International Journal of Engineering, Management and Humanities (IJEMH)
Volume 4, Issue 3, May-June, 2023 pp: 24-34 www.ijemh.com

"Study On Internet Of Things (IoT): ITS Evolution, Applications And Challenges"

DEEKSHITHA RAMI REDDY
BACHELOR's IN COMPUTER APPLICATION
2021-2024

Date of Submission: 25-04-2023 Date of Acceptance: 05-05-2023

Abstract
Internet is a revolutionary invention that is known for making our lives easier. One such technology that has contributed to the same is the Internet of Things. The Internet of Things (IoT) is an emerging model that has resulted for a change from the traditional method of living to a highly technological lifestyle. Few of such transformations include smart meters, digital locks, connected vehicles, smart homes and smart factories, etc. There is a lot of technological research that is being conducted to enhance the efficiency of this new paradigm i.e. Internet of things. This paper provides an overview of how this technology has emerged along with the standard architecture consisting of 4 layers. It also discusses the applications of IoT in three main fields namely Healthcare, Agriculture and Vehicles. This technology has a lot of advantages to make our lives easier. In spite of that, there are still a lot of challenges and issues associated with it which we need to overcome in order to make sure that the Internet of Things (IoT) works at its full potential. This paper highlights few such challenges that are associated with the Internet of things.

I. Introduction

The term "Internet of Things" has been existing for 16 years till now. However, the actual concept of connected devices had existed since at least the 1970s. At the time, the concept was frequently referred to as "pervasive computing" or "embedded internet." However, Kevin Ashton invented the term "Internet of Things" in 1999 while working at Procter & Gamble.

Internet of Things is a network of responsible devices and everyday objects that are connected via the internet for achieving a defined purpose .They are embedded with sensors, software and more that enable them to collect and exchange information without human-to-human interaction or human-to-computer interaction. It is one of the most exciting and dynamic development in the communication and information technology. Internet of Things (IoT) can include any natural or manmade object that is given an IP address to be identified in a network and also to be able to transfer data over a network.

Let us look into the main components of IoT:-

i) Low power embedded systems:-The inverse factors that play a significant role in the design of electronic systems are low battery consumption and high performance.

ii) Availability of big data; - We are aware that sensors play a significant role in IoT, particularly in real-time. The use of these electronic devices will result in a huge flow of big data as they are spread across all fields.

iii) Sensors: - The most important part of any IoT application is the sensor. It is a physical device that converts a measured or detected physical quantity into a signal that can be used as an input to a control or processing unit for analysis.

iv) Networking connection: - Connectivity to the internet, where each physical object has an IP address, is very much necessary for communication. However, according to IP naming, only a finite number of addresses are available. This method of naming devices will no longer be practical due to the increasing number of devices. As a result, researchers are looking for a different way to name each physical object.

v) Control units: - It is a small computer unit with a microprocessor or processing core, memory, and programmable input/output devices or peripherals on a single integrated circuit. It performs all logical operations and is in charge of the majority of IoT device processing.

vi) Cloud computing: - The vast amount of data gathered by IoT devices must be stored on a

dependable storage server. Cloud computing comes into play in this situation. Because the data is processed and learned, we now have more room to find the locations of things like electrical errors and faults in the system.

The Internet of Things (IoT) is typically a network of Internet-connected physical devices or systems that can sense an environment and intelligently alter it. Typically, embedded processors with a small form factor and low power are used to accomplish this on internet-connected devices. In other words, the Internet of Things could be thought of as a collection of connected machines, tools, and devices; these things are made up of processors and sensors/actuators that connect wirelessly to the Internet. A different school of thought holds that wired internet access is a part of the IoT paradigm as well.

Emergence of the Internet of Things (IoT):-

The Internet of Things as we know it today is the result of a few decades' worth of technological paradigm shifts. The technologies that resulted as the foundation of associated systems by accomplishing simple coordination to day to day routines, enormous acceptance from the common people, and enormous advantages by utilizing connected solutions can be considered as the establishing solutions for the improvement of IoT. The sequence of the technological advancements towards the evolution of modern day IoT is represented below in detail:-

- **ATM: -** ATM or Automated Teller Machines connected online and came into existence for the first time in 1974. They are the distribution of machines of cash that are linked to the bank account of the user. Cash is dispensed from an ATM after a specially coded card is used to verify the user's identity and their account. The availability of financial transactions even when banks were closed beyond their normal business hours was the central idea behind ATMs. These ATMs were universal cash dispensers.

