**CHAPTER 2**

**THEORETICAL BACKGROUND OF BUILDING THE SYSTEM**

**2.1. System Requirements**

This system is used Raspberry Pi, ESP8266, Breadboard, Jumper wires and Push Button. This project is associated with IoT platform.

2.1.1. Internet of Things(IoT)

The network of smart devices approach was discussed in 1982, with a revised Coke machine at Carnegie Mellon University comely the first internet connected machine, in a position to report its catalogue and whether newly loaded drinks were cold or not. However, the word “Internet of Things” was coined by British entrepreneur Kevin Ashton the executive director of Auto-ID centre in the year 1999. The Internet of Things(IoT) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers(UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. The Internet of Things(IoT) is emerging as the next technology trend with powerful and remarkable effects across the business spectrum. IoT connects to the internet, billions of everyday devices, which range from fitness bracelets to industrial equipment. IoT is merging the physical and online worlds and providing new opportunities and challenges for enterprises, companies, governments and consumers. The Internet of Things is predicted to permeate almost every sphere and industry. Data can be collected from practically any conceivable source.

In IoT, everyday things and machines are in the lead role and communicate with each other. Unlike the Web, which uses a single standard messaging protocol HTTP, IoT cannot rely on a single protocol for all its need. Consequently, hundreds of messaging protocols are available to choose for various types of requirements of the IoT system. Some of them have been designed to address applications requiring fast and reliable business transactions. A numerous have been designed to address applications requiring data collection in constrained network such as MQTT. Thus, IoT lies on several messaging protocols and any one protocol cannot deal with all possible IoT use cases. Consequently, it is necessary to investigate the pros and cons of the widely accepted and emerging messaging protocols for IoT systems to determine their best-fit scenarios.

The Internet of Things thus promises a strong added value to each organization. By connecting objects, people and environments, it becomes possible to develop improvements that can only be beneficial. The main benefits are

* Productivity improvement : IoT allows the monitoring and the control of the different processes, which optimizes the different operations that increase productivity and efficiency.
* Predictive analysis :Thanks to the collection of a large amount of data. IoT’s new technologies make it possible to examine recurring patterns and contribute to predictive analysis, which can be use mainly in maintenance.
* Rapid response : the data makes it possible to monitor the systems in place in real time and even remotely. They facilitate the optimization of maintenance interventions, but also give the company a strategic advantage in monitoring market developments
* Reduction of human errors : thanks to the complementarity of technologies such as artificial intelligence. IoT makes it possible to reduce human errors due to mundane or repetitive tasks.

The IoT helps people live and work smarter, as well as gain complete control over their lives. Some of the pros of IoT include the following:

* ablility to access information from anywhere at anytime on any device;
* improved communication between connected electronic devices;
* transferring data packets over a connected network saving time and money;and
* automating tasks helping to improve the quality of a business’s services and reducing the need for human intervention.

Some cons of IoT include the following:

* As the number of connected devices increases and more information is shared between devices, the potential that a hacker could steal confidential information increases.
* Enterprises may eventually have to deal with massive numbers-may be even millions of IoT devices, and collecting and managing the data from all those devices will be challenging,
* If there is a bug in the system, it is likely that every connected device will become corrupted.
* Since there is no international standard of compatibility for IoT, it is difficult for devices from different manufacturers to communicate with each other.

2.1.2. Raspberry Pi

The Raspberry Pi is a series of small single-board computers developed in the United Kingdom by the Raspberry Pi Foundation to promote teaching of basic computer science in schools and in developing countries. The original model became far more popular than anticipated, selling outside its target market for uses such as robotics. It now is widely used even in research projects, such as for weather monitoring because of its low cost and portability. It does not include peripherals (such as keyboards and mice) or cases. However, some accessories have been included in several official and unofficial bundles.

