Journal of Science and Technology
ISSN: 2456-5660 Volume 7, Issue 09 (Sep -2022)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2022.v07.i09.pp217- 229*

The Internet of Things (IoT): Revolutionizing Connectivity

Ms. FARHEEN SULTANA[1], Mrs. TAHERA ABID[2], Mrs. NAZIA AMREEN[3]
Department of Information technology

Nawab Shah Alam Khan College of Engineering and Technology (NSAKCET)

To Cite this Article
Ms. FARHEEN SULTANA[1], Mrs. TAHERA ABID[2], Mrs. NAZIA AMREEN[3], "The Internet of Things (IoT): Revolutionizing Connectivity", *Journal of Science and Technology, Vol. 07, Issue 09, Sep 2022, pp36-42*

Article Info

Received: 18-06-2022 Revised: 20-07-2022 Accepted: 05-09-2022 Published: 15-09-2022

ABSTRACT

The things we do every day are controlled by information and communications technology (ICT). It's an important part of our life-critical system because it lets different kinds of gadgets talk to each other in many ways. Many things use it, like personal computers, sensors, monitoring, smart houses, entertainment, transportation, and live videos. As an important live thing, the Internet is constantly changing and growing, which makes new technologies, apps, protocols, and algorithms possible. As portable communication trends speed up, new ways to connect to the internet and get high-speed mobile broadband are being created all the time. Communication gadgets that don't need infrastructure become more common, smart, strong, connectable, smaller, cheaper, and easy to set up and use. In the world of ICT, this means a new path forward: the Internet of Things (IoT). The Internet of Things (IoT), which was first called Machine-to-Machine (M2M) interactions, is now a major issue in the ICT and study fields. This essay gives an overall look at the IoT model, including its ideas, rules, and possible advantages. We specifically look at the major IoT devices, new standards, and widely used apps. This summary can help people who are new to the IoT world and want to learn more about it and help it grow.

Keywords: ICT, IOT, M2M, Smart Objects, Heterogeneous Devices.

I. INTRODUCTION

If there was no Internet, how would the world be? It is hard to think of a situation like that that we haven't seen before. The Internet is becoming more and more important for everyone in their personal and business lives these days. Everything we do every day involves smart gadgets like cell phones, monitors, laptops, and many other types of smart items. These and other technologies connected to the Internet of Things have a big impact on new ICT and business systems technologies [1]. In its early stages, it was called the "Internet of Computers." Later, it was called the "Internet of People." And now, thanks to fast progress in ICT, it is called the "Internet of Things." The Internet of Things (IoT) includes many different gadgets and smart items that connect to it and can be individually recognised. It's now possible to connect to "anything" at "any time, any place" instead of just "anyone" [2]. People are paying more attention to technologies that are connected to the internet of things (IoT). This is because IoT is seen as one of the most important ways to promote these technologies and see the future bright. The major goal is to make it possible for the real world and cyberspace to connect and become one [3]. The Internet of Things (IoT) is seen as a key part of the future Internet and will likely allow smart gadgets to communicate and work together in smart ways. things, programs, and services. As it turns out, this is a big change in communication technology that will give everything, from tires to hairbrushes, a unique number so that it can be talked to, linked to other things, and share data. There isn't a clear or agreed upon description of the IoT yet. According to [3], the Internet of Things (IoT) is a network that connects everyday items with unique addresses so that they can access smart services. It is based on standard information providers like the Internet, telecommunication networks, and so on. As the term "Internet of Things" comes from the words "Internet" and "Things," the author of [4] recommended that it be defined as "a worldwide network of interconnected objects uniquely addressable, based on standard communication protocols." IoT's real value, though, lies in its ability to connect a wide range of different devices, such as everyday objects, smart objects, traditional computing networks, and smart sensors that are built into everyday objects. These devices are different in their design, systems, protocols, intelligence, applications, vendors, and sizes. Through management and application systems that live in data centres or network clouds, these groups can talk to each other and work together to gather, create, process, and share data. This makes it easier to work together on complicated jobs and smart processes and to make decisions on your own.

