A Comprehensive Study Of Architecture, Protocols And Enabling Applications In Internet Of Things (Iot)

Srinivasa A H, Dr.Siddaraju,

Abstract: Internet of Things (IoT) is the latest technology enabled by the developments in technologies such as smart devices, communication technologies and internet protocols. Smart devices can able to communicate with each other without human involvement. The technologies like internet, mobile and Machine-to-Machine (M2M) communication are treated as the first phase of IoT. Applications of IoT are wide in range. Any application of the IoT accomplished with the help of different functions and functions can be treated as layers. This paper provides a detailed architecture of IoT in the form of layers. The paper covers layers starting from business to perception layer. Both hardware and software play an important role in the IoT, so the paper covers details of the hardware as well as software along with the challenges of IoT

Keywords: Internet of Things (IoT), CoAP, MQTT, AMQP, XMPP, DDS

1. INTRODUCTION

The IoT is the interconnection of things or objects for sharing the information. Here Things refers to any system, device, or any other physical objects which can communicate with each other. It can also see as internet connecting with various things. [1-2] IoT is considered as a compound system with various functions such as processing, perception, transmission, service providing and deciding. It also integrates differing technologies from device perception, the communication network to intelligent data processing. It has attributes such as perceiving, ubiquitous interconnection and intelligent processing.[3-4] Applications of IoT are not limited so that it can be used in many applications such as smart transportation, smart city, and e-health.[5] Based on applications, changes can occur in IoT architecture. So the IoT architecture design is generally based on applications. The paper proposes the study of the IoT architecture in detail. The architecture is in the form of layers and the paper covers each layer in detail. The paper also covers the components and challenges of IoT. The remainder of this paper is structured as follows. Section two introduces some of the related work on IoT architecture. Section III proposes a detailed IoT architecture in the form of layers. This section gives complete information of layers. Section IV consists of details IoT components such as hardware and software. Finally, in section V some of the challenges of IoT are discussed.

- *Srinivasa A H is currently Currently persuing Ph.D degree in JJT University, Jhunjhunu, rajasthan. He is wotking as Associtae Professor in the Department of Computer Science & Engineering at Dr. Ambedkar Institute of Technology, Bengaluru, Karnataka, India. He completed his M.Tech in Computer Network Engineering from Visvesraya Techlogical University(VTU), Belagavi, Karnataka, India, in the year 2007.*
- *Dr. Siddaraju is currently wotking as Professor and Head in the Department of Computer Science & Engineering at Dr. Ambedkar Institute of Technology, Bengaluru, Karnataka, India. He completed his Ph.D in the year 2010. He completed his M.E in Computer Science & Engineering from Bangalore University (BU), Bengaluru, Karnataka, India, in the year 2000. He completed his BE in Computer Science & Engineering from mysrore University, karnataka, India in the year 1994. His research interests include Internet of Things, Machine Learning and Neural Networks.The remainder of this paper is structured as follows. Section two introduces some of the related work on IoT architecture. Section III proposes a detailed IoT architecture in the form of layers. This section gives complete information of layers. Section IV consists of details IoT components such as hardware and software. Finally, in section V some of the challenges of IoT are discussed.*

2. RELATED WORK

In [6] a unified architecture of IoT system, on which IoT node model, virtual things, the basic service of things and overall hierarchical model of services had been described. IoT nodes must be connected directly to the Internet and provide basic services of things in this architecture. The application-oriented IoT architecture proposed [7] based on IoT layered architecture. The architecture considered Quality of Service (QoS) sets agent in lower layers then transmits QoS requirements, trying to guarantee the consistency. IoT heterogeneity is the sequence of different multiple approaches and standards. [8]Proposed reference architecture for IoT to tackle the issues that may lead to comprehension problems occurring during the design. A generic architecture [9] to modularize physical objects into the digital world. The design is based on existing communication standards and component-based communication. The integration of physical objects and services can be virtualized as middleware components. The architecture [10] for IoT can measure the parameters of the health of an individual. Storing the data securely in the server for analysis. Alerts can be applied to analyze data to take precaution measurements. The solution [10] can provide clinical health care for homebound patients, elderly people and who are located in remote places.

3. IOT ARCHITECTURE

The context architecture is defined as a framework for the physical components specification, functional organization, configuration, operational principles and procedure. It also includes data formats used in its operation [11] Figure 1 shows the IoT architecture which gives detail about components of the Internet of Things. The architecture can be in the form of layers and the layers are named as a business layer, application layer, middle layer, network layer, and the perception layer [12]