After the release of the second board type, the Raspberry Pi Foundation set up a new entity, named Raspberry Pi Trading, and installed Eben Upton as CEO, with the responsibility of developing technology. The Foundation was rededicated as an educational charity for promoting the teaching of basic computer science in schools and developing countries. The Raspberry Pi is one of the best-selling British computers. As of December 2019, more than thirty million boards have been sold. Most Pis are made in a Sony factory in Pencoed, Wales, while others are made in China and Japan.

Several generations of Raspberry Pis have been released. All models feature a Broadcom system on a chip (SoC) with an integrated ARM-compatible central processing unit (CPU) and on-chip graphics processing unit (GPU). The first generation (Raspberry Pi Model B) was released in February 2012, followed by the simpler and cheaper Model A. In 2014, the Foundation released a board with an improved design, Raspberry Pi Model B+. These boards are approximately credit-card sized and represent the standard mainline form-factor. Improved A+ and B+ models were released a year later. A "Compute Module" was released in April 2014 for embedded applications. The Raspberry Pi 2, which featured a 900 MHz quad-core ARM Cortex-A7 processor and 1 GiB RAM, was released in February 2015. A Raspberry Pi Zero with smaller size and reduced input/output (I/O) and general-purpose input/output (GPIO) capabilities was released in November 2015 for US$5. Raspberry Pi 3 Model B was released in February 2016 with a 1.2 GHz 64-bit quad core processor, on-board 802.11n Wi-Fi, Bluetooth and USB boot capabilities. On Pi Day 2018, the Raspberry Pi 3 Model B+ was launched with a faster 1.4 GHz processor and a three-times faster gigabit Ethernet (throughput limited to ca. 300 Mbit/s by the internal USB 2.0 connection) or 2.4 / 5 GHz dual-band 802.11ac Wi-Fi (100 Mbit/s).Other features are Power over Ethernet (PoE) (with the add-on PoE HAT), USB boot and network boot (an SD card is no longer required). Raspberry Pi 4 Model B was released in June 2019[2] with a 1.5 GHz 64-bit quad core ARM Cortex-A72 processor, on-board 802.11ac Wi-Fi, Bluetooth 5, full gigabit Ethernet (throughput not limited), two USB 2.0 ports, two USB 3.0 ports, and dual-monitor support via a pair of micro HDMI (HDMI Type D) ports for up to 4K resolution. The Pi 4 is also powered via a USB-C port, enabling additional power to be provided to downstream peripherals, when used with an appropriate PSU. The initial Raspberry Pi 4 board has a design flaw where third-party e-marked USB cables, such as those used on Apple MacBooks, incorrectly identify it and refuse to provide power. Tom's Hardware tested 14 different cables and found that 11 of them turned on and powered the Pi without issue. The design flaw was fixed in revision 1.2 of the board, released in late 2019.

The early designs of the Raspberry Pi Model A and B boards included only 256 MiB of random access memory (RAM). The early beta Model B boards allocated 128 MiB to the GPU by default, leaving only 128 MiB for the CPU. On the early 256 MiB releases of models A and B, three different splits were possible. The default split was 192 MiB for the CPU, which should be sufficient for standalone 1080p video decoding, or for simple 3D processing. 224 MiB was for Linux processing only, with only a 1080p framebuffer, and was likely to fail for any video or 3D. 128 MiB was for heavy 3D processing, possibly also with video decoding.In comparison, the Nokia 701 uses 128 MiB for the Broadcom VideoCore IV.

The Raspberry Pi 2 has 1 GiB of RAM. The Raspberry Pi 3 has 1 GiB of RAM in the B and B+ models, and 512 MiB of RAM in the A+ model. The Raspberry Pi Zero and Zero W have 512 MiB of RAM. The Raspberry Pi 4 is available with 2, 4 or 8 GiB of RAM. A 1GiB model was originally available at launch in June 2019 but was discontinued in March 2020, and the 8 GiB model was introduced in May 2020.

