INTERNET OF THINGS

Author: Abinayasree C

Masters of computer Application’s

St. Francis College

Bangalore, India

abinayasree211@gmail.com

  **ABSTRACT**

The term "Internet of Things" (IOT) refers to a particular type of network that uses the internet to connect numerous devices. IOT helps with device-to-device data transmission, device tracking and monitoring, and other things. By enabling data transmission and task automation without physical intervention, IOT makes objects "smart." One easy, everyday application of IOT in our lives is a wearable health monitoring gadget. A smart city is one that has sensors in every area, uses a variety of physical devices and things around the neighborhood, and is connected to the internet. Kevin Ashton first proposed the term IOT in 1999. The next section illustrates the basics of IOT. It disburses a number coverage used in IOT and many basic denominations connected. It is largely an expansion of online assistance. IOT can be used to automate homes, offices, or other units when household equipment are connected to the internet. IOT is being utilized for contact tracing during the COVID-19 pandemic.

**I.INTRODUCTION**

 The term "internet of things" refers to a technology that enables physical items or things to connect with one another over the internet. Things categorized as identifiable communication devices served as the foundation for the internet of things. IOne type of identity communication device is a radio frequency identification device (RFID). Things are attached to these devices in order to identify them in the future, and remote computers connected to the internet can track, control, and monitor them.

In order to monitor, coordinate, or control a process across the internet or another data network, a network of physical things (objects) must send, receive, or communicate information using the internet or other communication technologies and network, just like computers, tablets, and mobile phones do.

**II.APPLICATIONS OF IOT**

IoT applications significantly improve our lives. Without the need for human-to-human or human-to-computer interaction, the Internet of Things enables items, computing equipment, or unique identities and individuals to transport data across a network.

The applications of the internet of things are found in many different fields, such as (but not limited to) home, cities, environment, energy systems, retail, logistics, industry, agriculture, and health.

Wearables: One of the first businesses to adopt IoT was the wearable technology sector, which is the defining feature of IoT applications. These days, we have smartwatches, fitbits, and heart rate monitors.

To assist diabetics, the Guardian glucose monitoring device has been created. It connects a radiofrequency monitoring device to a tiny electrode known as the glucose sensor to measure the levels of glucose in our bodies.

Smart home applications: When discussing IoT applications, the smart home is likely the first thing that comes to mind. As an example, Mark Zuckerberg uses AI to automate his home. The home automation system invented by Alan Pan employs built-in capabilities to play a series of musical notes.

Health care: Reactive medical-based systems can become proactive wellness-based systems with the help of IoT technologies. Resources used in current medical research lack crucial information from the real world. For clinical studies, it makes use of controlled surroundings, old data, and volunteers. The power, accuracy, and availability of the gadget are all improved through the Internet of Things. IoT concentrates on creating systems as opposed to merely tools. This is how the IoT-enabled medical equipment functions

Smart cities: The majority of you are familiar with the term "smart city." Technology is used in smart cities to deliver services. The smart city comprises enhancing social services and transportation, encouraging stability, and providing inhabitants a voice.

Mumbai's issues are considerably dissimilar from Delhi's. Even global problems like access to clean water, deteriorating air quality, and rising urban density exist in cities of various intensities. Thus, they have an impact on all cities.

The Internet of Things is used by engineers and governments to evaluate the intricate components of each metropolis. IoT applications support waste management, emergency preparedness, and water management.

Agriculture: The world's population is predicted to increase to roughly 10 billion people by the year 2050. Agriculture must successfully integrate technology to feed such a vast population. There are numerous options in this regard. The Smart Greenhouse is one of them.

Crops are grown via farming methods according to environmental factors. However, manual handling is less efficient since it incurs personnel expenses, energy losses, and production losses.