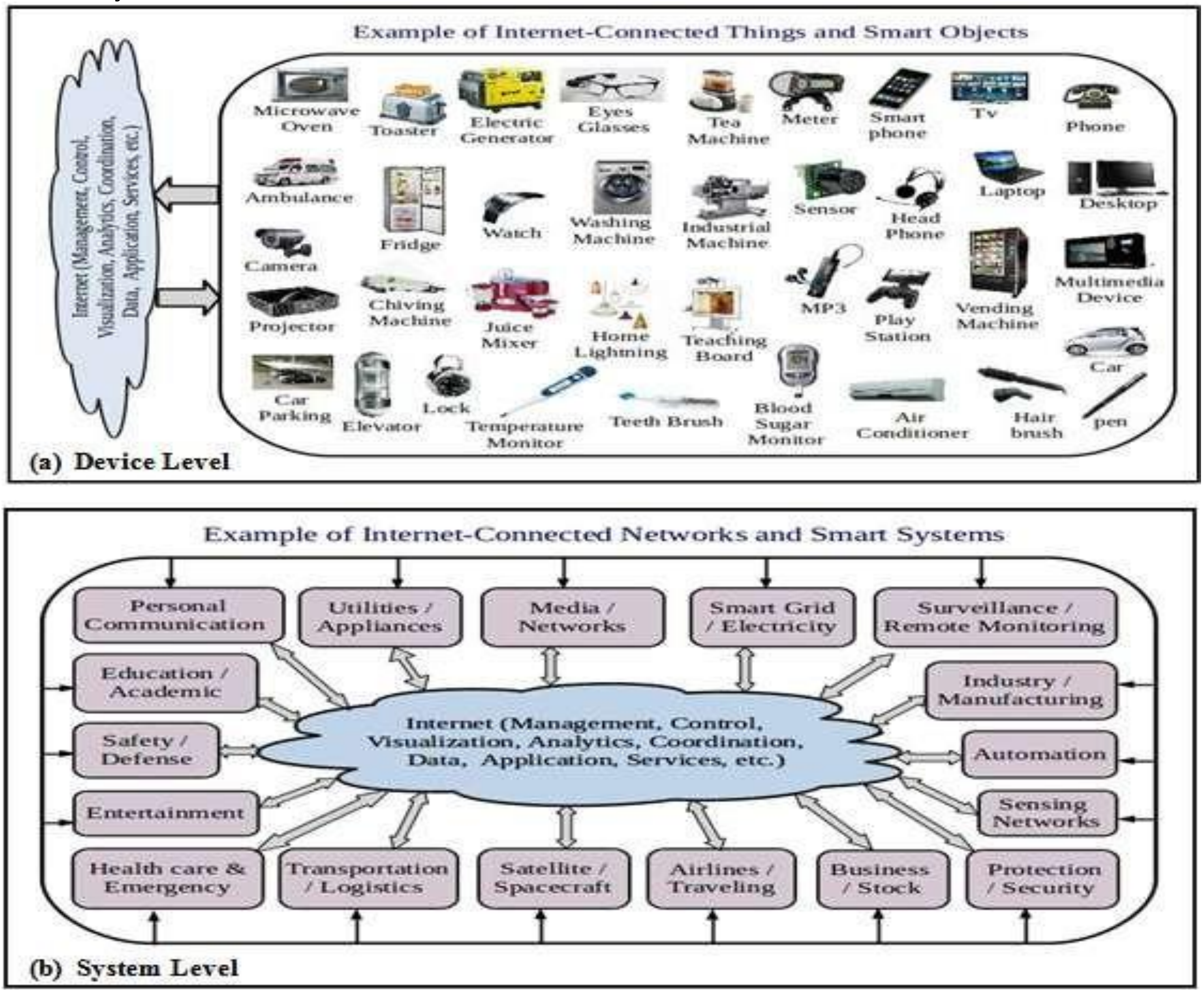

Fig. 1: Internet of Things: Devices and Systems Level Interconnection.

without human interventions. Fig. 1.a and Fig. 1.b depict the offered interconnection of different ubiquitous objects in the IoT in terms of individual devices and connected systems.

This paper provides the reader with a comprehensive view of the key aspects of the IoT and enabling factors in one integrated article; systematically organized and briefly illustrated. The rest of the paper is organized as follows: Section II presents vision and concepts of the IoT, more specifically M2M, key features, and LLNs (Low Power and Lossy Networks). Section III provides a discussion of the IoT elements and major technologies. In Section IV, we give briefs about protocols and standards considered for the IoT. Section V introduces the most relevant applications; while the research directions/future challenges, as discussed in literature, are listed in Section VI. We conclude the paper in Section VII.

II. VISION AND CONCEPTS

In not too distant future, there will be many more things connected to the Internet than people. Things are all around our In some way, surroundings will be connected to the Internet. When the real world and the world of computers and technology are brought together, it opens up new possibilities that aren't possible with current networks. Information will not be shared between people, nor will people be able to view it. People will be represented by machines that talk to other machines [5]. An IoT would include a lot of different communication technologies and goods, like cell phones (from GSM to HSDPA), satellites, Ethernet, WiFi, WiMAX, Bluetooth, ZigBee, and more. These would all have M2M features built in [6]. Adding smart things is the most important part of the IoT strategy. These things are effortlessly linked to the Internet and equipped with smart features like computing, sensing, tracking from afar, and controlling.

A. From M2M to IoT

Machine to Machine "M2M" stands for "machine to machine," which is a broad term for technologies that let mechanical or electronic devices talk to each other and send and receive data and measurements automatically over wireless networks.

A small piece of hardware built into a bigger device, like a sensor, tracking system, car, air conditioner, security camera, or alarm system, is an important part of M2M. This module usually needs to talk to other devices on the network. To be honest, there isn't a lot of difference between this small part and the radio or transmitter circuits that are built into cell phones and smart items. The main difference is that an M2M device doesn't need some of these items' features, like a screen, camera, MP3 drivers, audio codecs, sound control, or a computer [6]. There is no need for any direct help or human involvement in the connection and data sharing process. In many ways, M2M and IoT are the same. People are more likely to use IoT in their daily lives, while M2M is more commonly used in business [7]. When talking about ICT in a wider sense, the two names mean the same thing. In fact, IoT is the new name for the idea of M2M, which uses IP-based networks. During World War II, the idea of M2M was first used to tell neutral from enemy targets so that planes wouldn't hit them. In [6], Juan Conti starts off with an early look at the rise of M2M interactions. He said that many M2M systems were already in place, but they weren't called that. Instead, these systems were given names based on what they did, like "stolen vehicle recovery system," "building automation," "patient monitoring," "automated meter reading," "fleet management," or "automated asset tracking."

M2M technology, on the other hand, has been growing quickly and now touches every part of our lives. Many business and industry fields, including computer, food, agriculture, power, mining, oil and gas, and more, use M2M interactions in a wide range of ways. Some examples are measuring, maintaining machines, keeping things safe, watching and directing them from afar, providing chains, and keeping track of assets. This technology also helps end users in many ways, such as with smart cars, personal tech, and home control. There are three technological factors in [6] that make M2M more important: (i) more and more industrial machines and home appliances have powerful and cheap processing units built in; (ii) the Internet is becoming a standard distribution network; and (iii) the prices of wireless technologies are going down. With today's IP-based networks, the Internet of Things (IoT) can connect a bigger range of different gadgets and smart items, handle and analyse large amounts of data, and keep the connection stable and scalable. Gartner said that by 2015, there would be 4.9 billion things linked to the Internet.