The contribution of IoT in case of an ATM is: -

Improving the ATM up - time : - Automated incident processing and resolution flow for preventative maintenance; graphical reports, maps, and inventory via a web-based GUI; Work with pattern examination; determining the reasons behind slow or unsuccessful customer transactions; minimizing service interruptions and maximizing ATM uptime at a cost-effective rate , Asset failure monitoring and alerts when a threshold is crossed.

Security includes the detection and notification of intruders, the prevention of cash theft, the repair of an ATM's customer panel from damage caused by skimming devices, and software attacks.

A bank can track its ATM network using IoT and analytics to help predict outages caused by cash shortages or maintenance issues.

Predictive analytics can offer suggestions for ATM maintenance and cash replenishment. The forecasts can point exact areas of ATMs, where activity needs to occur.

Optimizes the bank's cash stockpiling and planning at ATMs.

Investigating the recurrence of ATM use inside a specific region and focusing on unambiguous zones for ATM establishment where people walking through are most elevated.

- **Web: -** Also known as World Wide Web is a global platform for communicating and sharing information. In 1991, the web became operational for the first time. Since then, it has been largely responsible for numerous technological and communication revolutions.

IoT contributes to transformation in the Web by enhancing valued experiences and operational efficiencies. However, rather than fostering innovation, the early adopters use IoT to make money. The Web Services domain's scope was extended as a result of the developments. It gives many benefits to both application improvement and upkeep, for example, a very much organized application comprising of various administrations carrying out just a solitary part of the application. While creating programming for the installed space, one needed to manage equipment cooperation like reading a sensor.

Because they have access to so many technologies, web developers are better able to produce high-quality web applications in a short amount of time. The developers face a challenge as they try to decide which approach to take when developing a particular component of web applications in light of changing standards or approaches.

- **Smart meters: -** The IoT-enabled smart meter makes use of embedded system features, which are software and hardware in combination. It is the most effective method for integrating smart meters into its infrastructure. Utilizing smart meters, smart metering is a method of digitizing the energy system that enables businesses to track how much energy they use and adjust their consumption as necessary.

A smart digital meter is designed to take the place of the traditional gas and electricity meters. It tends to be outfitted with a presentation screen that shows the specific energy utilization continuously. By allowing you to control and reduce your energy use, installing a smart meter helps you get rid of estimated bills.

It has features that enable remote information collection and sending of meter readings to energy suppliers. Smart meters can be used to collect information about population, infrastructure, and public services in smart cities.

- **Digital locks: -** One of the earliest attempts at connected home automation systems can be digital locks. The Internet of Things has always pushed hard for smart home technology. Smart phones can be used to control modern digital locks because they are so robust. Using smart phones, it is simple to perform tasks like locking and unlocking doors, changing key codes, and adding new members to access lists. Although smart lock technology is still relatively new, many households are implementing it. Homeowners benefit from the peace of mind offered by a smart lock, and as the cost of smart locks decreases, this sense of security is increasingly appealing to those who have not yet adopted the Internet of Things.

- **Connected Healthcare:** - Remote monitoring in the healthcare industry has been made possible by Internet of Things (IoT)-enabled devices, allowing physicians to provide exceptional care and unleashing the potential to keep patients safe and healthy.

IoT for Patients: Wearable appliances such fitness bands and other wirelessly connected devices like cuffs for checking the heart rate and blood pressure, glucometers, and more to provide patients with individualized care. These devices can be set to remind you to count calories, check your exercise, remind you of appointments, and more.

IoT for Hospitals: Medical devices like wheelchairs, defibrillators, nebulizers, oxygen pumps, and others can be tracked in real time using IoT devices with sensors. Real-time analysis of medical staff deployments at various locations is also possible. IoT devices also help in managing the devices, like controlling the inventories of pharmacies, and environmental monitoring, such as checking the refrigerator's temperature and humidity and temperature control.

