Internet of Things: A Survey on Architecture, Technologies, Protocols and Challenges

Gaurav Choudhary
Research Scholar
Dept. of Instrumentation & Control Engineering
National Institute of Technology, Jalandhar, India
gauravlohan04@gmail.com

Dr. A.K.Jain
Professor
Dept. of Instrumentation & Control Engineering
National Institute of Technology, Jalandhar, India
jainak@nitj.ac.in

***Abstract*— Internet of Things (IoT) can be thought of as the next big step in internet technology. It is enabled by the latest developments in communication technologies and internet protocols. This paper surveys IoT in respect of layer architecture, enabling technologies, related protocols and challenges.**

Keywords— Internet of Things (IoT); Evolution; Architecture; Protocols; IoT Applications.

I. INTRODUCTION

IoT incorporates a network of things that aims to enhance the different modes of communication and plays a leading role in a number of domains, like transportation, health care, home automation, smart environmental, personal and social etc [1]. IoT can be called as Future Internet because it permits physical objects to think, hear and perform various tasks by sharing information with other helps [2] by providing each object a unique identification and accessibility to the internet. In the beginning IoT was used to support RFID technology and the first device was designed in 1999, by using RFID communication, which had a range of around 10cm- 200m. IoT starts gaining popularity in 2010-2011 as the number of objects associate to the internet was around 12.5 billion, making a number of interconnected devices per person more than 1 [3], and it is assumed that by 2050 the number of objects associated to the internet will be 5x more than the users [4]. IoT offers wide opportunity for application organizers, internet service providers, and products manufactures. The annual economic impact by IoT is around $2.69 trillion to $6.201 trillion by 2025 [5]. Fig.1 Wikibon predicts that Return on Investment (ROI) from the industrial Internet grows to 149% in 2020 as compared to 13% in 2012 [6].

IoT basically transform physical objects from conventional to smart by exploiting data acquisition and networking technologies. Data acquisition technologies like sensor, RFID and Two dimensional code equipment allow smart devices such as tablet, smart phone, to collect data from the outside world and networking technologies like Wireless local area networks (WLANs), Bluetooth and Internet helps to provide a network for data (packets) to be sent in IoT. IoT not only provide human-human communication, but also helps objects or devices to communicate over the internet, so we can conclude that through IoT new form of communication would Likely be formed like human-things, and things-things [7],[8]. For such type of communication, IoT have information sensing equipments and systems which help to get information from the objects so in IoT all objects are outfitted with information sensing equipments and systems by using internet network.

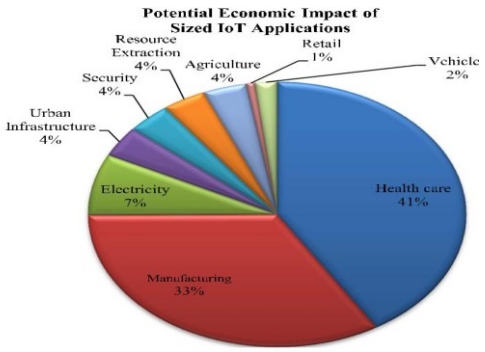

Fig. 1. Estimated market share of IoT applications by 2025 [6].

Smart devices are now linked to the Internet by the use of communication protocols like Zigbee, Z-wave etc. [9], that helps in continuously collecting and processing the data. There are different issues that likely to be in IoT relies upon the technologies and also solutions to enhance IoT are most probably to be found in underlying technologies as discussed before. Fig. 2 give a descriptive sketch of internet evolution with a lot of youth services with the help of sensors, RFID tags, actuators, cell phones, etc. [10].

IoT aims to construct a ongoing static internet into a entirely integrated future internet. This innovation will definitely improve the quality of living standard and helps to grow the world economy. Realizing the emergence and development of IoT, is not an easy assignment due to many challenges like reliability, mobility, availability, scalability, performance, interoperability, management, security and privacy that need to be addressed by application programmers and service providers to execute their services efficiently.

The rest of the paper is organized as follows: Section II discusses the overall architecture of the IoT. Empowering technologies of IoT are presented in Section III. Protocols are discussed in Section IV, Section V presents applications of

[978-1-5090-2807-8/16/$31.00 ©2016 IEEE]

IoT. Finally, Section VI concludes survey study with reference at the end.

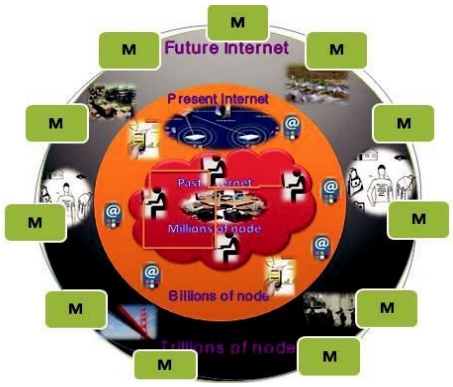

Fig. 2. Internet evolution prospective and different IoT services [9].

II. ARCHITECTURE

IoT having layered architecture should be capable of connecting a enormous number of objects through the internet. So to fulfill this criterion, IoT need a layered architecture that is flexible in nature. The constantly increasing number of objects will create a massive traffic, therefore large amount of data capacity is needed. The very basic model of IoT is having 3 layer architecture [11], [12], [13] which consists of Perception, Network and Application Layers. IoT will face a number of challenges, especially in the field of privacy and security [14], so to overcome these issues new standard architectures needs to be more focus on many essential factors like Quality of Services (QoS), sustainability, data integrity, confidentiality, reliability etc. Fig. 3 illustrates some standard common architecture among them 5-layer architecture model is briefly described below.