Table 1: IoT Units Installed Base by Category. Source: Gartner Inc [8].

Category	2013	2014	2015	2020
Automotive	96.0	189.6	372.3	3,511.1
Consumer	1,842.1	2,244.5	2,874.9	13,172.5
Generic Business	395.2	479.4	623.9	5,158.6
Vertical Business	698.7	836.5	1,009.4	3,164.4
Grand Total	3,032.0	3,750.0	4,880.6	25,006.6

and will be 25 billion by 2020 [8] (see Table 1). Even though this is extremely large, Cisco says it will be 50 billion [9]; Morgan Stanley says 75 billion [10]. The IoT would support total services spending of $69.5 billion in 2015 and $263 billion by 2020 [8].

B. Key Features and Characteristics

The Internet of Things (IoT) is not the same as standard networks of gadgets that are all the same. Things in the Internet of Things (IoT) are a wide range of integrated devices and smart items that are meant to work together to make communication and processing easier and more possible in most areas. In [11], the writers broke the Internet of Things into three groups: (i) the network that connects different types of smart devices, which is like the traditional Internet; (ii) the technologies that are needed to make this network work (like RFIDs, sensor/actuators, etc.); and (iii) the services and apps that use this vision in different areas. Wireless Sensor Networks (WSN) were first suggested as a way to create environmental intelligence. A lot of smart sensors are used to keep an eye on the surroundings and send a warning signal to a control system whenever something changes. The control system then takes the right action. Different areas can use this kind of system for different reasons, such as health care, home control, security systems, and so on. The Internet of Things (IoT) is the concept that aims to make these kinds of networks work automatically and in real time. There are three key building blocks for the IoT that are described in [11]: a thing should be able to (i) be recognised, (ii) talk to other things, and (iii) connect with other things. In [3], three goals for the IoT are put forward: (i) "more extensive interconnection," which means that there are more devices, different types of devices, and different ways for them to connect; (ii) "more intensive information perception," which means that people work together to combine data from different objects that isn't always accurate or consistent; and (iii) "more comprehensive intelligent service," which means that smart objects offer a wide range of services.

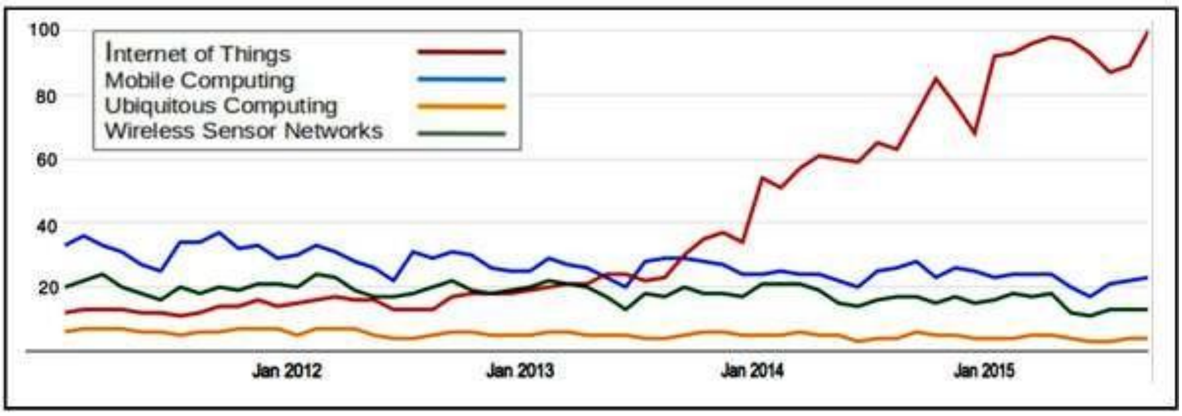

Fig. 2: Research popularity since 2011 of the Internet of Things, Mobile Computing, Ubiquitous Computing, and Wireless Sensor Networks (source: Google search trends [12]).

Journal of Science and Technology
ISSN: 2456-5660 Volume 7, Issue 09 (Sep -2022)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2022.v07.i09.pp217- 229*

.
But the IoT is hard to understand because it's not clear how to reach these goals by growing and changing the regular Internet. Adding some important technologies (Section III) to IP-based networks would make this possible. Development trends show three steps: (i) adding intelligence to things so they can act naturally and on their own; (ii) connecting things to other things; and (iii) letting these things talk to each other and share information [5]. A key part of the IoT is the intelligence built into smart things that doesn't rely on a network or the Internet. This intelligence has already been seen in a number of devices and apps. The air conditioner can keep the temperature where you want it; a sliding door can open, wait, and close; and RFID technology can be used to read information about the food from a distance, just to name a few. Ubiquitous computing, mobile computing, and portable sensing networks are all important parts of the IoT as a whole. Based on Google search data [12], Fig. 2 shows how popular these models and the IoT have been on the web over the last five years. This shows that the IoT is more popular. It's clear that it's grown a lot in the last two years. It's likely to keep going as more people pay attention and better IoT technologies come out, making the future of the Internet look bright.

C. LLNs

As discussed above, billions of things and smart objects are integrated together in a network making up the IoT. The types of these things at most are battery-powered entities, deployed in mesh topology and wirelessly connected. Therefore, these devices typically are embedded with limited power, memory, and processing resources. The IoT network generally is optimized for energy saving and operates under a variety of such working constraints [13], [14]. Such formed networks also referred as so celled Low power and Lossy Networks (LLNs) or IP smart objects networks [13].