None of the Raspberry Pi models have a built-in real-time clock. When booting, the time is either set manually or configured from a state previously saved at shutdown to provide relative consistency for the file system. The Network Time Protocol is used to update the system time when connected to a network. The Raspberry Pi Foundation provides Raspberry Pi OS (formerly called Raspbian), a Debian-based (32-bit) Linux distribution for download, as well as third-party Ubuntu, Windows 10 IoT Core, RISC OS, and specialised media centre distributions.It promotes Python and Scratch as the main programming languages, with support for many other languages.The default firmware is closed source, while an unofficial open source is available.Many other operating systems can also run on the Raspberry Pi. Third-party operating systems available via the official website include Ubuntu MATE, Windows 10 IoT Core, RISC OS and specialised distributions for the Kodi media centre and classroom management.The formally verified microkernel seL4 is also supported.

2.1.3. ESP8266

The ESP8266 is low-cost Wi-Fi microchip, with a full TCP/IP stack and microcontroller capability, produced by Espressif Systems in Shanghai, China. The chip first came to the attention of Western makers in August 2014 with the ESP-01 module, made by a third-party manufacturer Ai-Thinker. This small module allows microcontrollers to connect to a Wi-Fi network and make simple TCP/IP connections using Hayes-style commands. However, at first there was almost no English-language documentation on the chip and the commands it accepted. The very low price and the fact that there were very few external components on the module, which suggested that it could eventually be very inexpensive in volume, attracted many hackers to explore the module, the chip, and the software on it, as well as to translate the Chinese documentation. ESP8266 is a 3V WiFi module very popular for its Internet of Things applications ESP 8266 maximum working Voltage is 3.6V and its very important to note. The user must know how to power it, how to serial-connect it safely, how to ping and many other things.ESP8266 has eight pins such as

* RX
* VCC
* GPIO 0
* RESET
* CH\_PD
* GPIO 2
* TX
* and GND

VCC and GND are powering pins. RX and TX are used to communicate. There are many ways to power ESP8266 WiFi module: the user can use 2 AA sized batteries for powering, PC port if the user has a TTL-Serial-to-USB adapter (Don't try to connect the module to a PC serial port directly, the user could cause damage to the module or to the computer!). The user can use LIPO batteries to power the ESP Dev Thing board. The user can use LM117 3.3V voltage regulator. The ESP8266’s maximum voltage is 3.6V, so the thing has an onboard 3.3V regulator to deliver a safe, consistent voltage to the IC. That means the ESP8266’s I/O pins also run at 3.3V, so it will need to Logic Level Controller any 5V signals running into the IC.

2.1.4. Breadboard

A breadboard is a construction base for prototyping of electronics. Originally the word referred to a literal bread board, a polished piece of wood used for slicing bread. In the 1970s the solder less breadboard (a.k.a. plug board, a terminal array board) became available and nowadays the term "breadboard" is commonly used to refer to these. Because the solder less breadboard does not require soldering, it is reusable. This makes it easy to use for creating temporary prototypes and experimenting with circuit design. For this reason, solder less breadboards are also popular with students and in technological education. Older breadboard types did not have this property. A strip board (Vero board) and similar prototyping printed circuit boards, which are used to build semi-permanent soldered prototypes or one-offs, cannot easily be reused. A variety of electronic systems may be prototyped by using breadboards, from small analog and digital circuits to complete central processing units (CPUs Breadboards have evolved over time, with the term now being used for all kinds of prototype electronic devices. For example, US Patent 3,145,483,was filed in 1961 and describes a wooden plate breadboard with mounted springs and other facilities US Patent 3,496,419,was filed in 1967 and refers to a particular printed circuit board layout as a Printed Circuit Breadboard. Both examples refer to and describe other types of breadboards as prior art. The breadboard most commonly used today is usually made of white plastic and is a pluggable (solder less) breadboard. It was designed by Ronald J. Portugal in 1971.

A modern solder less breadboard socket consists of a perforated block of plastic with numerous tin plated phosphor bronze or nickel silver alloy spring clips under the perforations. The clips are often called tie points or contact points. The number of tie points is often given in the specification of the breadboard.