- **Connected vehicles:-** For the purpose of triggering important communications and events, connected vehicles connect to a network to allow bidirectional communications among the vehicles For example:-cars, trucks, buses, and trains, and mobile devices & infrastructure. On account of city traffic and convergence wellbeing, for instance, those correspondences can empower vehicles equipped with associated vehicle innovation to consistently convey their areas and to get close to continuous data that sets off a robotized reaction. Vehicles, trucks, transports, and different vehicles will actually want to "talk" to one another with in-vehicle or post-retail gadgets that ceaselessly share significant security and portability data with one another. Wireless communication can also be used by connected vehicles to "talk" to infrastructure like traffic lights, work zones, toll booths, school zones, and others. The system is safe from tampering and vehicles cannot be tracked due to the anonymity of the communicated vehicle information. Another use case is connected entertainment systems that connect to Internet-connected vehicles and the driver's mobile phone.
- **Smart cities;** - The Internet of Things (IoT) is used to connect various kinds of sensors to the Internet to share relevant information about a city. The goal is to qualify the city, make the most use of its resources, current data for better city management, and provide high-quality information to the population in real time to make the city more sustainable. Smart cities is not a concept that is going to be evolved in the future. At the moment, the primary goals of hundreds of cities all over the world is to improve the quality of life for their residents by providing green spaces, transportation, and infrastructure, reduction of CO2 emissions, and encourage the use of clean energy. Smart Cities use cutting-edge technology and innovation to accomplish this goal. In many cities, real-time data about an area's air quality, water-use-control sensors, zero-emission public transportation, and environmentally friendly building materials are being implemented.

For greater energy efficiency, city officials and managers have implemented a set of measures, such as switching public lighting to low-consumption bulbs and increasing the use of clean sources like green hydrogen for mass public transportation. In public buildings, smart grids, or smart grids that automatically regulate energy supply and demand, are also installed.

- **Smart Dust:**- A wireless network of autonomous computing and sensing platforms smaller than a grain of sand is referred to as "smart dust." Smart dust wirelessly transmits information about its environment to larger computer systems, including light, temperature, sound, toxins, and vibrations.

Smart dust is a vision of the networked future in which trillions of tiny sensors constantly feel, taste, smell, see, and hear what's going on in their environment and communicate with one another to share information.

Smart dust is progressive on the grounds that the sensors are sufficiently little to be put anyplace, even

in tight and troublesome regions. Another tremendous benefit is that these gadgets work with no human mediation as they are pre-customized and, despite their little size, have their own power supply.
In addition to monitoring drug-making processes, building controls, pipelines, factory equipment, and authentication, sensing and tracking, industrial and supply chain monitoring, and defense applications, this technology is expected to lead to ubiquitous autonomous artificial intelligent computation close to the end user.

- **Smart Factories:** - Managers of factories can use smart manufacturing to automatically collect and analyze data in order to optimize production and make better-informed decisions. IoT connectivity solutions installed at the factory level transmit machine and sensor data to the Cloud.

After these data have been analyzed and contextualized, they are made available to authorized stakeholders.
This data flow is made possible by IoT technology, which makes use of both wired and wireless connectivity. It also makes it possible to remotely monitor and manage processes and make changes to production plans quickly and in real time when they are needed.
It dramatically enhances manufacturing outcomes by reducing waste, accelerating production, enhancing yield and product quality.
To put it another way, there are a lot of advantages to switching from the hierarchical model of the "shop floor" to a more open, flatter, and fully interconnected model that connects R&D processes and supply chain management.
They include improving resource management, performance, quality, cost, and global manufacturing processes.
Additionally, it enables the manufactured goods to actively participate in the design and development of the manufacturing process.
Since associated savvy items can take care of data back to the plant with the goal that quality issues can be identified and fixed during the assembling stage by changing item plan or the assembling processes.

- **UAV's:-** A class of aircraft known as unmanned aerial vehicles (UAVs) can fly without pilots on board.