LLNs have some characteristics that make them distinguished from other traditional networks and open promised opportunities in the near future research. These features, in some cases, my limit their construction, architecture and communication capabilities; and affect, in general, the main attributes such as power efficiency, link reliability, and maximum achievable throughput [14]–[16]. As most of the network devices are autonomous and battery- powered, the LLNs work with a very small bound “on” state to reduce energy consumption; a majority of nodes are asleep most of time and wake up periodically [14], [17]. Both the network nodes and links are put to the work under predefined constraints. For nodes, the constraints may be on processing power, memory, or energy (battery power); while constraints on links may include high loss rates, low data rates, and instability [14], [16]. LLNs are optimized to minimize the time a packet is en-route; therefore, it is proposed to work with restricted frame-size links. The links are unidirectional and have asymmetric property to support uplink and downlink directions separately with substantially different bandwidth in most cases [16]. Moreover, LLNs support different types of traffic patterns, not only simple unicast point-to- point, but also Multipoint-to-Point (MP2P) and Point- to-Multipoint (P2MP) [14]–[17]. For such characterized networks, to successfully interact with the surrounding world and efficiently utilize these resource-limited devices, a number of IETF working groups and industry alliances have addressed LLNs. Several protocols are developed (see Section IV).

III. ELEMENTS AND MAJOR TECHNOLOGIES

For the IoT to become a fully connected Internet of the future, it needs certain technologies.

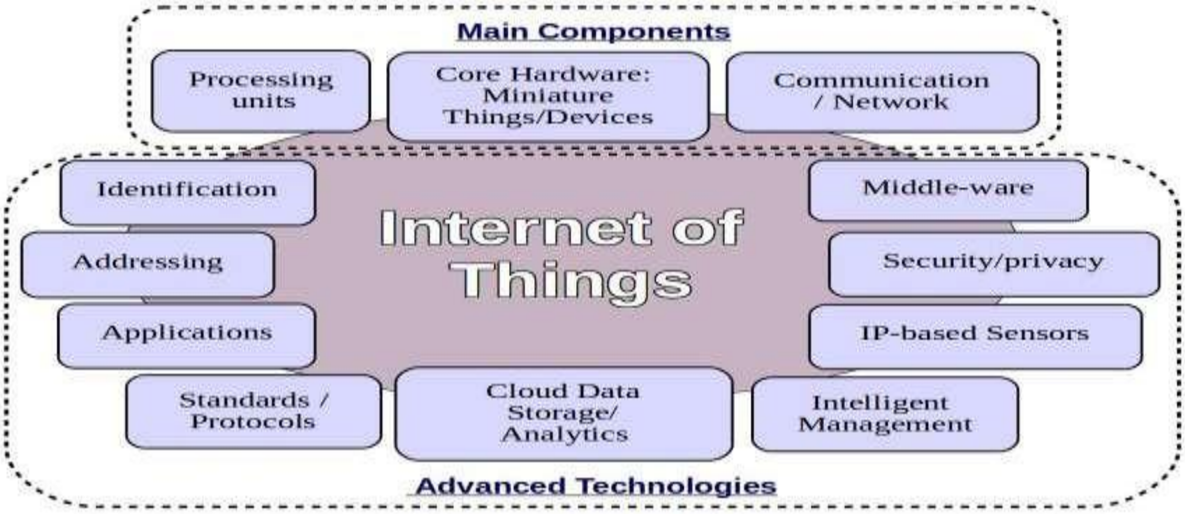

Fig. 3: Key Elements and Technologies for the IoT.

components that are incorporated together to form the IoT world (see Fig. 3). In this section we discuss the key enabling technologies. The aim is to present a brief about each element indicating its role in the IoT paradigm.

A. Identification & Addressing

Because there are so many things spread out in the IoT, recognition, finding, and naming methods are important tools for it. Everything that is connected to an IoT network needs to have a unique identification number. This helps to not only tell the difference between IoT elements based on where they are and what they do, but also to handle these elements instantly and from afar over the Internet [18]. So, different technologies and methods have been used to reach these goals, such as uID [19], URN [20], RFID [21], [22], and IPv6 addressing [23], [24]. RFID stands for radio frequency identification. It is a wireless communication system that is used to identify things from a distance. A tiny electronic chip called an RFID tag is put on the thing (a person, an animal, or anything else) and acts like a barcode to store the thing's unique number and other information in the form of an Electronic Product Code (EPC). An RFID reader that is far away can get the ID and information automatically and without any problems. Radio frequency activation of the tag lets the reader send the right transmission signal. Based on the signal that was sent, the RFID tag sends the ID and/or other information that it has saved. RFID tags come in three different types: passive, active, and semi-passive. The live RFID tags are driven by batteries and have receivers that let them talk to each other. Active RFID tags, which are the majority, usually get their power from the signal sent by the reader. Some tags only have batteries for the microchip and use power from the reader to talk to each other wirelessly.

RFID technology can be used to keep an eye on and track things quickly, even if they are out of sight [25]. This means that it has been used a lot in many IoT applications, including tracking goods, electronic tolls, remote sensing, asset management, making medicines, and medical labs [1, 26]. The Internet of Things (IoT) uses IPv6 instead of IPv4, which couldn't keep up with the fast growth of addressing space needs [23, 24]. It makes sure that the addressing pool has enough space for the expected sharp growth in the future. IPv6 has been used to support flexible addressing methods and safe access to resources both locally and globally. It has also added more complicated features to help people move around the Internet and switch between devices. A light IPv6 is also an important development method that is used to address home gadgets and smart items [18, 27].

B. Embedded Sensors

With the recent advances in the sensing technologies, WSN has been improved more and more, gaining the ability of working in harsh and hazardous environments. WSN typically utilizes a large number of spatially distributed sensors or sensor-embedded devices which can be efficiently cooperate with RFID technology. These elements have different functionalities such as monitoring physical/environmental conditions and tracking the status of things like their locations, temperature, and movements [25]. Optimizations such as the reduction of device size, weight, energy consumption and cost as well as the enhancements in wireless communications have enabled the IoT to employ intelligent sensors as an essential technology in a major part of its networks. Such Intelligent sensors, which use real-time remote sensing, enable the ability to gather, analysis, process, share, and distribute, to centralized systems, a variety of environmental information [18]. As such, they can augment the awareness of a certain environment and, thus, act as a further bridge between physical and digital world [25]. Moreover, RFID sensor networks (RSN) can be built by integrating of sensing and RFID technologies to support the sensing, computing, and communication capabilities in a passive system [25].

