IOT COMMUNICATION TECHNOLOGIES

Abstract

Internet of Things (IoT) communication is the process of exchange of data between two or more smart devices wired or wirelessly over the internet to perform certain tasks with or without human involvement. Presently the popularity and demand for IoT is ever increasing due to its widespread applications from simple home automation to interconnections of smart cities, autonomous vehicles, wearable devices etc. In the near future, IoT is expected to dominate the networking and technological service interconnections between the millions of smart devices/systems that will be available by then. In this chapter, current state, various types, application scenarios, challenges and future trends of IoT communication technologies are briefly described.

Keywords: Internet of Things; smart devices; communication technologies; smart cities

Author

Sreenivasappa B V
Department of ECE
Presidency University
Bangalore, India
sreenivasappabv@presidencyuniversity.in

I. INTRODUCTION

The Internet of Things (IoT) is the networking of physical objects with electronics integrated into its architecture to allow communication and the detection of interactions between the devices, networks, sensors, home appliances, automobiles, or the environment. IoT essentially offers a framework for things to communicate and work together. In 1970, the idea of networked gadgets was initially proposed. In 1990, John Romkey created a toaster that could be operated remotely through the Internet. In 1995, Siemens revealed the initial cellular module created for M2M. While working at P&G in 1999, Kevin Ashton coined the concept "Internet of Things," which immediately gained traction. Important journals like the Boston Globe, Scientific American, and the Guardian all used the word in 2004. The International Telecommunications Union (ITU) of the UN released its initial study on this subject in 2005. The Internet of Things made its debut in 2008. The market research firm Gartner began looking into "The Internet of Things" technologies in 2011. IoT-based technology will provide a wider range of services in the upcoming years, fundamentally altering how people go about their daily lives. A few applications of IoT include advances in healthcare, energy, gene therapies, agriculture, smart cities, and smart homes. IoT makes it possible for commonplace devices like toasters and relatively straightforward technology like computers, cellphones, and tablets to connect to the internet. By enhancing parts of our lives through the use of data collecting, AI algorithms, and networks, IoT makes practically everything “smart.” An animal with tracking devices or a person with a diabetes monitor implant might all be things in an IoT system. The gadgets themselves, such as smartphones, smartwatches, and electrical appliances like TVs and washing machines that allow you interface with the IoT platform, are where the entire IoT process begins. For the development of IoT systems, the following are essential elements: (1) Device (2) Sensor (3) Gateway (4) Connectivity (5) Cloud (6) Analytics (7) User interface (8) Integration (9) Artificial Intelligence, etc.

The set of guidelines used to convey data between smart devices is known as the communication technologies or protocols utilised in Internet of Things applications. The following features/requirements should be present in the communication technologies that allow communication between smart devices and networks: Low bandwidth requirements, symmetric networking architectures to provide seamless communication, low power consumption during data transmission and reception, and high data rates reduced computational complexity, which reduces computing power and delays during transmission and receiving. IoT connectivity systems and protocols are currently divided into two categories (wired and wireless). The type of network that is selected is based on the network range, bandwidth, power consumption, intermittent connectivity, and security. Even though the IoT system mostly uses wireless communication technologies, wired communication technologies can occasionally be more convenient and effective. In some cases, IoT system utilizes the combination of these two technologies.

1. **Wired communication technologies:** In wired Communication, the transfer of data from the transmitter to the receiver and vice-versa is through a wired medium such as metal wires, fiber optic cables etc.

   This is of two types (i) Internal system protocol technologies: The devices in the same circuit/sub-system communicate with one another using these protocols. Examples:

I2C, SPI (ii) External system protocol technologies: These protocols are used to establish communication between two circuits / sub-systems. Example: USB, UART/USART, RS-232, RS-485, Ethernet. In addition to the above, data protocols are used at the application layer, they are Advanced Message Queuing Protocol (AMQP), Extensible Messaging and Presence Protocol (XMPP), Message Queuing Telemetry Transport (MQQT), Constrained Application Protocol (CoAP), Data Distribution Service (DDS) and Light Weight Machine to Machine (LWM2M) [12].

2. **Wireless communication technologies:** In wireless Communication, the transfer of data from the transmitter to the receiver and vice-versa is through electromagnetic waves that travel through free space.

   There are many wireless communication technologies such as Low Power Wide Area Networks (LPWANs)-Sigfox and Random phase multiple access (RPMA), Bluetooth and Bluetooth Low Energy (BLE), Zig-Bee, Z-Wave, Wi-Fi, Radio Frequencies Identification (RF-ID), Cellular (1G/2G/3G/4G/5G/6G), Near Field Communication (NFC), Long-Range Radio-Wide Area Network (LoRaWAN) and Light Fidelity (Li-Fi). The data routing, data management, event identification, event handling, remote management and interoperability are just to name a few of the functionality and features that these IoT communication protocols are intended to make possible for various IoT networks and implementations.

   Any combination of device-to-device, device-to-gateway-to-cloud, device-to-data center/cloud, device-to-cloud, or device-to-remote infrastructure communication is possible with each IoT protocol. There is no one IoT communication protocol that is optimum or appropriate for all deployments. Which IoT protocol is best for an IoT deployment relies on elements including geographic and special location, data rate, bandwidth, power consumption needs, battery-operated choices, the presence of physical barriers, and cost [1]-[5], [14].

II. COMPONENTS OF IOT COMMUNICATION TECHNOLOGIES

1. **Node:** It is a point of connection, or a center of distribution, or a terminus of communication is network and protocol dependent. A node is a network connected active electrical device that has the ability to create, information transmission or reception over a communications channel.

2. **Device:** It is a hardware component having technical capability for collaboration with other information technology systems. A device can have a gadget attached to it, or embedded inside a physical system, or monitor nearby electronic objects within its boundary.

3. **Address of device:** A device resource or service can be found and reached using an identity or address or location. Though identity and the address may occasionally match, but they may vary conceptually.

4. **Gateway:** A data center's highly scalable computer storage and memory capabilities allow for the quick and flexible scaling up and down of application resources. Public, private, or hybrid clouds are available for use.

5. **Connectivity:** It is a generic term for attaching devices to one another, so that data can be sent and received. As well as backbone networks, it frequently refers to network connections, which include bridges, routers, switches, and gateways. In addition, it could include attaching a digital camera to a computer or printer or linking a house or place of business to the internet. Today's world uses a wide variety of techniques. In the literature many examples can be found for the emerging technologies such as 4G, LTE, BTLE, GSM, NFC, WiFi, Zigbee and LiFi etc.

6. **Network:** Several linked computers, servers, mainframes, network devices, peripherals, or other data-sharing devices make up a network. One type of network is the one that connects millions of people globally through the Internet. On the right, a picture of a home network with many connected computers and other network devices can be seen.

7. **Cloud:** A data center that has highly scalable computer storage and memory capabilities needed for the quick and flexible scaling up and scaling down of application resources. Public, private, or hybrid clouds are available for use.

8. **Sensors:** A device used to determine specific chemical or physical qualities and change them into an electrical signal to create them digitally capable of being processed. Sensor is considered as node in the IoT system, which aids in bridging the gap between both digital and tactile.

9. **User interface:** The user interface is made up of the elements that let a user interact with a computer system. This encompasses everything from screens to pages to buttons to icons to forms. The most obvious examples of user interfaces are the programmes and applications on computers and cellphones.