The spacing between the clips (lead pitch) is typically 0.1 inches (2.54 mm). Integrated circuits (ICs) in dual in-line packages (DIPs) can be inserted to straddle the centerline of the block Interconnecting wires and the leads of discrete components (such as capacitors, resistors, and inductors) can be inserted into the remaining free holes to complete the circuit. Where ICs are not used, discrete components and connecting wires may use any of the holes. Typically the spring clips are rated for 1 ampere at 5 volts and 0.333 amperes at 15 volts (5 watts). The edge of the board has male and female dovetail notches so boards can be clipped together to form a large breadboard.

Solder less breadboards connect pin to pin by metal strips inside the breadboard. The layout of a typical solder less breadboard is made up from two types of areas, called strips. Strips consist of interconnected electrical terminals.

In the middle of a terminal strip of a breadboard, one typically finds a notch running in parallel to the long side The notch is to mark the centerline of the terminal strip and provides limited airflow (cooling) to DIP ICs straddling the centerline[citation needed. The clips on the right and left of the notch are each connected in a radial way; typically five clips (i.e., beneath five holes) in a row on each side of the notch are electrically connected. The five columns on the left of the notch are often marked as A, B, C, D, and E, while the ones on the right are marked F, G, H, I and J. When a "skinny" dual in-line pin package (DIP) integrated circuit (such as a typical DIP-14 or DIP-16, which have a 0.3-inch (7.6 mm) separation between the pin rows) is plugged into a breadboard, the pins of one side of the chip are supposed to go into column E while the pins of the other side go into column F on the other side of the notch. The rows are identified by numbers from 1 to as many the breadboard design goes. Most of the breadboards are designed to accommodate 17, 30 or 64 rows in the mini, half, and full configurations respectively.

A bus strip usually contains two columns: one for ground and one for a supply voltage. However, some breadboards only provide a single-column power distribution bus strip on each long side. Typically the row intended for a supply voltage is marked in red, while the row for ground is marked in blue or black. Some manufacturers connect all terminals in a column. Others just connect groups of, for example, 25 consecutive terminals in a column. The latter design provides a circuit designer with some more control over crosstalk (inductively coupled noise) on the power supply bus. Often the groups in a bus strip are indicated by gaps in the color marking.

A "full size" terminal breadboard strip typically consists of around 56 to 65 rows of connectors, each row containing the above-mentioned two sets of connected clips (A to E and F to J). Together with bus strips on each side this makes up a typical 784 to 910 tie point solder less breadboard. "Small size" strips typically come with around 30 rows. Miniature solder less breadboards as small as 17 rows (no bus strips, 170 tie points) can be found, but these are only suitable for small and simple designs.

2.1.5. Jumper Wires

A jump wire (also known as jumper wire, or jumper) is an electrical wire, or group of them in a cable, with a connector or pin at each end (or sometimes without them – simply "tinned"), which is normally used to interconnect the components of a breadboard or other prototype or test circuit, internally or with other equipment or components, without soldering Jumper wires are simply wires that have connector pins at each end, allowing them to be used to connect two points to each other without soldering. Jumper wires are typically used with breadboards and other prototyping tools in order to make it easy to change a circuit as needed. Fairly simple. In fact, it doesn’t get much more basic than jumper wires Individual jump wires are fitted by inserting their "end connectors" into the slots provided in a breadboard, the header connector of a circuit board, or a piece of test equipment There are different types of jumper wires. Some have the same type of electrical connector at both ends, while others have different connectors. Some common connectors are:

* Solid tips are used to connect on/with a breadboard or female header connector. The arrangement of the elements and ease of insertion on a breadboard allows increasing the mounting density of both components and jump wires without fear of short-circuits. The jump wires vary in size and color to distinguish the different working signals.
* Crocodile clips are used, among other applications, to temporarily bridge sensors, buttons and other elements of prototypes with components or equipment that have arbitrary connectors, wires, screw terminals, etc.
* Banana connectors are commonly used on test equipment for DC and low-frequency AC signals.
* Registered jack (RJnn) are commonly used in telephone (RJ11) and computer networking (RJ45).
* RCA connectors are often used for audio, low-resolution composite video signals, or other low-frequency applications requiring a shielded cable.
* RF connectors are used to carry radio frequency signals between circuits, test equipment, and antennas.
* RF jumper cable is a smaller and more bendable corrugated cable which is used to connect antennas and other components to network cabling. Jumpers are also used in base stations to connect antennas to radio units. Usually the most bendable jumper cable diameter is 1/2".