C. Protocols & Middleware

In the IoT, billions of devices and smart objects, having different capabilities, require a means for exchanging and transmitting the information collected or generated at the device level. However, the IoT devices are expected to be connected together and able to talk in a way or another. An IoT object must be able to communicate with other devices: identify the proper path to the destination, understand the received messages, and consequently respond with an appropriate manner. Thus, standard protocols become key requirements for the IoT world. This makes it straightforward to achieve the full functionality of such constrained devices while maintaining the desired level of network performance. The mobility in the IoT is one of the major issues. A mobile device frequently moves from one place to another. It requires, in most cases, to be handed-over from the current attachment point to another. The communication protocols must be aware of such nature in the majority of the IoT devices [25]. Intelligent mechanisms are required in order to provide a seamless handover and reduce the delay imposed at different layers. In Section IV, we discuss some of the protocols considered for the IoT devices [25]. Intelligent mechanisms are required in order to provide a seamless handover and reduce the delay imposed at different layers. In Section IV, we discuss some of the protocols considered for the IoT.

The middleware software layer also is an essential in such massive networks having different application systems, different functionalities, and variable data types. Middleware enables the interaction between the „"Internet" and "things". It acts as an interface enabling the various applications on heterogeneous systems to easily and seamlessly communicate with each others. Middleware software layer has a major role in hiding the underlying details. This facilitates developing of new applications and software services for distributed environment independently of the underlying technologies [25].

D. Cloud-based Storage & Analytics

The IoT dense networks result in unprecedented amount of data. This data needs to be intelligently gathered, analyzed, processed, and stored for more efficient and smart monitoring, actuation and real- time decision making [18]. Some of applications in the IoT also require big data storage, large processing rate to realize real-time control, and high speed broadband networks to flow data, audio, or video [26]. However, intelligent algorithms need to be developed for making sense of such big data and efficiently manage the IoT applications requirements. Cloud computing, cloud-based storage, and cloud-based analytics provide an ideal solution paradigms for handling, storing and real time processing such massive data from unpredictable number of devices [18], [26]. The data is collected from different IoT devices into the cloud. Then, it can be aggregated/consolidated with other data from Internet resources, analyzed, and processed using cloud-based services. Thus, provide useful information for the end users. Moreover, it may be used by intelligent systems for better automatic actuation and remote control.

E. Applications

Without applications, the IoT makes no sense. IoT applications provide a real-time message delivery and reliable communications. They introduce all the system functionalities to the end-user through myriad of connected devices. The physical connectivity is achieved by networks and devices, whereas the robust interactions of device-to-device and human-to- device are provided by the IoT applications [26]. In the human-device applications, visualization is considered as one of the key features that allows user to easily interact with the environment and efficiently present and understand the collected information [18], [26]. In device-to-device applications, intelligence is usually implemented for enabling dynamic interactions. This allows devices to automatically monitor the environment, identify the problems, collaborate, and independently make the proper decisions without human intervention [26]. In Section V, we discuss more about the IoT applications.

F. Core Hardware

In addition to what are mentioned above, IoT devices/smart objects, whatever they are (consumer electronics devices, home appliances, intelligent cars, wireless sensors, or industrial machineries), typically consist of main entity components (IoT core hardware). This includes memory, processing units, power supply, transceiver capabilities, etc. Here, the things almost comprise a variety of communication technologies and terminals integrated to support M2M connectivity between various objects and making them more versatile. Moreover, they

Journal of Science and Technology
ISSN: 2456-5660 Volume 7, Issue 09 (Sep -2022)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2022.v07.i09.pp217- 229*

usually contain several A/D for sensor interfacing with the main intelligent system [18]. However, these things, integrated with other technologies, are able to capture

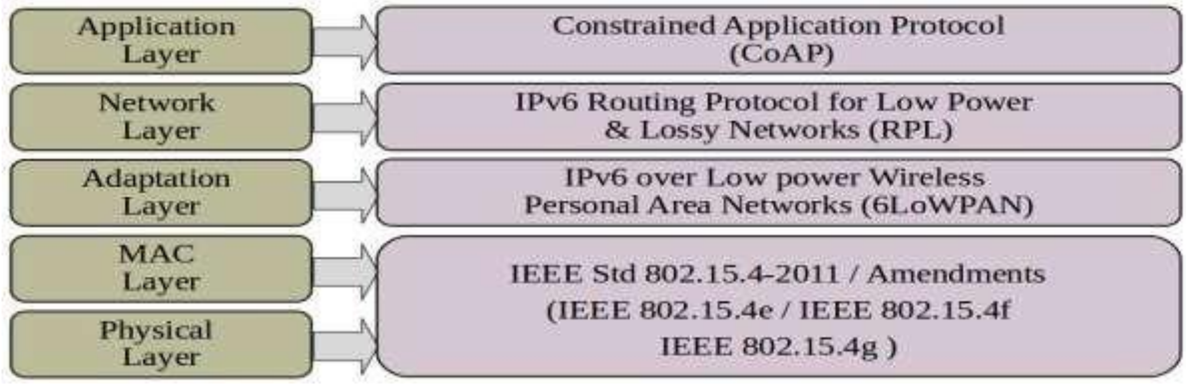

Fig. 4: Emerging Protocols for the IoT.

an internal change or environmental event and pass to the applications which are able to interpret this event into meaningful information. This information then can be used to automatically control the situation in self-managed autonomous systems, shared with the other objects in proximity to make some decisions of their own, or sent through communication hardware to the intelligent system in cloud.

