ISSN XXXX XXXX © 2019 IJESC

Research Article Volume 9 Issue No.3

The Future of Internet of Things (IoT) and Its Empowering Technology

Yusuf Perwej[1], Majzoob K. Omer[2], Osama E. Sheta[3], Hani Ali M. Harb[4], Mohmed S. Adrees[5]
Assistant Professor[1, 2, 3, 4, 5]
Department of Information Technology[1], Department of Computer Science[2], Department of Information System[3, 5], Department of Computer Engineering[4]
Al Baha University, Al Baha, Kingdom of Saudi Arabia

Abstract:
The Internet of Things is an intelligent network, which concatenates all things to the Internet for the purpose of interchange information and communicating via the information sensing devices in conformity with agreed protocols. We could also elucidate the IoT as the next stage in the Internet as some do, whereby things and objects with sensors and actuators are concatenated to the Internet so they can accumulate, send and get data, leading to intelligent solutions and in some cases also act upon data. In this paper, we survey state-of-the-art methods, internet of things (IoT) and its enabling technology in this new emerging area. Because, in the IoT physical objects may also make conclusion about the amassed, processed, and interchange information, as well as take expeditions to control the physical objects and the environment in which they are embedded. The capacities that enable the physical objects to get involved with in the IoT are ordinarily composed of an assemblage of various types of advanced technologies including software, actuators, sensors, and electronics. The IoT assents actuators and computer interfaced sensors to encourage to novel products and services by minimizing costs, increase efficiency, and enhancing the user-friendliness of existing systems. These capacities are either concatenate to or integrated into traditional products and systems. In the end, we will thoroughly analyze the technical details about the IoT enabling technology.

Index Terms: Internet of Things (IoT), SigFox, MEMS, ZigBee, Web of Things (WoT), Long-Range (LoRa), MQTT, Wireless HART, Z-Wave.

I. INTRODUCTION

Imagine a world where trillion of objects can sense, interact and share information [1], all interconnected over private or public internet protocol networks. These interconnected objects have data steady collected, analyzed and used to begin action, make available for wealth of intelligence for planning, handle and decision making [2]. As a definition, the Internet of Things originated in 1999, with the work of two Massachusetts Institute of Technology research labs, the Auto-ID Center and the MIT Media Lab. In this scenario, Kevin Ashton and Neil Gershenfeld respectively, argued for the unfolding of things into the internet in an effective role either in terms of making the world intelligible for things, or adding things to the internet. In this context, the IoT was seen as a paradigmatic shift from the internet of discrete desktop and mobile computers, to a broadly defined comprehensive connectivity permeating frivolous [3] material artefact, consequently granting them agency visible to humans. The IoT devices need to be alive in environments in which information can be collected and either sent to another device or straight to the internet [4]. IoT devices can be programmed to action according to particular conditions. The IoT devices by nature are suited to a network of devices that can interact with each other via other nodes in the same network. The IoT is a network [5] of devices that are connected to the internet through communications technologies, in order to confer a range of new and innovative services and applications [6]. Networks and devices which are competent of realizing huge scale applications have recently begun to emerge. Most of today's wearable and connected subscriber devices use a Bluetooth or homogeneous connection of the device to the owner's smartphone, to confer a connection to the broader internet and applications that confer suitable user interfaces. There are many vital elements that are needed in the comprehension of the IoT [5]. The firstly the communication networks that enable devices, probably using dissimilar operating systems, to communicate with one another. This element influences the existing internet standards of the TCP/IP protocol suite. The secondly is the enormous and economical information storage and processing power available in modern integrated circuits. At present, a range of competing technologies for the connectivity of IoT devices, each making various design agreement between like considerations as data rate, device battery life, vary, range usage and the number of devices supported. This level of fragmentation of technologies is expected to decrease as a small number emerge as leaders and gain satisfactory scale to drive decrease module costs. The Internet of Things (IoT) [7] is a description for embedded and network cloud technologies that enable remote invigilate and control of sensors and systems. IoT can be used in business, industrial, utility and suburban applications and also IoT remote monitoring and parking lots, shipping departments, control applications in hospitals.

II. THE IoT DEVICES AND THEIR ABILITY

The IoT devices are their capabilities to actuate and sense, control, the ability of limiting power and energy, connection to the physical world, intermittent connectivity and mobility. Some must be fast and credible and provide trustworthy security and privacy, while others might not [8]. A number of these devices have physical defense, whereas others are neglected. Actually, in IoT environments, devices should keep safe against

any threats that can affect their functionality. The capacity to sense is enabled via the use of sensors, and the capacity to control is enabled via the use of both sensors and actuators, combined with decision-making capabilities enabled by integrated circuit (IC) devices such as microcontrollers and microprocessors. Sensors are devices whose motive is to monitor some physical parameter of interest and provide an appropriate output signal that is in the form of information that is an actual representation of that parameter. The actuators, such as sensors, are another form of transducer device. Actuators take an energy input, generally in the form of an electrical signal, and generally convert this energy into [9] a mechanical physical motion. This physical motion can be used to undertake steps to control physical objects and potentially ameliorate the environments in which they are located. The concept of control is a little more complicated. The control includes many elements, including the knowledge of a desired state of a system, the capacity to actively determine the present state of the system, and the capacity to direct and cause the system to move toward the desired state. Control system generally includes one or more sensors to measure the state of a system as well as one or more actuators to direct the system to the required state. Both actuators and sensors have been around for a very long time. In spite of, most IoT devices are vulnerable to external and internal attacks due to their features. It is challenging to implement and use a powerful security mechanism due to resource limitation in terms of IoT [4] computational competence, battery power, and memory.

III. THE MEMS

The MEMS is a technology that in its most common form can be defined as microminiaturized electromechanical devices that are made using the techniques of micro and nanofabrication. MEMS are a process technology used to create tiny integrated devices or systems that integrate mechanical and electrical components [10]. They are fabricated using integrated circuit batch processing techniques and can range in size from a few micrometers to millimeters. They are economical systems that use alters device fabrication technology. Generally MEMS devices integrate sensing, processing and actuating functions change the way that the physical world is perceived and controlled. They generally combine two or more electrical, mechanical, biological, magnetic, optical or chemical properties on a single microchip. The kinds of MEMS devices can vary from comparatively normal structures having no moving elements. To vastly complex electromechanical systems with multiple moving elements under the control of integrated microelectronics. Last two decades, researchers and developers have demonstrated an extremely huge diversity and number [11] of MEMS-based sensors for almost every possible sensing application, including magnetic fields, radiation, temperature, pressure, inertial forces, chemical species etc. The one primary criterion of MEMS is that there are at least some elements having some sort of mechanical functionality whether or not these elements can move. The micro-sensors and micro actuators are suitably categorized as “transducers”, which are defined as devices that transform energy from one form to another show in figure 1. In the case of micro sensors, the device generally transforms a measured mechanical signal into an electrical signal [12]. Besides, is the performance of MEMS devices extraordinary. However, their method of production leverages the same batch fabrication techniques used in the integrated circuit manufacturing, which can translate into low per-device production costs, as well as many other mileages.