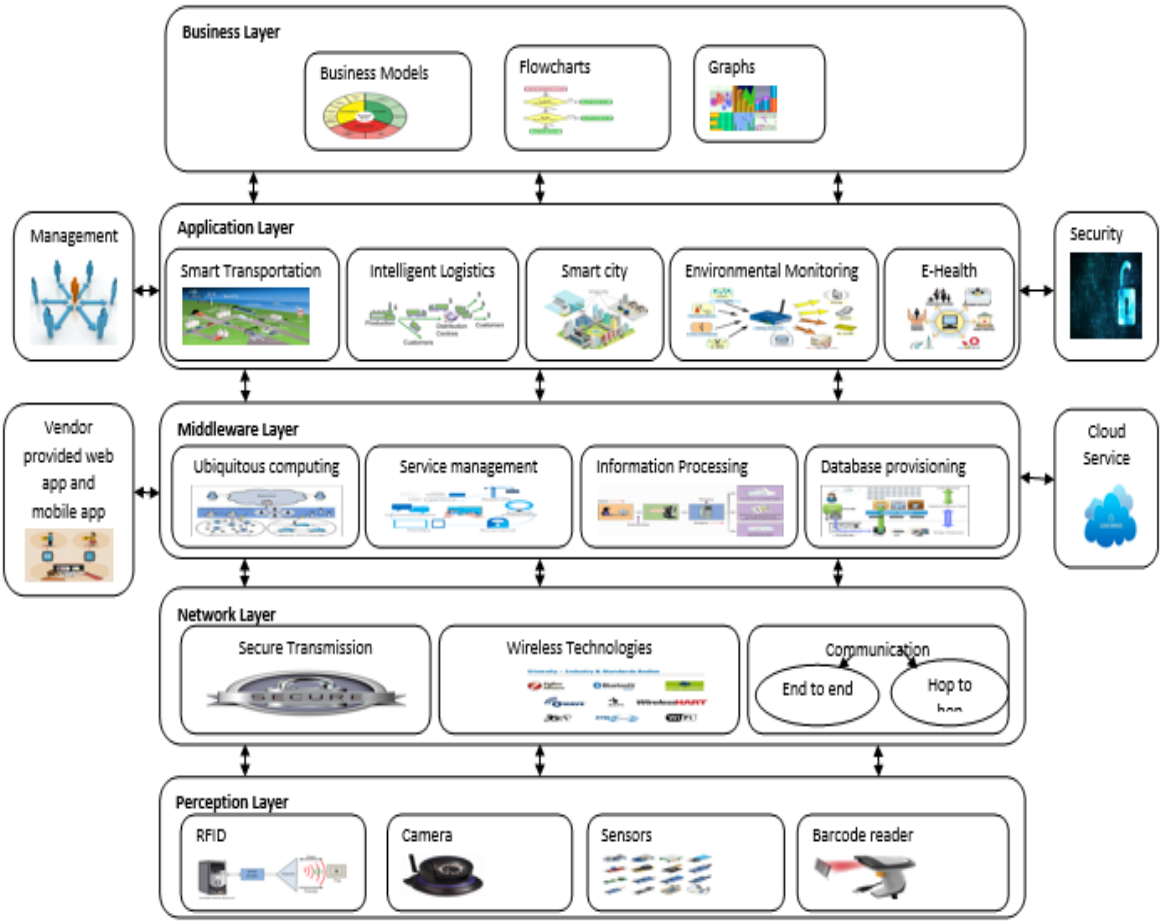

Figure 1 *IoT architecture*

3.1 Business Layer

The business layer manages the IoT system services and activities. Building business models, graphs and flowcharts are the primary functions of this layer. The models are building based on application layer data. To develop, design, analyze, implement, evaluate and to monitor the IoT system related elements business layer can be used. Based on big data analysis this model can also use decision-making process. Business models: It is an arrangement of an action plan which can be executed by an organization. The arrangement can be benefited from operations and can also lead to the generation of revenue. The IoT business models differ according to the different layers. To serve different levels of IoT maturity and adoption, different IoT business models can be identified. Each business model plays an important role in an IoT stakeholder organization's overall IoT strategy. All the companies which are active in the field of IoT can be assigned to at least one of the reference model layer. To define the IoT business models, [13] it needs to address the IoT challenges. The challenges areThe diversity of Things: It refers to the challenge for business models where heterogeneity of connected things and devices without commonly accepted standards are considered. It also considered the ways how things are connected with other things, business and end-users. The models can also integrate with other applications and physical things which may require specific business logic. Immaturity of innovation: It refers to the huge number of emerging technologies, components, devices and IoT platforms. It is better to connect IoT solutions together to help developers to create and experiment products and its services for a variety of IoT systems. With the help of immaturity of innovation, developers can experience the market to develop business models. To adopt a business model rapidly, new IoT products are perfected with a few end users and the majority of the market embraces them [13]. Unstructured ecosystems: The existing IoT ecosystems lack in defining underlying structures, stakeholders, governance and value creating logics. New business models are demanding the creation of new relationships in new industrial sectors, an extension of existing relationships and the penetration of new sectors. Many stakeholders such as software infrastructure suppliers, devices suppliers, smart services, IoT operators, service integrators, IoT platform providers are pushing the business model innovation development. To make up a business model, there is no common options, but the components can make up the business model. The four dimensions, who, what, how and why are considered for illustration of the business model architecture. Who: It identifies the definition of target customer in new business model design. It also addresses the issue of business model service to a certain customer group. What: It describes the target customer offer or customer values. This can be viewed based on the company's offer and services which are of value to the customer. How: It generally considered the company's processes and activities to build and distribute the value proposition. Value: It relates to the revenue and the financial viability of the business model. It also unifies the cost structure, revenue mechanisms and points to question such as how to generate value.It needs to

address the why, who and what in the IoT business model framework which can be shown in Figure 2.

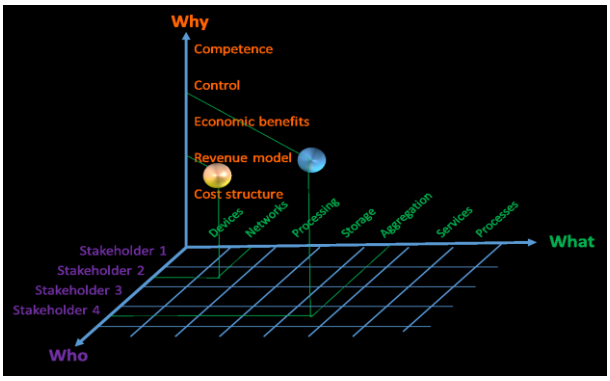

Figure 2 *IoT business model framework [14]*

New innovative IoT business models are required for new revenue opportunities and risks. The opportunities consist of software, security and system integration [14] One of the important business models is the value chain. It defines the service delivery of IoT. IoT has a very complex value chain because it impacts a large number of processes. These are more complicated than traditional models. It breaks down activities into a sequence of value-generating activities from the conception to end use.

3.2 Application layer

The application layer is used to build applications to satisfy the needs of the business. It builds a variety of applications. It acts as an interface between the Internet of Things and users. This layer provides the customer services. The most important function of this layer is to provide high-quality smart services to satisfy customer requirements. For all kinds of applications, it achieves information storage, data mining and decision making. To realize IoT application intelligence, the layer is combined with the industry standards. The layer includes key technologies such as distributed computing, intelligent processing of massive information, information findings. The layer covers the application such as intelligent transportation, intelligent logistics, smart city, environmental monitoring, e-health and precision agriculture. [15] It also provides global facilities to manage the applications. Intelligent Transportation: Intelligent transportation is the up-and-coming technology for improving road safety, driving experience, traffic efficiency, and shortest time travel path optimization. In this system, vehicles are equipped with RFID tags, sensors and actuators with some embedded system. The embedded system can gather important information and send it to the traffic control for better routing, congestion control. The sensors and actuators available in the vehicle can avoid the collisions and also prevents the accident. [16] The main benefit of smart transportation is a vehicle to vehicles communication in a systematic manner without human intervention. This can improve the existing traffic system. Intelligent logistics: Because of the huge potential of IoT, it can almost connect with everything using some embedded sensors. In intelligent logistics also IoT connected with things such as assets and trucks. IoT facilitates assets tracking, remote fleet management in intelligent logistics. Generally, IoT can be used in logistics to provide real-time tracking and monitoring solutions. Smart city: In the view of public sector leadership cities can be considered as interconnected networks for building a clean, energy-efficient, and sustainable society. So the smart cities include smart parking, smart street lights, smart waste management, and smart buildings. Because of the popularity of IoT devices, many IoT protocols and standards have been developed for smart cities. Generally, IoT devices are battery operated, so power efficient communication protocols are important for the smart cities. The IEEE802.15.4 has been widely adopted in many IoT devices as the MAC and physical layer protocol. The use of standard protocols guarantees the interoperability of different IoT devices. Generally, the smart city environment uses RFID, WSN, addressing and middleware as some of IoT technologies. In a smart city, the data use should ensure the reusability of the data for different applications. The collected data accuracy can be maintained when data are shared among critical applications and services. It has many end users like government agencies, citizens, industrial patterns, etc. [17] there may be a set of requirements and services for each end user in any smart city. Environmental Monitoring: [18] Environmental monitoring used to access an object's real-time status and to control the behavior of a specific object by using different types of sensors and actuators. Some of the environmental monitoring are controlling air pollution, waterways, noise monitoring, industry monitoring. Depending on the application different sensors are used. For example, noise pollution can be a monitor with the help of atmospheric dioxide sensors.