IV. PROTOCOLS

The IoT typically is a very large scale network consisting of heterogeneous constrained devices and smart objects. Such constrained network imposes a significant impact on designing of different protocols. However, taking this into account, generally, enables for designing a broad set of standards and protocols. These protocols are supposed to offer efficient and scalable communications and allow developing and deploying applications/services adopted for a variety of environments. In the next subsections, we discuss some developed protocols that are considered for the IoT/LLNs as shown in Fig. 4.

A. IEEE 802.15.4

The IEEE 802.15.4 is a standard designed by IEEE 802.15 working group in IETF which defines the physical (PHY) and media access control (MAC) layers for low data rate, low-power, and short-range wireless personal area network (LR-WPANs) [17], [29]. The original version is provided in 2003 supporting data rates of 20, 40, and 250 kb/s with a 10-meter communications range of ubiquitous communication between devices. Afterward, EEE 802.15.4a/c/d are provided as improvements expanding the PHY layer with several additional frequency bands and transmission techniques. IEEE Std 802.15.4-2011, a revision for the previous amendments, is provided to roll them in a single standard supporting a maximum data rate of 850 kb/s with a focus on the interoperability technical requirements [29]. Later, a number of amendments are introduced such as IEEE 802.15.4e, IEEE 802.15.4f, and IEEE 802.15.4g [30]–[32]. The IEEE 802.15.4e [30] is released in order to improve and add functionality to the MAC sub-layer. A channel hopping strategy is adopted to enhance the support for industrial markets, and improve the robustness to overcome the multi-path fading and external interference. In IEEE 802.15.4f [31], the PHY is improved to support flexibility and better performance in the high dense deployments of autonomous devices, and active RFID systems wherever in the world. This amendment supports a wide range of applications that characterized with several constraints such as low cost, low power consumption, multiyear battery life, reliable communications, precision location, and reader options [17], [31]. The IEEE 802.15.4g supports out- door low data rate, wireless, smart-grid networks requirement and offers a higher transmission range equal to 1km and a large packet size of 2047 byte [17], [32].

The IEEE 802.15.4 provides real-time appropriateness with provision of guaranteed time slots, secure communications, transfer reliability, CSMA/CA, link quality indication (LQI) and energy detection. Moreover, it offers a technological simplicity and very low manufacturing and operation costs [29]. The IEEE 802.15.4 is the foundation for several protocol stacks such as ZigBee, WirelessHART, MiWi, and RPL and 6LoWPAN [17].

B. 6LoWPAN

The IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) is a standard for adaptation layer allowing IPv6 packets to be sent and received over IEEE 802.15.4 based links [33]. It realizes the idea of applying Internet protocol to the small autonomous devices, as the only available solution for smart object networks or

Journal of Science and Technology
ISSN: 2456-5660 Volume 7, Issue 09 (Sep -2022)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2022.v07.i09.pp217- 229*

LLNs. Thus, enabling such constrained devices to be connected in a very large number, to the Internet [17], [33], [34]. Moreover, 6LoWPAN supports mobility where the devices, at most, are deployed in an ad-hoc fashion without predefined locations and move continuously. For mapping from IPv6 network to that of IEEE 802.15.4, 6LoWPAN performs three key functions:

(i) IPv6 header compression, (ii) IPv6 packet fragmentation, and (iii) layer-2 forwarding [17].Foreach,aseparate6LoWPANheader is included when necessary. In the first, the IPv6 header is compressed down where the fields that can be obtained from the context are omitted and the remaining are send unmodified. In the second, the packets larger than IEEE 802.15.4 MTU are fragmented at the sender and re-assemble at the destination. In the third function, which is called mesh-under and suitable for small & local networks, the IP routing is not performed. The packets are forwarded to the destination over multiple radio hops by adaptation layer. This routing is made at link layer level depending of 6LoWPAN header and IEEE 802.15.4 frame [17], [34].

C. RPL

The IPv6 Routing Protocol for LLNs (RPL) is a network layer protocol designed for low power and lossy networks [14], [35]. RPL has been developed with the objective of meeting application-specific requirements for LLNs (Section II-C) identified by ROLL (Routing Over LLNs) working group in IETF. These requirements are define for, but not limited to, a set of application areas: industrial, building automation, home automation, and urban sensor networks. As per the evaluation, ROLL have found that the existing protocols such as OSPF, IS-IS, AODV, and OLSR do not satisfy all the specified requirements. These protocols which use only static link metrics, do not take devices statues such as processing resources, memory, residual energy or hardware failures into account when creating best/shortest path [14], [17].

The RPL is an extensible proactive IPv6 distance vector protocol which supports for mesh routing environments, shortest-path constraint-based routing (on both links and nodes) and different traffic patterns including MP2P, P2MP and P2P. It considers routing optimization objectives independently of packet processing & forwarding and can be run over various different link layers. That includes constrained link layers or those utilized in conjunction with highly constrained devices such as, but not limited to, low power WPAN (802.15.4) or PLC (Power Line Communication) technologies [35]. In addition, the RPL includes measures for power conservation such as adapting the sending rate of control messages and updating the topology only when data packets have to be sent [16]. On a network, more than one instance of RPL can be run simultaneously. Each such instance may consider a set of different and potentially antagonistic constraints or optimization objectives [35]. The RPL builds a loop free Destination Oriented Directed Acyclic Graph (DODAG) based on such criteria. Objective Function (OF) defines such constraints and objectives and identify how to use them for building such graph (DODAG & OF are out of scope here. For more about the RPL, see [14], [16], [17], [35]).