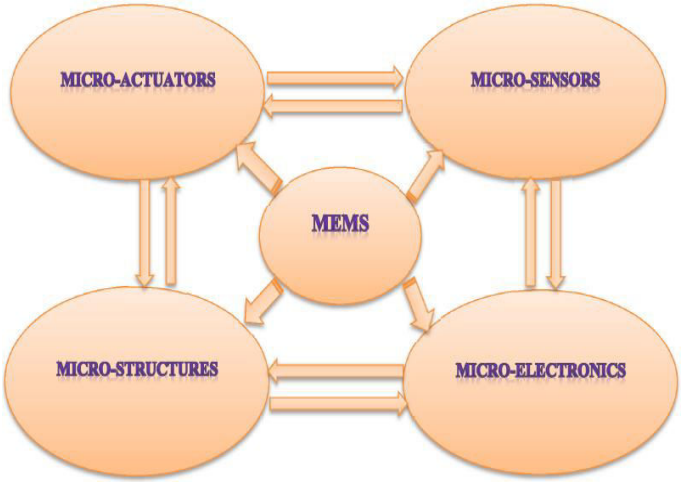

Figure.1. The MEMS

The actual potential of MEMS starts to become fulfilled. When these miniaturized actuators, sensors, and structures can all be incorporated onto a common silicon substrate along with integrated circuits. Meanwhile the electronics are fabricated using integrated circuit process sequences. The micromechanical components are fabricated using favorable micromachining processes that choicely etch away parts of the silicon wafer or add new structural layers to form the electromechanical and mechanical devices. It is even more interesting if MEMS can be incorporated not only with microelectronics, but with other technologies like as Photonics, Nanotechnology, etc. This is sometimes called miscellaneous integration. MEMS fabrication is an extremely exciting effort due to the accommodating nature of process technologies and the [13] diversity of processing capabilities. MEMS fabrication uses many of the same techniques that are used in the integrated circuit domain like as ion implantation, LPCVD, oxidation, diffusion, sputtering etc., as well as integrate these capabilities with highly specialized micro-machining processes. MEMS technology every conceivable product and system can be outfitted with any type of MEMS device. As a result of that, enabling every product and system to become smart wherein it incessantly is monitoring any and all parameters of interest to the user, processes this information, and, based on desired or best conditions, can perform functions to alter or convert these parameters to the best state. Hereupon, it is expected that MEMS devices will have an even huge role to play in vehicle technologies as the concept of IoT rolls out into the wider markets in the time to come.

IV. MEMS IN THE INTERNET OF THINGS (IoT)

MEMS are an enabling technology for the IoT in view of the MEMS manufacturing makes possible small, affordable, high level performance actuators and sensors. The MEMS sensors on the other hand, especially when coupled with huge information processing power, do not get overwhelmed and can incessantly and at the same time monitor a very huge number of important parameters of interest in the environment without distress sensory overload circumstances. This makes for a protected, more productive and pleasing environment. MEMS sensors can at the same time monitor parameters of interest to us over both short and long periods of time and analyze this collected data to give the user information about inclination, warn the user about inconsistency, or unexpected incident occurring, inhibit failures and misadventure, inhibit disruptions and failures of activities

and services, as well as maintain higher-quality and secure services [14]. The MEMS sensors and their associated massive processing power can incessantly reciprocation information with the environment and thereby give us increased contextual familiarity and perceptive capabilities about our environments. In spite of, MEMS sensors as [15] Azoic devices can operate almost indefinitely without exhausting. Probably, these are enormously powerful advantage that can provide considerably more capability for the IoT than is presently possible using human senses alone, or extensively discrete sensor devices.

V. ELECTRO-OPTICAL INFRARED SENSOR IN THE INTERNET OF THINGS (IoT)

Normally speaking, a sensor is a device that is able to detect variation in an environment. By itself, a sensor is futile, but when we use it in an electronic system, it plays a primary role. A sensor is able to measure a physical incidence and change it into an electric signal [16]. The Internet of Things is one of the most vital and promising technological topics at present. Some market researchers estimate that there are more than 22 billion connected devices and counting. Around us, there are smartphones, wearable, and other devices, all of which use sensors. At the present time, sensors play a vital role in our everyday life and in IoT. Sensors monitor our home security, health status, air quality, [17] and are widely used in the Industrial Internet of Things (IIoT) to monitor production processes. There are a number of ways of sensing the environment using electrochemical, electromechanical, and chemical sensors, optical sensing plays a dominant role due to its suddenness and accuracy. The electro optical (EO) sensing denotes the process by which optical indicators are transforming to electrical signals.

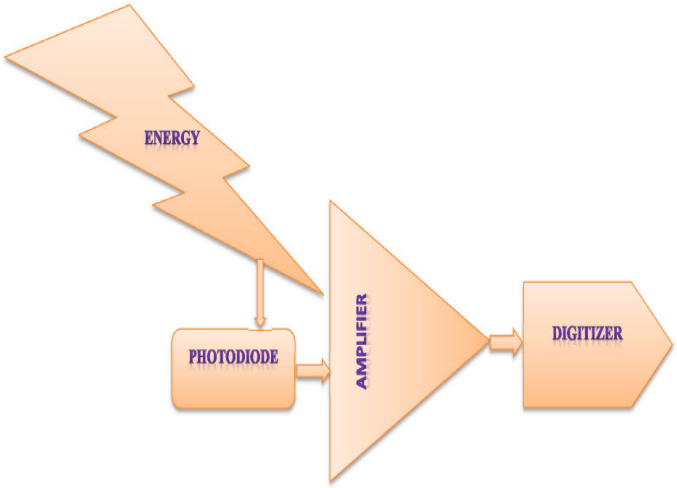

Figure.2. The Energy can be Amplified, Digitized, and Transmitted

The simple electro optical devices are found ubiquitously in the form of photodiodes that sense a break in a beam of infrared (IR) light as used in an elevator and garage doors to inhibit closing on a person or in a water faucet to sense the presence of a hand. The electro optical sensors operate in the IR wavelength suitable for the [18] process temperature being sensed for instance, Short Wave Infrared (SWIR) for semiconductor growth and processing, Near Infrared (NIR) for steel manufacturing processes, and Mid Wave Infrared (MWIR) for cement temperature monitoring. While sensors in the visible range (350–700 nm) have some applicability in IoT devices, the real influence of electro optical sensors for IoT is in the IR range (>750 nm). The core of an optical sensor is a detector material element, like as a photodiode, which converts incoming photon energy into electrical energy or the modulation of electrical energy show in figure 2. The electrical power can then be amplified, digitized, and transmitted. This is a wide diversity of materials that can be employed to perform this energy transmutation. The photo detectors cover a broad spectral wavelength range, from ultraviolet (10-400 nm), visible (400-750 nm), X-ray (0.01-10 nm), IR (750 nm-100's μm) to millimeter waves. For IoT, IR detectors play a critical role due to the pertinent wavelength range of interest [19]. IR photo detectors can be divided into many groups based on their spectral response wavelength range. In this context, there are two main types of IR detectors, thermal detectors and photon detectors. In Thermal IR detectors are based on temperature increase of IR materials from absorption of IR illumination, which can cause transform of certain material characteristics, like as resistance transform effect, thermoelectric effect, or pyro-electric effect. In Photon detectors are [20] based on absorption of photons by particular semiconductor materials due to IR illumination, which generates electron–hole pairs with the output signal being either photo voltage or photocurrent.

A. The Domain View of the IoT with Controller & Sensor

The Internet of Things (IoT) solutions created a need for the next generation sensors and loaded with characteristics to solve the modern day automation challenges. The IoT sensors are intelligent and have the capability to communicate with other sensors and remote computers as well [21]. There are state-of-the-art IIoT technologies like equipment, sensors and real-time analysis [22]. These are successively growing digitally and changing the way digital industrial processes and efficiency move forward. The paradigm of connected things has made evidently that industries are able to work intelligently with a huge amount of data being collected by the IoT sensors.