10. **Data processing:** The process of gathering and transformation of data into something usable is known as data processing.

11. **Analytics:** In order to make sense of the enormous volumes of data generated by connected Internet of Things devices, analytics is the application of tools and methods for data analysis. The promise of IoT analytics in relation to industrial IoT is widely emphasized.

12. **Artificial intelligence:** The IoT infrastructure is being integrated with artificial intelligence technologies to better data management, analytics, human-machine interfaces, and IoT operations.

III. DESCRIPTION OF IoT COMMUNICATION TECHNOLOGIES

Despite the wide variety of IoT communication technologies, only the most essential ones are briefly described in this section.

1. **Low Power Wide Area Network (LPWAN):** A wireless wide area network protocol called LPWAN connects low-bandwidth, battery-operated devices over long distances at low bit rates. It is intended to function more cheaply and efficiently than conventional mobile networks. Additionally, they can accommodate more linked devices over a bigger region LPWANs support uplink rates of up to 200 Kbps and packet sizes ranging from 10 to 1,000 bytes. Depending on the technology, the long range of an LPWAN ranges from 2 km to 1,000 km. The majority of LPWANs feature a star topology, in which every endpoint is directly connected to a few central access points.

   The term LPWAN refers to a collection of numerous low-power, wide area network technologies that come in a variety of formats. LPWANs have options for proprietary or open standards as well as licenced or unlicensed frequencies.

   One of the most frequently used LPWANs at the moment is the proprietary, unlicensed Sigfox. Only one operator is permitted per nation using the ultra-narrowband technology, which operates via a public network in the 868 MHz or 902 MHz frequencies. Its packet size is restricted to 150 messages of 12 bytes each day, and it can only send messages over distances of 30 to 50 km in rural areas, 3 to 10 km in urban areas, and up to 1,000 km in line-of-site applications. Downlink packets are smaller and are restricted to four 8-byte messages per day. It can also be susceptible to interference when sending data back to endpoints. Ingenu Inc.'s Random Phase Multiple Access, or RPMA, is a proprietary LPWAN. In spite of having a shorter range than Sigfox (up to 50 km line of sight and 5–10 km nonline of sight), it provides more effective bidirectional communication. Though it is susceptible to interference from Wi-Fi, Bluetooth, and physical structures because it operates in the 2.4 GHz frequency. Additionally, it often consumes more power than other LPWAN solutions [6]-[7].

2. **LPWAN network architecture:** The fundamental LPWAN design necessitates wireless communication to the cloud and Internet. A particular group of architectural elements may be necessary for typical LPWAN technology, as depicted in Figure 1.

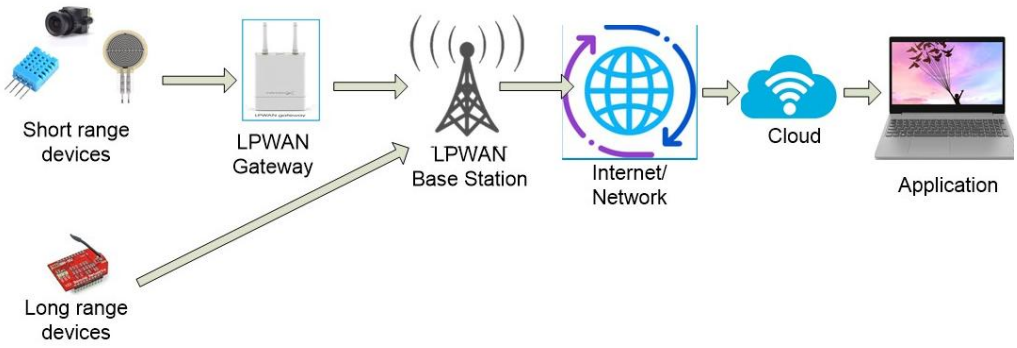

Figure 1: LPWAN network architecture

The main duties of an LPWAN device are to collect data and respond to LPWAN inputs. Over a predetermined radio channel, the wireless access point and the IoT network receive the gathered data. The access station provides the radio link for managing devices and exchanging device traffic. By addressing acceptable bit error rates, admissions, security, and other issues, it preserves the integrity of the radio link. The

gateway/concentrator—sometimes referred to as a core—interfaces with the access station. Depending on whether proprietary or standards-based LPWAN technology is being explored, there are many implementations. Control and user plane traffic management falls under the purview of the core. It functions as a channel of communication between the access station and the IoT network and permits protocol translation between access station-supported protocols and network-supported protocols. A concentrator may offer edge processing and storage facilities to offload the cloud, depending on the technology. Due to its close proximity to the end devices, this is particularly appropriate in circumstances when the device needs real-time support with little latency.

For some LPWAN systems, the core may provide robust admittance, priority treatment, and, if required, mobility support. The task of registering, providing, and managing LPWAN entities falls under the purview of the LPWAN server. Furthermore, it might enhance or combine the crucial elements of priority handling, security, and traffic routing. The application servers and cloud support the LPWAN by helping to maintain the database that contains the messages received from all connected objects. To evaluate and exploit the data, it might employ big data analytics.

3. **Bluetooth:** Bluetooth is a wireless protocol used for sending and receiving audio, images, video and data through 2.4GHz wireless link. It is one of the safe and seamless protocol that works well for wireless transfers between short-range, low-power, low-cost smart devices such as mobile phones, headsets, home stereos, MP3 players, laptops, desktops, tablets, digital camera, printers etc.

The name Bluetooth has come from the fact that, the code name was chosen by the Bluetooth SIG as a tribute to the Viking ruler Harald Blatand, who in the eleventh century amicably brought together several minor kingdoms that were operating under various sets of regulations, just as Bluetooth technology does today. Because he enjoyed eating blueberries, Harald's teeth acquired the hue that earned him the moniker “Bluetooth”. The name of the sign is very well-known, and it has a fascinating history. The Nordic runes Hagalaz (represented by the letter "H") and Berkana (represented by the letter “B”) are combined into one symbol in the logo. This is, Harald Blatand-like HB [8].

- **Bluetooth network architecture:** As indicated in Figure 2, the Bluetooth standard's protocols can be roughly divided into lower layers that specifies hardware-based radio system, middleware layers comprise software stack that specifies the linkages between the layers, and application layer for user interface.

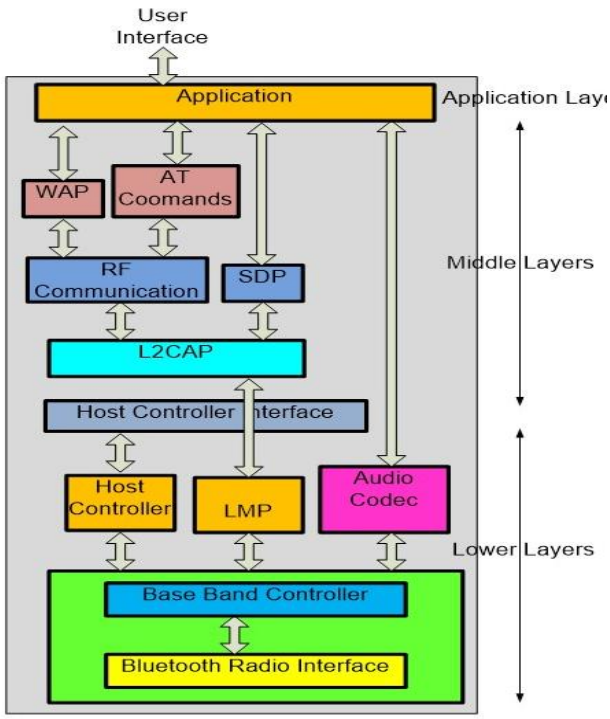

Figure 2: Bluetooth network architecture

The fundamental core specifications for Bluetooth are found in the lower layers. The radio layer, or module, serves as the foundation of the Bluetooth protocol stack. The transceiver's physical features are described in the radio layer. It is in charge of data modulation and demodulation for 2.4 GHz radio frequency transmission and reception.