Unmanned aerial vehicles, also known as UAVs, have emerged as robust public-domain solutions that can be used for a variety of tasks, including agriculture, surveys, surveillance, deliveries, stock maintenance, asset management, and other activities.
Various operations and tasks that would otherwise be either impossible to carry out, costly, labor-intensive, or, in some instances, dangerous have been made possible by the technological advancements made in the field of unmanned aerial vehicles (UAVs). This technology has positioned itself as a key enabling technology for revolutionizing the entire energy industry.
Due to their adaptability, unmanned aerial vehicles (UAVs) have been widely used in the renewable energy sector, where they have proven to be an extremely useful tool for increasing the autonomous operation of renewable energy systems, lowering their operational, monitoring, and maintenance costs, increasing their operational efficiency, assisting in their design phase, and other related tasks, and in dealing with problems that can't be properly solved by just using IoT networks that are based on land.
In the renewable energy sector, renewable energy power plants and even the management of radiological scenarios in nuclear plant emergencies are examples of adopting the use of UAVs for specific tasks.
Lately, the utilization of UAVs by military for vital activities has likewise improved a lot.
The Internet of Things (IoT) of today covers a wide range of fields and uses. The capability to act as a technology enabler across domains is this paradigm's main strength. Over IoT-based platforms, multiple domains can be supported and operated simultaneously. Support for heritage advances and independent ideal models, alongside current turns of events, makes IoT very vigorous and prudent for business. Smart parking, smart phone detection, traffic congestion, smart lighting, waste management, smart roads, structural health, urban noise maps, river floods, water flow, silos stock calculation, water leakages, radiation levels, explosive and hazardous gases, perimeter access control, snow level monitoring, liquid presence, forest fire detection, air pollution, smart grid, tank level, photovoltaic installations, NFC or Near Field Communications payments, intelligent shopping applications, landslide and avalanche prevention, early detection of earthquakes, supply chain control, smart product management and other applications are just a few of the many examples of the Internet of Things (IoT) applications.

Architecture of Internet of things:-

The term "IoT architecture" refers to the web of layers, protocols, sensors, actuators, cloud services, and other components of IoT networking systems. It is generally divided into layers that give administrators the ability to evaluate, monitor, and preserve the system's integrity. Data flows from sensors-connected devices through a network,

through the cloud for processing, analysis, and storage, as part of the IoT architecture's four-step process. With additional turn of events, the Web of Things is ready to develop considerably further, furnishing clients with better than ever encounters. On the other hand, there isn't universally adhered-to, standardized work architecture. The specific business task at hand determines the complexity and number of architectural layers. A four-layer design is the standard and most broadly accepted design.

- **Sensing Layer :-**In the sensing layer, smart systems on tags or sensors are able to automatically sense the environment and exchange data between devices. IoT is expected to be a widespread physical inner-connected network in which things are connected continuously and can be controlled from anywhere. For a variety of purposes and applications, things can be uniquely identified, and the surrounding environments can be monitored. A universal unique identifier (UUID) is a method for giving an object a unique identity so that it can be used to track any object easily. These identifiers can include names and addresses. A UUID is a number with 128 bits that is used to identify an object or person on the Internet in a unique way. The following factors should be taken into account when selecting an IoT's sensing layer:

  ○ Size, cost, and the amount of energy and resources used:- The things may be outfitted with detecting gadgets, for example, RFID labels, sensor hub. Intelligent devices ought to be made in a way that reduces the amount of resources and money required due to the large number of sensors in applications.

  ○ Deployment:- The things that are sensing (RFID tags, sensors, etc.) can be put into use once, in stages, or at random, depending on the requirements.

  ○ Communication:-Things can only be accessed and retrieved if sensors can communicate with one another.

  ○ Network:- The items are arranged in multi-hop, ad hoc, or mesh networks.

- **Connectivity Layer :-** The connection of all services, sensors, and devices that work together is the next step. There are two ways these can be linked together:

  → Gateway connection (using modules that can translate, encrypt, and decrypt data)

  → direct connection (TCP, UDP/IP)

There are various network techniques that can be used to establish a communication. Few of them are as follows:

  ○ Addressed by a group of associated devices inside a Local Area Network(LAN), the Ethernet interfaces gadgets through an actual link as per various guidelines. It is utilized extensively in a variety of industries, including home security.

  ○ Wi-Fi innovation requires no wiring to transfer information or do different activities. Radio waves or rapid light are used in this system. Wi-Fi, for instance, is frequently utilized in smart homes to connect mobile phones to the lighting system.

  ○ Near Field Communication, or NFC, is the method by which compatible gadgets in close proximity can communicate with one another. The data is sent and received by one of the devices. Some devices can send and receive data simultaneously. A smartphone is a good example of such a device.

  ○ Bluetooth :- This technology transmits data between devices that are close by by means of radio waves. Wiring is not required. However, large documents cannot be shared because data can only be transferred in small amounts.

  ○ Low-power networks (LPN):-Long-radius connections between devices with sensors that frequently send data at a low bit rate are provided by low-power networks (LPN). This technology is frequently used in agriculture, smart buildings, and smart infrastructure.

  ○ ZigBee is a wireless technology that uses digital signals with low power. This connection allows for the interaction of multiple devices. It is mostly used to automate home IoT systems, but it can also be used in science, industry, and healthcare.