3.2.1 Application layer protocol

It is required to consider the protocols which can handle the communication between the gateways, internet, and the final applications. The application layer protocols are used for command carrying from application to end devices and also toupdate servers with the devices' latest values. MQTT: It was developed by IBM 1999 and standardized in 2013 by OASIS for M2M communication. It uses publish/subscribe protocol architecture. MQTT protocol is considered because of its simplicity and it does not require high CPU and more memory. It supports different devices of wide range and mobile platforms. The protocol aims to minimize the bandwidth requirement and guarantee the reliability of packet delivery. The main features of the protocol: support of multicast communication, the establishment of communication between remote devices and the minimization of network traffic. MQTT is suitable for many IoT applications because it is a lightweight protocol. This protocol runs over TCP/IP, so it provides ordered, lossless bidirectional connections. In [19] the protocol provides three types of Quality of Services (QoS) for message delivery.

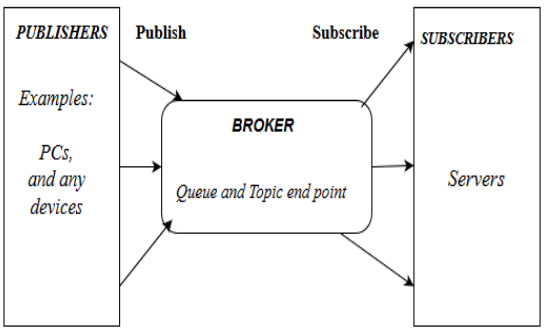

Figure 3 *Components of MQTT [30]*

Figure 3 shows three components of MQTT publishers, broker and subscribers. Publishers: A lightweight sensors which are connected with a broker is known as publishers and which are used to send data to a broker. Broker: These are used to send interesting data to subscribers. Subscribers: These are applications of IoT which are interested in sensor data and also connect with a broker.

AMQP: It is same as MQTT but has the advantage to store data and then forward it. In this security is managed with the help of TLS/SSL protocols. Generally, it runs over TCP.

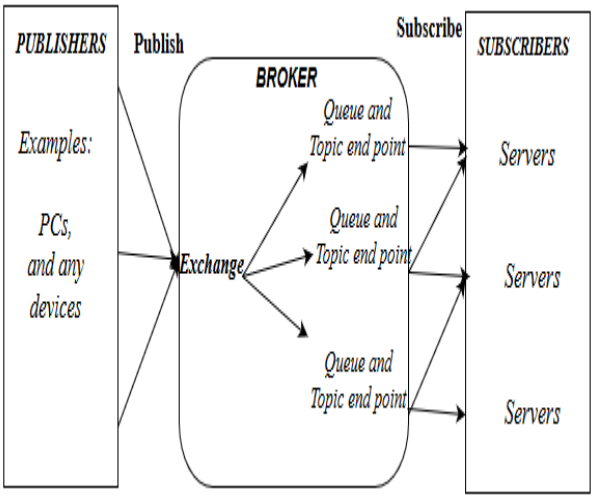

Figure 4 *AMQP publishers and subscribers [30]*

Figure 4 Shows the AMQP publishers and subscribers. In the figure a broker divide into two parts exchange and queue. Exchange responsibility to receive publishers messages and distribute to queue. Queues are based on pre-defined roles and condition and it sends a message to subscribers who subscribe to those data. Extensible Messaging and Presence Protocol (XMPP): It is considered as one of the most common messaging and communication protocol for IoT. It can address the need for IoT because it supports low latency and small messages. Figure 5 shows the structure of XMPP. The models supported by XMPP are publish/subscribe and request/response. Request/response allows bidirectional communication and publish/subscribe allows multi-directional communication. It uses XML for text communications.

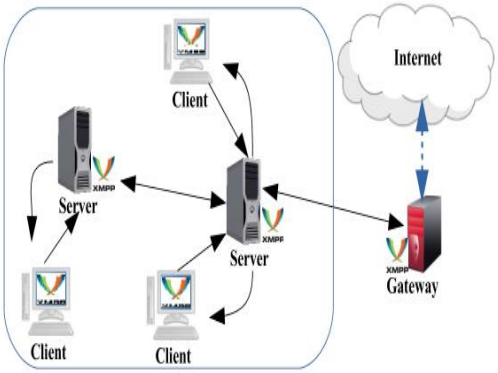

Figure 5 *Structure of XMPP [30]*

Advantages: It is simple and used in projects of heterogeneous applications. It is both flexible and extensible protocol. Drawbacks: It needs high CPU usage and bandwidth. In this QoS is not guaranteed and restricted for simple data types. It is not suitable for real-time and constrained environment applications. XMPP can be rarely used IoT, but its architecture can be enhanced to support IoT applications. Constrained Application Protocol (COAP): This protocol is similar to client/server protocol, so it is known as the request/response protocol. Figure 6 shows the structure of COAP. It is suitable for a constrained environment such as low RAM or CPU capability, a constrained network such as low power Wireless Personal Area Network (WPAN). Generally, the constrained environment creates bad packet delivery and high overhead. COAP was mainly designed for machine to machine applications and automation of systems. By interfacing with HTTP, it is possible to reduce overhead, enhancing packet delivery which may lead the work simple. The publish/subscribe architecture supports more users and provide better performance.

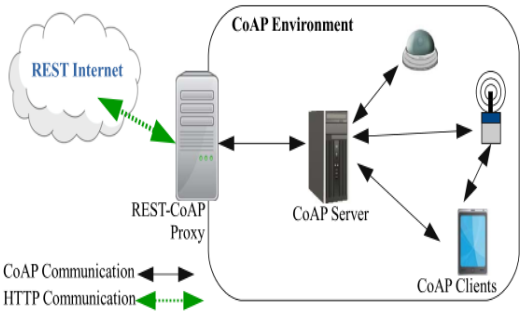

Figure 6 *COAP structure [30]*

The most important feature of COAP is its simplicity and reliability because it supports both unicast and multicast by using UDP. This protocol having two layers first one is messaging layer used to achieve reliability and second one is request/response layer used for interactions. [20] It uses different types of messages and they areComfortable message: In this, it uses an acknowledgment method for reliable communication Non-conformable Message: In this, it does not require any acknowledgment for the message.

Acknowledgment Message: This message indicates arrive of the comfortable message. Reset Message: In this reset message to propagate to empty acknowledgment message when required critical part will miss the message interpretation. Piggybacked Response: In this the receiver directly responds after receiving the acknowledgement message. Separate Response: It is a separate message from the acknowledgement message from the receiver responses. Restful Services: Representational State Transfer (RESTFUL Services) is an engineering that gives web administrations which permit trade between HTTP utilizing gadgets of IoT. It utilizes GET, POST, PUT and DELETE strategies of HTTP for the framework. For secure and reliable HTTP service RESTful uses TLS/SSL. It is a better choice for IoT because it supports different types of applications. Many test beds prove the benefits of the protocol in the IoT environment for M2M communication. The applications supported by the RESTFUL perform better compare to other protocols and are easy to learn and implement. Data Distribution Service (DDS): It is also a publish/subscribe protocol generally designed for M2M communications by the Object Management Group (OMG).