Baseband and the link manager protocol (LMP) are layers above the radio layer. The baseband's role in correctly structuring data for transmission to and from the radio may be the best way to conceptualize these levels. It establishes the link's timing, framing, packets, and flow management. The link management controller establishes and maintains the link while translating host controller interface (HCI) directives from the top stack. It is in charge of controlling the connection, ensuring fairness among the slaves in the piconet, and managing the power.

The top stack tiers are profile specifications that specify how to design devices that will connect with one another while leveraging the core technology. The HCI serves as a link between the system's hardware and software components (i.e., the device driver). In the higher stack, the HCI layer is situated above the L2CAP (logical link control and adaptation protocol) layer. Among other things, it is necessary for communication between the top and bottom layers of the Bluetooth stack. It keeps track of the origin and destination of data packets. Each and every Bluetooth system must have it. Finally, in the application layer a user data which is obtained from real world or to be sent to the real world will be interfaced.

4. **Zig-Bee:** For wireless applications requiring low costs, low power, and low data rates, Zigbee is now quite popular. Everywhere, including smart energy, healthcare, and home automation, uses Zigbee technology. Zigbee products are used in smart energy applications to monitor and regulate energy and water use, allowing consumers to save both resources and money. It is used in the medical profession to connect an infinite number of health monitoring devices in addition to many others. It manages household lighting, including switches, dimmers, occupancy sensors, and load controllers, as part of home automation. It operates on two frequencies: 868/915 MHz and 2450 MHz. Data speeds in the 868/915 frequency range from 20 to 40 kbps, whereas those in the 2450 MHz spectrum are around 250 kbps. The Zigbee devices provide a sleep mode that reduces battery usage.

More recently the Zigbee Alliance's member firms developed and approved the Zigbee 3.0 protocol. The Zigbee Alliance membership consists of more than 300 top original equipment manufacturers (OEMs), technology companies, semiconductor makers, and service providers. The zigbee protocol was developed to provide a simple wireless data solution with safe, trustworthy wireless network topologies. In order to transport data across RF noise, which is typically present in commercial and industrial applications, the zigbee 3.0 protocol was developed. The present zigbee standard is improved in version 3.0, which also unifies the market-specific application profiles to enable wireless network access for all devices regardless of their market classification and function [9].

2. Zigbee network architecture

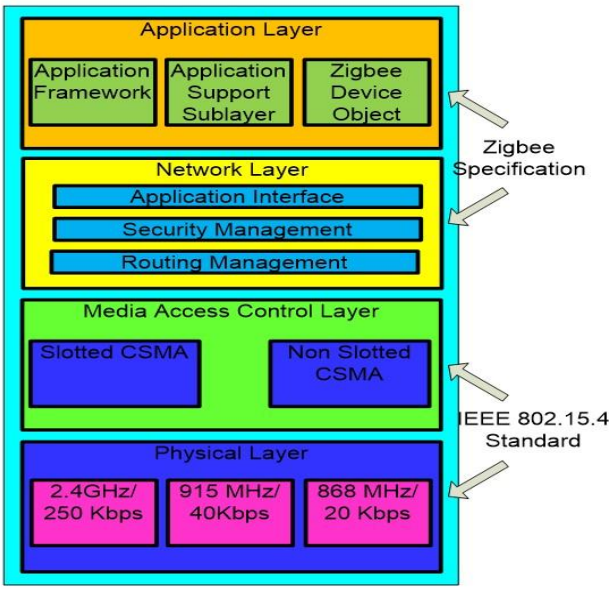

Figure 3: Zigbee network architecture

In the year 2004, the Zigbee specification similar to IEEE 802.15.4-2003, was accepted. The Zigbee Alliance released the Specification 1.0 in the year 2005. Three main types of devices - the Zigbee Coordinator, Router, and End Device - make up the backbone of the Zigbee system. Every Zigbee network needs to have a coordinator, who serves as the network's root and bridge. The coordinator is responsible for managing,

storing, and carrying out data activities when receiving and sending data. Zigbee routers serve as intermediaries, enabling data transfer between them and other devices. End devices are only partially able to link with parent nodes in order to conserve battery power. The quantity of routers, coordinators, and end devices varies depending on the type of network, such as star, tree, or mesh networks. The Zigbee protocol architecture, which is made up of a stack of additional layers that comprise the physical, network, and application layers particular to Zigbee as depicted in Figure 3, is defined by the IEEE 802.15.4 physical and MAC levels.

- **Physical layer:** When a signal is transmitted or received, the physical layer performs modulation and demodulation operations, respectively. The following table includes the frequency, data rate, and channel count for this layer.

- **Media Access Control (MAC) layer:** This layer connects to several networks employing carrier sense multiple access collision avoidances to provide secure data delivery (CSMA). Additionally, this method is used to transmit the beacon frames that synchronise communication.

- **Network layer:** All network-related tasks, such as network setup, end device connection and disengagement from the network, routing, device configurations, etc., are handled by this layer. The interface between the application layer and the MAC layer is provided by the network layer. It is in charge of setting up various Zigbee network topologies and performing routing.

- **Application layer:** As part of the Zigbee design, the Application Layer is divided into two sublayers (1) Application Support Sub Layer (APS) (2) Application Framework.

- **Application support sub layer:** is in charge of filtering packets for end devices and looking for duplicate packets, which are frequent in networks with automatic retries. When the sender requests an acknowledgement, it automatically retries the transmission to increase the likelihood of success. It takes part in keeping up with binding tables. Binding is the link that connects a node's endpoint to one or more endpoints on other nodes.

- **Application framework:** offers generic message services and key-value pair data services as two different sorts of data services. While the key-value pair is used to retrieve properties from application objects, the generic message is a format that developers construct. Application objects and the APS layer in Zigbee devices can communicate with one other through Zigbee Device Object (ZDO). Other devices must be found, started, and bound to the network by it.

5. **Wi-Fi:** Computers, tablets, cellphones, and other devices can be wirelessly connected to the internet using Wireless Fidelity (Wi-Fi) technology. In the Netherlands in 1991, NCR Corporation/AT&T developed the first Wi-Fi system. Wi-Fi is the radio signal that a wireless router transmits to a device within its network coverage area, which then converts the signal into information you can see and use. A radio signal is sent from the device back to the router, which has a wired or wireless connection to the internet. There should be two options for connecting to the Wi-Fi network for communication: either client to client connection or access point to client connection [10].

   - **Wi-Fi architecture:** In Wi-Fi architecture, antennas and routers send radio signals, which are picked up by Wi-Fi receivers, such as computers, cell phones, printers, and other devices equipped with Wi-Fi cards. Whenever the Wi-Fi devices, detects signals from the router within its 100 to 150-foot range, it automatically connects the device. The Wi-Fi signal's range depends on whether it is being used indoors or outdoors. In order to establish an internet connection between the user and the network, the Wi-Fi cards will read the signals. When connected to Wi-Fi, the speed of the device improves as it goes nearer to the main source and decreases as it gets farther away.