**III.TYPES OF IOT NETWORKS**

**Cellular**

Cellular networks, the same mobile networks used by smartphones, may be utilized by IoT devices to communicate. Due to the fact that these networks were first developed for power-hungry devices like smartphones, they weren't always regarded as the best choice for IoT devices. Later, new technologies developed by the cellular industry were more suited for Internet of Things use cases. This type of wireless network is popular nowadays and is regarded as a reliable and secure method of IoT connection. Cellular service is available in most parts of the country, and this type of network has a wide coverage area. Cell coverage is usually absent in the areas where monitoring sensors are most important, such as in utility closets, elevator shafts, basements, etc.

**Wifi**

WiFi is a common option for IoT networks because many businesses already have WiFi coverage throughout their infrastructure. WiFi is a dependable option for stationary IoT sensors that must transmit data over a medium distance. WiFi administrators could group IoT sensors on a separate subnet and use quality of service to help and increase the dependability of their sensors. IoT WIFI networks do, however, have some drawbacks. Due to their power limitations, WiFi networks don't have the same level of coverage as cellular networks. Since WiFi networks don't manage device handover as efficiently as cellular networks do, mobile IoT sensors may experience connection issues on WiFi networks.

**Local And Personal Area Networks(LAN/PAN)**

Local area networks (LAN) and personal area networks (PAN) are examples of networks that only cover comparatively short distances. Although it is frequently believed that data transit across PAN and LAN networks is cost-effective, it is not always dependable. IoT connectivity solutions frequently employ the wireless personal and local area network technologies WiFi and Bluetooth. WiFi can be used for remote applications in addition to local ones when many access points are integrated into a larger network. When using Bluetooth Low Energy (BLE), a single battery may last up to five years if the device is not constantly receiving data. BLE is a wireless network standard that uses less energy.

**Lower Power Wide Area Networks (LPWAN)**

LPWAN-enabled IoT devices rarely and infrequently send little data packets across long distances. The early problems with cellular communication led to the development of this type of wireless network. Compared to WiFi and Bluetooth, LPWAN is advertised as having a better range and using less power. In this category, LoRaWAN, which runs on the LoRa (long-range) communication network, is a well-known and popular IoT network protocol. IoT devices benefit from LoRaWAN's lower power requirements (for longer battery life) and reasonably priced chipsets. Under the correct conditions, a single base station or gateway running on a long-range network is capable of providing service to a very large area—a few kilometers in crowded metropolitan regions.

**Mesh Networks**

Mesh networks can best be described by their connection configuration, or how its components interact with one another. To ensure that data reaches the gateway in mesh networks, all sensor nodes cooperate to share information among themselves. The Zigbee wireless network technology is an example of an IoT. In order to get the coverage you require for your application because mesh networks have a very short range, you might need to place more sensors throughout a building or use repeaters. Additionally, the nature of how these networks interact can result in excessive power consumption, particularly if you need quick communications, as in the case of an application for intelligent lighting. Mesh networks are a common option because they are also incredibly resilient, skilled at finding the data transmission pathways that are both quicks and reliable, and simple to set up.

**IV.FEATURES OF IOT**

The key IoT components that it relies on include connectivity, analysis, integration, active engagement, and many others. Following is a list of some of them:

**Connectivity:** Connectivity is the establishment of a secure link between all IoT devices and IoT platforms, which might be server or cloud-based. To enable dependable, secure, and bidirectional communication when the IoT devices are connected, high-speed messaging is required between the devices and cloud.

**Analysing:** After tying everything together, it's time to analyze the data in real-time and apply it to create efficient business intelligence. We refer to our system as having a smart system if we have good insight into the data obtained from all of these sources.

**Integrating:** The Internet of Things (IoT) integrates the numerous models to enhance user experience as well.

**Artificial intelligence:** IoT uses data to make things smarter and improve life. For instance, if we have a coffee maker whose beans are about to run out, the maker will order the desired coffee beans from the retailer.

**Sensing:** The sensor devices used in IoT technologies track any environmental changes, measure them, and provide status updates. With the aid of IoT technology, inactive networks become active networks. A true or functional IoT environment cannot exist without sensors.