  ○ Cellular network:-A system with a lot of capacity and high speed known as a cellular network makes it possible for mobile devices to communicate with one another. It is utilized for emergency communications, data sharing, business collaboration, and telephone calls.

  ○ IoT infrastructure employs messaging protocols for secure data sharing. These are the guidelines for messages that are sent between smart sensors-equipped devices. In accordance with these regulations, messages must contain a particular type of data in a predetermined format.

- **Processing Layer:-** Pre-processing and data analysis are handled by the structured data processing layer. This layer can be in the cloud or at the gateway, depending on the application and implementation. Applications for edge analytics can access this data in use cases like autonomous vehicles that require real-time data. During the processing, data is monitored and managed.

Data from various sensors, including images and readings, are received by the edge devices and gateways at the level of data processing. For instance, Bushnell's system uses cellular data to send images from its wireless trail cameras to the cloud, where

they are automatically processed to determine whether people, animals, or automobiles are present.
Cloud stage suppliers like AWS, Azure and others have IoT-explicit administrations to empower the ingestion and directing of the information stream to the cloud. This gives the infrastructure more processing and routing power to keep up with the growing number of device deployments and make it easier to manage and store this data.
The refrigeration monitoring system developed by Devices Solutions has multiple layers of processing. At the device level, a number of sensors are sampled every five minutes. Once an hour, these samples are sent to the cloud through a gateway. However, the gateway will immediately send readings to the cloud if the device determines that the temperature is above configurable limits. In the cloud, if a reading is out of range, additional filtering can be done to get rid of false alarms caused by things like a brief door opening before end users are told about a problem. In the cloud, extra handling should be possible to distinguish issues which require a bigger number of tests, information from different gadgets, or different sources like climate or timetable data.

- **Application Layer:-** Numerous connected devices are present in IoT; Different people own these gadgets, so they don't always adhere to the same standards. Compatibility plays a major role and acts as a solution for interaction among various things. Information exchange, communication, and event processing are all aspects of compatibility. To make things easier to manage and connect, there is a need for an efficient interface mechanism. It acts as a link between the IoT device and the network handoff of the data it produces and handles data formatting and presentation.

Top IoT application layer protocols:-
Engineers can choose from a wide range of IoT application layer protocols that cover a wide range of functionality. The type of device involved and the function it will perform determine which protocol is best suited for a given IoT application:

→ Latency of data. How quickly must data be transported? How much time can a data packet reasonably travel from one location to another?
→ Reliability. How serious is the IoT application's data loss? How much must device communication be redundant?
→ Bandwidth. What is the amount of information that should be accommodated?
→ Transport. Which is the most suitable IoT application transport protocol? Each of TCP, UDP, and HTTP has features that can be used by application layer protocols that are compatible with them.

The following are five of the most important protocols and their features for IoT:

- Constrained Application Protocol: - CoAP is used by organizations with limited hardware that has a low transmission rate due to its lightness. The protocol uses two fundamental message types and is compatible with HTTP: solicitation and reaction. There are confirmable and non-confirmable messages. Since data packets are small, there are few message losses. The drawback is the convention needs security, which designs ordinarily can cure with datagram transport layer security, however DTLS is of restricted use in IoT.

- Message Queue Telemetry Transport: - MQTT is a publish/subscribe protocol that minimizes data loss and works well for lightweight machine-to-machine (M2M) connectivity over TCP. Clients don't have to call for updates when using publish/subscribe for IoT, which reduces network traffic and processing load. A variety of quality enforcement levels, ranging from a single handshake delivery to an acknowledgment requirement, are also included in the protocol.

- Extensible Message and Presence Protocol: - The document-encoding markup language XML, which is well-known for its ease of readability, serves as the foundation for XMPP. XMPP is a useful HTML extension for instant messaging, presence, and other forms of real-time communication. The protocol provides devices with data-bearing nodes that can connect with other nodes upon request to create complex local networking and data-sharing. The protocol is highly scalable.

- Advanced Message Queuing Protocol: - AMQP is an offbeat convention. Like MQTT, it utilizes a distribute/buy in approach. Engineers prefer to use the protocol over TCP, but it can also be used with other types of transport. The protocol offers an optional one-or-more delivery guarantee in addition to being quality-flexible. AMQP uses Secure Sockets Layer and Transport Layer Security to implement security.

