networks (RPL) is distance-vector protocol that can support a variety of datalink protocols. It builds a Destination Oriented Directed Acyclic Graph (DODAG) that has only one route from each leaf node to the root in which all the traffic from the node will be routed to. RPL nodes can be stateless, which is most common, or stateful. A stateless node keeps tracks of its parents only. Only root has the complete knowledge of the entire DODAG. Hence, all communications go through the root in every case. A stateful node keeps track of its children and parents and hence when communicating inside a sub-tree of the DODAG, it does not have to go through the root.

2) CORPL: An extension of RPL is CORPL, or cognitive RPL, which is designed for cognitive networks and uses DODAG topology generation but with two new modifications to RPL. CORPL utilizes opportunistic forwarding to forward the packet by choosing multiple forwarders (forwarder set) and coordinates between the nodes to choose the best next hop to forward the packet to. DODAG is built in the same way as RPL.

3) CARP: Channel-Aware Routing Protocol (CARP) is a distributed routing protocol designed for underwater communication. It can be used for IoT due to its lightweight packets. It considers link quality, which is computed based on historical successful data transmission gathered from neighboring sensors, to select the forwarding nodes. CARP is the only distributed hop based routing protocol that is designed for IoT sensor network applications. CARP is used for underwater communication mostly.

C. Network Layer Encapsulation Protocols [3]

In IoT applications, IPv6 addresses are too long and cannot fit in most IoT datalink frames which is too small. Hence, IETF develops set of standards to encapsulate IPv6 datagrams in different datalink layer frames for use in IoT applications.

1) 6LoWPAN: IPv6 over Low power Wireless Personal Area Network (6LoWPAN) is the first and most commonly used standard in this category. It efficiently encapsulates IPv6 long headers in IEEE802.15.4 small packets, which cannot exceed 128 bytes. The specification supports different length addresses, low bandwidth, different topologies, power consumption, low cost, scalable networks, mobility, unreliability and long sleep time. The standard provides header compression to reduce transmission overhead, fragmentation to meet the 128-byte maximum frame length in IEEE802.15.4.

2) 6TiSCH: 6TiSCH working group in IETF is developing standards to allow IPv6 to pass through Time-Slotted Channel Hopping (TSCH) mode of IEEE 802.15.4e datalinks. It defines a Channel Distribution usage matrix consisting of available frequencies in columns and time-slots available for network scheduling operations in rows. This matrix is portioned into chucks where each chunk contains time and frequencies and is globally known to all nodes in the network.

*3)*6Lo: 6LowPAN and 6TiSCH, which cover IEEE 802.15.4 and IEEE 802.15.4e, were developed by different working groups, so 6Lo working group was formed. Two specifications of 6Lo are “IPv6 over G.9959” and “IPv6 over Bluetooth Low Energy” have been approved. G.9959 defines a unique 32-bit home network identifier that is assigned by the controller and 8-bit host identifier that is allocated for each node. IPv6 over Bluetooth LE, reuses most of the 6LowPAN compression techniques. However, since the Logical Link Control and Adaptation Protocol (L2CAP) sublayer in Bluetooth already provides segmentation and reassembly of larger payloads in to 27 byte L2CAP packets, fragmentation features from 6LowPAN standards are not used.

D. Session Layer Protocols

Most of the IP applications use TCP or UDP for transport. There are several message distribution functions that are common for IoT applications. These functions are called Session Layer protocols which are given below.

1) MQTT: Message Queue Telemetry Transport (MQTT) was introduced by IBM. It is designed to provide embedded connectivity between applications and middleware’s on one side and networks and communications on the other side. It consists of publisher, subscribers, and a broker. From IoT point of view, publishers are basically the lightweight sensors which send their data connect to the broker and go back to sleep whenever possible. Subscribers are applications or sensory data they connect to brokers to be informed whenever new data are received.

2) SMQTT: An extension of MQTT is Secure MQTT (SMQTT) which uses encryption based on lightweight attribute based encryption. The main advantage of using such encryption is the broadcast encryption feature, in which one message is encrypted and delivered to multiple other nodes, which is quite common in IoT applications.

3) AMQP: The Advanced Message Queuing Protocol (AMQP) is another session layer protocol that was designed for financial industry. It runs over TCP and provides a publish/subscribe architecture which is similar to that of MQTT. The difference is that the broker is divided into two main components: exchange which receives publisher message and distributes to queues and queues represent the topics and subscribed by subscriber.