Figure 4: Wi-Fi architecture

One of the nicest features of the majority of modern laptops and smartphones is the included Wi-Fi cards. A login ID and password will be requested from the user if the network connection is free-based. In some places, the free base network connections operate rather effectively. Hotspots are being produced in the cities by the Wi-Fi network connection. The Wi-Fi network's hot spots serve as a point of connection. It is a tiny unit that is permanently connected to the internet. Public spaces like restaurants, hospitals, airports, hotels, businesses, universities, etc. all have plenty of Wi-Fi hotspots.

6. **RF-ID:** Radio Frequency Identification (RF-ID) employs electromagnetic or electrostatic coupling in the radio frequency part of the electromagnetic spectrum to uniquely identify a thing, an animal, or a person. Charles Walton officially invented RF-ID in 1983 when he submitted the first patent application containing the term RF-ID and gained attention in 2002 and has since continued to advance [11*]*.

- **RF-ID architecture:** The components of an RF-ID system as shown in Figure 5, consists of radio transponder/tag, a reader, and middleware installed on the computer database. An antenna, a wireless transducer, and an encasing substance make up an RFID tag. These tags come in active and passive varieties.

Figure 5: RF-ID architecture

While active tags have power on-chip, passive tags use the power generated by the RFID reader's magnetic field. In comparison to active tags, passive tags are therefore less expensive but have a shorter range (10 mts) and are more sensitive to environmental and regulatory restrictions. An antenna, transceiver, and decoder make up an RFID reader, which sends out periodic signals to check on nearby tags. Any signal it receives from a tag, it transmits to the data processor. The methods for processing and storing the data are provided by the data processing subsystem. The frequency range that an RFID system employs can also be used to distinguish between them. Low-Frequency (LF: 125–134.2 kHz and 140–148.5 kHz), High-Frequency (HF: 13.56 MHz), and Ultra-High-Frequency are the common ranges (UHF: 868 MHz - 928 MHz).

Short reading ranges and lower system costs are two advantages of low-frequency systems. They are most frequently utilized in applications for asset tracking, security access, and animal identification. For uses like railroad vehicle tracking and automated toll collection, high-frequency systems are employed because they have extensive read ranges (more than 90 feet) and fast reading speeds. High-frequency RFID systems function better, but at a larger expense to the system.

- **Cellular (1G/2G/3G/4G/5G):** The cellular wireless communication technology evolution is categorized as 1G, 2G, 3G, 4G, 5G and in all the technologies G stands for “Generation” which denotes how they have evolved over time.

Prior to the release of 2G, the word 1G was rarely used to describe cellular phone technology. The wireless telephone technology it uses is of the first generation. The early to mid-1980s saw the introduction of these analogue telecommunications standards. Because they used analogue technology, phones typically had short battery lives and poor voice security. It could essentially only make basic phone calls. 1G can go as fast as 2.4 Kbps (Kilo-bits per Seconds).

The switch from analogue (1G) to digital wireless phone technology (2G) was the biggest transformation ever. The introduction of data services for mobile through 2G digitization allowed the various mobile phone networks to offer services like text messaging, image messages, and MMS, starting with SMS (Short Message Service) and simple text-based messages (Multimedia Message Service). Radiolinja, now a part of Elisa Oyj, commercially introduced this generation of cellular communication networks in Finland in 1991 using the GSM (Global System for Mobile) standard. General Packet Radio Service (GPRS) and Enhanced Data Rates for GSM Evolution together offer a maximum speed of 50 Kbps or 1 Mbps (Megabits per Seconds) (EDGE).

Many of the data services we've come to know and love are available with a 3G wireless network, including email, video downloads, image sharing, and other Smartphone technology. In order to support more voice and data capacity, a wider range of applications, and more data transmission at a reduced cost, it was commercially introduced in 2001. Information may be transferred at a rate of at least 200 kbps thanks to 3G technology.

As can be expected, 4G is an advance over 3G and is designed for speeds of at least 100 Megabits per second and as high as 1 Gigabit per second. Additionally, 4G enables the sharing of network resources to accommodate more concurrent connections. Examples of possible and real-world uses include modified mobile web access, IP telephony, gaming services, high-definition mobile TV, video conferencing, 3D television, and cloud computing.

A generation called 5G is currently being developed. It designates the following significant stage in mobile telecommunications standards after the 4G era. The Next Generation Mobile Networks Alliance estimates that the new technology will be implemented around the year 2020, but given how quickly things are changing today, it will probably happen much sooner. Data rates of many tens of Mbps should be provided for tens of thousands of users, and 1 Gbps should also be made available, simultaneously, to tens of users, as part of the requirements for the 5G network [12].

- **Cellular architecture:** Three essential elements make up the high-level network architecture of LTE:

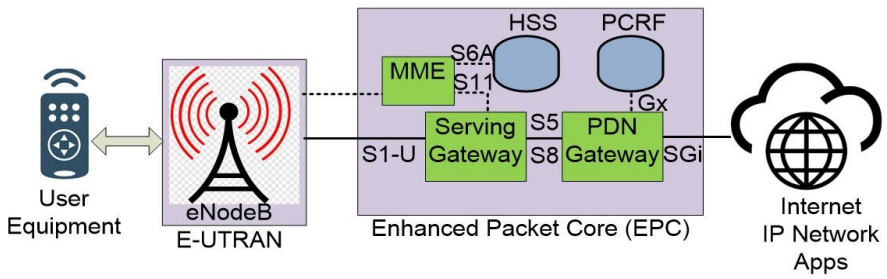

Figure 6: Cellular architecture

the user Equipment (UE), the Evolved UMTS Terrestrial Radio Access Network (E-UTRAN), and the Evolved Packet Core (EPC).

With packet data networks, such as the internet, a business' private network, or the IP multimedia subsystem, an upgraded packet core can connect. As depicted in Figure 6, the interfaces connecting the system's various components are designated Uu, S1, and SGi.

- **User Equipment (UE):** The internal architecture of the LTE user equipment, which is mobile equipment, is exactly the same as that of UMTS and GSM (ME). The following essential modules make up the mobile equipment:

  - Mobile Termination (MT) handles all communication-related tasks.
  - Terminal Equipment (TE) terminates the data streams.
  - The Universal Integrated Circuit Card (UICC) is the name for the SIM card used with LTE equipment. Known as the Universal Subscriber Identity Module, this programme (USIM).

  Similar to a 3G SIM card, a USIM card stores user information such their phone number, home network identity, and security keys.

7. **Evolved UMTS terrestrial radio access network (E-UTRAN):** An evolved packet core, or ePC, is responsible for controlling the various data packets that are sent between mobile devices and the core network. In contrast to an eNB, which is a base station that controls mobile devices in one or more cells, an eNodeB governs radio communication between an evolved packet core, or ePC, and mobile devices. According to the EPC, each eBN may connect to nearby base stations using the S1 interface or the X2 interface for signalling and packet forwarding during changeover.