D. CoAP

The Constrained Application Protocol (CoAP) is a web based application layer protocol designed by the Constrained RESTful Environments (CoRE) working group in IETF [36]. It offers interactive M2M communications for autonomous devices and smart objects through the standard Internet. It is intended to be used in the low power and constrained networks such as LLNs/IoT and 6LoWPAN that require remote monitoring & manipulating. CoAP is a lightweight version of HTTP that supports simplicity, low message overhead, reduced parsing complexity, and limited need for packet fragmentation in such constrained environments and devices. Moreover, it is a platform that provides a request/response interaction model between applications and easily facilitates the integration of the embedded networks with existing web [36], [37]. Plus, it has more features for M2M such as built-in discovery, proxy-mode support, multicast support, reliable delivery, and asynchronous message exchanges [17], [36]. The packets in the CoAP are much smaller, simpler to generate and easier to parse with less memory used. CoAP is datagram based which runs over UDP, not TCP. However, it may be used on top of SMS and other packet based communication protocols [38].

V. APPLICATIONS

Advancements in the IoT motivate for adoption more and more applications of such innovative technology. IoT applications have increasingly overspread industries and public/private sector organizations saving our time, resources and efforts. Applications of the IoT have been categorized in literature based on different classification criteria and factors putting them into several distinguished domains such as presented in [2], [11], [18], [39], [40] and [28]. In [28], three major domains of IoT applications are identified: industry, environment, and society (see Table 2). These fields are cohesively linked and interrelated with each others and can not be isolated. Within each broad domain, more and more applications can be further identified. The base requirements of these applications in such domains are often the same with a marginal difference depending on the main functionality of the application. In this section we briefly investigate some of the common and widely used applications of the IoT.

Monitoring and controlling systems are common applications of the IoT. Data about environment or networked objects is collected (sensed or calculated), sent to an intelligent system (centralized or

Table 2: IoT Application Domains - Description and Examples. (Source: CERP-IOT [28]).

Domain	Description	Indicative examples
Industry	Activities involving financial or commercial transactions between companies, organizations and other entities	Manufacturing, logistics, service sector, banking, financial governmental authorities, intermediaries, etc.
Environment	Activities regarding the protection, monitoring and development of all natural resources	Agriculture & breeding, recycling, Environmental management services, energy management, etc.
Society	Activities/initiatives regarding the development and inclusion of societies, cities, and people	Governmental services towards citizens and other society structures (eparticipation), einclusion (e.g. aging, disabled people), etc

Journal of Science and Technology
ISSN: 2456-5660 Volume 7, Issue 09 (Sep -2022)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2022.v07.i09.pp217- 229*

distributed), and then the right choice is made. In this way, the working behaviour can be tracked all the time, running settings can be changed, and the system's performance can be adjusted immediately. WSN was one of the first technologies to be used in these kinds of situations, and it has since become an important part of security and temperature control systems. These days, IP-based WSN is seen as a part of IoT networks that makes environmental tracking apps more flexible, interactive, and dynamic [18]. This includes tracking things like wind, storms, rain, weather, pollution, river height, and more, as well as keeping track of moving items in real time, anywhere and at any time [26]. IoT-based WSN technologies are also being used more and more for security and surveillance in places like homes, markets, shops, businesses, and more.
A digital system that works with everything else is used in a smart city. Intelligent automation manages the key services in a way that makes them more efficient and cuts down on running costs. For instance, a smart meter is used in the smart grid to keep an eye on all the energy points in a city. By collecting data, this kind of system can help make better use of energy and keep the load balanced and the quality of service high [18]. Also, the smart traffic system offers improved traffic control that keeps an eye on both roads and traffic in big towns. This method helps drivers by giving them options for different routes to take to avoid traffic jams [11]. Everything in a smart home or building is handled instantly by a smart management system. This includes the washing machine, oven, fridge, air conditioner, ventilation, hating, sliding door and more. For example, a computer might get information about the surroundings of a building and tell devices what to do, or the devices themselves might be smart enough to do this. These kinds of systems make living spaces more unified by making it easier to schedule jobs, get reminders, keep things safe, and handle resources in a way that saves energy. IoT technology also helps health care systems run more smoothly by making care services more efficient. Body Area Network (BAN) is a type of data analytics that constantly checks on a patient's health and behaviour. For example, [40] imagines networked nanosensors that are inside the body. These nonosensors work with on-body monitors, which are worn or put on a person's body, to measure different bodily factors. These data are sent to the central computers or tracking system through a number of IP-based connections. The experts and doctors can get to this information and use it to make quick, effective interventions and treatments [18].

Artificially intelligent systems are used in business to find and fix problems so that the right action can be taken and customers are happy [26]. In the supply chain and distribution operations, for example, RFID technology is often used to track things and goods that go bad quickly. Using the data gathered, the buyer or seller from afar can constantly keep an eye on the goods' state and movement, such as where they are, how many are there, what the weather is like, and when they should be available in the market [11]. This means that customers can automatically get this information. Smart plants have become popular in making because they help make the process better. The intelligence is built into the machines and tools in these kinds of systems. This gave them the self-management skills they needed to improve their work. These parts are also linked together by a strong system for directing and coordinating them. Because people aren't involved as much, there are a lot of important benefits, like faster production and delivery times, lower costs, better quality, and safer workplaces [1, 28].

Information sharing and trade, business teamwork, smart banking, crowd tracking, infrastructure monitoring, smart transportation, water measurement, and many other things

are just examples of the IoT applications. Extremely increase in the smart applications is expected to invade our life in the near future.