4) CoAP:The Constrained Application Protocol (CoAP) is another session layer protocol designed by IETF Constrained RESTful Environment (Core) working group to provide lightweight RESTful (HTTP) interface. Representational State Transfer (REST) is the standard interface between HTTP client and servers. CoAP enable low-power sensor built over UDP. CoAP architecture is divided into two main sublayers: messaging and request/response. The messaging sublayer is

responsible for reliability and duplication of messages while the request/response sublayer is responsible for communication.

5) XMPP: Extensible Messaging and Presence Protocol (XMPP) is a messaging protocol that was designed originally for chatting and message exchange applications. This protocol is highly efficient over internet and used for IoT because of its use of XML which is easily extensible. It is designed for near real-time applications and, thus, efficiently supports low-latency small messages. It does not provide any quality of service guarantees and, hence, is not practical for M2M communications. XML creates additional overhead due to lots of headers and tag formats which increase the power consumption hence rarely used for IoT.

6) DDS: Data Distribution Service (DDS) is another publish/subscribe protocol that is designed by the Object Management Group (OMG) for M2M communications. The excellent quality of service levels and reliability guarantees as it relies on a broker-less architecture, which suits IoT and M2M communication. It offers 23 quality-of service levels which allow it to offer a variety of quality criteria including: security, urgency, priority, durability, reliability, etc.

VII. SECURITY AND PRIVACY

Internet of Things is a network of real world systems with real-time interactions done virtually[11]**.** Unattended operation without human intervention is possible for long periods of time by the wireless area network (WAN) or WLAN. It creates various security threats to IoT. Because of the wireless communication there is a possibility to eavesdropping. IoT components are having low energy and low computation resource so that the complex security support cannot be provided. Authentication and data integrity is also a major problem for security.

Front-end sensors and equipment receives data via sensors. Then they transmit the data using modules or M2M device. An intruder can easily access the nodes which are distributed and damage or imply illegal actions on these nodes. Possible threats are unauthorized access to data, threats to the Internet and denial of service. Since large number of machines sending data to large number of nodes and groups network congestion may occur. This may results denial of service attack on IoT. Back-end IT systems form the gateway, middleware, which has high security requirements, and gathering, examining sensor data in real time or pseudo real-time to increase business intelligence.

A. Pivacy

Data collection, mining and provisioning will be different in IoT. For human individuals it will be impossible to personally control the disclosure of their personal information. Once information is collected, that will be retained indefinitely. In traditional Internet, privacy problem arises only for the Internet users whereas in IoT the privacy problem arises even for people not using any IoT service. Hence when the data is collected for authorization by the service provider it should be stored only until it is strictly needed. Privacy should be addressed in various perspectives like[11],

1) Privacy in Device: The device may hold sensitive information which may be accessed by unauthorized persons and reprogrammed. Hence the location of the device should be non-identifiable which means protecting the exact nature of device.

2) Privacy during Communication: During data transmission, data confidentiality can be ensured by applying encryption**.** Encryption on certain occasions adds data to packets which provides a way for tracing, e.g. sequence number, IPsec-SecurityParameterIndex, etc. These data may be victimized for linking packets. In order to avoid unnecessary collection of location information by the network after a certain period of inactive devices will detach from the network. Secure Communication Protocol could be the suitable approach.

3) Privacy in Storage: For protecting privacy of information storage, the least possible amount of information should be stored that is needed. In case of mandatory then only personal information retained. Information is brought out on the basis of “need-to-know”. To conceal the real identity tied with the stored data Pseudonymization and Anonymization could be used. Without disclosing any specific record, a database could allow access only to statistical data.

4) Privacy at Processing: Firstly, personal data must be treated in a way that it should be simpatico with the intended purpose. Secondly, without explicit acceptance and the knowledge of the data owner, their personal data should not be disclosed or retained to third parties. Digital Rights Management (DRM) systems [12] are most suitable which controls the consumption of commercial media and defends against re-distribution illegally. DRM requires trusted devices, secure devices to work efficiently and effectively

VIII. APPLICATIONS

IoT enables information gathering, storing and transmitting the data to and from the things which are equipped with the tags or sensors [4][5]. The tags have been widely used in supply chain management, manufacturing**,** environmental monitoring, retailing, smart shelf operations, healthcare, food and restaurant industry, logistic industry, travel and tourism industry, library services, and many other areas. Currently, IoT has already been deployed in many areas successfully.

A. Transportation and Logistic

Advanced cars, trains, buses as well as bicycles Advanced cars, trains, buses as well as bicycles along with roads and/or rails are becoming more instrumented with sensors, actuators, and processing power. Roads themselves and transported goods are also equipped with tags and sensors that send important information to traffic control sites and transportation vehicles to better route the traffic, help in the management of the depots, provide the tourist with appropriate transportation information, and monitor the status of the transported goods.