Figure 7 shows the DDS protocol structure. The protocol defines two sub-layers which are
Data-centric publish-subscribe: The main responsibility of this layer is to deliver the message to subscriber.

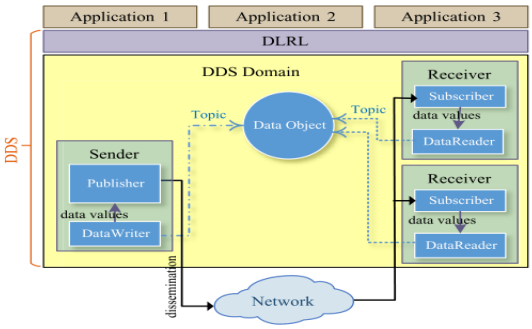

Figure 7 *DDS protocol structure [30]*

Data-local reconstruction: It is considered in the application layer for simple integration of DDS and which can be optional. Because of this protocol ability to achieve reliability and QoS, it should be considereda better choice for M2M and different IoT applications. It uses various QoS standard such as security, durability, priority, etc. The data transmission between publisher and subscriber in DDS is known as a topic. The data on the topic for the subscriber is generated by Data Reader and for the publisher by Data Writer. Web Socket: It is a single channel TCP which can use the full-duplex communications which are suitable for browser applications. It also provides communication between clients and a remote server in two ways. The protocol starts session without publish/subscribe and request/response models like other protocols. It also provides security similar to the web browser security model. Once the session starts, it keeps running until both the client and server end.

3.3 Middleware Layer

This layer exists between the application and network layer. The main task of this layer is to hide details of the hardware and allows developers to concentrate on the application development process. This layer is also responsible for ensuring interoperability, scalability, abstraction and providing service for customers. User's authentication along with efficient delivery service considered as a secure environment for the layer [21]. The layer has more critical functionality, such as aggregating and filtering the received data from the hardware devices, performing information discovery and providing access control to the devices for applications. Ubiquitous computing: In this information, the processing is linked with each activity. [22] It is also connecting different electronic devices and embedded processors to communicate information. The devices used are constantly available and completely connected. Ubiquitous computing operation is shown in figure 8.

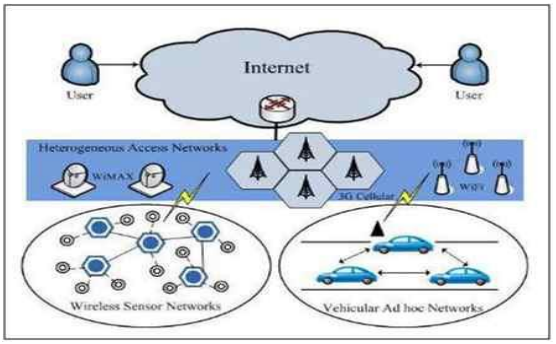

Figure 8 *Ubiquitous computing*

Service management: This layer pairing the service with requester based on addresses and names. It enables the IoT application programmers to work with heterogeneous objects without considering a specific platform. This layer also processes the received data, makes a decision, and delivers required services over the network. Information processing: Extracting the raw sensory data from IoT devices and converting this data into human understandable or machine understandable form is treated as information processing. The process characterized by meaningful abstractions from the raw data. The meaningful abstractions to be in a human and or machine-understandable form. Database provisioning: IoT has many challenges for database administrator regarding flexibility, scalability and connectivity. RDBMS such as MySQL can be extended to handle unconventional sources of data [23]. Generally, DBMS such as NoSQL is appropriate for data collection from intelligent devices and sensors in IoT. The best way to provision the database through a secure, reliable, and scalable platform for a data network is database provisioning. Morpheus Virtual Appliance supports MongoDB, MySQL, Elastic search, and Redis with a simple point and click database provisioning setup.

3.4 Network Layer

In IoT, the main function of this layer is information transmission across the network. [24] This layer can handle the risks such as the denial of service attacks, unauthorized access; man-in-the-middle attacks, virus attacks, confidentiality, the integrity of data. It can be implemented in the basic communication framework. Generally, IoT involves sensing and acquisition of data from heterogeneous data with heterogeneous data formats and character. In [25] the transferring of these data in IoT can lead to complex network related problem such as congestion. The network layer should maintain reliable data fusion, transmission, mining and communication.

3.4.1 Secure transmission

Secure transmission is the important asset in IoT which gives assurance to error-free communication. A popular hardware platform for both IoT basic devices and advanced devices such as gateway can be used for secure transmission. In IoT, the protocol MQTT and COAP are used for secure data access at the device level as well as a secure transmission.

3.4.2 Wireless technologies:

NFC (Near Field Communication): It is a short range that is less than 1 meter and high frequency such as 13.56 MHz RFID technology used to exchange information between two NFC enabled devices. It helps in simplifying the connection of

devices in contactless applications. These are low cost and consume low or zero power for operation. These are ideal for IoT connectivity in devices that need to connect occasionally. In IoT applications, the NFC-enabled devices can talk to each other and then to cloud. Wi-Fi: It is the most commonly used environment providing near-ubiquitous internet access in schools, campuses, office buildings, lodging, residual homes and so on. The service of WiFi is shown in figure 9. It is not a standard but covers the streams of IEEE 802.11 standards along with details implementation. It has limited range of approximately 120 feet indoors and 300 feet outdoors. It consumes more power compared to other standards. Wi-Fi access point can handle up to 255 connected devices. To support more devices multiple access points can be deployed. In view of reliability, it provides a high degree of interference immunity. Depends on standards different bandwidth can be considered. Generally, 802.11a and 802.11g support up to 54 Mbps bandwidth and 802.11n support 100 Mbps. Because of Wi-Fi's ubiquitous wireless technology, it can be considered for most of the IoT applications and devices. Wi-Fi connectivity can be considered for all smartphones, tablets, and laptops and so on. Wi-Fi ubiquity is one of the fundamental factors in the rapid growth of IoT.