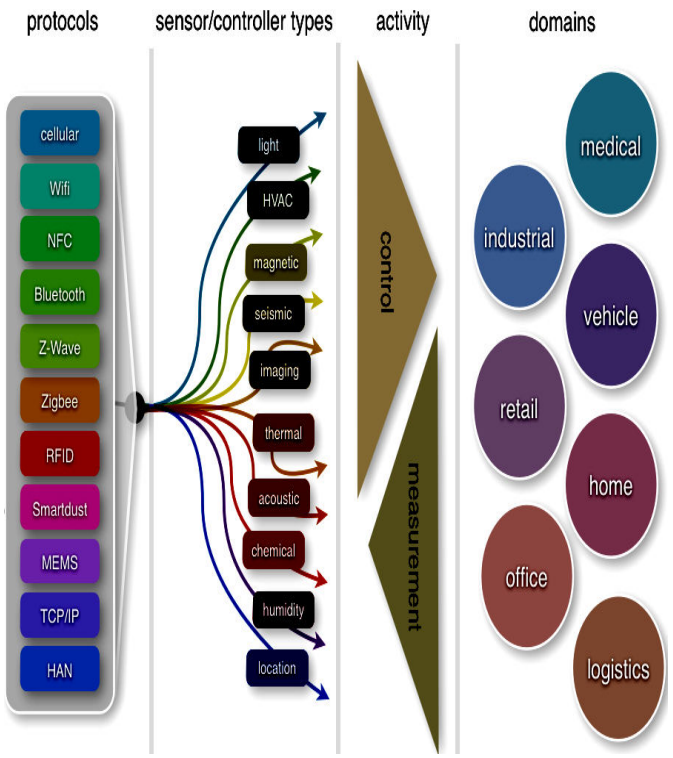

Figure.3. The Domain View of the IoT with Controller & Sensor

The Industrial Internet of Things (IIoT) to take processes which are conventionally handled on the factory floor by people and machines and move them to the cloud where they can be handled

remotely and even independently [22]. As data are at the crux of an industrial IoT setup, the role of sensors is mandatory for making the entire ecosystem smarter figure 3 shows the domain view of the IoT with sensor & controller. The material technologies have make sure that the sensors are more actual, low on cost, power demand and of diminished size. As most industrial IoT applications are far from the control center, the sensors necessity to have a very low power step. They are now able to collect diversify of data, thus enabling the industries to work with improve efficiency.

VI. NETWORK TECHNOLOGIES IN INTERNET OF THINGS (IoT)

The Internet of Things (IoT) is a collection of dissimilar components that connect software, systems, and people through internet technology [4]. One of these important components is the communication network, enabled by IoT wireless technology, [23] the communication network is the gateway between an IoT device and a software platform. To connect all the expected billions of devices to the Internet, more Internet addresses were needed than were existing via the IPv4 protocol. Once connected, all these devices necessity networks to communicate with other devices and computer systems [24]. There are many various types of networks that are available and each has dissimilar strengths for dissimilar applications. The IoT wireless technology in its simplest form needs a radio capability that can receive and broadcast radio waves as a means for transmitting signals or data [7]. Data transfer rates and energy necessity are two key considerations when selecting a network technology for a given application. This technology such as 4G (LTE, LTE-A) and 5G are suited for IoT applications, given their higher data transfer rates. Further down, we are discussing select wireless network technologies that could be used for IoT applications.

A. ZigBee

ZigBee communication in particular built for control and sensor networks on IEEE 802.15.4 standard for wireless personal area networks (WPANs), ZigBee is a self-healing, secure, robust, and mesh-capable protocol. It can scale to thousands of nodes across huge areas [25]. ZigBee enabled devices, which enable cost and power efficient wireless networking over huge distances via mesh networks, Within a ZigBee system architecture, there are 3 device types first ZigBee Router (ZR), second ZigBee Coordinator (ZC), and third ZigBee End Device (ZED). There is only one coordinator in the network. The coordinator chooses the network topology, establishes the network, and administers configuration information. Its action as the gateway in and out of the network, so it must have the power to be on and execute at all times. ZigBee routers broadcast information and move data via the network and they may also function as a sensor node.

B. Low-Power Wide-Area (LPWA) Networks

Low-power wide-area technology (LPWA) is the response to the need for pervasive, battery-efficient, professionally managed, and out-of-the-box connectivity to unlock massive value for tens to hundreds of billions of devices [26]. The LPWA networks are entering the IoT space to address some of the unique needs of IoT devices. For example, LPWA networks extend coverage into arduous radio environments.

C. Long-Range (LoRa)

LoRa (short for Long Range) continues to advantage attention in the marketplace. It overture a compelling mix of long range, low power consumption, intensive indoor coverage, and secure data transmission show in figure 4. LoRa operates in the unlicensed 1GHz frequency range. It uses spread spectrum technology so that impending transmitters are less likely to tamper with each other. This increases the capacity of each gateway. Spread spectrum communications also confer a coding gain over narrow band communications 27]. This outcome in a powerful communications link, which can support huge range communications. LoRa data rates range from 0.3 kbps to 50 kbps and can support a range of up to 15km.

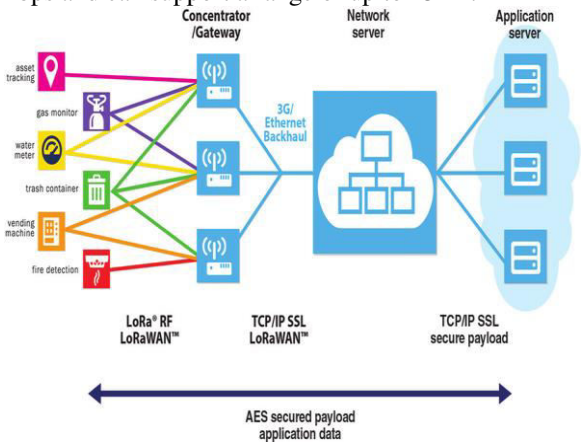

Figure.4. The LoRa Network

D. Ingenu

This IoT wireless technology fundamentally focused on smart meter and oil and gas applications. It has since expanded into other IoT wireless applications contain urban and agricultural environments [28]. The Ingenu solution uses Random Phase Multiple Access technology and it enables data rates in the hundreds of thousands of bits per second. The system uses the 2.4 GHz unlicensed and universal frequency band. This proposes huge bandwidth, greater pliability, and decrease the eventuality of interference. The Ingenu also uses channel coding Viterbi algorithm to assurance data delivery and provide high quality of service. It is firmly synchronized to support low delay applications and uses 256-bit encryption and two-way authentication to confer enterprise level security. The Ingenu may be one of the best IoT wireless technologies dealing with a difficult situation.

E. Thread

A Thread is an IoT wireless technology that is mainly used to connect and control products in the home. For ease of integration with an IoT system, it endues a make simpler bridge between a Thread mesh network and the Internet. The Thread permits, home automation devices to communicate through power lines [29], radio frequencies or a combination of both. It is an IPv6 based protocol built on the IEEE802.15.4 link layer. The Thread is not an application protocol. It clarifies how to send data within the network, but not how to interpret it. Thread can support IP-based application layers. The Thread is driven by Google and Nest and is gaining traction in house automation.

F. Bluetooth

Introduced in 1999, Bluetooth technology is a wireless technology known for its capability to transfer data over short distances in personal area networks. Bluetooth Low Energy (BLTE) is a recent inclusion to the Bluetooth technology and consumes about half the power of a Bluetooth classic device, the main version of Bluetooth. The energy efficiency of BLTE is attributable to the shorter scanning time needed for BLTE devices to detect other devices such as 0.6 to 1.2 milliseconds [30]. The Bluetooth is already integrated into smartphones and many other personal, mobile devices. This is a major benefit Bluetooth has over many competing IoT wireless technologies.