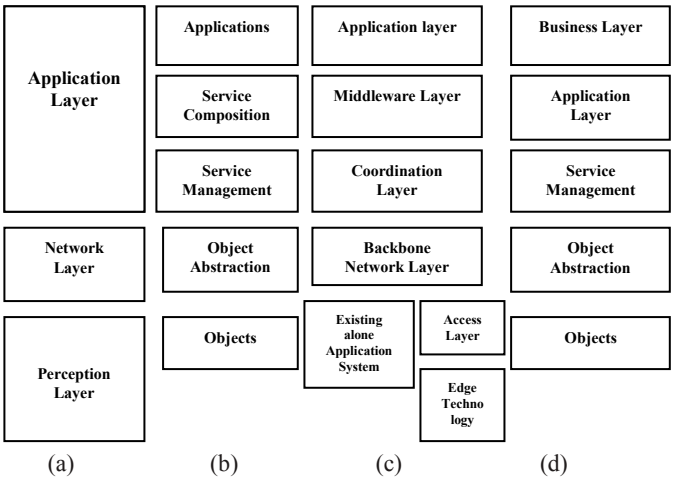

Fig. 3. IoT architecture (a) Three layer (b) SOA (c) Middleware based (d) Five layer [14].

A. Perception Layer

The bottom layer of the IoT architecture is similar to the physical layer in the OSI model. The object layer is a hardware layer which collects information from the physical world and the process gathered information and finally transferred to the upper layer. This layer includes data-acquisition technologies like sensor, RFID and two-dimensional code equipment which gather information like temperature, weight, vibrations, pH level, humidity, amount of dust in the air etc. Perception layer digitizes the data or we can say convert information into signals and transfer to the Network layer/Object Abstraction layer through secure channels [12], [15].

B. Object Abstraction Layer/Network Layer

Object Abstraction is mainly responsible for transferring the information from the object layer to upper layers through secure channels. Data can be transferred to the central information processing system through networking technologies like ZigBee, Z-wire, 3G, GSM, UMTS, WiFi, infrared, 6LoWPAN etc. This layer performs some other important tasks like cloud computing process and data management process [14]. 6LoWPAN is used to associate wireless sensor networks (WSNs) to the internet. Z-Wire and ZigBee are non standard WSN protocols [16].

C. Service Management/Middleware Layer

Middleware is a software layer or a set of sub layers which serves an interface between the components of the IoT that makes all possible communication between elements that would not otherwise be capable. This layer plays a major role in the development of new technologies and also provides a connectivity layer for application layer and sensors that ensure effective communication among software. A middleware layer proposed of IoT follow Service Oriented Architecture [17] and also have some essential functions like service management, aggregating, filtering the received data from the hardware devices and also store the lower layer information into the database [18]. Moreover, this layer has the capability to make decisions, complete information and deliver the services over the network wire protocols [19].

D. Application Layer

This layer does not have any contribution towards building up of IoT architecture, but it provides various application services as requested by the customer and all the information interpretation occurs at this level. For example, the application layer provides logistics, retail, and healthcare report to the customers. IoT application layer is responsible for application management and to provide high quality services to the customer based on the processed information in the Middleware layer. This layer covers enormous application like smart health, smart transport, smart store, smart factory, smart car, smart farm etc. [13], [20].

E. Business/Management Layer

The Business/ Management layer performs monitoring and management of underlying four layers, manages the whole IoT applications and services and provides high level analysis reports. It has some responsibilities to create graphs, business model, etc depending upon the data retrieve from the application layer and effective data analysis process. This layer helps the managers or executives to make accurate decisions about their business [18]. It also supports decision making processes and compares each layer output to enhance user's privacy [15].

III. ENABLING TECHNOLOGIES

Understanding the integration of several empowering technologies (like data acquisition and networking), provide a improved insight into the actual meaning and functionality of IoT. This section provides a general overview how these technologies play a vital role in the IoT.

A. Data Acquisition Technologies

1) Two Dimensional Barcode: It is basically an optical machine readable representation of data, whose information can be read by a bar code reader machine to retrieve the data. Barcode can be One dimensional barcode (1D) or Two dimensional barcode (2D).

a) 1D Barcode: It stores encoded data by using the series of variable width lines and spaces. 1D barcodes can be scanned with camera-based imaging scanners or by using laser scanners. They are well suited for identifying items that may be connected with some different information that changes regularly. 1D has a small data storage capacity and can store only numbers and letters in encoded form.

b) 2D Barcode: It is a technology which uses patterns of square, dots, hexagons, and other shapes to encode the data, and information is read by special bar code reader machine to retrieve the data [21]. It not only contains alphanumeric information, but also contains images, voice and other type of binary data. 2D have large storage capacity and use white and black pixels laid out on 2D plane to store data information and also it has some specific advantages like fewer errors, easy to read, easy to transmit, more secure. The 2D bar codes are generated by using algorithms [22] then this code will be read by scanners. Scanner consists of three different parts, i.e. illustration system, sensor and the decoder. First barcode scanning machine "scans" white and black pixels of barcode by using illustration system (generally used red light for processing), then the sensor in the barcode scanner generates an analog signal by detecting the reflected light from the illustration system and finally sent to the decoder. The decoder reads the analog signal and uses a check digit to validate the barcode and finally convert into text form.