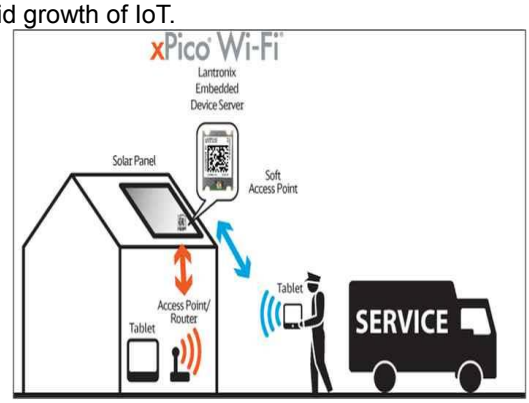

Figure 9 *Wi-Fi service*

ANT+: It is an Ultra-Low power wireless technology consumes approximately 1mW. The coverage distance for this nearly 100 meters with 1 Mbps data rate. It can operate in the frequency range of 2.4 GHz. ZigBee: It is IEEE 802.15.4 based standard and operates in the frequency range of 2.4 GHz as shown in the figure 10. It can cover a range of 10 to 100 meter with data rate of 250 Kbps. The main advantages of ZigBee are less power consumption for operation, robustness, high scalability, and high security [26]. Because of these advantages, ZigBee will be in most of the M2M and IoT applications. ZigBee can be available in two standards such as ZigBee and ZigBee Pro. Because of low power consumption, it can be used in different IoT applications such as smart home, remote controls and health care systems.

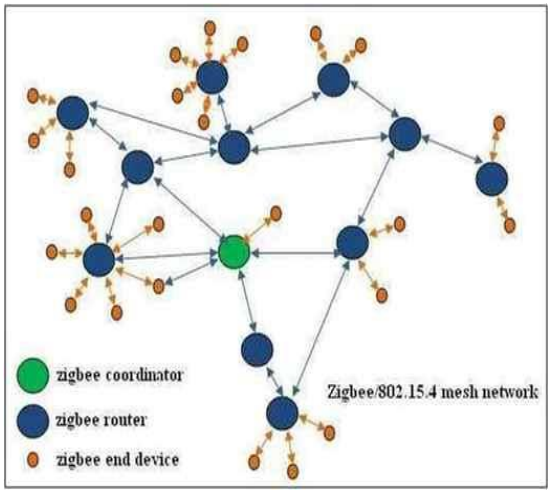

Figure 10 *ZigBee network*

Bluetooth: It is short-range communication technology and can be considered in wearable products. [blue]It can be connected to the IoT through smartphones. It operates in 2.4GHz range. It covers a range of 50 to 150 meters with data rate of 1 Mbps. Bluetooth Low Energy(BLE) or Bluetooth smart is the new technology to be considered in most of the IoT applications. BLE or Bluetooth smart is not designed for file transfer and is suitable for transfer of small chunks of data. Bluetooth cannot connect to the internet directly s it require a gateway to connect to the internet. Bluetooth is available in different versions and the latest one is Bluetooth 4.2. This Bluetooth 4.2 can allow the devices to access the internet directly through the internet protocol. Z Wave: It is a low power RF communications technology generally designed for IoT applications such as light control, energy control, wearable healthcare control and others. It is considered as reliable for low latency communication with small data packets with data rates up to 100 Kbps. It operates in 1GHz. It covers the range of 30 meters with data rates 100 Kbps. Wireless HART (Highway Addressable Remote Transducer Protocol): This protocol is considered as data link protocol and which operates on top of IEEE 802.15.4. It adopts Time Division Multiple Access (TDMA). It should be considered as secure and reliable because of its advanced encryption method for messages. This standard offers peer-to-peer, per-hop and end-to-end security mechanisms. It can operate at 2.4 GHz and it requires a gateway to connect to IP networks. It allows full wireless connectivity to HART-enabled devices enabling real-time communication. It covers a range of several tens of meters for low-frequency information updates.

3.4.3 Low Power Wide Area Network (LPWAN) Technologies:

SigFox: It is a low power wireless technology for communicating objects with a different range of low energy. These can be generally used in sensors and M2M applications. It can cover a range up to 50 km. SigFox uses Ultra Narrow Band (UNB) technology which can be designed to handle low data transfer speeds from 10 to 1000 bits per second and can run on a small battery. It supports star network topology. Cellular: If any IoT application requires operation over longer distances then cellular communication capabilities such as GSM/3G/4G can be used. It is capable of sending high quantities of data. The power consumption for 4G is too high for many IoT applications. The available

standards are GSM, GPRS, EDGE (2G), UMTS/HSPA (3G), LTE (4G). It can operate in the frequency ranges 900 MHz, 1800 MHz, 1900 MHz, 2100 MHz it can cover the range maximum 35 km for GSM and 200 km for HSPA. Data rates available are 35 Kbps to 170 Kbps for GPRS, 120 Kbps to 384 Kbps for EDGE, 384 Kbps to 2 Mbps for UMTS, 600 Kbps to 10 Mbps for HSPA and 3 Mbps to 10 Mbps for LTE.

3.4.4 Network layer protocols

In IoT application, many protocols can be used for routing. These protocols can be categorized as standard and nonstandard. The network layer should be partitioned into two sublayers and they are routing layer and the encapsulation layer. Routing layer handles the packet transfer from source to destination. The encapsulation layer forms the packets [27]. RPL protocol: To operate on top of link layers PHY and MAC a distance vector and source routing, RPL protocol has designed. It mainly focuses on the collection of periodic measurements in collection based networks. The main feature of this protocol is to provide a routing solution for both lossy and low power networks [28]. When routes are inaccessible, the alternative is provided by this protocol. It uses dynamically formed network topology to disseminate information over the network. This type of protocol generally suitable for where energy constrained devices are used in the applications.

Advantages:

- This protocol does not require translation gateways for accessing the nodes within the network from the outside world and provide end to end IP based solution.
- Dynamic adaptation of control messages sending rating of the routing in the unstable network condition.
- It will consider the optimized network for different application scenarios and deployment.

Disadvantages

- The protocol will not support the multipath routing.
- It will not consider the load and energy balancing.

CORPL (Cognitive RPL): It is generally designed for cognitive networks and should be considered as an extension of RPL. It uses topology DODAG with some modifications. It uses opportunistic forwarding for packet transmission by selecting multiple forwarders and coordinates with the help of best hop selection. In this DODAG topology is built similar to RPL. In CORPL each node maintains the forwarding set and updates along with parent node using DIO messages. This updated information can be used to update the neighbor dynamically to construct a forwarder set [29] CARP (Channel Aware Routing Protocol): For the underwater communication this type of distributed routing protocol can be used. It uses lightweight packets so that it can be used in many IoT applications. Based on historical data delivered, the link quality can be computed by this protocol and also selecting the forwarding nodes. The protocol has two scenarios like network initialization and data forwarding. Hello packet broadcasting from a sink to other nodes is considered in network initialization and the packet routing has to be considered in data forwarding with a hop by hop method. Next hop is calculated independently. The main drawback of this protocol is reusability of previously collected data is not possible.