G. SigFox

Sigfox is an ultra-narrowband technology. It uses a standard radio transmission procedure called binary phase-shift keying, and it takes very narrow chunks of the spectrum and transformation the phase of the carrier radio wave to encode the data [31]. The Sigfox uses low data rate transmission and sophisticated signal processing to effectively keep away from network interference, and ensures the integrity of the transmitted data show in figure 5. This IoT wireless technology solution permits bidirectional communication, but always commence by the device. The Sigfox is emphatic for communications from endpoints to base stations (uploads). However, it is not emphatic for communications from base stations to endpoints (downloads Sigfox consumes a fraction (1%) of the power used via cellular communication. This network solution would be perfect for one-way systems, including environmental sensors, basic alarm systems, and agricultural and simple metering as well as this technology is a good fit for any application that needs to send small, unusual bursts of data.

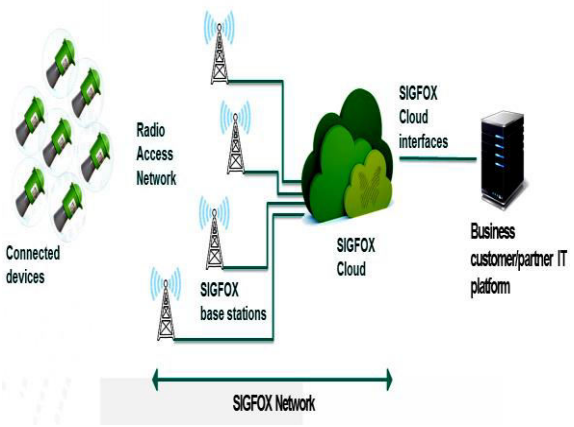

Figure. 5. The SigFox Network

H. Z-Wave

Z-Wave is a low-power, IoT wireless technology, mainly designed for home automation. It is a possessory solution, originally developed by Zen-Sys and later acquired by Sigma Designs. The Z-Wave proposed authentic and low-latency communication with data rates up to 100kbit/s [32]. A Z-Wave network consists of internet of things (IoT) devices and a mainly controller, also known as a smart home hub, which is the only device in a Z-Wave network that is normally connected to the internet. When a Z-Wave hub receives a command from a smart home application on a user's tablet or computer, smartphone, it routes the command to its destination device across networks of up to 232 devices including the hub show in figure 6.

Figure. 6. The Z-Wave Network

I. RFID

Radio Frequency Identification (RFID) technology uses radio waves to recognize people or objects. There is a device that reads information contained in a wireless device or tag from a distance without making any physical contact or need a line of sight. The tags [33] contain electronically stored information. Passive tags collect energy from a nearby RFID reader's cross-examines radio waves. The active tags have a local power source and may operate hundreds of meters from the RFID reader. The RFID is able to endue several write and reads functions per second, despite the fact that, it is not a very high data rate system; it is enough for most data monitoring applications.

VII. WEB OF THINGS (WoT)

You might have noticed that the IoT feels very much like IoT to communicate with ten dissimilar devices from your phone; you have to install ten dissimilar apps. The difficulty is that there's not a single "lingua franca" spoken by each and every object. Things could then comfortably exchange data with each other, but not necessarily comprehend what that data means. This is what Web protocols like HTTP introduces to the Internet, a universal way to describe images, text, and other media elements so that machines could comprehend each. The Web of Things is simply the next stage in this evolution, using and adapting [34] Web protocols to connect anything in the physical world and give it an existence on the World Wide Web. The WoT architecture is an effort to structure the galaxy of Web protocols and tools into an advantageous framework for connecting any object or device to the Web [35]. The WoT architecture stack is not composed of layers in the rigid sense, but rather of levels that add extra functionality. Each layer helps to integrate Things on the Web even more warmly and hence making those devices more reachable for applications and humans.

A. Accessibility Layer 1

This layer is accountable for turning any Thing into a Web Thing that can be communicated with using HTTP requests just like any other resource on the Web [35]. In other words, a Web Thing is a REST API that permits to communicate with something in the real world, such as opening a door or reading a temperature sensor located across the planet.

B. Findability Layer 2

This layer makes sure that your Thing can not only be comfortably used by other HTTP clients, but can also be findable and automatically used by other WoT applications. The procedure here is to reuse web semantic standards to describe things and their services. This enables the discovery of things via quest engines and other web indexes as well as the automatic generation of user interfaces or tools to communicate with Things.

C. Sharing Layer 3

The Internet of Things will only thrive if Things have a way to safely share data across services. This is the trustworthiness of the share layer, which specifies how the data generated by Things can be shared in an efficient and safely manner over the web. At this level, another batch of Web protocols bestead.

D. Composition Layer 4

Finally, once Things are on the Web layer 1 where they can be found by humans and machine layer 2 and their resources can be shared safely with others layer 3, it's time to look at how to build huge scale and worthwhile applications for the Web of Things [35]. In this context, we need to comprehend the integration of data and services from miscellaneous Things into an immense

ecosystem of web tools like as mixture platforms and analytics software.

VIII. INTERNET OF THINGS (IoT) PROTOCOLS AND STANDARDS

A large ecosystem of connected devices, named the Internet of Things, has been expanding over the globe for the last two decades. Presently, the immense number of objects around us is enabled to collect process and send data to other objects, servers or applications [36]. The intense evolution of the mobile Internet, micro computing, mini hardware manufacturing, and machine-to-machine (M2M) communication has enabled the IoT technologies. The hidden language permits physical objects to talk to each other consist of IoT standards and protocols. The common protocols used for personal computers, smartphones or tablets may not be suitable [37] for specific requirements such as bandwidth, range, power consumption of IoT-based solutions. The IoT proceeds to a perfectly different Internet, so that not all existing protocols were able to meet the expectations its needs and provide seamless connectivity. An IoT system has a three-level architecture, devices, gateways and data systems show in figure 7. The data moves between these levels through four types of transmission channels.

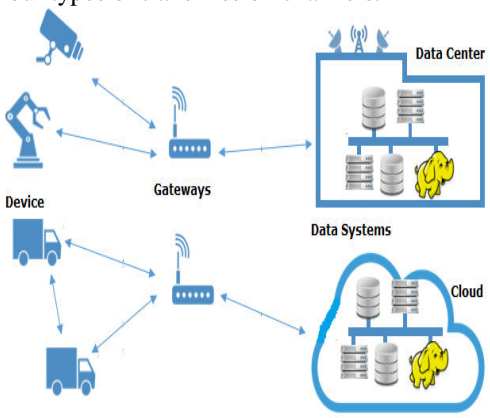

Figure.7. The Three Level of IoT Architecture

In the device to device, when the devices necessity to contact with other devices, the use case likely needs that they receive data instantly, therefore the timeliness of the incoming data is a high-priority. This type of affined is not very common yet, because most devices are not able to handle such processes. Subsequently, each "thing" needs to send its data to an aggregating gateway node via what is sometimes called the "fog" layer. They call it the fog because gateways can physically live in a wide range of places depending on necessity, including clouds and datacenter DMZs keep safe by security firewalls. The gateways perform two general functions, firstly they bring together and route data from sensor devices to the suitable data systems within the datacenter or cloud. Secondly, they can examine or combined device data and forward that data to the core systems and reply back to devices if [38] a time-sensitive exception circumstances is noticed. There are several IoT gateway protocols that may preferable compatible this or that solution depending on the gateway computing capabilities, network capacity and credibility, the frequency of data generation and its standard. At the gateway to data systems, gateway is normally a much more competent for computing device than the sensor, with credibility and a fast network connection. So here the determination of what message protocols and standard of service to use is driven not by the gateway's computing ability or connectivity. Unless by data traffic patterns like as periodic burstiness and obstruction, number of concurrent connection needs, and security requirements [39]. Within the secure datacenter, needs like as integration with live applications, high level throughput, high level availability, calamity recovery and ease of deployment become the critical decision factors. Next section, we are discussing specifics of IoT protocols, standards. There are numerous options and alternatives, but we'll discuss the most famous ones.