   - **Evolved Packet Core (EPC):** The Home Subscriber Server is the main database that houses all of the network operator's subscribers' data (HSS). The Home Subscriber Server (HSS) component houses this data, which has been brought over from UMTS and GSM. In order to communicate with the P-surrounding GW's packet data networks, or PDNs, SGi is used. An APN is used to uniquely identify each packet data network. The P-GW serves as a GPRS support node (GGSN) and a serving GPRS support node (SGSN) for UMTS and GSM in addition to carrying out the same tasks as the GSN and SGSN in packet data networks. The S-GW acts as a router and controls data forwarding between the base station and PDN gateway. The mobile device's high-level operation is managed by the Home Subscriber Server (HSS), the highest level control entity of a mobile network operator (MNO). The PCRF is a part of the PCEF that controls policy control charging functions (Policy Control and Charging Rules Function). S5/S8 is used to communicate between the serving and PDN gateways when the two devices are connected to the same network. The network configuration determines whether S5 or S8 is used of the two interfaces.

   - **Near Field Communication:** Near-field communication (NFC) is a wireless short-range technology that improves the smarts of your smartphone, tablet, wearables, payment cards, and other devices. Near-field communications represent the peak of connectivity. You may quickly and easily use NFC to transfer data between two Android-powered smartphones or between an NFC tag and an Android-powered device with just one touch. This includes bill payments, business card exchanges,

coupon downloads, mobile payments, car door unlocking, access authentication for office doors, etc.

The NFC Forum, a nonprofit group dedicated to bringing the convenience of NFC technology to all facets of life, was founded in 2004 by Philips (PHG), Nokia (NOK) and Sony (SNE) and it served as a catalyst for the growth of near-field communication technology. The Forum officially established the NFC technology architecture in 2006, and its specifications continue to act as a road map for any parties interested in creating powerful new consumer-driven products. In 2007, Nokia released the first NFC-enabled phone, and by 2010, the telecommunications sector had launched more than 100 NFC trial projects. In 2017, the New York City Metropolitan Transit Authority (MTA) progressively put in place a system that enables passengers to pay their subway fares using NFC technology [13].

- **Near Filed Communication architecture:** NFC has its roots in RFID technology and operates on the same principals as RFID. Using the 13.56 MHz spectrum, NFC devices produce a low frequency radio wave field. Magnetic inductive coupling occurs when this gadget approaches another NFC device closely enough to make contact with the field, transferring energy and data from one device to the other as shown in Figure 7. The primary difference between NFC & other communication technologies is the usage of magnetic coupling.

There are three NFC devices that can be used for NFC communication: NFC readers, NFC tags, and NFC mobile. Three different operating modes for NFC technology exist: reader/writer, peer-to-peer, and card emulation. In each case, communication takes place between an NFC mobile on the one side and an NFC tag, an NFC mobile, or an NFC reader on the other. Mobile devices with NFC technology built in (NFC enabled) often include a variety of integrated circuits, such as a secure element (SE) for carrying out secure transactions and maintaining a secure environment for storing sensitive data and an NFC communication interface, as shown in Figure 7.

- **Long-Range radio-wide area network :** A low-power, long-range wide-area networking protocol called LoRaWAN was constructed on top of the LoRa radio modulation method. It wirelessly connects devices to the internet and regulates communication between end-node devices and network gateways. Devices can run for ten years on a little battery because LoRaWAN is a widely available long-range, bidirectional communication protocol with very low power consumption. It uses unlicensed ISM (Industrial, Scientific, and Medical) radio bands for network installations. Activation by Personalization (AP) and Over-the-air Activation (OTAA) are two ways that a LoRaWAN end device can join a network (ABP) [14].

- **LoRaWAN architecture:** The LoRa network makes use of a LoRaWAN-based communications network to route data from the end node through a LoRaWAN gateway to the necessary organisations as indicated in Figure 8. Additionally, LoRaWAN specifies how information is distributed throughout the network, including the answers of the LoRaWAN gateways and the LoRa network server.

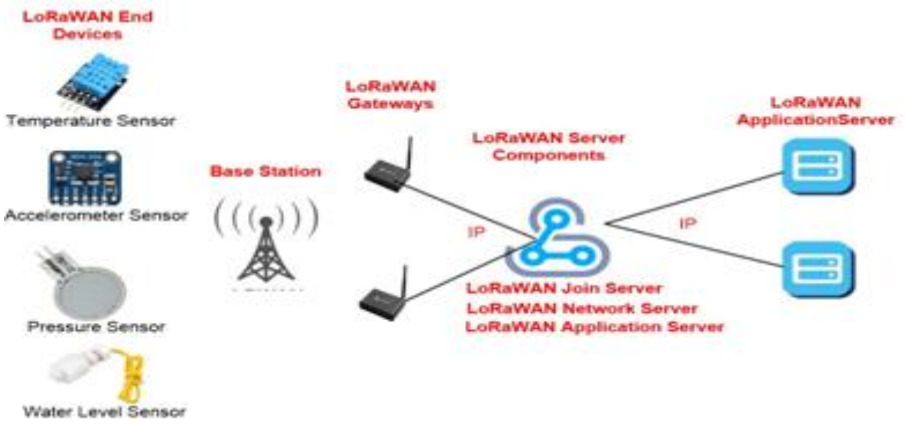

Figure 8: lorawan architecture

- **LoRaWAN end device:** Small amounts of data are sent over great distances at low frequencies using a LoRaWAN end device. It can be used in many different contexts, including logistics, smart cities, smart buildings, factories, farms, and automated systems.

- **LoRaWAN gateways:** All received LoRaWAN radio packets are forwarded by the radio gateway to the network server, which is linked by an IP backbone. Its function is to decode uplink radio packets in the air and forward them directly to the network server without further processing. Without interpreting the packet content for downlinks, the radio gateway forwards the LoRaWAN network server's requests for packet delivery.

- **LoRaWAN server:** The network's central server oversees it all. It removes redundant packets from packets it receives, runs a security check, and then chooses the best gateway to send an acknowledgement message back to the sender.

- **LoRaWAN application server:** All of the application layer payloads from the end devices are handled by the application server. Additionally, it creates all of the application layer downlink payloads for the linked endpoints.

8. **Li-Fi:** A wireless communication technique called Light Fidelity (Li-Fi) capable of sending data at high speeds over the visible light, ultraviolet, and infrared spectrums, uses light to convey information and coordinates between devices. Currently, the only lights that may be utilized to transmit data in visible light are LED lamps. The phrase was first used by Harald Haas at an Edinburgh TEDGlobal talk in 2011. Due to the fact that LiFi does not result in an electromagnetic reaction, it can be used efficiently in a variety of industries, including healthcare, life sciences, and medicine applications [15].

   Li-Fi architecture: LED lights and photodetectors (PDs) are two crucial optoelectronic components that are used in the Li-Fi system's architecture as shown in Figure 9. Since LEDs operate at a speed of less than 1 s, they can be turned on and off quicker than the human eye can notice, giving the impression that the light source is always on. Binary coding is used for data transmission through this inconspicuous on-off process. An LED can be turned on using binary 1 and turned off with binary 0. By changing the rate at which LEDs turn on and off to produce distinct strings of 1s and 0s, it is feasible to encrypt data in light. Humans are unable to detect modulation because of its rapidity. The signal is subsequently captured by a photo detector, which converts it back into its original form.