- REST or Representational State Transfer :- The most widely used REST protocol uses HTTP to provide IoT synchronous request-response functionality. The protocol is both JSON- and XML-compatible, which is useful for machine-to-machine and communication smartphones and tablets that is a boon for IoT. It is also feature-rich and capable of authentication and caching, both of which are useful

in complex environments but difficult to implement in IoT.

Applications of Internet of things:-
Let us discuss about how IoT is implemented in 3 major sectors:

1)Agricultural IoT :- At the moment, IoT-enabled technologies are widely used to boost crop productivity, generate a lot of money, make farming more efficient, and cut down on the overhead of manually operating agricultural equipment in the fields.

Different sensors must be placed over agricultural fields in an IoT-based agricultural system, and the sensed data from these sensors must be sent to a real entity like a server, cloud, or fog services. In addition, the provision of agricultural services necessitates the processing and analysis of these data. Finally, a user ought to be able to use either a computer or a handheld device to access these services.

The following is a discussion of the various components of an agricultural IoT:

→ Cloud computing: Because the data from the sensors may be useful for serving future applications, it needs to be stored for a long time. As a result, the cloud plays a very important role in agricultural data analysis and storage.

→ Sensors: Sensors are an essential part of agricultural IoT applications. Sensors for temperature, water level, soil moisture, and humidity, among other things, are frequently utilized in agriculture.

→ Cameras: - They are used to estimate the nitrogen status, water stress, thermal stress, crop damage from flooding, and infestation damage. Crop security entails the use of video cameras.

→ Satellites: -They extricate data from field symbolism which is utilized to screen various parts of the harvests, for example, observing the crop health and assessing dry zone over a large area.

→ Analytics: It can be used to estimate how much fertilizer and water is needed in an agricultural field and what kinds of crops need to be grown this season. Additionally, crop demand estimation in the market can be done with the help of data analytics.

→ Wireless connectivity:-It is one of the most important components of Agricultural Iot. It enables the transmission of information captured by the sensors from the field to the cloud/server.

→ Handheld services: It is one of the fundamental components of the E-agriculture which has become extremely popular in the last few years. Through the use of their smart phones, farmers can gain access to a variety of agricultural data, including market trends and the soil and crop conditions of their fields. They can also use their phones to control pumps and other equipment.

→ Drones: It offers visual of land mapping at a higher resolution than satellite imaging does. They can be used for irrigation, spraying pesticides, and crop monitoring.

Agricultural productivity has gradually increased as a result of modern technological advancements and the rapid development of components of IoT. Different agricultural operations can be carried out independently as a result of agricultural IoT. The following are some specific benefits of the IoT in agriculture:

→ Automatic seeding: Autonomous seeding and planting of agricultural fields is possible with IoT-based agricultural systems. Delay in seeding and planting, error probability and manual labor is significantly reduced by these systems.

→ Effective distribution of pesticides and fertilizers: Solutions that are effective at applying and controlling the amount of fertilizers and pesticides have been developed using agricultural IoT. The analysis of the crop health is done on the basis of these solutions.

→ Water management: Crop growth may be hindered by an excessive distribution of water in agricultural fields. However, there is a finite supply of global water resources. A significant driving factor for the judicious and effective distribution of agricultural water resources is the constraint of limited and frequently scarce usable water resources. Water can be efficiently distributed through the use of the various IoT solutions for agricultural use, thereby increasing yields and field productivity. The IoT-empowered rural frameworks are fit for observing the water level and moisture in the soil, and distribute the water to the farms accordingly.

→ Remote and real-time monitoring: In contrast to traditional agriculture, IoT-based farming allows a stakeholder to remotely monitor a variety of agricultural parameters, including crop and soil conditions, plant health, and weather conditions. Additionally, a farmer can use a smart handheld device to actuate on-field farming machinery, such as a water pump, valves, and other pieces of machinery.

→ Easy yield estimation:-Data can be recorded and compiled using agricultural Internet of Things (IoT) solutions over extended time spans that may be spatially or temporally diverse. Estimates related to farming and farm management can be derived from these records. The most noticeable among these assessments is crop yield, which is done on the basis of historical trends and established crop models

→ Product overview:- In order to estimate optimized yield of the harvest and decide upon the crucial steps for cropping practices in the future, the detailed analysis of the crop production, demand in the market and market rates serve as the fundamental factors . IoT-based agriculture, in contrast to more conventional methods, empowers farmers to gain greater control over their farming and crop management practices, largely autonomously. Agricultural IoT provides a comprehensive product overview on the farmer's handheld devices.