A. Data Link Layer Protocols in Internet of Things (IoT)

In this section, we are discussing the data link layer protocol standards.

IEEE 802.15.4e

The IEEE 802.15.4 is the most generally used IoT standards for MAC. It defines a frame format; headers contain the source and destination addresses, and how nodes can connect with each other. The frame formats used in conventional networks are not appropriate for low-power multi-hop networking in IoT due to their overhead. It uses time synchronization and channel hopping to enable high credibility and low cost and meet IoT communications necessity [40]. The standard does not define how the scheduling is done, but it needs to be constructed cautiously such that it manages mobility scenarios. It can be centralized by a manager node which is accountable for building the schedule and informing others about the schedule, and other nodes will merely follow the schedule. Network formation contains advertisements and components. A new device should pay attention for advertisement commands, and upon receiving at least one such command, it can send a join entreaty to the advertising device.

Wireless HART

The Wireless Highway Addressable Remote Transducer protocol is a data link protocol that operates at the top of IEEE 802.15.4 PHY and adopts time division multiple access (TDMA) in its MAC. The HART is an open standard and vendor independent. Therefore, it is the world's most broadly supported protocol in the process industry, with thousands of HART based products available from various vendors. It is a secure and authentic [41] MAC protocol that uses advanced encryption to encrypt the messages and calculate the integrity in order to offer trustworthiness. In the wireless HART consists of a network manager, a security manager, a gateway to connect the wireless network to the wired networks, wireless devices as field devices, access points, routers, and adapters shown in figure 8. The standard proposed per-hop, end-to-end, or peer-to-peer security mechanisms, in end-to-end security mechanisms enforce security from sources to destinations, while per-hop mechanisms secure it to next hop only.

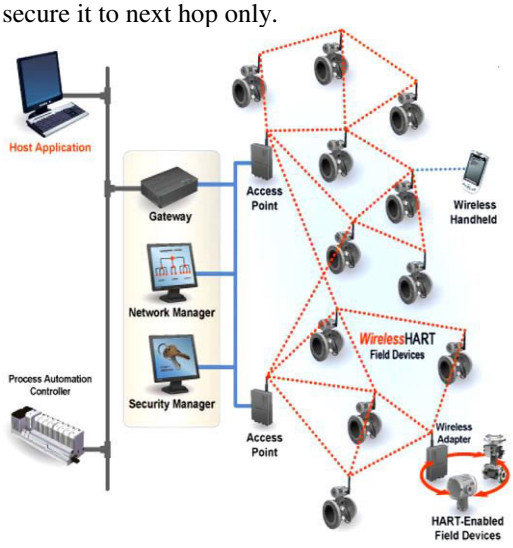

Figure. 8. The Wireless HART Architecture

IEEE 802.11ah

The IEEE 802.11ah is a light version of the original IEEE 802.11 wireless medium access norm and designed with less overhead to meet IoT requirements. IEEE 802.11 standards are the most commonly used wireless standards. They have been extensively used and adopted for all digital devices, including laptops, mobiles, tablets, and digital televisions (TVs) [40]. In spite of, the actual Wi-Fi standards are not appropriate for IoT applications due to their frame overhead and power consumption. Consequently, IEEE 802.11 working group initiated 802.11ah task group to develop a norm that supports lowest level overhead, power congenial communication appropriate for sensors and motes. 802.11ah designed for low-power sensors and, consequently, it permits a longer sleep period of time and waking up occasionally to exchange data only.

HomePlug

The HomePlug Green PHY is another MAC protocol developed by the HomePlug Power line Alliance that is used in home automation applications. HomePlug appropriate for both PHY and MAC layers and has three editions, first HomePlug audio visual (HomePlug AV), second HomePlug AV2, and third HomePlug GP [42]. HomePlug AV is the basic power line communication protocol, which uses TDMA and CSMA and CA as MAC layer protocol endorsement adaptive bit loading which permit it to transform its rate depending on the noise level, and uses Orthogonal Frequency Division Multiplexing and four modulation techniques. HomePlug GP is designed for IoT generally and in particular for home automation and smart grid applications. It is mainly designed to decrease the expenditure and power consumption of HomePlug AV while keeping its interoperability, trustworthiness, and coverage. HomePlug GP has a power-save mode that permits nodes to sleep much more than HomePlug by synchronizing their sleep time and waking up only when essential.

B. Network Layer Protocols in Internet of Things (IoT)

In this section, we are discussing the standard and non-standard protocols that are used for routing in IoT applications.

RPL

The Routing Protocol for Low-Power and Lossy Networks (RPL) is distance vector protocols that can endorsement a diversity of data link protocols. It constructs a Destination Oriented Directed Acyclic Graph (DODAG) that has only one path from each leaf node to the path in which all the traffic from the node will be routed to. At first, each node sends a DODAG Information Object (DIO) advertising itself as the path [43]. This message has disseminated in the network and the whole DODAG is gradually built. When communicating, the node sends a Destination Advertisement Object (DAO) to its begetter, the DAO is disseminating to the root, and the root adjudges where to send it depending on the destination. When a new node wants to join the network, it sends a DODAG Information Solicitation (DIS) entreaty to join the network and the root will respond back with a DAO Acknowledgment (DAO-ACK) ratify the join.

CARP

The Channel-Aware Routing Protocol (CARP) is a distributed routing protocol developed for underwater communication. It has lightweight packets so that it can make use of IoT. It contemplates link quality, which is computed based on historical well-turned data transmission gathered from vicinal sensors, to select the forwarding nodes. It performs two different functionalities first network initialization [44] and second data forwarding. In network initialization, a HELLO packet is simulcast from the sink to all other nodes in the networks. In data forwarding, the packet is routed from sensor to sink in a hop-by-hop manner. Each next hop is determined autonomously. The CARP protocol does not support earlier collected data. Hence, it is not favorable for those IoT or other application where data are altered very often.

6LoWPAN

The IPv6 over Low-power Wireless Personal Area Network (6LoWPAN) is the first and most generally used standard in this class. It efficiently encapsulates IPv6 long headers in IEEE802.15.4 small packets, which cannot be more than 128 bytes [45]. The specification supports various length addresses, low bandwidth, various topologies including star or mesh, low cost, scalable networks, power consumption, mobility, unfaithfulness, and prolonged sleep time. The standard provides header compression to decrease transmission overhead, fragmentation to meet the 128-byte maximum frame length in IEEE802.15.4, and endorsement of multi hop delivery. It has the finite processing capability to transfer information wirelessly using an internet protocol. So, it is primly used for house and building automation.

C. Session Layer Protocols in Internet of Things (IoT)

In this section, we are discussing the standards and protocols for message passing in IoT session layer proposed by different standardization organizations.