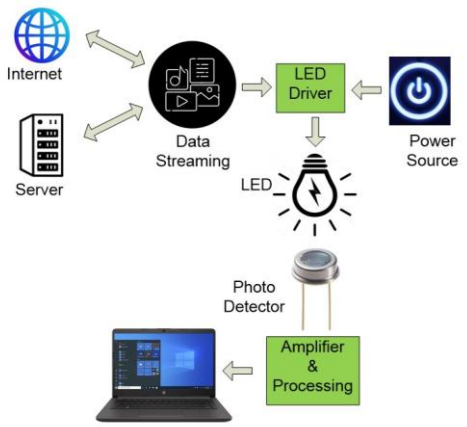

Figure 9: Li-Fi architecture

IV. COMPARISION STUDY OF IoT COMMUNICATION TECHNOLOGIES

In this section, various IoT communication technologies are comparison in terms of communication standard, operating frequency, type of modulation, operating range, data rates and areas of applications are tabulated in Table 1.

Table 1: Comparison of IoT communication protocols

Protocols	Standard	Operating Frequencies	Modulation	Operating Range	Data Rates	Applications
I2C (Inter Integrated Circuit)	synchronous serial data	100 kHz, full speed 400 kHz, fast speed 1000 kHz, high speed	NA	1 m at 100 Kbaud 10 m at 10 Kbaud	100 kbps, full speed 400 kbps, fast speed 1000 kbps, high speed	Communicating multiple microcontrollers, sensors data reading, accessing ADCs and DACs
SPI (Serial Peripheral Interface)	asynchronous serial data	50 MHz	NA	10 m	60 Mbps	LCD, RTC, ADC, DAC, Audio Codec interface
USB (Universal Serial Bus)	Industry USB 2.0 USB 3.0	50 MHz 2.4 GHz	NA	5 m 15 m	60 Mbps 5 Gbps	Printer, keyboard, mouse, digital cameras
UART/USART (RS232, RS485)	asynchronous serial communication	80 MHz	NA	15 m to 1000 m	5 Mbps	RFID, GPS receivers, Bluetooth modules, GSM and GPRS modems etc.
Ethernet	IEEE 802.3	100 MHz	NA	100 m over twisted pair, up to 100 km over optical fiber	10 Mbps	connect different devices in a network with each other
Advanced Message Queuing Protocol (AMQP)	Open standard	NA	NA	Receives streaming data	NA	Application layer protocol for message-oriented middleware
Extensible Messaging and Presence Protocol (XMPP)	RFC 6120	NA	NA	instant messaging, voice, video calls	NA	Network management, file sharing, gaming, remote systems control and monitoring, geolocation
Message Queuing Telemetry Transport (MQQT)	OASIS standard	NA	NA	NA	NA	Standard for IoT messaging

Constrained Application Protocol (CoAP)	RFC 7252	NA	NA	NA	NA	Intended for restricted devices like sensors at the application layer and web based protocol
Data Distribution Service (DDS)	Open Standard	generate frequencies from less than 1 Hz up to 400 MHz	NA	NA	56 Kbps	Open standard for real-time applications
Light Weight Machine to Machine (LWM2M)	LWM2M Standard	NA	NA	NA	NA	It is an IoT application layer protocol that was developed by OMA to link IoT platforms and devices.
Low Power Wide Area Networks (LPWANs)	IEEE 802.15	865-870 MHz	Ultra Narrowband	2 km to 1,000 km	0.3 kbit/s to 50 kbit/s per channel	IoT, Smart metering, smart lighting, smart cities, Power grid, Agriculture etc.
SigFox	IEEE 802.15.1	868/915 MHz	UNB/GFSK/BPSK	10 km (urban), 40 km (rural)	100 bps	smart metering, healthcare, transportation
Random Phase Multiple Access (RPMA)	IEEE 802.15	2.4GHz	RPMA	200 square miles	624kbps DL 156 kbps UL	IoT and M2M applications
LTE-M (CATM1)	IEEE 802.16m	In band LTE	OFDMA/SC-FDMA	1 km in urban areas 10 km in rural areas	1 Mbps	Asset tracking, wearable technology, smart city services, and e-health solutions
Nwave (Wireless Access in Vehicular Environments)	IEEE 802.11p standard Weightless	315/433/470/868/915 MHz	DBPSK	up to 10 miles line of sight	100 bps	Smart parking and vehicle counting applications
NB-IoT (Narrow Band)	3GPP International Standards	In band LTE, guard band & stand alone	OFDMA/SC-FDMA	1 km (urban), 10 km (rural)	26 kbps for DL and 62 kbps for UL	Smart buildings with intruder and fire alarms, Track people or animals or objects, Smart metering (gas, electricity, and water meter)
Bluetooth and Bluetooth Low Energy (BLE)	IEEE 802.15.1	2.4GHz	GFSK	10 meters	3 Mbps	Transfer data files, images, videos, MP3 or MP4 files, mouse and keyboards etc.

Weightless -P	Open standard	169/433/470/780/ 868/915/923 MHz	FDMA+ TDMA	100 km	0.2 – 100 kbps	healthcare, asset tracking, sensors, and automobiles
Zig-Bee	IEEE 802.15.4	2.4 Ghz, 900 MHz 868 MHz	OQPSK with DSSS as spreading technique	10–100 m	250 kbps, 40 kbps, 20 kbps	Wireless sensor networks, Medical data collection, Home automation, Smoke warning, Industrial control systems etc.
Z-Wave	Closed N/W Standards	908.42 MHz	FSK/GFSK	100 meters	upto 100kbps	Smart home, Smart hubs, Smart sensors, security and alarms etc.
Wi-Fi	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ad	5 GHz 2.4 GHz	Wi-Fi 5 uses 256-QAM and Wi-Fi 6 uses 1024-QAM	92 meters 46 meters	54 Mbps 11 Mbps 54 Mbps 150 Mbps 866.7 Mbps 7 Gbps	Mobile, Business, Home, Automotive, IoT etc.
WirelessHART	IEC 62591, IEEE 802.15.4	2.4 GHz	OQPSK with DSSS as spreading technique	225 m	250 kbps	Process automation, real time monitoring of oil and gas
Radio Frequencies Identification (RF-ID)	IEEE 802.15 RFID	125KHz, 134 KHz 13.56 MHz 860 to 956 MHz	ASK	12 meters with passive tag & 100 m with active tags	Varies with frequency, Up to 424 Kbps	Inventory tracking, vehicles number plate reading, patients tracking etc.
Cellular (1G/2G/3G/4G/5G /6G)	NMT (1G) GSM/GPRS/ EDGE (2G) UMTS/HSPA	850 MHz and 1900 MHz GSM: 900MHZ, 1800MHz CDMA: 800MHz	FM GMSK QPSK	30 km 35 km 50–150 km	2.4 kbps 1 Mbps 2 Mbps	Analog mobile wireless applications GSM wireless voice telephony, mobile Internet access, video calls Mobile phones, tablets, hotspots Mobile phones, tablets, hotspots,

	(3G) LTE (4G) IEEE 802.11be (5G) IEEE 802.15.3d (6G)	800 MHz – 2100 MHz 2 - 8 GHz 28 GHz and 39GHz over 95 gigahertz (GHz) to 3 THz	OFDM OFDM OFDM with Subcarrier Power Modulation	50–150 km 250–300 m 10 m	100 Mbps 35.46 Gbps Up to 1 Tbps	automated cars Automated cars, cellular surfaces, Wi-Fi implants
Near Field Communication (NFC)	ISO/IEC 18092	13.56 MHz	ASK	10 cm	424 kbps	Keyless access, e-wallets, smart tickets, wearable technology, credit cards, and smart tags for medical uses
Long-Range Radio-Wide Area Network (LoRaWAN)	Open Standard	868/902 – 928 MHz	DSS with Chirp spread spectrum	up to 5 km in urban areas, and up to 15 km or more in rural areas (line of sight)	0.3 - 50 kbps	Smart cities, smart parking, farming, smart buildings etc.
Light Fidelity (Li-Fi)	IEEE 802.15. 7	200 THz	Single carrier modulation	Approximately 10 m	224 Gbps	Under water communication, smart homes etc.