2) Radio Frequency Identification (RFID): It is a wireless object identification technology that is used to monitor objects in real-time by using radio frequency signals. It mainly consists of one or more than one RFID readers and several RFID tags and a administer computer. The RFID tag is a simple microchip or a radio frequency card used to keep data about the object, so each RFID tag is loaded full of data and combined to the object for their identification. Every RFID tag has its unique identification number. At present three types of RFID tabs are there: passive, active and semi passive RFID tag. Generally RFID tags are passive, i.e. they do not need batteries for their operation instead they receive their power required for transmitting the RFID tag ID from the query signal broadcast by the RFID reader. Active RFID tag battery influence the transmission of the radio signal and in semi passive RFID tag battery will provide power only while receiving radio signal from the RFID reader. RFID reader generates a query modulated radio signal and uses its antenna to emit the modulated signal at any given specified frequency that will represent the existence of tags in the neighboring area and receives the reflected radio signal from the tag i.e. is finally passed to the database. It also contains a microprocessor, memory, actuators, a controller, a power supply and input/output channels for external sensors [23]. Object identification is done at a processing center on the ground of the received reflected signal from the data base.

RFID is now compared with 2D barcodes. Data in 2D barcode data is stored in an optical image where as in RFID data is in RFID tags. 2D is having more wear and tear as compared with RFID. 2D barcode require line of sight between the barcode and the reader, whereas RFID does not require line of sight. RFID has strong anti-interference ability, good range and long service life as compared with 2D barcode.

3) Sensors: Sensors are also used for data acquisition and it is defined as a transducer that measures a physical quantity and convert into an electrical signal that can be go through by any instrument or by any observer. Sensors can describe an object that can acquire data so we can say that sensors can play a big part in IoT. Sensors basically classified into two types: chemical sensors and physical sensors. Chemical sensors transforms chemical information like concentration, chemical activity, etc. into electrical signals, where physical sensor measures physical quantities like temperature, liquid level, humidity, etc. and transform into an analytically useful signal i.e. an electrical signal. There are eight specifications that should be studied while selecting a sensor for data acquisition in IoT: Sensitivity, Minimum Sensitivity, Environment compatibility, Operating range, Frequency response, Usage and ruggedness.

Few commonly used sensors are presented below:

a) Pressure Sensor: It measures the pressure of a liquid or a gas and converts into an electrical signal. Pressure gauges and barometer are two most common pressure sensors used in IoT. Pressure gauge can work in various areas of IoT such as biomedical instrumentation, manufacturing industries etc.

b) Thermal Mass Flow Sensors: This sensor use thermodynamics to determine the mass flow. For example, as the gas stream passes through the sensor and is warmed up by heaters R1 and R2, so the measured temperature drifts by T1 and T2, as we know from basic concepts of thermodynamics that mass flow is directly proportional to measured temperature difference. Finally, signals measured in the sensors are amplified and converted into an electrical signal [24].

c) Temperature Sensor: It measures the heat or temperature of a medium. They are used to control the performance of the IoT devices at varying temperatures. It measures the amount of heat energy generated by the object, allow us to detect any physical change corresponding to the temperature producing effect. Temperature sensor can be of two types: contact temperature sensor and non-contact temperature sensor.

d) Optical Sensor: They are used to detect electromagnetic energies like electricity, light, etc. by converting light energy into electrical energy. Optical sensors

are used in digital cameras which is one of the physical devices of an IoT.

e) Proximity Sensors: This sensor is used to detect motion by utilizing electromagnetic radiation. They are commonly used in security, safety applications of IoT.

B. Networking Technologies

Networking technologies of IoT associate heterogeneous objects in the network to provide some smart services. IoT nodes usually operate using low power in the noisy and lossy communication links [15]. However, in IoT, WSNs is used as a leading network for objects to communicate with each other. WSNs coordinate with RFID to track the status of objects like temperature, movements and their locations, etc. WSNs in IoT consists of high number of sensors node and also data-acquisition tools to model a short range wireless sensor adhoc networks communicating in wireless multi hop fashion [17]. All sensor nodes are based on battery supply, nodes can be stationary or moving, they can be homogeneous or not, nodes do not require careful pre-planning i.e. they established short-term connection according to the user needs and temporary conditions to create a communication network, sensor node density can vary in different places in the network and also it can vary during time, sensor nodes are "smart" terminals like laptop, every node can be a router towards another node [25], so this variety of adhoc topology network combined with bigger network like internet to form the Internet of Things. WSNs can be single-sink WSN, single-sink single-hop WSN or single-sink multi-hop WSN.

Mostly WSNs is based on IEEE 802.15.4 protocol standard generally defines sub-layer for Medium Access Control (MAC) and physical layer (PHY) for low data rate, low-power wireless personal area network (WPAN) [26]. It provides encryption, authentication, high level of security services, high message throughput, low cost communication, limited power consumption, making it a popular for WSNs, IoT and M2M. The IEEE 802.15.4 LR-WPAN supports standard topologies like star, tree and mesh networks as shown in figure 4. It generally supports two popular types of network node: Full Functional and Reduced Function Devices. Full functional devices (FDD) work as a personal area network (PAN) coordinator, i.e. it executes coordination and sensing tasks, routing mechanism and it is responsible for regulation and overall maintenance of the network, it can also act as a network coordinator. Reduced function devices (RFD) are simple nodes with limited resources, they do not route data packets and only communicate with a FDD. It can associate with a single FDD at a time Star network topology contains some RFDs and at least one FDD.