MQTT

MQTT (Message Queue Telemetry Transport) is a messaging protocol, which was proposed by IBM in 1999. At the beginning built for monitoring sensor node and far away tracking in IoT. Its compatible are small, cheap, low-memory and low-power devices [46]. The MQTT confer embedded connectivity between applications and middleware in one side and other side it connects networks and communicators. In the MQTT system consists of three main components publishers, subscribers, and a broker shown in figure 9. From IoT viewpoint, publishers are basically the lightweight sensors that connect to the broker to send their data and go back to sleep whenever feasible. In this scenario, subscribers are applications that are concerned with a certain topic, or sensory data, so they connect to brokers to be informed whenever new data are received. The brokers classify sensory data in topics and send them to subscribers concerned with the topics.

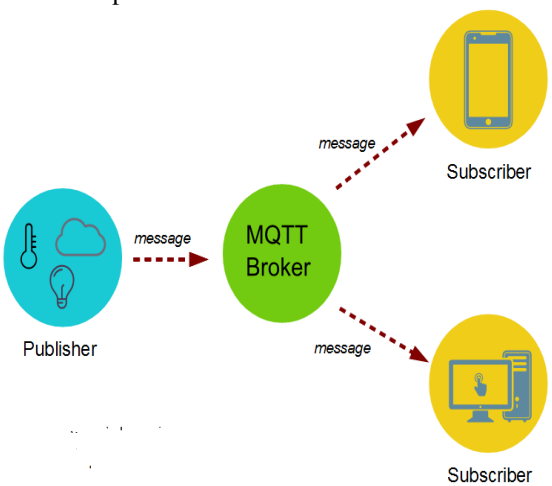

Figure.9. The Message Queuing Telemetry Transport (MQTT) Architecture

AMQP
The Advanced Message Queuing Protocol (AMQP) is another session layer protocol that was developed for the financial industry. It executes over TCP and provides a publish subscribe architecture which is the same as to that of MQTT. The dissimilarity is that the broker is divided into two main components, queues and swapping [47]. The swapping is accountable for receiving publisher messages and distributing them to queues based on pre-determined roles and conditions. The queues basically symbolize the topics and subscribed by subscribers which will get the sensory data whenever they are accessible in the queue. Despite the fact that, AMQP may not be appropriate for sensor devices with limited memory, power or network bandwidth, it's the only protocol, feasible for end-to-end uses for select IoT use cases.

XMPP
Extensible Messaging and Presence Protocol (XMPP) is a messaging protocol that was developed fundamentally for chatting and message exchange applications. Consequently, it is well known and has proven to be highly dexterous over the Internet. A short time ago, it has been reused in IoT applications as well as a protocol for SDN. This reusing of the same standard is due [48] to its use of Extensible Markup Language (XML) which makes it effortlessly extensible. The XMPP endorsements both publish subscribe and request response architecture and it is up to the application developer to select which architecture to use. It is developed for near real-time applications and, thus, efficiently supports low-latency little messages. It does not endue any quality-of-service assurance and, therefore, is not practical for M2M communications. Besides, XML messages create additional overhead due to lots of headers and tag formats which raise the power consumption that is unfavorable for IoT application. Consequently, XMPP is rarely used in IoT, but has obtained some attention to enhancing its architecture in order to support IoT applications.

D. Other Protocols in Internet of Things (IoT)
In this section, we are discussing the other protocols in IoT. .

REST
The RESTful interactions rely on HTTP methods, which mean no client library is needed on the client side. This could be useful for a much uncomplicated device and sensor that only need one-way communication; therefore it means any service that can gain RESTful POSTs can gain data from that sensor. The compromise is that you don't get any of the behavior of a messaging protocol [49]. If the server is unattainable or backlogged, data from the sensor will be missed, while the sensor application handles buffering and retries in the application code.

Sigfox
The Sigfox is known as one of the best substitute technologies which bear the attributes of both Cellular and WiFi. As Sigfox IoT Protocol was proposed and designed for the M2M applications, it can only send data of low-level. By taking the help of UNB or Ultra Narrow Band, Sigfox can grip speeds of 10 to 1000 bits per second for relocating low-data. It only consumes 50 microwatts of the power. The frequency of the IoT connectivity protocols Sigfox is 900MHz, and it has Could-access [50]. In countrified environments, Sigfox IoT protocol covers a range of 28 km to 52 km. In the metropolitan areas, the range of this protocol is 2-10 km.

CoAP
The Constrained Application Protocol (CoAP) is a protocol that specifies how low-power computes-constrained devices can operate on the internet of things (IoT) and a subset of HTTP methods like REST, but adds finite quality of service and works with UDP only, [51] not TCP. It was developed for constrained device connectivity in the early days of IoT emergence. Since MQTT's arrival as a standard, with its equal handling of constrained devices, and much broader feature set beyond that, few people are select CoAP for new efforts. You are likely to select CoAP only if it is the embedded preference for a sensor device, and you must support an application that previously uses it.

EnOcean
The EnOcean takes an innovative turn. It is a wireless sensing and energy harvesting platform. It is ideal for designing devices that need a response in different situation such as alteration in temperature, lighting and other patchy circumstance. Most of the applications of this IoT protocol are currently exercised in transportation, home automation, industrial automation, and logistics. The EnOcean energy harvesting wireless technology [52] can also power radio communication in the worldwide open IEEE 802.15.4 standard. This absolute package enables various wireless applications, which work in the absence of batteries and wires. In set up this extensive platform, EnOcean has handled to keep the integration barriers extremely low. This enables trouble-free integration processes, without the need for in-depth knowledge of battery-less technology.

DDS
The Data Distribution Service was developed to connect devices to other devices with the least overhead. DDS implementations have direct device-to-device data bus. To use DDS, you create a set of subject, with their own data types [53]. Alternatively, relying on a message broker, data publishers and consumers get matched via the data bus based on their types, subject and quality of service parameters. Also, it can run over UDP, TCP, shared memory, and other proprietary networks. Alternatively, relying on the transport layer for faithfulness, it has its own per-stream trustworthiness protocol.

IX. INTERNET OF THINGS (IoT) CHALLENGES

After developing a successful IoT application is still not a trouble-free task due [54] to multiple complications. These complications include maneuverability, [55] trustworthiness, scalability, handle, accessibility, interoperability [56]. In the following, we briefly describe each of these complications.

A. Maneuverability
In this context, IoT devices need to move freely and transformation their IP address and networks based on their location. Thus, the routing protocol, [54] like as RPL, has to reconstruct the DODAG each time a node goes off the network or joins the network which adds a large amount overhead [57]. Besides, mobility might outcome in a transformation of service providers which can add another layer of complexity due to service interruption and alter gateway.

B. Trustworthiness
The system should be completely working and delivering all of its specifications properly. It is a very critical need in applications that requires [58] emergency reaction. In IoT applications, the system should be highly trustworthy and fast in collecting data, communicating them, and making judgment [55]

and eventually the wrong judgment can lead to calamitous scenarios.

C. Scalability

The scalability is another issue of IoT applications where millions and trillions of devices could be linked to the same network. To handle their distribution is not a convenient task. Besides, IoT applications should be tolerant of new services and [59] devices continually joining the network and, consequently, must be designed to enable extensible services and operations.

D. Handle

To handle all these devices and keeping track of the lack of success, configurations, and performance of such huge number of devices is [60] definitely a trouble in IoT. Providers should handle imperfection, configuration, and performance of their interconnected devices.

E. Accessibility

The accessibility of IoT includes software and hardware levels being endowed at any time [54] and anywhere for service subscribers. Software accessibility means that the service is endowing to [4] anyone who is authorized to have it. Hardware accessibility means that the live devices are convenient to access and are favorable with IoT functionality and protocols.