Though jumper wires come in a variety of colors, the colors don’t actually mean anything. This means that a red jumper wire is technically the same as a black one. But the colors can be used to your advantage in order to differentiate between types of connections, such as ground or power. While jumper wires are easy and inexpensive to purchase, it can also be a fun task to challenge students to make their own Doing so requires insulated wire and wire strippers. However, beware that it is important not to nick the wire when stripping off the insulation

Jumper wires typically come in three versions: male-to-male, male-to-female and female-to-female. The difference between each is in the end point of the wire. Male ends have a pin protruding and can plug into things, while female ends do not and are used to plug things into. Male-to-male jumper wires are the most common and what you likely will use most often. When connecting two ports on a breadboard, a male-to-male wire is what the user will need.

2.1.6. Push Button

A push-button (also spelled pushbutton) or simply button is a simple switch mechanism to control some aspect of a machine or a process Buttons are typically made out of hard material, usually plastic or metal. The surface is usually flat or shaped to accommodate the human finger or hand, so as to be easily depressed or pushed Buttons are most often biased switches, although many un-biased buttons (due to their physical nature) still require a spring to return to their un-pushed state Terms for the "pushing" of a button include pressing, depressing, mashing, slapping, hitting, and punching.

The "push-button" has been utilized in calculators, push-button telephones, kitchen appliances, and various other mechanical and electronic devices, home and commercial. In industrial and commercial applications, push buttons can be connected together by a mechanical linkage so that the act of pushing one button causes the other button to be released. In this way, a stop button can "force" a start button to be released. This method of linkage is used in simple manual operations in which the machine or process has no electrical circuits for control.

Red pushbuttons can also have large heads (called mushroom heads) for easy operation and to facilitate the stopping of a machine. These pushbuttons are called emergency stop buttons and for increased safety are mandated by the electrical code in many jurisdictions. This large mushroom shape can also be found in buttons for use with operators who need to wear gloves for their work and could not actuate a regular flush-mounted push button.

Button shaped as an octagon. As an aid for operators and users in industrial or commercial applications, a pilot light is commonly added to draw the attention of the user and to provide feedback if the button is pushed. Typically this light is included into the center of the pushbutton and a lens replaces the pushbutton hard center disk. The source of the energy to illuminate the light is not directly tied to the contacts on the back of the pushbutton but to the action the pushbutton controls. In this way a start button when pushed will cause the process or machine operation to be started and a secondary contact designed into the operation or process will close to turn on the pilot light and signify the action of pushing the button caused the resultant process or action to start. To avoid an operator from pushing the wrong button in error, pushbuttons are often color-coded to associate them with their function. Commonly used colors are red for stopping the machine or process and green for starting the machine or process.A broad subset of ANSI SQL 99,as well as extensions.

In popular culture, the phrase "the button" (sometimes capitalized) refers to a (usually fictional) button that a military or government leader could press to launch nuclear weapons. Akin to fire alarm switches, some big red buttons, when deployed with suitable visual and audible warnings such as flashing lights and sirens for extreme exigent emergencies, are known as "scram switches" (from the slang term scram, "get out of here"). Generally, such buttons are connected to large scale functions, beyond a regular fire alarm, such as automated shutdown procedures, complete facility power cut, fire suppression like halon release, etc.A variant of this is the scramble switch which triggers an alarm to activate emergent personnel to proactively attend to and go to such disasters. An air raid siren at an air base initiates such action, where the fighter pilots are alerted and "scrambled" to their planes to defend the base.