Mesh network topology consists of a PAN coordinator, and other various nodes that communicate through intermediate nodes to another network or in the same network. Mesh network allows full peer-to-peer communication. The cluster tree network is a specialized case of mesh topology and it is a combination of both star and mesh network. It contains coordinator, a cluster head and normal nodes.

IEEE 802.15.4 generally use carrier sense multiple access with collision avoidance (CSMA/CA) protocol with optional time slot to reduce packet collisions, it is basically based on a direct sequence spread spectrum (DSSS) [27] as DSSS transmission requires more bandwidth but less power than a conventional signal. IEEE 802.15.4 support 2.4GHz and 868/915MHz physical layer (PHY). The 2.4GHz support 250kbps by using Quadrature phase shift keying (QPSK) and 868/915 support 240kbps using binary phase shift keying (BPSK). IEEE 802.15.4 does not provide QoS guarantees and can handle immense number of nodes in a network

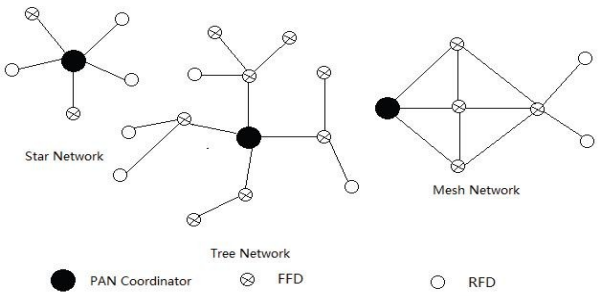

Fig. 4. Different network Topologies

1) RFID Wireless Sensor Network: RFID and WSNs are both vital components of pervasive computing. RFID is used to identify the object under sensed by using RFID tags and WSNs is used to sense and monitor chemical, biological and physical through sensing of light, temperature, etc. RFID system has serious limitations like lack of standardization, high cost, collision while reading several tags, faulty manufacture of tags, possible virus attack, low range, security and privacy issues. WSNs offer some advantages over RFID. First, sensors gather more information in WSNs as compared with RFID tags such as measurement of pressure, humidity, pollutant level, etc. Second, the sensors in WSNs are intelligent where there is no intelligence in RFID tags. RFID requires line of sight communication between reader and RFID tag whereas WSNs is multi-hop communication network. But there are some limitations of WSNs such as security, routing, computing capabilities and battery power issues are there [28], [29].

Communication in RFID system is single hop and there is no communication between RFID tags, RSN is basically the integration of RFID system and WSNs that provide RFID to work in multi- hop way that helps the RFID system to operate in wider area. Both RFID tag and sensor nodes are functioning on the same layer and RFID reader and gateway work on higher layers. There are basically four types of integration: integrating tags with wireless sensor nodes, integrating tags with sensor networks, integrating RFID reader with sensor nodes and mix of sensors and RFID. Higher layers in RSN fetch data from the lower layers and forward data to the agent layer [21]. RSN opens immense number of applications in the robotics field, it helps in obtaining additional information about the surrounding objects, and reading range of objects is higher in RSN as compared with RFID system. RSN require no additional hardware to work with existing infrastructure.

2) Near Field Communication (NFC): It is a short range wireless technology which provides secure and easy communication between various devices. Its range is up to a few inches and it depends upon inductive coupling between connecting transmitting and receiving devices in a network. Communication basically occurs with 13.56MHz frequency and its utmost data transfer rate is 424Kbps (slower than Bluetooth). NFC communication occurs in two mechanism: active and passive. In passive mode, the only active device will generate an RF field and the target device make use of energy generated by active device, but in active mode, both (active and passive devices) will use his energy to bring out RF field [30]. NFC consumes far less power (greater than Bluetooth) and doesn't require pairing.

IV. PROTOCOLS

Protocols are the agreed upon format for transmitting data between two devices in the same/different network. IoT requires distinct protocols for various activity, like it requires protocols for gathering the data from RFID tags, sensors etc., protocols for Machine to Machine (M2M) communication, Device to People (D2P) communication, and Device to Device (D2D), communication protocols to send the data to the server.

A. Constrained Application Protocol (COAP)

It is a web transfer protocol depends on RE presentational State Transfer (REST), for use with constrained and low power nodes. It is also called an application layer protocol [31] for IoT related applications. COAP use an interaction model identical to the client / server model of HTTP. This model is deliberately designed for M2M applications implemented using REST architecture such as building applications, smart farm. COAP is basically organized in two sub-layers: Request/ Response sub-layer handles REST based communication. Messaging sub-layer handles single message exchanged between end users and provide reliable communication over the UDP transport layer. COAP does not support broadcasting and it employ four category of messages conformable, non conformable, acknowledge and reset. It provides some important features like Resource observation, Block–wise resource transport, Resource discovery, Interaction with HTTP, Security [15].