3.4.5 Network layer encapsulation protocols

In most of the IoT applications, the IPv6 addresses are too long for most of the data link frames which are small hence a set of standards are developed to encapsulate IPv6 datagrams in various data link layer frames for IoT applications use. Some of the protocols are 6LoWPAN, 6TiSCH, 6Lo and so on. 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks): This is the most commonly used standard protocol which can encapsulate IPv6 long headers in IEEE 802.15.4 small packets efficiently and size cannot exceed 128 bytes. It can support variable length addresses, low bandwidth, power consumption, different topologies, low cost, scalable networks, mobility, unreliability and long sleep time. It reduces transmission overhead by providing header compression. The protocol uses dispatch header for multicasting and IPv6 header compressions. It is better to divide long IPv6 header to smaller fragments which can be a maximum of 128 byte length, so this protocol can use the mesh headers and which can be broadcasted. 6TiSCH: IETF working group developed standards to allow IPv6 to pass through Time-Slotted Channel Hopping (TSCH) mode of IEEE 802.15.4e datalinks. In this protocol, the nodes which are sharing the same application can assign the time slots to a group of neighboring nodes. It does not specify the detail of scheduling but it allows maximum flexibility for different IoT applications. Depending on topology or application used in the MAC layer the scheduling can be distributed or centralized. 6Lo: This protocol generally considered for resource constrained nodes and named IPv6 over Networks of Resource-constrained Nodes (6Lo). IETF has developed a set of standards for transmission of IPv6 on different data links.

3.5 Perception layer

The perception layer is also known as a sensing layer. The main function of this layer is to get a data sample from the environment using different kinds of perception devices. It also processes the data to obtain useful information and then transmits to the network layer through the network access devices such as WSN gateways. The layer consists of integrated hardware for the acquisition of data and perception. The most popular sensing technologies are RFID, Camera, sensors, barcode and others. RFID (Radio Frequency Identification): It plays a major role in the design of microchips for wireless communications. RFID tags may be active or passive and embedded into objects for automatic identification. RFID technology plays an important role in solving issues of objects identification for IoT applications. The active tags are self-powered used to initiate the communication and passive tags have no internal power. The passive tags are generally deployed in transportation, retail, logistics, road toll, and smart bank cards. Active RFID tags are used in auto manufacturing and remote monitoring applications. It has small transceiver used for both receiving query from the reader and transmitting the tag id to the reader. Wireless Sensors: These are electronic chips generally used for remote sensing applications. The main features are a minimal cost, small size, high efficiency and ability to gather, process, analyze information, etc. In cooperation with RFID WSN can better track environmental changes and status of things such as location, temperature and movement. Camera: To solve logistical problems and for home safe, intelligent cameras are used. It can also be used in cars for navigation. Intelligent cameras can detect and capture the exact moment.

Cameras are installed along roads to optimize the driving by notifying empty space in a lane. Some smart cameras in IoT save only relevant data which can be used later for analysis.

4. COMPONENTS OF IOT

To make IoT devices interconnection smoother to provide smarter, safer and better services the components of IoT play the major role. The main components of IoT are hardware and software. 30% hardware and 70% of software constitute the components of IoT. Hardware: These are the devices or physical objects having the capability of sensing, retrieving and responding to instructions. In most of the IoT applications hardware can be used for device control, remote dashboard, device control, routing, system activation, security and communication. Following are some of the hardware devices Sensors: In most of the IoT applications, sensors play a major role. Sensors consist of RF power management and this module is used for managing communications with the help of Wi-Fi, ZigBee, Bluetooth, radio transceiver, duplexer. The sensing module in the sensor used for sensing with the help of active and passive measurements devices.

TABLE 1 *TYPES OF SENSORS*

Sl. No	Type of Sensor	Description	Applications
1	Temperature Sensor Ex: Thermocouples, Resistor temperature detectors, thermistors, infrared sensors	This device generally used to measure heat energy by detecting temperature change in the environment in some particular form and converting it for user or device.	A/C control, refrigerators, manufacturing processes, agriculture and health industry.
2	Proximity sensor Ex: Capacitive sensor, photoelectric sensors, ultrasonic sensors	This type of sensor is used to detect the presence or absence of a nearby object and its properties. It can also be used to convert properties of an object into user readable form or machine-understandable form.	The retail industry, parking availability in malls, stadiums or airports.
3	Pressure sensor Ex: Pirani gauge	A sensor which detects pressure and converts it into an electric signal. The amount of pressure depends on the level of pressure applied.	Manufacturing, maintenance of water systems and heating systems
4	Water Quality Sensor Ex: Organic carbon sensors, Turbidity sensor, pH sensor, Oxygen-reduction potential sensor,	This type of sensors used to measure water quality and iron monitoring in distribution systems of water.	River and stream gaging, wastewater and effluent measurement.
5	Chemical sensor Ex: chemiresistor, electrochemical gas sensor, hydrogen sulphide sensor, pH gas electrode, potentiometric sensor, zinc oxide Nano rod sensor	To detect chemical changes in air or liquid, a chemical sensors are used. This type of sensors considered in various industries.	Industrial environmental monitoring, process control, harmful chemical detection, explosive and radioactive detection
6	Gas sensor Ex: carbon monoxide sensor, hydrogen sensor, oxygen sensor, ozone monitor, gas detector, hygrometer, nitrogen oxide sensor, air pollution sensor	These sensors used to detect changes in air quality and the presence of various gases similar to chemical sensors.	Manufacturing, agriculture and health, air quality monitoring, Detection of toxic or combustible gas, Hazardous gas monitoring in coal mines, Oil & Gas industries, chemical Laboratory research, Manufacturing – paints, plastics, rubber, pharmaceutical & petrochemical.

7	Smoke sensor Ex: Optical smoke sensor, Ionization smoke sensor	To detect airborne particulates of gases and its level, the smoke sensors are used. These can be used for a long period of time.	Manufacturing industry, HVAC, buildings and accommodation infra to detect fire and gas incidences.
8	IR sensor	The sensors used to detect characteristics of surroundings by emitting infrared radiation. It also measures the heat emitted by the object.	In Healthcare to monitor blood flow and blood pressure a simple an array of regular smart devices such as smartwatches and smartphones, Home appliances & remote control, Breath analysis, Infrared vision wearable electronics, optical communication, non-contact based temperature measurements, Automotive blind-angle detection.
10	Level sensor Ex: Point level sensor, continuous level sensor	This sensor detecting amount of liquids, fluids or other substances which flow in an open or closed system.	Fuel gauging & liquid levels in open or closed containers, Sea level monitoring & Tsunami warning, water reservoirs, Medical equipment, compressors, hydraulic reservoirs, machine tools, Beverage and pharmaceutical processing, High or low-level detection
11	Image sensor Ex: CCD (charge coupled device), CMOS (Complementary Metal oxide semiconductor)	This type of sensor generally used to detect and conveys the information that constitutes an image.	Digital camera & modules, medical imaging and night vision equipment, thermal imaging devices, radar, sonar, media house, Biometric and IRIS devices.
12	Motion detection sensor Ex: Passive Infrared(PIR), Ultrasonic, microwave	The motion detector is used to detect physical movement in a given area and transform it into an electric signal.	Intrusion detection systems, Automatics door control, Boom Barrier, Smart Camera Toll plaza, Automatic parking systems, Automated sinks/toilet flusher, Hand dryers, Automated lighting, AC, Fan, Appliances
13	Accelerometer Ex: capacitive accelerometer, piezoelectric accelerometer	Accelerometer generally used to convert mechanical motion into an electrical output. It also measures the acceleration of an	cellular and media devices, vibration measurement, Automotive control