2.1.7. IoT Protocols

A Protocol is a set of rules that use for specific purposes. To successfully send and receive information, devices on both sides of a communication exchange must accept and follow protocol conventions. Standardized network protocols provide a common language for network devices. Without them, computers wouldn't know how to engage with each other. As a result, except for specialty networks built around a specific architecture, few networks would be able to function, and the internet as we know it wouldn't exist. Virtually all network end users rely on network protocols for connectivity. Network protocols break larger processes into discrete, narrowly defined functions and tasks across every level of the network. In the standard model, known as the Open Systems Interconnection (OSI) model, one or more network protocols govern activities at each layer in the telecommunication exchange.

IoT protocols are a crucial part of the IoT technology stack — without them, hardware would be rendered useless as the IoT protocols enable it to exchange data in a structured and meaningful way. Out of these transferred pieces of data, useful information can be extracted for the end user and thanks to it, the whole deployment becomes economically profitable. IoT communication protocols are modes of communication that protect and ensure optimum security to the data being exchanged between connected devices. The IoT devices are typically connected to the Internet via an IP (Internet Protocol) network. However, devices such as Bluetooth and RFID allow IoT devices to connect locally. Connection through IP networks are comparatively complex, requires increased memory and power from the IoT devices while the range is not a problem. On the other hand, non-IP networks demand comparatively less power and memory but have a range limitation.The internet of things protocols can be divided into two basic types: IoT Network Protocols and IoT Data Protocols. IoT protocols and standards can be broadly classified into two separate categories.

2.1.7.1. IoT Network Protocols

IoT network protocols are used to connect devices over the network. These are the set of communication protocols typically used over the Internet. Using IoT network protocols, end-to-end data communication within the scope of the network is allowed. Followings are the various IoT Network protocols:

* HTTP (HyperText Transfer Protocol) - HyperText Transfer Protocol is the best example of IoT network protocol. This protocol has formed the foundation of data communication over the web. It is the most common protocol that is used for IoT devices when there is a lot of data to be published. However, the HTTP protocol is not preferred because of its cost, battery-life, energy saving, and more constraints. Additive manufacturing/3D printing is one of the use cases of the HTTP protocol. It enables computers to connect 3D printers in the network and print three-dimensional objects and pre-determined process prototypes.
* LoRaWan (Long Range Wide Area Network) - LoRaWAN or the Long Ranged Wide Area Network is one of the IoT Protocols for the wide area networks. LoRaWAN IoT Network Protocols is specifically designed for supporting the vast networks with the help of million low-power devices. Smart cities use this kind of protocol.It is a long-range low power protocol that provides signal detection below the noise level. LoRaWan connects battery operated things wirelessly to the Internet in either private or global networks. This communication protocol is mainly used by smart cities, where there are millions of devices that function with less power and memory. Smart street lighting is the practical use case of LoRaWan IoT protocol. The data rates of this Internet of Things Protocols runs between 0.3-50 kbps. In the urban areas, the range LoRaWAN varies from 2 km to 5 km. In the suburban areas, the range of this IoT protocol is about 15 km.
* Bluetooth - Bluetooth is one of the most widely used protocols for short-range communication. It is a standard IoT protocol for wireless data transmission. This communication protocol is secure and perfect for short-range, low-power, low-cost, and wireless transmission between electronic devices. BLE (Bluetooth Low Energy) is a low-energy version of Bluetooth protocol that reduces the power consumption and plays an important role in connecting IoT devices. Bluetooth protocol is mostly used in smart wearables, smartphones, and other mobile devices, where small fragments of data can be exchanged without high power and memory. Offering ease of usage, Bluetooth tops the list of IoT device connectivity protocols. One of the most broadly used wireless technologies of short-range is Bluetooth.
* Wi-Fi - For IoT integration, Wi-Fi is a favored choice according to many electronic designers. It is because of the infrastructure it bears. It has quick data transfer rates along with the aptitude to control a large quantity of data. The widespread WiFi standard 802.11 presents you the ability to transfer hundreds of megabits in only one second. The only own drawback of this IoT protocol is it can consume excessive power for some of the IoT Application. It ranges approximately 50 m, and along with working on internet protocol standards, it includes IoT Cloud infrastructure access. The frequencies are 2.4GHz and 5GHz bands.
* ZigBee - ZigBee is an IoT protocol that allows smart objects to work together. It is commonly used in home automation. More famous for industrial settings, ZigBee is used with apps that support low-rate data transfer between short distances. ZigBee and the popular ZigBee Remote Control are popular as famed IoT Security Protocols for supplying secure, low-power, scalable solutions along with high node counts. The ZigBee 3.0 has taken the protocol to a single standard. It made it handier. ZigBee is easy to install and maintain because it is based on self-assembly and self-healing grid topology. It also easily scales to thousands of nodes, and nowadays there are many suppliers offering devices that support this open standard. ZigBee-based networks are characterized by low power consumption, low throughputs (up to 250 kbps) and connectivity range of 100 meters between nodes. Typical applications include sensor networks, personal networks (WPAN), home automation, alarm systems and monitoring systems. Street lighting and electric meters in urban areas, which provides low power consumption, use the ZigBee communication protocol. It is also used with security systems and in smart homes. Just like Bluetooth, there is a vast user base of ZigBee. Among the internet of things protocols, ZigBee is designed more for the industrials and less for the consumers. It usually operates at a frequency of 2.4GHz. This is ideal for the industrial sites where data is generally transferred over small rates amongst home or a building.