B. Message Queue Telemetry (MQTT)

MQTT is a light weight Client Server broker-based publish or subscribe message transport protocol build on top of TCP/IP. MQTT is based on hub and spoke architecture having three components: subscriber, publisher, and broker, it uses a publish and subscribe messaging pattern with quality of service i.e. it clearly suggest that any source of relevant information such as sensor can broadcast its data information and then any client can subscribe to that respective data, all this is proceeding in the broker they keep track of all the publication and subscription, so whenever a publisher sense a update with new data he broadcast a message, the broker takes responsibility of sending a new data to all subscriber, the built in support of quality of service (QoS) means that the broker can insure the delivery of the message.

MQTT is basically a binary format that desires a minimum of bandwidth, it has a fixed header of 2 bytes, and it also having a small implementation footprint that requires less battery, and these efficiencies make it simple to scale in IoT. This protocol is appropriate for resource constrained devices (RCD), that use low bandwidth links. MQTT not really established, but has an OASIS standard (backed by IBM). Two major specifications exist for MQTT: MQTTv3.1 and MQTT-SN [32].

C. Advanced Message Queuing Protocol (AMQP)

It is an application layer protocol for messaging in IoT concentrating on message oriented environments. This protocol is work out for interoperability operation between clients and message middleware servers. The AMQP is binary protocol that supports reliable communication having potential of routing, security, reliability. AMQP is having two layers: Functional layer handles messaging capabilities and Transport layer handles channel multiplexing, framing, heart beating, error handling and data representation. It also supports publish/subscribe model [33] and point to point routing [34].

D. Extensible Messaging and Presence Protocol (XMPP)

It is an IETF instant messaging (IM) standard designed for message exchanging and chatting. It is well-proven protocol allow users to communicate with each other by using internet. It supports publish/subscribe communication protocol and quest/response message systems. It supports low latency message exchange [35] and has TLS/SSL security. It is a impractical M2M communication and allows IM applications to achieve access control, end-to-end encryption, and authentication. It connects client-server by using message stanzas [36]. Message stanzas utilize a push method to retrieve data that contains source and destination address, IDs of XMPP entities. This protocol is more suitable for IoT as it supported by all over the internet.

E. Data Distribution Service (DDS)

DDS is an Object Management Group (OMG) public-subscribe protocol for M2M communication that enables interoperable data exchange between publisher and subscriber. It is a data centric protocol relies on broken less architecture to provide better QoS (support 23 services) and high reliability to its application. DDS describes two layers: Data Centric Publish Subscribe (DCPS) and Data Local Reconstruction Layer (DLRL). DCPS aims the adequate delivery of the useful information to proper receipt and DLRL is elective layer, which grants for a simple integration into the application layer. DDS transfers the bulk of data information simultaneously to the multiple receivers.

F. Zigbee

Zigbee is a low cost, low speed, low power, high level communication protocol, specially drafted for Personal Area Network (PAN), having low rate sensors with 128-AES encryption Technology. It is developed by Zigbee alliance using IEEE802.15.4 and adds new features to meet required functionalities. This protocol lacks in security due to its simplicity, and low cost. Zigbee has a maximum range of 10-100 meters and has a maximum throughput of 250Kbps and

allows 65000 nodes in a network. This short range transmission, low data transfer rate provides good battery life for Zigbee devices. Zigbee WSNs supports three network topologies: star, mesh and cluster tree. The mesh allows multi hop communication, so it is reliable, secured and scalable, the star does not support multi-hop communication, where as cluster is the special case of mesh technology. Zigbee is defined in four layers: Physical layer, Medium access layer, the network layer, and the application layer. Both physical layer and MAC layer are based on IEEE802.15.4 standards, while upper layers are Zigbee specific. Physical layer modulates outgoing signals and demodulates incoming signals, MAC layer use CSMA/CA to access the network, Network layer provide network establishment, neighbor discovery and routing, address assigning, add and remove devices from the network [37]. Application layer is the highest protocol layer and it hosts the application layer. This layer is built up of Application framework, Zigbee device object (ZDO), and Application Support Sub-layer [38].

G. *Z-wave*

It is a low power wireless communication protocol used for remote control applications as well as small size commercial domains [39]. It supports 232 nodes in a network and cover about 32 meters point to point communication. It operates near about 900 MHz frequency and permit the transmission rate of 40kbps [15]. It is a low bandwidth half duplex protocol not designed to transfer any kind of streaming or large amount of data. It is having four layers in its defined architecture: MAC layer, transfer layer, routing layer, and application layer. MAC layer collision avoidance, benefits, and reliable transmission are possible with optional ACK [39], the Transfer layer basically manages the transmission and reception of packets between nodes, Routing layer controls routing of packets and application layer manage the payload in the packets.

H. *Low Power Wireless Personal Area Network (LoWPAN)*

LoWPAN is wireless networks having special characteristics like low bandwidth, limited packet size, various address length [15]. It is generally an adaptation layer that allows IPv6 packets to transport over 802.15.4 links. This protocol is basically based on IEEE 802.15.4-2003. To use 6LoWPAN protocol in a network it is necessary every node have to recognize to the same protocol, 6LoWPAN include better connectivity with pre-existing architectures.

V. IoT Challenges and QoS Criteria

This section provides a brief review of the key challenges faced in the evolution and development of the IoT. In order to ensure proper IoT diffusion and adoption, it is necessary to address these issues very carefully. Some of the key challenges includes: reliability, mobility, availability, scalability, performance, interoperability issues. [15].