DISCUSSION

The Internet of Things (IoT) is a new technology that is growing quickly. It opens up new ways to invest in and improve ICT. But new issues and problems show up that need more study and care. A lot of new research, polls, and studies talk about these issues that people who make IoT devices have to deal with. The Internet of Things (IoT) is still in its early stages and has problems with things like data management, privacy and security, scale, big data and analytics, clock synchronisation, energy management, protocols, visuals, and quality of service (QoS) [1, 11, 18, 26, 41, 44]. Two new areas that have been talked about are social IoT and nano-IoT [40, 45]. People need to work together more and talk about these kinds of issues more often. We want to stress how important it is to pay close attention to these two things: one of the main goals of making IoT devices is to save energy. The amount of power used goes up very quickly as the number of related things goes up. To make green IoT systems, we need to find ways to use less power [1, 11, 41]. ii) synchronising clocks, which is a key part of getting global systems to work together. To make sure that data is always the same, people can work together better, and tasks can be planned, time synchronisation needs to be fluid [11, 42]. With dynamic timed alignment, an IoT device can also set a time to go to sleep, which saves even more energy [40]. In order for these tech problems to not be as bad, we hope that more people will join. Building an Internet of Things (IoT) world that makes sense and is constant so that things, also called "smart objects," can live, talk to each other, and change so they can be connected and work anywhere.

CONCLUSION

The Internet of Things (IoT) is a cyber-physical system that connects billions of different gadgets and smart items. Technologies like recognition, integrated devices, clever management, protocols, data storage, processing, and analytics, and more make these things possible. In the last few years, a lot of different IoT apps have been used. This essay gives an overall look at the Internet of Things, going over its goals, ideas, features, and exciting future. It gives short talks on the main IoT technologies, the newest standards, and the most popular uses of the technology. For more work to be done soon, the study paths and future tasks are written down. We stress how important power economy and time synchronisation are as future trends that we think need a lot more attention and research. This paper's main addition is that it presents the main ideas about the Internet of Things (IoT) and why it's important in a clear and concise way.

REFERENCES

It was written by L. D. Xu et al. and can be found in IEEE Transactions on Industrial Informatics, vol. 10, no. 4, November 2014.
The Internet of Things: A Look Into the Future by L. Coetzee and J. Eksteen is part of the 2011 Proceedings of the IST-Africa Conference.
[3] H.-D. Ma, "Internet of Things: Goals and Scientific Challenges," Computer Science and Technology, Springer, vol. 26, no. 6, November 2011.

A workshop report from the European Commission in May 2009 by M. Botterman is called "Internet of Things: an Early Reality of the Future Internet."

A paper by L. Tan and N. Wang called “Future internet: The internet of things” was published in 2010 at the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE).

6. J. Conti, "The Internet of Things," Communications Engineer, IEEE, vol. 4, no. 6, Dec. 2006.

"M2M/IoT software and services" from EuroTech Inc. can be found at http://www.eurotech.com/en/products/software+services as of September 2010.

[8] Gartner Inc., "In 2015, 4.9 billion connected things will be used," Nov. 17, 2014, at http://www.gartner.com/newsroom/id/29057 17.

[9] N. Earle, "50 billion things are coming to a cloud near you," Cisco, go to http:

50 billion things are coming to a cloud near you, Cisco Blog, June 2015.

10. T. Danova, "Morgan Stanley: By 2020, 75 billion things will be linked to the internet of things," The story can be found at http://www.businessinsider.in/articleshow/ 23426604.cms in October 2013.

It was written by D. Miorandi et al. and was published in Ad Hoc Networks (Elsevier), vol. 10, no. 7, September 2012.

Google Trends, Google (n.d.), http://www.google.com/trends.

[13] J. Hui and J. Vasseur, "Routing architecture in low-power and lossy networks (LLNs)",

draft-routing-architecture-iot-00," https://tools .ietf .org / html/draft-routing- architecture-iot-00, RFC draft, Mar 2011.

[1] IETF ROLL WG., "Routing over low power and lossy networks(ROLL)," https://datatracker.ietf.org/wg/roll/charter/, Apr 2015.

[2] J. Vasseur et al., "RPL: The IP routing protocol designed for low power and lossy networks," IPSO Alliance, Apr 2010.

[3] T. Tsvetkov and A. Klein, "RPL: IPv6 routing protocol for low power and lossy networks," July 2011, http://www.net.in. tum.de/fileadmin /TUM/NET/NET-2011-07- 1/NET-2011-07-1 09.pdf.

[4] J. Apcar, "The internet of things: Routing and related protocols," Cisco Live, https://www.ciscolive.com/online/connect/se ssionDetail. ww?SESSION ID=77716&back Btn=true, 2014.

[5] J. Gubbi et al., "Internet of things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, Elsevier, vol. 29, no. 7, Sept 2013.

[6] K. Sakamura, "Challenges in the age of ubiquitous computing: A case study of t- engine, an open development platform for embedded systems," in Proceedings of the 28th International Conference on Software Engineering, 2006.

[7] L. Daigle et al., "Uniform resource names (URN) namespace definition mechanisms," https://tools.ietf.org/html/rfc3406, RFC 3406, Oct 2002.

[8] E. Welbourne et al., "Building the internet of things using RFID: The RFID ecosystem experience," Internet Computing, IEEE, vol. 13, no. 3, May 2009.

[9] C. Roberts, "Radio frequency identification (RFID)," Computers & Security, Elsevier, vol. 25, no. 1, Feb 2006.

[10] A. J. Jara et al., "The internet of everything through IPv6: An analysis of challenges, solutions and opportunities," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), vol. 4, no. 3, Sept 2013.

[11] S. Deering and R. Hinden, "Internet protocol, version 6 (IPv6) specification," https://www.ietf.org/rfc/rfc2460.txt, RFC 2460, Mar 1998.

[12] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer Networks, Elsevier, vol. 54, no. 15, 2010.

[13] I. Lee and K. Lee, "The internet of things (IoT): Applications, investments, and challenges for enterprises," Business Horizons, Elsevier, vol. 58, no. 4, Ju