2.1.7.2. IoT Data Protocols

IoT data protocols are used to connect low power IoT devices. These protocols provide point-to-point communication with the hardware at the user side without any Internet connection. Connectivity in IoT data protocols is through a wired or a cellular network. Some of the IoT data protocols are:

* Message Queue Telemetry Transport (MQTT) - One of the most preferred protocols for IoT devices, MQTT collects data from various electronic devices and supports remote device monitoring. It is a subscribe/publish protocol that runs over Transmission Control Protocol (TCP), which means it supports event-driven message exchange through wireless networks. MQTT is mainly used in devices which are economical and requires less power and memory. For instance, fire detectors, car sensors, smart watches, and apps for text-based messaging. It works on top of the TCP for supplying reliable yet simple streams of data. This MQTT protocol is made of three core components or mechanisms: Subscriber, Publisher, and Broker.
* Constrained Application Protocol (CoAP) - CoAP is an internet-utility protocol for restricted gadgets. Using this protocol, the client can send a request to the server and the server can send back the response to the client in HTTP. For light-weight implementation, it makes use of UDP (User Datagram Protocol) and reduces space usage. The protocol uses binary data format EXL (Efficient XML Interchanges). The CoAP or Constrained Application Protocol, an internet productivity and utility protocol, is mainly developed for the restricted smart gadgets. The design of CoAP is for using it among the devices that have an identical restricted community. It includes general nodes and devices on the internet and different restrained networks and devices that are joined on the internet. CoAP protocol is used mainly in automation, mobiles, and microcontrollers. The protocol sends a request to the application endpoints such as appliances at homes and sends back the response of services and resources in the application. IoT systems based on the HTTP protocols can go tremendously with CoAP IoT Network Protocols. It uses the protocol-UDP for implementation of lightweight data. Just like the HTTP, it also uses the restful architecture. It is also used inside the mobiles and the other social communities that are basic programs. CoAP helps in getting rid of ambiguity through HTTP get, put up, delete and placed strategies.
* Advanced Message Queuing Protocol (AMQP) - AMQP is a software layer protocol for message-oriented middleware environment that provides routing and queuing. It is used for reliable point-to-point connection and supports the seamless and secure exchange of data between the connected devices and the cloud. AMQP consists of three separate components namely Exchange, Message Queue, and Binding. All these three components ensure a secure and successful exchange and storage of messages. It also helps in establishing the relationship of one message with the other. Advanced Message Queuing Protocol or AMQP is an application layer protocol. It is basically message oriented and designed for middleware environments. The AMQP IoT messaging protocols got the approval as an international standard. The processing chain of AMQP IoT Protocol consists of 3 necessary components, and those are Exchange, Message Queue and Binding.
* Machine-to-Machine (M2M) Communication Protocol - It is an open industry protocol built to provide remote application management of IoT devices. M2M communication protocols are cost-effective and use public networks. It creates an environment where two machines communicate and exchange data. This protocol supports the self-monitoring of machines and allows the systems to adapt according to the changing environment.M2M communication protocols are used for smart homes, automated vehicle authentication, vending machines, and ATM machines.