B. Healthcare domain:

Many are the benefits provided by the IoT technologies to the healthcare domain and the resulting applications can be grouped mostly into: tracking of objects and people (staff and patients), identification and authentication of people, automatic data collection and sensing.

C. Smart environments domain:

Comfortable homes and offices Sensors and actuators distributed in houses and offices can make our life more comfortable in several aspects: rooms heating can be adapted to our preferences and to the weather; the room lighting can change according to the time of the day; domestic incidents can be avoided with appropriate monitoring and alarm systems; and energy can be saved by automatically switching off the electrical equipments when not needed.

D. Personal and social domain

The applications falling in this domain are those that enable the user to interact with other people to maintain and build social relationships. Indeed, things may automatically trigger the transmission of messages to friends to allow them to know what we are doing or what we have done in the past, such as moving from/to our house/office, travelling, meeting some common mates or playing soccer.

IX. Challenges and Future Direction

The challenges facing the emergence of the IoT are numerous [1]. They are both technical and social. These challenges must be overcome in order to ensure IoT adoption and diffusion. Standardization Activity, Addressing and Networking, lack of common architecture, security and privacy, Innovation on IoT, Miniaturization, Semantic Technology and Virtualization.

Standardization can support the entry of new service providers and users and improve interoperability. But, the rapid growth of IoT makes the standardization difficult. IoT includes an incredibly high number of nodes which sends and receives signals or information to authorized user. This requires effective addressing policies. Number of IPv4 addressing is decreasing and it will zero very soon. Hence, IPv6 addressing can be used. But the number of bits used for addressing on a RFID tag is a challenging one. Same manner more objects are interconnected in a distributed manner and operated without human intervention raises security and privacy problem which should be addressed properly. Likewise more issues yet to be solved on IoT. Hence, IoT can be a challenging research area for the current and future researchers.

Future Direction

Since the IoT has not yet been realized, it might seem precocious to forecast the future directions of the IoT[8]. However, future visions of the IoT will affect its current development and must therefore be considered. One future vision for the IoT is the Web of Things. The Web of Things proposes the use of web standards to fully integrate smart objects into the World Wide Web.

X. Conclusion

The concept of combining computers, sensors, and networks to monitor and control devices are the key technologies for the Internet of Things. IoT promises a revolutionary, fully interconnected “smart” world with relationship between objects and their environment and objects and people. It represents a growing aspect of technology. But a number of challenges like security, privacy, standardization, legal and right issues are to be addressed. Hence there is a need to address its challenges and maximize its benefits while reducing its risks.

XI. References

1. Shashank Agrawal, Dario Vieira, “A survey on Internet of Things”, Um estudo sobre Internet das Coisas, vol. 1, n. 2, p. 78 – 95, maio 2013 – ISSN:2316–9451
2. Luigi Atzori a, Antonio Iera b, Giacomo Morabito, “The Internet of Things: A survey”, 1389-1286, Computer Networks 2010, Science Direct, Elsevier B.V.doi:10.1016/j.comnet.2010.05.010
3. Tara Salman, “Networking Protocols and Standards for Internet of Things”
4. http://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot/index.html
5. Shancang Li & Li Da Xu & Shanshan Zhao, “The internet of things: a survey”, Published online: 26 April 2014, # Springer Science+Business Media New York 2014.
6. https://www.micrium.com/iot/internet-protocols/
7. The Internet Of Things: An Overview – The Internet Society (ISOC), 2015.
8. Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic,” Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions”
9. http://www.c-sharpcorner.com/UploadFile/f88748/internet-of-things
10. Mallikarjun Talwar, “Routing Techniques and Protocols for Internet of Ihings: A Survey”, Indian Journal of Sciencetific Research, Proceeding of NCRIET-2015
11. J. Sathish Kumar, Dhiren R. Patel, “A Survey on Internet of Things: Security and Privacy Issues”, International Journal of Computer Applications, Vol.90, No.11, March 2014.
12. E. Liu, Z. Liu, and F. Shao, "Digital Rights Management and Access Control in Multimedia Social Networks" In Genetic and Evolutionary Computing, Springer International Publishing, 2014,pp.257-266.
13. Somayya Madakam, R. Ramaswamy, Siddharth Tripathi, “Internet of Things [IoT]: A Literature Review, Journal of Computer and Communications, 2015,3, 164-173.