F. Interoperability

The interoperability means that miscellaneous devices and protocols need to be able to interwork with each other. This is challenging due to the [55] huge number of various platforms used in IoT systems. Interoperability should manage by both the application developers and the device manufacturers.

X. CONCLUSION

The Internet of Things (IoT) is still in its infancy as an incidence. IoT has components that range in complexity, from simple recognition tags to complex machine-to-machine communication. The objects are becoming ameliorated with computing and communication powers capable of reproducing and supersede human scanning and senses in the virtual world. The Internet of Things empowering a smarter bridging of digital, physical and human spheres by together these capacities in a safely way to a networked environment. It is not just about the connected devices, but also about the software, hardware, connectivity and communication protocols, middleware and so much more to create an Internet of Things solutions. The Internet of Things (IoT) is also about many processes and technologies such as cloud computing, fog computing, big data, analytics, IoT platform software, and IoT gateways etc. Which are requiring doing something with the IoT. In this paper proposes a novel taxonomy for IoT technologies, highlights some of the most important protocols and standards, an electro-optical infrared sensor in the internet of things, Web of Thing (WoT), and lastly is discussing the IoT challenges. These IoT fields will surely mature and influence human life in unbelievable ways over the next decade.

XI. REFERENCES

[1]. Yusuf Perwej, An Experiential Study of the Big Data," International Transaction of Electrical and Computer Engineers System (ITECES), USA, ISSN (Print): 2373-1273 ISSN (Online): 2373-1281, Vol. 4, No. 1, page 14-25, March 2017 , DOI: 10.12691/iteces-4-1-3

[2]. Gartner, "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020," Gartner, 12 December 2013.

[3]. L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[4]. Yusuf Perwej, M. A. AbouGhaly, B. Kerim and Hani Ali M. Harb. "An Extended Review on Internet of Things (IoT) and its Promising Applications" Communications on Applied Electronics (CAE), ISSN : 2394-4714, Foundation of Computer Science FCS, New York, USA, Volume 9, Number 26, Pages 8– 22, February 2019. DOI: 10.5120/cae2019652812

[5]. Xia Feng et al., "Internet of things", International Journal of Communication Systems, vol. 25, no. 9, pp. 1101, 2012.

[6]. Nikhat Akhtar, Firoj Parwej, Yusuf Perwej, "A Perusal Of Big Data Classification And Hadoop Technology," International Transaction of Electrical and Computer Engineers System (ITECES), USA, ISSN (Print): 2373-1273 ISSN (Online): 2373-1281, Vol. 4, No. 1, page 26-38, May 2017, DOI: 10.12691/iteces-4-1-4

[7]. Yusuf Perwej, Firoj Parwej, Mumdouh M. M. Hassan, Nikhat Akhtar, "The Internet-of-Things (IoT) Security: A Technological Perspective and Review", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN: 2456-3307, Volume 5, Issue 1, Pages 462-482, February 2019. DOI: 10.32 628/CSEIT195193

[8]. L. Atzori, A. Iera, G. Morabito, "The Internet of Things: A survey", Computer networks, vol. 54, no. 15, pp. 2787-2805, 2010.

[9]. Kálmán Képes ; Uwe Breitenbücher ; Frank Leymann ," Integrating IoT Devices Based on Automatically Generated Scale-Out Plans", IEEE 10th Conference on Service-Oriented Computing and Applications (SOCA), Kanazawa, Japan, Nov. 2017

[10]. J. Lin, J. Zhu, Y. Chang, Z. Feng, M. Almasri, "Surface Micromachined MEMS Capacitors with Dual Cavity for Energy Harvesting", Journal of Microelectromechanical Systems, vol. 22, no. 6, pp. 1458-1469, 2013

[11]. C. He, M. E. Kiziroglou, D. C. Yates, E. M. Yeatman, "A MEMS self-powered sensor and RF transmission platform for WSN nodes", IEEE Sensors J., vol. 11, pp. 3437-3445, Dec. 2011.

[12]. F. Herrault, B. C. Yen, C. H. Ji, Z. S. Spakovszky, J. H. Lang, M. G. Allen, "Fabrication and performance of silicon-embedded permanent-magnet microgenerators", J. Microelectromech. Syst., vol. 19, pp. 4-13, 2010.

[13]. S. B. Kim, H. Park, S. H. Kim, H. C. Wikle, J. H. Park, D. J. Kim, "Comparison of MEMS PZT cantilevers based on and modes for vibration energy harvesting", J. Microelectromech. Syst., vol. 22, pp. 26-33, 2013.

[14]. Mohamed El-Sharkawy, Seemein Shayesteh, Maher Rizkalla ," Integrating NEMS/MEMS with IoT applications into an innovative ECE senior elective course", IEEE Frontiers in Education Conference (FIE), Indianapolis, IN, USA, Oct. 2017

[15]. R. Want, B. N. Schilit, S. Jenson, Enabling the Internet of Things, IEEE computer society, pp. 28-35, 2015.

[16]. C. Kachris, T. Ioannis, "A survey on optical interconnects for data centers", IEEE Communications Surveys & Tutorials, pp. 1021-1036, 2012.

[17]. Patrick Gill; Thomas Vogelsang ," Lensless Smart Sensors: Optical and thermal sensing for the Internet of Things , IEEE Symposium on VLSI Circuits (VLSI-Circuits), Honolulu, HI, USA, June 2016

[18]. Erickson Evan et al., "Miniature lensless computational infrared imager", IS&T Electronic Imaging Conference 2016, February 2016.

[19]. S. Arnon, Visible Light Communication, Cambridge University Press, 2015, ISBN 978-1107-4479-81.

[20]. Kaustubh Dhondge ; Kaushik Ayinala ; Baek-Young Choi ; Sejun Song," Infrared Optical Wireless Communication for Smart Door Locks Using Smartphones ", 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN), Hefei, China, Dec. 2016

[21]. V. Bhuvaneswari, R Porkodi, "The Internet of Things (IoT) applications and communication enabling technology standards: An overview", International Conference on Intelligent Computing Applications, pp. 324-329, 2014.

[22]. L. Da Xu, W. He, S. Li, "Internet of things in industries: A survey", IEEE Trans. Ind. Inform., vol. 10, no. 4, pp. 2233-2243, Nov. 2014.

[23]. Augustine Ikpehai ; Bamidele Adebisi ; Khaled M. Rabie ; Kelvin Anoh ; Ruth E. Ande ; Mohammad Hammoudeh, Haris Gacanin, Uche M. Mbanaso," Low-Power Wide Area Network Technologies for Internet-of-Things: A Comparative Review ", IEEE Internet of Things Journal, November 2018

[24]. eith E. Nolan ; Wael Guibene ; Mark Y. Kelly," An evaluation of low power wide area network technologies for the Internet of Things", International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE ,Paphos, Cyprus, Sept. 2016

[25]. Chunxiao Fan ; Zhigang Wen ; Fan Wang ; Yuexin Wu ," A middleware of Internet of Things(IoT) based on Zigbee and RFID", IET International Conference on Communication Technology and Application (ICCTA 2011), Beijing, China, Oct. 2011

[26]. Zhijin Qin; Frank Y. Li; Geoffrey Ye Li ; Julie A. McCann ; Qiang Ni," Low-Power Wide-Area Networks for Sustainable IoT ", IEEE Wireless Communications, January 2019

[27]. Alexandru Lavric, Valentin Popa, "LoRa Wide-Area Networks from an Internet of Things Perspective", ECAI 2017 - International Conference − 9th Edition Electronics Computers and Artificial Intelligence, 2017.