A. *Reliability*

Reliability attribute to the ability of the system to perform consistently according to its basic specifications. It aims to boost the resistance of IoT to security problems, long term usability, application robustness in case of uncertain information, etc. Reliability must be ensure to implemented throughout all layers in IoT. IoT network and the application running on the network must able to pass information in the reliable manner. [40] proposes a reliable and energy efficient mechanism for packet loss recovery and route quality evaluation called as Adaptive Joint protocol based on Implicit ACK (AJIA). [41], [42] authors evaluate the reliability and cost of the IoT systems by using probabilistic model checking methods.

B. *Mobility*

With it, large numbers of mobile objects are equipped with sensing devices so most of the services are delivered to mobile users. One of the major challenges in IoT is to support IP mobility between connecting users with their desired services, when they are moving in different locations and access methods. [43] provide a mobility management scheme to manage the mobility of the sensor devices by distributed service lifecycle management mechanism which helps to build to build up the concept of the Web of Things. [42] the authors implemented a prototype for the proposed resource mobility schemes with two operating modes: caching and tunneling to access the sensory data when a resource becomes unavailable. [44] proposes a group mobility management mechanism for large scale machine to machine (M2M) mobile network where all machines having similar mobility patterns are grouped at the location database (LDB) and the mobility management will perform only by the leader machine from that group .

C. *Availability*

Most of the IoT applications require hardware and software levels availability to provide quality services to its customers. Availability and reliability became a major IoT challenge as most of the IoT applications have stringent dependability requirements, as a system faults may lead to overall IoT system failure, it may result in financial losses and have environmental damages [45]. We have to use proper design tools to maximize the availability of IoT system so as to minimize the effects of faults on the network devices. [46] the authors use a dependability evaluation tool for IoT systems while considering hardware faults and permanent link faults. [47] proposed a mathematical model to estimate availability by using redundancy aspects.

D. *Scalability*

As the technology grows, customers demand new devices and services with some different type of communication and technologies to be added in existing IoT system without giving any negative impact on QoS, so it is not an easy task to add new devices in the existing IoT system as it involves various issues like information management and service management etc. [48]. In order to improve the scalability in case of a large expansion of the IoT system [49] the authors proposed distributed interoperability architecture of such type of youth systems. Using generic IoT architecture, some of the scalability issues is addressed by introducing Secure, Hybrid, Cloud enabled architecture of IoT (SHCEI) [50]. Security and privacy concerns should be kept be kept in mind before solving the scalability challenge in IoT systems. In [51] the authors presented a hierarchical identification mapping server

(IMS) that use separation mechanism of identification and location to address routing scalability challenges in IoT systems.

E. Performance

For the advancement of IoT industry, it is mandatory to evaluate the services provided by IoT. Evaluation of all the services is not an easy assignment as we have to precisely test all the internal computation between devices and network infrastructure like packet loss, bandwidth, etc. The devices in it should be continuously evaluated to improve their services in order to fulfill customer requirement [15]. In [52] authors introduce a local level, IoT controller to add an additional layer in IoT architecture in order to improve the performance.

F. Interoperability

It is the term mostly related to the growth, success of the product and related services in order to meet customer requirements. In terms of IoT, Interoperability is defined as the capability of the objects to connect and communicate data information (packets) in such a way that can be quickly processed and easily accessible by other entities. So handling interoperability is another big issue for IoT applications as it includes large heterogeneous objects having different platforms. Initially interoperability involves various steps for the IoT, first interoperability at the IPv6 layer as it provides interoperability for the Internet of Things and second at the routing layer [53], the next step for interoperability is low power interoperability. RPL protocol provides a framework for interoperability as it is designed for running over radio layers such as IEEE 802.15.4. IEEE 802.15.4 radios are lower power than WiFi and Bluetooth radios. Contiki provides a set of radio duty cycling mechanisms to have a low power results such as Contiki MAC [54], XMAC [55]. Attaining low power, interoperability is an open problem because low power wireless protocols have no answer for duty cycling and present duty cycling have not designed for interoperability[53].

VI. CONCLUSION

IoT envisions the near future of the internet by allowing communication between people and things via. Internet, store and retrieve data, access data on the internet, intend to enhance the quality of life by fusing these technologies and applications. It leads to the vision of “anytime, anywhere, any media, anything” communication. This paper surveys the evolution, the generic architecture, its enabling technologies, protocols, and challenging aspects of the IoT.

REFERENCES

[1] L.Atzori, A.lera, G Morabito,” The Internet of Things: A Survey. Computer Networks Journal 2010: pp.2787-2805.

[2] L. Coetzee, J. Eksteen. The Internet of Things - Promise for the Future An Introduction. 1ST-Africa 2011 Conference Proceedings (CSIR). 2011.

[3] Keerti kumar M., Shubham M, R.M. Banakar,” Evolution of IoT in smart vehicles: An overview,” Green computing and Internet of things(ICGCIoT), 2015 International Conference , pp. 804-809.

[4] Committtee, "Global system for Mobile Communication," A report on GSM, 1987, pp. 1-2.

[5] J.Manyikaetal.,DisruptiveTechnologies: AdvancesthatWillTransform Life, Business, and the Global Economy. San Francisco, CA, USA: McKinsey Global Instit., 2013.

[6] D. Floyer, “Defining and sizing the industrial Internet,” Wikibon, Marlborough, MA, USA, 2013.