2) Vehicular IoT:- Along with the rapid increase in the use of connected vehicles across the globe, the number of accidents on road and mismanagement of traffic is also increasing consequently. Anyway, the evolution of IoT is used to establish a connected vehicular environment that helps to manage the transportation systems efficiently. Such an environment has made it possible to communicate and share information among one another and also makes a vehicle capable of sensing the internal and external environments to make various autonomous decisions. A vehicle owner living in the northern hemisphere can easily locate his vehicular asset remotely even if it is in the southern hemisphere with the help of the modern day infrastructure of IoT.

The architecture of a vehicular IoT includes the following 3 sub layers:-

• Device: It is the lowest layer that includes the basic infrastructure of the scenarios of a connected vehicle. Vehicles and roadside assistance units (RSU) are included in this layer. Certain sensors in these vehicles gather information about the vehicle's internal data. The RSU, on the other hand also manages the data from the vehicles as a local centralized unit.

• Fog: In vehicular IoT frameworks, quick navigation is appropriate to keep away from accidents and mismanagement of traffic. Fog computing plays a crucial role in these situations by making decisions in real time, close to the devices. As a result, in a vehicle IoT system, the fog layer aids in reducing the amount of time spent in transmitting the data.

• Cloud: In order to make decisions immediately, fog computing handles the processing of the data close to the devices. Fog computing, on the other hand, is insufficient for processing huge amounts of data. Therefore, cloud computing is utilized in this circumstance. Cloud computing aids in the management of processes involving a large amount of data in a vehicular IoT system. In addition, vehicular Internet of Things systems use cloud computing as a scalable resource for long-term storage.

Components of Vehicular IoT :-

Different kinds of sensors and electronic parts are used in modern automobiles. These sensors send data to a processor based on their observations of the vehicle's internal environment. The deployed on-road sensors detect the surrounding environment and send the resulting data to a centralized processor. From that point, in view of prerequisites the processor conveys the detected information to fog or cloud to carry out important functions. Although these procedures appear to be very simple, vehicular IoT practically involves a number of components and their associated challenges.

→ Sensors: - The sensors are used to observe various environmental conditions and are helpful to make the system more efficient, robust and economical. In Vehicular IoT, two types of sensors namely internal and external sensors are used traditionally

- Internal-These type of sensors are placed inside the vehicle. They are typically used to sense the specifications that are directly connected to the vehicle. Other electronic components like processing board and actuators are also equipped along with these sensors. Internal sensors transmit the sensed data to the processor board which is then processed to take certain actions that are pre-defined. GPS, Fuel gauge, accelerometer, temperature sensors, pressure sensors, proximity sensors, and ultrasonic sensors are few of the examples of internal sensors.
- External- These sensors assess the environmental information outside the vehicle. For Instance, they are utilized in the smart traffic system that can detect empty parking slots in a particular parking area. The essential inputs to generate such decisions are the still images and videos from the cameras. On-road cameras are therefore used as external sensors where the captured images are further processed either in the cloud or the fog layer to perform a few pre-programmed actions.

→ Satellites: - Few of the essential features available in Vehicular IoT are the crash system and automatic vehicle tracking. These are possible because of the use of satellites which can also be used to detect road blocks and on-road congestions.

→ Wireless Connectivity: - Communication plays a vital role as Vehicular IoT deals with connected vehicles. The collective information from both internal and external sensors needs to be processed in order to take any action or make decisions. Connectivity is very important as it enables transmission of data from various sensors to the Road Side Units (RSU) and from RSU to the cloud. The high mobility of vehicles has necessitated wireless communication for real-time and practical transmission of data.

Wi-Fi, Bluetooth, And GSM are common communication technologies used in Vehicular IoT.

→ Road Side Unit (RSU) :- It is a static entity that works with both internal and external sensors collaboratively to take real time decisions. They are equipped with communication units, fog devices and sensors. The Fog devices that are attached to the RSUs process the data from sensors to take appropriate actions. If the vehicular system requires heavy computation, then the sensed data is transmitted to the cloud end instead of fog devices. It also sometimes works as a intermediate communication agent in between two vehicles

→ Cloud and Fog computing: - Fog computing is used to handle the processes that require minimal computation and those geographically closer to the vehicle for fast computation. Cloud computing can be used for processing heavy -weight processes. For example, Fog computing can be used to avoid short on-road congestions whereas cloud computing can be used to determine regular on-road congestions where huge amount of data needs to be processed

→ Analytics: - It helps to anticipate various static and dynamic conditions.