V. CHALLENGES AND FUTURE TRENDS IN IoT COMMUNICATION TECHNOLOGIES

1. **Challenges:** The IoT has quickly expanded to play a significant role in how people live, interact, and conduct business. Web-enabled devices are transforming our universal rights into a larger switched-on space to live in all over the world. The IoT is facing a variety of challenges that are described as follows.

    - **Lack of Encryption in security of the system:** Systems need to be secure with cryptographic encryption algorithms and security protocols in order to be created and implemented. It is necessary to use a variety of powerful encryption algorithms techniques to secure every element of embedded systems from the prototype to the finished product which results in lot of power consumption.

    - **Connectivity Issue:** When integrating devices, programmes, and cloud platforms, it is the fundamental problem. Devices that are connected and provide useful information and front are quite valuable. Weak connectivity, however, poses a challenge when IoT sensors are required to monitor process data and deliver insights.

    - **Inadequate upgrading and testing:** As the number of IoT devices increases, manufacturers are more eager to create and deliver their device as soon as possible without giving security much care. Most of these IoT devices and goods don't get adequate testing or updates, leaving them open to security dangers like hackers.

    - **Default password risk:** Due to faulty credentials and login information, almost all IoT devices are vulnerable to password hacking and brute force attacks. Any business that uses default factory passwords exposes not only its own assets but also the sensitive data of its clients to the risk of a brute force attack.

    - **Compatibility issue:** Communication between various applications from various producers is frequently hampered by a lack of standards. There are, however, specific methods for enabling devices to communicate and exchange information.

    - **Energy consumption issue:** IoT devices consume a lot of energy for computing, connectivity, and data collection and exchange. These gadgets must be able to handle those activities independently, which results in high energy consumption and reduced battery life.

    - **Gathering and processing of data:** Data is a crucial component of IoT development. The processing or usability of the stored data is more important in this situation. In addition to security and privacy, development teams must make sure they have a solid plan in place for how data will be gathered, kept, or processed within an environment.

2. **Future trends*:*** Using IoT technology in conjunction with cutting-edge innovations like 5G and cloud computing can boost operational efficiency, cut costs, improve decision-making, and improve customer experience. Businesses must keep an eye on how things are evolving as the market landscape changes over the next years. Businesses that

creatively consider how technology are changing have a tendency to be some of the most prosperous ones. Without keeping an eye on these developments, it is impossible to come up with concepts for creative applications of and combinations of these technologies. The following sections cover some of the potential IoT communication technology trends.

- **Artificial Intelligence & IoT Technology (AIoT):** Supporting artificial intelligence software is one of the most exciting applications of IoT technology. The Internet of Things and artificial intelligence are mutually beneficial. With distributed data, IoT benefits from AI, and AI benefits from IoT with better management.

- **Industrial Internet of Things (IIoT):** As the name implies, the Industrial Internet of Things (IoT) is the application of IoT in the business and industrial sectors. It has specific effects on every facet of company, from production to upkeep and customer service. Every sector of business and industrial activities has seen significant IoT penetration. This has produced a number of benefits, including the robotic automation of repetitive tasks using IoT devices and sensors.

  IoT devices make it simple to carry out numerous industrial activities, including performance measurement and unit maintenance time forecast. Through the gathering of data with IIoT, data may be better examined and worked on. Personalization of the user experience, improved security, effective management of third-party system skills, and communication.

- **IoT Connectivity:** Wireless data rates have been the biggest issue that IoT networks have had to solve recently. IoT components including sensors, edge computing, wearables, smart homes, and more will advance as these technologies do. IoT solutions are now more practical because to recent infrastructure development for newer connectivity kinds. Satellites, WiFi 6, LPWAN, and 5G are examples of connectivity technologies.

- **IoT Cybersecurity:** A recent trending topic is cybersecurity, which is a major focus area that requires the highest attention. IoT data must be kept secure and private as more individuals and businesses access it over the network. It might be accomplished by setting a default password for all relevant devices and sensors. People are not aware of the necessary security standards due to the manner it is being used. The standard cybersecurity practices may not be adequate to safeguard the entire infrastructure. This year's trends in IoT will focus on the need to develop specialized rules, laws, tools, and processes. The need for effective countermeasures will become more apparent as cyberattacks, DDOS, and other destructive activities increase.

- **Intelligent edge computing:** Edge computing is necessary for real-time applications. Edge networks process information closer to the user and lessen the strain on the entire network for all users as opposed to processing everything at a central location.

  Edge computing has the ability to improve data processing security in addition to reducing the latency of IoT technologies. There are fewer options for data to be captured by hackers if it may be processed on an edge device rather being sent to a central server. All that is required is for the user to immediately receive the

information that was shared with the edge device. In this scenario, memory storage is not necessary for the data. Edge computing is advantageous in any situation where quick decisions are necessary. This is especially true when it comes to safety and security issues. IoT edge computing can be used to protect people from harm by turning off machines when someone enters a factory area that is off limits. When autonomous vehicles require data to make critical decisions in real-time, it might mean the difference between life and death on the road.

- **Wearable IoT technology:** It was once predicted that wearable technology, and specifically smartwatches, will eventually displace smartphones and desktop computers. It doesn't appear like this forecast will come true any time soon, either. Wearable gadgets, such smartwatches, are significantly less likely to be beneficial for tasks you could perform on a smartphone or laptop due to their restricted feasibility. But because it can monitor patients' vital signs, wearable IoT technology has a lot of promise to help in medical jobs. These gadgets are capable of accumulating ongoing health records and automatically alerting others in case of crises.

- **Smart homes:** A focus on smart home automation is among the next phases. IoT networks for smart homes are now improving their capacity to automate processes like security, climate management, and lighting. Consumers can manually adjust them, or AI systems that analyse sensor and use data can automatically adjust them.

- **Smart cities:** When creating networks for smart cities, IoT technology has various uses. The most urgent concern is traffic monitoring. Improved control over intersections for better traffic management is made possible by the ability to monitor traffic using sensors positioned around the city. Monitoring of water levels can be helpful in alerting the public to current and impending flooding. Additional actions to stop future flooding can also be guided by this information.

- **Adoption iot in healthcare segment:** When it comes to implementing innovative technologies and procedures, the healthcare sector has been at the forefront of revolution. IoT has been on the list for a while, and this year will see the healthcare sector adopting more IoT-driven solutions. The current healthcare system includes a number of unique implementations, such as wearable gadgets and sensors, tracking devices, indoor navigation devices, lighting systems with health monitors, telemedicine, enhanced heart rate monitoring, and oxygen monitoring.

- **5G driven IoT prospects:** The power of 5G connectivity is already popular and will have a significant impact on how the Internet of Things is implemented. It will expand the possibilities for IoT-powered tools and technology. Since low latency and hyperconnectivity are essential for a successful IoT application, 5G will prove useful. Increased flexibility, mobility, dependability, and security will be made possible with 5G. It will combine wireless technology with the flexibility of wired technology to provide the best of both worlds.