[7] N. Bari, G. Mani, and S. Berkovich, “Internet of things as a methodological concept,” in Computing for Geospatial Research and Application (COM. Geo), 2013 Fourth International Conference on. IEEE, 2013, pp. 48-55.

[8] Y. Liu and G. Zhou, “Key technologies and applications of internet of things,” in Intelligent Computation Technology and Automation (ICICTA), 2012 Fifth International Conference on. IEEE, 2012, pp. 197–200.

[9] G. Tripathi, D. Singh, "EOI: Entity of Interest Based Network Fusion for Future Internet Services", ICHIT2011, September 23-25,2011, Daejeon, Korea.© Springer-Verlag Berlin Heidelberg, CCIS, vol. 206, 2011, pp.39-45.

[10] G. Tripathi, D. Singh, “ A survey on internet of things: Future vision, architecture, challenges and services”, internet of things (WF-IoT), 2014 IEEE World Forum on, pp. 287-292

[11] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, “Future Internet: The Internet of Things architecture, possible applications and key challenges,” in Proc. 10th Int. Conf. FIT, 2012, pp. 257–260.

[12] Z. Yang et al., “Study and application on the architecture and key technologies for IOT,” in Proc. ICMT, 2011, pp. 747–751.

[13] M. Wu, T. J. Lu, F. Y. Ling, J. Sun, and H. Y. Du, “Research on the architecture of Internet of Things,” in Proc. 3rd ICACTE, 2010, pp. V5-484–V5-487.

[14] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, “Future Internet: The Internet of Things architecture, possible applications and key challenges”, in Proc. 10th Int. Conf. FIT, 2012, pp. 257–260.

[15] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, Moussa Ayyash,” Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”, IEEE Communications Surveys and Tutorials, vol.17, Issue 4, 2015, pp. 2347-2376.

[16] Jasper Tan, Simon G.M. Koo,” A survey of Technologies in Internet of Things”, 2014 IEEE International Conference on Distributed Computing in Sensor Systems, 2014, pp. 269-274.

[17] Luigi Atzori, Antonio lera, Giacomo Morabito,” Internet of Things: A Survey, ELSEIVER (2010), Volume 54, Issue 15, pp: 2787-2805.

[18] Surapon Kraijak, Panwit Tuwanut, “A Survey on Internet of Things Architecture, Protocols, Possible Applications, Security, Privacy, Real-world implementation and Future Trends”, 2015 IEEE 16th International Conference On Communication Technology, 18-20 Oct.2015, Hangzhou, pp-26-31.

[19] M. A. Chaqfeh and N. Mohamed, "Challenges in middleware solutions for the internet of things," in Collaboration Technologies and Systems (CTS), 2012 International Conference On, 2012, pp. 21-26.

[20] L. Tan and N. Wang, "Future internet: The internet of things," in Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference On, 2010, pp. V5-376-V5-380.

[21] Hetal B Pandya, Tushar A Champaneria,” Internet of Things: Survey and Case Studies, Electrical, Electronics, Signal, Communication and Optimization (EESCO), 2015 International conference on IEEE, pp.1-6.

[22] H. Xuechen, “The two-dimensional bar code application book management,” in Web Information Systems and Mining (WISM), 2010 International Conference on, vol. 1. IEEE, 2010, pp. 409–411.

[23] S. Lahiri, RFID sourcebook. IBM press, 2005.

[24] M. Ashauer, H. Glosch, F. Hedrich, N. Hey, H. Sandmaier, and W. Lang, “Thermal flow sensor for liquids and gases based on combinations of two principles,” Sensors and Actuators A: Physical, vol. 73, no. 1, 1999, pp. 7–13,

[25] A. Yamanouchi, T. Hashimoto, T. Ohta, H. Kojima, and Y. Kakuda, “Re-source management middleware using mobile agents for mobile ad hoc networks,” in Distributed Computing Systems Workshops (ICDCSW), 2010 IEEE 30th International Conference on. IEEE, 2010, pp. 1–6.

[26] IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std. 802. 15. 4-2011, 2011.

[27] M. Petrova, J. Riihijarvi, P. Mahonen, and S. Labella, "Performance study of ieee 802.15. 4 using measurements and simulations," in Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE, vol. 1. IEEE, 2006, pp. 487–492.

[28] Mandeep Kaur, Manjeet Sandhu, Neeraj Mohan and Parvinder S. Sandhu, "RFID Technology Principles, Advantages, Limitations, & Its Applications", International Journal of Computer and Electrical Engineering, vol.3, pp. 1793-8163.

[29] Heshem A. El Zouka, "Challenges in Securing Wireless Sensor Networks", The Seventh International Conference on Sensor Technologies and Applications (SENSOR COMM), 2013,pp. 145-150.

[30] Vedat Coskum, Busra Ozdenizci, Kerem OK, " A Survey on Near Field Technology", Springer, Wireless Pers Commum, 2013, pp. 2259-2294.

[31] Z. Shelby, K. Hartke, C. Bormann, and B. Frank, "Constrained Application Protocol (CoAP).draft-ietf-core-coap-18," Internet Eng. Task Force (IETF), Fremont, CA, USA, 2013.

[32] U. Hunkeler, H. L. Truong, and A. Stanford-Clark, "MQTT-S—A publish/subscribe protocol for wireless sensor networks," in Proc. 3rd Int. Conf. COMSWARE, 2008, pp. 791–798.