**Active Engagement:** IoT enables active engagement between connected technologies, goods, or services.

 **V.LAYERS OF IOT**

**Layer 1: Physical Devices and Controllers Layer**

The physical devices and controllers layer is the top layer of the IoT Reference Model. The many endpoint devices and sensors that transmit and receive information reside in this layer, which is home to the "things" of the Internet of Things. These "things" come in a variety of sizes, from almost tiny sensors to enormous factory machinery. Their main job is to produce data and have network access to be queried and/or managed.

**Layer 2: Connectivity Layer**

The IoT Reference Model's second layer focuses on connectivity. The timely and reliable conveyance of data is this IoT layer's most crucial function. This covers communications between Layer 1 devices and the network as well as between the network and Layer 3 (the edge computing layer) information processing.As you may have noticed, the connectivity layer includes all networking components of the Internet of Things (IoT) and doesn't really distinguish between the backhaul, gateway, or last-mile networks (the network between a sensor or endpoint and the IoT gateway, detailed later in this chapter).

**Layer 3: Edge Computing Layer**

The function of Layer 3 is edge computing. Edge computing, sometimes known as the "fog" layer, is covered in the section "Fog Computing," which is found later in this chapter. Data reduction and turning network data flows into information that is prepared for storage and processing by higher layers are the main focuses at this layer. This reference model's fundamental tenet is that information processing is started.

The review of data to see if it can be filtered or aggregated before being delivered to a higher layer is another significant function that takes place at Layer 3. Additionally, this enables data to be reformatted or decoded, simplifying further processing by other systems. Assessing the data to see whether predefined criteria are crossed and whether any action or warnings are required is thus a crucial job.

**VI.M2M COMMUNICATION**

The term "machine-to-machine communication," or M2M, refers to two machines exchanging data or "communicating," without the use of a human interface or other human contact. This covers wireless communications in the industrial Internet of Things (IoT), powerline connections (PLC), and serial connections. By moving to wireless, M2M communication has become considerably simpler, and more applications can now be connected.

In general, cellular communication for embedded devices is often meant when someone mentions M2M communication. In this instance, M2M communication examples include vending machines transmitting inventory data or ATMs receiving authorization to disburse cash.

The Internet of Things (IoT) is the new moniker for M2M as corporations have come to understand its significance. IoT and M2M both promise to significantly alter how society functions. Similar to IoT, M2M enables almost any sensor to communicate, opening the door to systems monitoring themselves and automatically reacting to environmental changes with a significantly decreased requirement for human involvement. The difference between M2M and IoT is that M2M can refer to any two machines—wired or wireless—communicating with one another. IoT, the more recent term, primarily refers to wireless communications.

M2M has traditionally concentrated on "industrial telematics," which is a fancy term for data transfer for some kind of economic gain. But many of the initial M2M applications, such as smart meters, are still relevant today. Since the introduction of 2G cellular networks in the middle of the 2000s, cellular has dominated wireless M2M. Due to this, the cellular industry has attempted to position M2M as something that is intrinsically cellular by providing M2M data plans. However, cellular M2M shouldn't be viewed as a cellular-only niche because it is merely one segment of the business.

**How M2M Works**

The Internet of Things is made possible through machine-to-machine connectivity, as was previously mentioned. Forbes claims that M2M technologies, which allow for the connection of millions of devices within a single network, are among the connected device technologies that are now experiencing the highest market growth. Anything from vending machines to medical equipment to vehicles to structures is included in the variety of connected devices. Any object that contains sensor or control technologies can be linked to a wireless network.

The underlying principle of this may seem complicated, but it is actually fairly straightforward. M2M networks are essentially LAN or WAN networks with the exception that they are only utilized to support machine, sensor, and control communication. These devices transmit the data they gather to other network nodes. Through this procedure, a person (or intelligent control unit) is able to evaluate the state of the entire network and give the relevant orders to participating devices.

**VII.M2M APPLICATIONS**

Four key use examples, which we've outlined below, highlight the potential of M2M:

**Manufacturing:** Every manufacturing environment, whether it be for the production of food or other goods, depends on technology to ensure that costs are controlled and operations are carried out effectively. It is anticipated that automating production operations in this fast-paced environment would enhance processes even further. This can entail highly automated equipment maintenance and safety processes in the manufacturing sector.