- **IoT as a service (IoTaaS):** IoTaaS companies offer a range of solutions to let businesses deploy IoT without the requirement for internal expertise. The technology seeks to simplify the deployment and management of linked devices for businesses. It

has evolved into a catalyst for enterprise IoT use, particularly in condition monitoring, sophisticated automation, and predictive maintenance.

VI. CONCLUSIONS

Various short- and long-range IoT wireless communication methods are briefly covered in this chapter, along with their components and architectures. Each wireless communication technology currently in use has distinct features, flexibilities, and requirements of its own. These technologies are compared and classed depending on a number of factors, including applications, operating frequency, coverage range, data rate, standard, and type of modulation employed. A suitable communication technology could be chosen for a particular IoT-related application depending on the necessity. Along with the aforementioned advancements in IoT communication technology, other challenges are also presented.

REFERENCES

[1] A. A. Bahashwan, M. Anbar, N. Abdullah, T. Al-Hadhrami, and S. M. Hanshi, “Review on Common IoT Communication Technologies for Both Long-Range Network (LPWAN) and Short-Range Network,” Advances on Smart and Soft Computing. Advances in Intelligent Systems and Computing, Springer, Singapore, vol. 1188, pp. 341-353, October 2020.

[2] S. M and B. R. Chandavarkar, "IoT’s Communication Technologies, Data Formats, and Protocols - A survey," 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), 2021, pp. 483-488, doi: 10.1109/ICSCCC51823.2021.9478093.

[3] S. Al-Sarawi, M. Anbar, K. Alieyan and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," 2017 8th International Conference on Information Technology (ICIT), 2017, pp. 685-690, doi: 10.1109/ICITECH.2017.8079928.

[4] M. M. Alam, H. Malik, M. I. Khan, T. Pardy, A. Kuusik and Y. Le Moullec, "A Survey on the Roles of Communication Technologies in IoT-Based Personalized Healthcare Applications," in IEEE Access, vol. 6, pp. 36611-36631, 2018, doi: 10.1109/ACCESS.2018.2853148.

[5] A. Rehman, K. Mehmood, and A. Baksh, “Communication Technology That Suits IoT - A Critical Review,” Conference In Wireless Sensor Networks for Developing Countries, Springer Berlin Heidelberg, Jamshoro, pp. 14-25, April 2013.

[6] Chaudhari, B.S.; Zennaro, M.; Borkar, S. LPWAN Technologies: Emerging Application Characteristics, Requirements, and Design Considerations. Future Internet 2020, 12, 46. https://doi.org/10.3390/fi12030046

[7] N. Islam, B. Ray and F. Pasandideh, "IoT Based Smart Farming: Are the LPWAN Technologies Suitable for Remote Communication?," 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), 2020, pp. 270-276, doi: 10.1109/SmartIoT49966.2020.00048.

[8] Q. Liu, W. IJntema, A. Drif, P. Pawełczak, M. Zuniga and K. S. Yıldırım, "Perpetual Bluetooth Communications for the IoT," in IEEE Sensors Journal, vol. 21, no. 1, pp. 829-837, 1 Jan.1, 2021, doi: 10.1109/JSEN.2020.3012814.

[9] P. D. P. Adi et al., "A Performance Evaluation of ZigBee Mesh Communication on the Internet of Things (IoT)," 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT), 2021, pp. 7-13, doi: 10.1109/EIConCIT50028.2021.9431875.

[10] J. Sheth and B. Dezfouli, "Enhancing the Energy-Efficiency and Timeliness of IoT Communication in WiFi Networks," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9085-9097, Oct. 2019, doi: 10.1109/JIOT.2019.2927588.

[11] K. Peng and Y. Xu, "Design of Low-Power Bandgap Voltage Reference for IoT RFID Communication," 2018 IEEE 3rd International Conference on Integrated Circuits and Microsystems (ICICM), 2018, pp. 345-348, doi: 10.1109/ICAM.2018.8596364.

[12] H. Zhang, B. Di, X. Zhang, K. Bian, L. Song and Z. Han, "Cellular Internet-of-Things (IoT) Communications over Unlicensed Band," 2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), 2018, pp. 1-10, doi: 10.1109/DySPAN.2018.8610466.
[13] L. T. Beng, P. B. Kiat, L. N. Meng and P. N. Cheng, "Field testing of IoT devices for livestock monitoring using Wireless Sensor Network, near field communication and Wireless Power Transfer," 2016 IEEE Conference on Technologies for Sustainability (SusTech), 2016, pp. 169-173, doi: 10.1109/SusTech.2016.7897161.
[14] A. Lavric and A. I. Petrariu, "LoRaWAN communication protocol: The new era of IoT," 2018 International Conference on Development and Application Systems (DAS), 2018, pp. 74-77, doi: 10.1109/DAAS.2018.8396074.
[15] R. A. A. Othman, D. a. Sagaran, M. Mokayef and W. I. I. R. b. W. M. Nasir, "Effective LiFi communication for IoT applications," 2018 IEEE 4th International Symposium in Robotics and Manufacturing Automation (ROMA), 2018, pp. 1-4, doi: 10.1109/ROMA46407.2018.8986698.
[16] Q. V. Khanh, N. V. Hoai, L. D. Manh, A. N. Le, and G. Jeon, "Wireless Communication Technologies for IoT in 5G: Vision, Applications, and Challenges," Wireless Communications and Mobile Computing, vol. 2022, pp. 1-12, February 2022.
[17] Sunguk Lee, "Communication Technology and Application of Internet of Things (IoT) in Smart Home Environment," International Journal of Control and Automation, vol. 10, no. 3, pp. 397-404, 2017.
[18] T. Watteyne, P. Tuset-Peiro, X. Vilajosana, S. Pollin and B. Krishnamachari, "Teaching Communication Technologies and Standards for the Industrial IoT? Use 6TiSCH!," in IEEE Communications Magazine, vol. 55, no. 5, pp. 132-137, May 2017, doi: 10.1109/MCOM.2017.1700013.
[19] A. Rakić, I. Popović, I. Petruševski, Đ. Begenišić, V. Spajić and M. Rakić, "Key aspects of narrow band internet of things communication technology driving future IoT applications," 2017 25th Telecommunication Forum (TELFOR), 2017, pp. 1-4, doi: 10.1109/TELFOR.2017.8249327.
[20] D. Santhadevi and B. Janet, "Security Challenges in Computing System, Communication Technology and Protocols in IoT system," 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET), 2018, pp. 1-7, doi: 10.1109/ICCSDET.2018.8821074.
[21] P. Danielis, H. Puttnies, E. Schweissguth and D. Timmermann, "Real- Time Capable Internet Technologies for Wired Communication in the Industrial IoT-a Survey," 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), 2018, pp. 266-273, doi: 10.1109/ETFA.2018.8502528.
[22] R. Singh, R. Angmo, V. Jha, P. Singh, V. P. Singh and N. Aggarwal, "Internet of Things (IoT) Protocols, Communication Technologies, and Services in Industry," 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), 2021, pp. 1407-1413, doi: 10.1109/ICAC3N53548.2021.9725410.
[23] Rolando Herrero, Fundamentals of IoT Communication Technologies, 1st ed., Springer Nature Switzerland AG, June 2021.