		object due to inertial forces.	and detection, free fall detection, aircraft and aviation industries, movement detection, sports academy or athletes behavior monitoring, consumer electronics,/ industrial and construction sites
14	Gyroscope sensor Ex: rotary gyroscopes, vibrating structure gyroscope, optical gyroscopes, MEMs(Micro Electro-Mechanical Systems) gyroscopes	This sensor used to measure angular velocity or angular rate. Angular velocity is defined as a measurement of the speed of rotation around the axis.	Car navigation systems, Game controllers, Cellular and camera devices, consumer electronics, Robotics control, Drone and RC control helicopter or UAV control, Vehicle control or ADAS
15	Humidity sensor	To detect water vapor content in an air atmosphere or from other gases the humidity sensor has to be used. The common humidity is Relative Humidity(RH)	Industrial and residential domain for heating, ventilatin9-74g, and air conditioning systems control, Automotive, museums, industrial spaces and greenhouses, meteorology stations, Paint and coatings industries, hospitals and pharma industries to protect medicines
16	Optical sensor Ex: photodetectors, fiber optics, pyrometer, proximity & infrared	This sensor detects the physical quantity of light rays and converts these rays into an electrical signal which can be easily read by the devices or user.	Healthcare, environment monitoring, energy, aerospace and many more industries.

Wearable devices: in IoT, wearable devices play a major role and devices can be worn on the head, arms, neck, torso and feet. These can be used in IoT to stay connect and to improve productivity by accessing them.
Some of the wearable devices are helmets, smart glasses which can be considered for the head, Jewelry, collars for the neck, smart watches, wristbands, and rings for arm, clothing, and backpacks for the torso, socks, and shoes for feet.
Standard devices: In addition to sensors and wearable devices, IoT also considers the standard devices such as desktop, laptop, tablet and cell phone. These devices remain integral parts of IoT as the remotes and command center.
Desktop: It provides the highest user level control of the system and its settings.
Tablet: It acts as a remote and provides access to the key features of the system.
Cell phone: It allows essential settings modifications and also provides remote functionality.
IoT can also include routers and switches in the standard network as connected devices.

Software: These components generally used for enabling data collection, processing, storing, manipulating and instructing about the processing. It also considers the Communication infrastructure which consists of technologies and protocols used for physical devices or objects communication for exchanging the data. It is also a key area of middleware, networking, and embedded systems.
The main responsibilities of IoT software are data collection, real-time analytics, device integration, application and process extension.
Data collection: The data collection software manages the sensing, measurement of data, aggregation of data, filtering of light data, data security. Various protocols are used in connecting with sensors of real-time and machine-to-machine networks. This software is able to collect data from multiple

devices and can distribute according to their settings. The collected data transmitted to a central server.

Device integration: This software supports the integration of system devices to build the body of the IoT system. This software ensures networking and cooperation between the devices. Various applications, protocols and limitation of each allow this software to manage communication.

Real-time analytics: This software takes the input data from different devices and converts the data into a clear pattern for human analysis. Information can be analyzed based on various settings and designs. It also provides the industry required data.

Application and process extension: This software generally used to extend the existing systems and software. This can also allow a wider and more effective system. The software also integrates predefined devices for specific purposes. It supports productivity improvement and more accurate data collection.

IoT operating system: There are many open source operating system for IoT devices. These operating systems can be used in a wide range of smart devices. Table 2 gives the details of the IoT operating systems.

All of these operating systems have properties of low memory footprint and high power efficiency.

TABLE 2 *TYPES OF OPERATING SYSTEMS*

Sl. No	Operating System	Description	Memory size of devices	Hardware supports	Communication technology supports
1	Brillo	It is an android based OS for embedded and constrained devices	128 MB of ROM 32 MB of RAM	Arm Intel MIPS	Wi-Fi Bluetooth Thread
2	Contiki	It was released by BSD. Comfortably work on constrained devices	30 KB of RAM 30 KB of ROM	TICC2538 nRF52832 TIMSP430x AtmelAtmega128fa1	Built-in TCP/IP stack

3	RIOT	Its having real-time capabilities It can run on 8-32 bit microcontroller. Supports multithreading run on constrained devices.	1.5 KB RAM 5 KB of ROM	MSP430 ARM 7 Cortex- M0, M3 & M4 x86	802.15.4 ZigBee 6LoWPAN ICMP6 IPv6 RPL COAP
4	LiteOS	It is real-time OS	10 KB	ARM DSP MIPS x86	LTE NB-IoT Wi-Fi 6LoWPAN
5	Apache Mynewst	Similar to RIOT and LiteOS Capable of running on constrained devices	8 KB of RAM 64 KB ROM	Arduino zero Arduino M0 pro Cortex	BLE Wi-Fi Bluetooth
6	Zephyr	Real-time OS run on a small memory device. Biggest strength is interconnectivity.	8 KB	ARM X86 ARC RISC-V NIOS-II	Bluetooth Bluetooth LE Wi-Fi 6LoWPAN COPA NFC

5. IOT CHALLENGES

IoT applications development is not so easy task due to challenges of IoT. The main challenges are Mobility, reliability, scalability, management, availability, interoperability, security and privacy. Mobility: The devices in IoT move freely in the network so the IP address of moving devices change according to their location. So, the mobility is one of the major issues in IoT. Some routing protocols such as RPL can manage such a mobility problem. The reconstruction of DODAG has to be considered by the protocol when each time node joins and goes off the network. Reliability: The applications of IoT requires highly reliable data and it should be collected fast, communicating them to take proper decisions. Generally, this required in emergency responses. Selection of devices in the perception layer, different routing and application layer protocol can enhance the reliability in IoT applications. Scalability: Scalability is also a challenge for the IoT applications because more number of devices are connected to the same network. Addition to this some new devices and services are adding to the network. Therefore the IoT design should support the extensible operations and services. Management: Management of all the devices, failure tracking, performance and configurations of such devices is a very big challenge for IoT. Providers of such devices are responsible for fault management, configuration, performance, accounting of their devices and each aspect. Availability: Providing hardware and software requirement anywhere and anytime to service subscriber in IoT is known as availability. The service provided to ensure systems are running and available most of the time is known as software availability. The service which guarantees the availability of hardware is known as hardware availability. Both hardware and software should be compatible with IoT protocols, functionality and compact with the constrained devices. Interoperability: Inter-work of heterogeneous devices and protocols with each other is known as interoperability. This is also one of the major challenges of IoT because of different devices and platforms. The device manufacturers and application developers can handle the problem of interoperability by providing service irrespective of the platform and hardware specification that could be used by the customer. Heterogeneity: Heterogeneity in IoT referred to as a platform which allows the various devices for communication. It is also a feature that the platform can handle various devices by various vendors. To support heterogeneity in IoT, it uses a variety of protocols such as MQTT, COAP, and Modbus.