[28]. Ingenu Plans Nationwide Wireless Network for Internet of Things, Xconomy. Retrieved 2015-09-14.

[29]. Thread Stack Fundamentals". Thread Group. 2015. Retrieved 1 April 2017

[30]. Yusuf Perwej , Kashiful Haq, Uruj Jaleel , Sharad Saxena , "Some drastic improvements found in the analysis of routing protocol for the Bluetooth technology using scatternet" International Conference on Computing, Communications and Information Technology Applications (CCITA-2010), Ubiquitous Computing and Communication Journal (UBICC) Seoul, South Korea, ISSN Online 1992-8424, ISSN Print 1994-4608, Volume CCITA-2010, Number 5, pages 86-95, 2010

[31]. M. Lauridsen, B. Vejlgaard, I. Kovacs, H. Nguyen, P. Mogensen, "Interference Measurements in the European 868 MHz ISM Band with Focus on LoRa and SigFox", IEEE WCNC, pp. 3, 2017.

[32]. Ishaq Unwala, Jiang Lu, ""IoT Protocols: Z-Wave and Thread" in International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRSCE), vol. 3, no. 11, pp. 355-359.

[33].Chunling Sun, "Application of RFID technology for logistics on Internet of Things", AASRI Conference on Computational Intelligence and Bioinformatics, vol. 1, pp. 106-111, 2012.

[34].D. Guinard, V. Trifa, E. Wilde, "Architecting a Mashable Open World Wide Web of Things", ETH Zurich Tech. Rep. CS-663, 2010

[35].Dave raggett," The web of things: challenges and opportunities", Computer, Volume: 48, Issue: 5, IEEE, Page(s): 26 – 32, May 2015

[36].R. Porkodi, V. Bhuvaneswari, "The Internet of Things (IoT) applications and communication enabling technology standards: An overview", Intelligent Computing Application (ICICA) 2014 International Conference, pp. 324-329, 2014.

[37].F. Samie, L. Bauer, J. Henkel, "IoT technologies for embedded computing: A survey", Hardware/Software Codesign and System Synthesis (CODES+ ISSS) 2016 International Conference, pp. 1-10, 2016.

[38].C. Goursaud, J. Gorce, Dedicated networks for IoT: PHY /MAC state of the art and challenges. EAI endorsed transactions on Internet of Things, 2015.

[39].Zemede, K. T. Martha, "Explosion of the Internet of Things: What does it mean for wireless devices", Keysight Technologies, 2015.

[40].A. Mishra, C. Na and D. Rosenburgh, "On Scheduling Guaranteed Time Slots for Time Sensitive Transactions in IEEE 802.15.4 Networks," MILCOM 2007 - IEEE Military Communications Conference, Orlando, FL, USA, 2007, pp. 1-7.

[41].Jianping Song, Song Han, Aloysius K. Mok, Deji Chen, Mike Lucas, Mark Nixon, "Wireless hart: Applying wireless technology in real-time industrial process control", Real-Time and Embedded Technology and Applications Symposium 2008, April 2008.

[42].L. Yonge," The HomePlug Powerline Alliance and HomePlug AV Overviews ", IEEE International Symposium on

Power Line Communications and Its Applications,IEEE, Orlando, FL, USA, March 2006

[43]. A. Mayzaud, R. Badonnel, I. Chrisment, "A taxonomy of attacks in RPL-based internet of things", International Journal of Network Security, vol. 18, no. 3, pp. 459-473, 2016.

[44]. Stefano B., Chiara P., Roberto P., Daniele S.," Channel-aware routing for underwater wireless networks", IEEE, Yeosu, South Korea, May 2012

[45]. S. Raza, "Securing communication in 6LoWPAN with compressed IPsec," in Proc. Int. Conf. Distrib. Comput. Sensor Syst. Workshops (DCOSS), Barcelona, Spain, Jun. 2011, pp. 1–8

[46]. JoramMQ a distributed MQTT broker for the internet of things" in white paper, Scalagent, September 2014.

[47]. J. Luzuriaga, M. Perez, P. Boronat, J. C. Cano, C. Calafate, P. Manzoni, "Testing AMQP Protocol on Unstable and Mobile Networks", Internet and Distributed Computing Systems 7th International Conference IDCS 2014 Italy Proceedings Lecture Notes in Computer Science, pp. 250-260.

[48]. M.-K. Liao, Y.-C. Chen, "An XMPP-based XML representation middleware to build universal service-oriented gateway in M2M environment", Proc. IEEE Int. Conf. Internet Things (IThings) Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Soc. Comput. (CPSCom), pp. 193-200, Sep. 2014.

[49]. F. Haupt, M. Fischer, D. Karastoyanova, F. Leymann, K. Vukojevic-Haupt, "Service composition for REST", Enterprise Distributed Object Computing Conference (EDOC) 2014 IEEE 18th International, pp. 110-119.

[50]. M. Lauridsen, B. Vejlgaard, I. Kovacs, H. Nguyen, P. Mogensen, "Interference Measurements in the European 868 MHz ISM Band with Focus on LoRa and SigFox", IEEE WCNC, 3 2017

[51]. Louis Coetzee ; Dawid Oosthuizen ; Buhle Mkhize ," An Analysis of CoAP as Transport in an Internet of Things Environment", IST-Africa Week Conference (IST-Africa), IEEE, Gaborone, Botswana, May 2018

[52]. Joern Ploennigs; Uwe Ryssel Klaus Kabitzsch," Performance analysis of the EnOcean wireless sensor network protocol ", IEEE 15th Conference on Emerging Technologies & Factory Automation (ETFA 2010),IEEE, Bilbao, Spain, Sept. 2010

[53]. H. Jaouani, Conception d'un middleware DDS develop pement d'un modèle de véhicule nouvelle génération et évaluation des performances de l'ensemble sur un réseau FlexRay, December 2015.

[54]. L. Shancang, X. Li, Da, Z. Shanshan, "The Internet of Things: a survey", Information Systems Frontiers, vol. 17, no. 2, pp. 243-259, Apr 2015.

[55]. L. Farhan, A. E. Alissa, S. T. Shukur, M. Alrweg, U. Raza, R. Kharel, "A survey on the challenges and opportunities of the Internet of Things (IoT)", Proc. IEEE 11th International Conference on Sensing Technology, Nov 2017.

[56]. J. Lloret, J. Tomas, A. Canovas, L. Parra, "An integrated IoT architecture for smart metering", IEEE Communications Magazine, vol. 54, no. 12, pp. 50-57, Dec 2016.

[57]. D. Airehrour, J. Gutierrez, S. K. Ray, "A lightweight trust design for IoT routing", Proc IEEE 14th Intl Conf on Dependable Autonomic and Secure Computing, pp. 552-557, Aug 2016.

[58]. M. B. Yassein, S. Aljawarneh, A. Al-Sadi, "Challenges and features of IoT communications in 5G networks", 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), Nov 2017.

[59]. M. Tehrani, M. Uysal, H. Yanikomeroglu, "Device -to-device communication in 5G cellular networks: challenges solutions and future directions", IEEE Communications Magazine, vol. 52, no. 5, pp. 86-92, 2014.

[60]. Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, "Internet of Things (IoT): A Vision Architectural Elements and Future Directions", Future Generation Computer Systems, 2013.

AUTHORS PROFILE

First Author personal profile which contains their education details, their publications, research work, membership, achievements, with photo that will be maximum 200-400 words.

Second Author personal profile which contains their education details, their publications, research work, membership, achievements, with photo that will be maximum 200-400 words.

Third Author personal profile which contains their education details, their publications, research work, membership, achievements, with photo that will be maximum 200-400 words.