[33] IoT, M2M, Protocols,[Online], IoT.eclipse.org/protocols.html.

[34] S. Schneider. (2013, October 9). Understanding the protocol behind the internet of things, online electronicdesign.com, embedded, understanding-protocols-behind- internet-things.

[35] Sven Bendel, Thomas pringer, Daniel Schuster, Alexander Schill, Ralf Ackermann, Michael Ameling, A Service Infrastructure for the Internet of Things based on XMPP, IEEE International Conference on Pervasive Computing and Communications Work-shops (PERCOM Workshops), 18-22 March 2013, pp. 385-388.

[36] P. Saint-Andre, "Extensible messaging and presence protocol (XMPP): Core," Internet Eng. Task Force (IETF), Fremont, CA, USA, Request for Comments: 6120, 2011.

[37] Omojokun G. Aju, " A Survey of ZigBee Wireless Sensor Network Technology: Topology, Applications and Challenge", International Journal of Computer Applications, vol. 130, 2015, pp. 47-55.

[38] Karl, H, Willing, A.: 2007. Protocols And Architectures For Wireless Sensor Networks. John Wiley & Sons, New Jersey. (2007).

[39] C. Gomez and J. Paradells, "Wireless home automation networks: A survey of architectures and technologies," IEEE Commun. Mag., vol. 48, no. 6, Jun. 2010, pp. 92–101.

[40] N. Maalel, E. Natalizio, A. Bouabdallah, P. Roux, and M. Kellil, "Reliability for emergency applications in Internet of Things," in Proc. IEEE Int. Conf. DCOSS, 2013, pp. 361–366.

[41] L. Li, Z. Jin, G. Li, L. Zheng, and Q. Wei, "Modeling and analyzing the reliability and cost of service composition in the IoT: A probabilistic approach," in *Proc. IEEE 19th ICWS*, 2012, pp. 584–591.

[42] F. Ganz, R. Li, P. Barnaghi, and H. Harai, "A resource mobility scheme for service-continuity in the Internet of Things," in *Proc. IEEE Int. Conf. GreenCom*, 2012, pp. 261–264.

[43] T. Elsaleh, A. Gluhak, and K. Moessner, "Service continuity for subscribers of the mobile real world Internet," in Proc. IEEE ICC Workshops, 2011, pp. 1–5.

[44] H. Fu, P. Lin, H. Yue, G. Huang, and C. Lee, "Group mobility management for large-scale machine-to-machine mobile networking," *IEEE Trans. Veh. Technol.*, vol. 63, no. 3, Mar. 2014, pp. 1296–1305,

[45] I. Silva, L. A. Guedes, P. Portugal, and F. Vasques, "Reliability and avail-ability evaluation of wireless sensor networks for industrial applica-tions," *Sensors*, vol. 12, no. 1, 2012, pp. 806–838.

[46] I. Silva, R. Leandro, D. Macedo, and L. A. Guedes, "A dependability evaluation tool for the Internet of Things," Comput. Electr. Eng., vol. 39, no. 7, Oct. 2013, pp. 2005–2018.

[47] D. Macedo, L. A. Guedes, and I. Silva, "A dependability evaluation for Internet of Things incorporating redundancy aspects," in *Proc. IEEE 11th ICNSC*, 2014, pp. 417–422.

[48] Ashvini Balte., Asmita Kashid., Balaji Patil., " Security Issues in Internet of Things (IOT): A Survey," International Journal of Advance Research in Computer Science and Software Engineering, ISSN 2277 128X, vol 5, Issue 4, 2015.

[49] C. Sarkar, S. N. A. U. Nambi, R. V. Prasad, and A. Rahim, "A scalable distributed architecture towards unifying IoT applications," in *Proc.IEEE WF-IoT*, 2014, pp. 508–513

[50] Avani sharma,Tarun Goyal, Emmanuel S. Pilli, Arka P. Mazumdar, M.C.Govil, R.C. Joshi, " A Secure Hybrid Cloud Enabled architecture for Internet of Things", Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum, pp. 274-279.

[51] Dhananjay Singh," Developing an architecture: "Scalability, mobility, control and isolation on future Internet services.", Advancing in Computing, Communications and Informatics (ICACCI), 2013 International Conference, pp. 1873-1877.

[52] Sushma Satpute, Bharat Sing Deora, " Improving performance of Internet of Things by using local IoT controller", Green Computing and Internet of Things (ICGCIoT), 2015 International Conference, pp. 1328-1330.

[53] A. Dunkels, J. Eriksson and N. Tsiftes, "Low-power interoperability for the IPv6-based internet of things," in Proceedings of the 10th Scandinavian Workshop on Wireless AdHoc Networks (ADHOC'11), Stockholm, Sweden, 2011, pp. 1011.

[54] A. Dunkels, L. Mottola, N. Tsiftes, F. Osterlind, J. Eriksson, and ¨ N. Finne. The announcement layer: Beacon coordination for the sensornet stack. In Proceedings of the European Conference on Wireless Sensor Networks (EWSN), 2011.

[55] M. Buettner, G. V. Yee, E. Anderson, and R. Han. X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks. In Proceedings of the International Conference on Embedded Networked Sensor Systems (ACM SenSys), Boulder, Colorado, USA, 2006.