6. CONCLUSION

In this paper, we have presented a comprehensive key research efforts on architecture, protocols and applications in an Internet of Things ubiquitous environment. There is an industry trend towards the adoption of wireless sensors and actuators in their products and services to improve efficiency and productivity. IoT is already showing signs of occupying a prominent place in our daily life. We need to design protocols in order to control the things in a resource constrained and heterogeneous system. But the development of IoT applications is technically complex due to the presence of different IoT protocols, lack of industry standards and interoperability issues. In such a complex and diversified scenario, this study helps in throwing light on a multifaceted discipline and contribute to the development of the IoT paradigm.

REFERENCES

[1] Alessandro Floris, Luigi Atzori, “Quality of Experience in the Multimedia Internet of Things: definition and practical use-cases”, IEEE International Conference on Communication Workshop (ICCW), pp. 2164-7038, 14 September 2015.

[2] Bruno Dorsemaine, Jean-Philippe Gaulier, Jean-Philippe Wary and Nizar Kheir, “Internet of Things: a definition & taxonomy”, 9th International Conference on Next Generation Mobile Applications, Services and Technologies, pp. 978-1-4799-8660-6/15, 2015.

[3] Xing Liu, Orlando Baiocchi, “A Comparison of the Definitions for Smart Sensors, Smart Objects and Things in IoT”, IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 978-1-5090-0996-1/16, 17 November 2016.

[4] Johana A. Manrique, Johan S. Rueda-Rueda, Jesus M.T.

Portocarrero, "Contrasting Internet of Things and Wireless Sensor Network from a conceptual overview", IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 978-1-5090-5880-8/16, 2016.

[5] Alba Amato, Antonio Coronato, " An IoT-Aware Architecture for Smart Healthcare Coaching Systems ", IEEE 31st International Conference on Advanced Information Networking and Applications, pp. 1550-445X/17, 2017.

[6] Weigong Lv , Fanchao Meng , Ce Zhang , Yuefei Lv , Ning Cao , Jianan Jiang, "A General Architecture of IoT System", IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Volume 1, pp. 659 – 664, 2017.

[7] Ren Duan , Xiaojiang Chen , Tianzhang Xing, " A QoS Architecture for IOT", International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, pp. 717 – 720, 2011.

[8] Jasmin Guth, Uwe Breitenbucher, Michael Falkenthal, Frank Leymann, and Lukas Reinfurt, "Comparison of IoT Platform Architectures: A Field Study based on a Reference Architecture", Cloudification of the Internet of Things (CIoT), pp. 1 – 6, 2016.

[9] Wei Wang, Kevin Lee, David Murray, "Building a Generic Architecture for the Internet of Things", IEEE Eighth International Conference on Intelligent Sensors, Sensor Networks and Information Processing, pp. 333 – 338, 2013.

[10] Srijanee Biswas, Sohum Misra, "Designing of a Prototype of e-Health Monitoring System", IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), pp. 267 – 272, 2015.

[11] Litun Patra, Udai Pratap Rao, "Internet of Things — Architecture, applications, security and other major challenges", 3rd International Conference on Computing for Sustainable Global Development, pp. 1201-1206, 2016.

[12] Dina Gamal Darwish, "Improved Layered Architecture for Internet of Things", International Journal of Computing Academic Research (IJCAR), Volume 4, Issue 4, pp.214-223, August 2015.

[13] Hubert C. Y. Chan, "Internet of Things Business Models", Internet of Things Business Models", Journal of Service Science and Management, pp.552-568, 2015.

[14] Hubert C. Y. Chan," Internet of Things Business Models", Journal of Service Science and Management, pp. 552-568, 2015.

[15] Makkad Asim, " A Survey on Application Layer Protocols for Internet of Things (IoT)", International Journal of Advanced Research in Computer Science, Volume 8, No. 3,pp. 0976-5697, April 2017

[16] Cao Xin ; Chu Na ; Bai Yeshuai, "Analysis on Key Technologies of Traffic Prediction and Path Guidance in IntelligentTransportation", international Conference on Intelligent Transportation, Big Data & Smart City (ICITBS), pp. 5 – 8, 2016.

[17] Emile Mardacany, "Smart cities characteristics: importance of buit environments components", IET Conference on Future Intelligent Cities, pp. 1 – 6, 2014.

[18] Shifeng Fang ; Li Da Xu ; Yunqiang Zhu ; Jiaerheng Ahati ; Huan Pei ; Jianwu Yan ; Zhihui Liu, "An Integrated System for Regional Environmental Monitoring and Management Based on Internet of Things", International journal of IEEE Transactions on Industrial Informatics, Volume: 10 , Issue 2, pp. 1596 – 1605, 2014.

[19] Ding Yi ; Fan Binwen ; Kong Xiaoming ; Ma Qianqian, "Design and implementation of mobile health monitoring system based on MQTT protocol", IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), pp. 1679 – 1682, 2016.

[20] Peter Peniak , Mária Franekova, " Model of integration of embedded systems via CoAP protocol of Internet of Things", International Conference on Applied Electronics (AE), pp. 201 – 204, 2016.

[21] Zhexuan Song ; Alvaro A. Cardenas ; Ryusuke Masuoka, "Semantic middleware for the Internet of Things", IEEE conference on Internet of Things (IOT), pp. 1 – 8, 2010.

[22] Noboru Koshizuka , Ken Sakamura," Ubiquitous ID: Standards for Ubiquitous Computing and the Internet of Things", IEEE Pervasive Computing, Volume: 9 , Issue: 4, pp. 98 – 101, 2010.

[23] C. Fischer ; V. Bawa,"An approach for network data provisioning in UMTS networks", 11th International Telecommunications Network Strategy and Planning Symposium. NETWORKS , pp. 179 – 183, 2004.

[24] Paul Loh Ruen Chze , Kan Siew Leong, "A secure multi-hop routing for IoT communication", IEEE World Forum on Internet of Things (WF-IoT)", pp. 428 – 432, 2014.

[25] Dimitrios Tomtsis ; George Kokkonis ; Sotirios Kontogiannis, "Evaluating existing wireless technologies for IoT data transferring", South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)", pp. 1 – 4, 2017.

[26] Taibur Rahman ; Swarnendu Kumar Chakraborty, "Provisioning Technical Interoperability within ZigBee and BLE in IoT Environment", 2nd International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech)", pp. 1 – 4, 2018.

[27] Cheena Sharma ; Dr. Naveen Kumar Gondhi," Communication Protocol Stack for Constrained IoT Systems", 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)", pp. 1 – 6, 2018.

[28] S. Umamaheswari ; Atul Negi, "Internet of Things and RPL routing protocol: A study and evaluation", International Conference on Computer Communication and Informatics (ICCCI)", pp. 1 – 7, 2017.

[29] Hwaiyu Geng, "NETWORKING PROTOCOLS AND STANDARDS FOR INTERNET OF THINGS", Internet of Things and Data Analytics Handbook, pp. 816, 2017

[30] 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 & Tutorials, Volume 17, Issue 4, pp. 2347-2376, 2015.