M2M solutions, for instance, enable business owners to receive alerts on their cellphones when a crucial piece of equipment requires maintenance so they can take care of problems as soon as they appear. Even replacement components might be automatically ordered through sophisticated networks of sensors that are connected to the Internet.

**Home appliances:** Through platforms like Nest, IoT already has an impact on the connectivity of home appliances. M2M is anticipated to advance home-based IoT, though. Smart home gadgets are already being steadily released by manufacturers like LG and Samsung to assist assure a greater standard of living for residents.

For instance, a smart refrigerator could automatically order goods from Amazon once its stock is low, and an M2M-capable washing machine may alert the owners' smart devices once it has finished washing or drying. There are numerous other examples of home automation that may enhance inhabitants' quality of life, such as programs that let family members utilize mobile devices to remotely regulate HVAC systems. If a homeowner chooses to leave work earlier than planned, he or she could call the heating system to ensure that the temperature at home would be cozy when they get there.

**The value of M2M**

There has been considerable growth in the M2M and IoT businesses, and many reports predict that this will continue. Low power, wide-area network (LPWAN) connections are expected to increase from 11 million in 2014 to 5 billion in 2022, according to Strategy Analytics.

The market for global IoT solutions, according to IDC, will grow from $1.9 trillion in 2013 to $7.1 trillion in 2020.

Numerous major cellular providers, including AT&T and Verizon, are launching their own M2M systems in response to this potential. All three companies—Intel, PTC, and Wipro—are investing extensively in M2M marketing in an effort to profit from this significant industry development. However, there is still a huge opportunity for startups in the technology sector to develop highly automated solutions that will assist streamline operations in almost any sector. In the next five years, there will undoubtedly be a massive flood of businesses starting to develop in this field.

Companies must decide how they will add value for clients and other organizations as the cost of M2M communication declines. The possibilities and value for M2M, in our opinion, do not reside in the more conventional communication levels. For instance, cell carriers and hardware producers are starting to consider full-stack solutions that support M2M and IoT product development.

We really believe that value is found in the application side of things, and going forward, intelligent apps will be what propel this industry's growth.

IoT and M2M should not be considered by businesses merely for their own sake. Instead, they ought to concentrate on improving their business strategies or giving their clients new benefits. For instance, if you own a logistics business like FedEx or UPS, you can choose from a number of obvious automated logistics options. However, if you work in retail, the shift toward automation might not be as clear. It's one thing to imagine a "cool" automated process—for example, using M2M technology to automatically link advertising to a particular customer—but you must first think about the value you will derive from it before moving further. What is the cost of implementation? Any organization thinking about entering the IoT market must comprehend its business strategy, how it will generate revenue, and how it will add value to clients or internal operations.

**VIII.CONCLUSION**

The internet of things creates a new world where anything can be connected and identified. It has the capacity to communicate and decide for themselves. The major drivers of traffic will be things. The internet of things has benefits for people's lives. IOT has the power to significantly alter human life. However, these significant issues must be solved to facilitate and hasten the implementation of this technology across industries. As consumers accept this technology and we grow closer to a completely linked world, the next wave of disruptive innovation will inevitably occur in this technology field.

The Internet of Things is at a point where several networks and sensors must unite and work together in accordance with a shared set of standards. Businesses, governments, standards bodies, and academia will need to collaborate on this initiative in order to achieve success. IoT is the next step in the development of the Internet.

**IX.REFERENCES**

[1] Arshdeep Bahga and Vijay Madisetti.”From Applications of IoT to Types of IoT Networks” Internet of Things.

[2] The Internet of Things – “From features of IoT to Layers of IoT”, Olivier Hersent, David

Boswarthick, Omar Elloumi and Wiley, 2012 (for Unit2).

[3]. “From Machine-to-Machine to the Machine-to-applications”– Introduction to a New Age

of Intelligence”,Jan Ho¨ ller, VlasiosTsiatsis, Catherine Mulligan, Stamatis,

Karnouskos, Stefan Avesand. David Boyle and Elsevier, 2014.