* Extensible Messaging and Presence Protocol (XMPP) Developed in 1999 by the Jabber open source community and originally meant for real-time messaging, this communication IoT protocol for message-oriented middleware is based on the XML language. It allows for real-time exchange of structured but extensible data between two or more network clients. Among the drawbacks of using XMPP in IoT communication, it should be noted that it offers neither Quality of Service nor end-to-end encryption. Due to these limitations, among others, it is predicted that its application within IoT will stay loosely connected to the industry, as the protocol definitely won’t become a standard used day-in day-out for the purposes of data exchange and management of resource-constrained devices, just as MQTT or LwM2M are. The XMPP is uniquely designed. It uses a push mechanism to exchange messages in real-time. XMPP is flexible and can integrate with the changes seamlessly. Developed using open XML (Extensible Markup Language), XMPP works as a presence indicator showing the availability status of the servers or devices transmitting or receiving messages. Other than the instant messaging apps such as Google Talk and WhatsApp, XMPP is also used in online gaming, news websites, and Voice over Internet Protocol (VoIP).
* DDS - The Data Distribution Service–DDA is developed and designed by OMG or Object Management Group. With the help of DDS, you can transfer data both in the low-footprint devices and with the Cloud platforms. The Data Distribution Service includes two significant layers. Those are the DCPS and the DLRL. The DCPS or Data-Centric Publish-Subscribe works by delivering information to the subscribers. The DLRL or Data-Local Reconstruction Layer does its job by providing an interface to the Data-Centric Public-Subscribe functionalities. Amongst the internet of things protocols, the IoT Messaging Protocols: DDS or Data Distribution Service is standard for high performance, expandable and real-time machine-to-machine communication.
* NFC - NFC from the IoT Protocols takes the benefit of safe two-way communication linking. Recently,we saw that NFC IoT Communication Protocols are applicable for the smartphones. The NFC or Near Field Communication allows the clients to connect to the electronic devices, to use digital contents and to do the contactless payment transaction. The essential work of NFC is to expand the“contactless” card technology. It works within 4cm (between devices) by enabling the devices for sharing information.
* Cellular - There are a lot of IoT applications that may call for operation over a longer remoteness. These IoT applications can take the help of Cellular communication capabilities like GSM/3G/4G. Cellular is one of the IoT Communication Protocols which can send or transfer a high amount of data. Here, you have to remember is the cost. The fee for sending a high quantity of data will be high too. Cellular does need not only high cost but also to need high power consumption for several applications. This Internet of Things Protocol is amazing for sensor-based data projects of low-bandwidth. This is because they can send a very insignificant amount of data or information on the Internet.
* Thread - One of the most recent internet of things protocols that have come in the scene is IoT security protocols Thread. The inventor of Next has designed this protocol. In the home automation application, this IoT Protocol is now ramping up its usage. This is an IP-based IPv6 networking protocol, and it is based on the 6LowPAN. It was chiefly designed for complimenting WiFi inside the home. This protocol is royalty-free. This protocol supports the mesh networking within radio transceivers of IEEE802.15.4. It can handle about 250 nodes along with encryption and authentication. The frequency of Thread IoT Protocol is 2.4GHz (ISM), and it can cover up to 10-30m.