3) Healthcare IoT :- IoT has given rise to the development of various technologies that has influenced the medical field, and wearable healthcare in particular. The prominent features of IoT has encouraged industries and researchers to develop the IoT based healthcare technologies which have given rise to power-efficient, small, diagnostic and health monitoring systems. This development has rapidly increased over the last few years. These healthcare devices provide information about the physiological conditions in a human via the handheld devices. People can also be aware of risks in different diseases and take appropriate precautions to prevent them.

Components of Healthcare IoT:-

→ Sensors:- Physiological sensors are being used in healthcare IoT that collect the values of various physiological parameters

→ Wireless Connectivity:- The communication between the sensors and a Local processing unit(LPU) takes place with Bluetooth or ZigBee whereas the communication between LPU and cloud/server is through Wi-Fi or WLAN.

→ Privacy and security:- Various healthcare service providers are implementing protection schemes and data encryption to increase the security of healthcare.

→ Analytics:- It plays an important role in providing different users(doctors, patients, nurses, etc) access meaningful information that is generated from raw data.

→ Cloud and Fog computing:- Cloud storage space is sued in order to store huge amounts of health data.

Interface:- It is the most important component for the users. Therefore, the user interface needs to be designed in such a way that it is easy for them to understand and the information is clearly depicted.

Advantages of Healthcare IoT:-

→ Real-time: - Various components in a healthcare sector can vary dynamically along with time. Real- timeliness acts as one of the most important features in such scenarios. Therefore, healthcare IoT system allows its users to receive real time information about the components of healthcare.

→ Low cost: - These systems helps the user to access various services at low cost. For example, a user can check the availability of beds using internet &web browser instead of visiting the hospital physically.

→ Easy management: - Healthcare IoT services provide easy and robust management of numerous tangible and intangible entities like the medical devices, users, security and costs.

→ Automatic processing: - A healthcare unit requires manual interventions. For instance, the user might have to enter their details manually to register with a hospital. But, the automatic processing facilities can help to remove such intervention of entering it manually with just a fingerprint sensor/device.

→ Easy record keeping: - In a Healthcare IoT system, timely delivery of health data of the patient is very important as it includes a huge number of patients who suffer from different diseases. Each disease requires a particular treatment. Permanent storage of the health data of the patient and also details of the staff and their regular activity is very essential. A healthcare IoT system also allows the user to have these data in a secure environment and provide them to authorized users as and when they require it. This recorded data is made accessible throughout the world.

→ Easy diagnosis: - A huge chunk of prior data is required in order to diagnose a disease. Therefore, the Healthcare IoT system provides the availability of prior datasets and certain learning mechanisms to make diagnosis easier.

Challenges associated with IoT: -

The Internet of things has a lot of advantages up its sleeve. In spite of that, with the heterogeneity and the development of these technologies, IoT also have various challenges which the researchers are actively trying to overcome. Few such challenges are mentioned below: -

→ Mobility: - M2M communication is supported indefinitely by IoT. Due to their varying configurations and uses, the system's devices, including pedestrians, vehicles, bicycles, drones, and robots, have distinct mobility patterns. Because these patterns cannot be accurately predicted and must be analyzed stochastically, it is difficult to achieve seamless connectivity and quality of service. Methods for efficiently making dynamic decisions regarding handoff, synchronization, and other similar issues must be developed by developers. Some of the research fields that are directly associated with addressing this challenge include tasks like allocating identifiers to mobile devices, handoff strategies, coverage estimation, path planning, mobility prediction, and others.

→ Addressing: - With the approach of IoT and its benefits, its acceptance by individuals as well as, industries developing at an uncontrollable rate. Such an outstanding expansion in the quantity of gadgets depletes the quantity of accessible IP addresses, which is in turn leading to IP clashes. Likewise, there are not many principles or industry-suggested plans toward addressing administrators of IoT. Strategies for addressing and subnetting, among others, are typical research challenges in this field.

→ Power: - In terms of power and computational power, IoT devices typically have limited resource availability. Despite their limited battery life, these gadgets need to last a long time. These restrictions necessitate eco-friendly power harvesting and consumption strategies. Alternately, it calls for new hardware designs that use less power. High-density batteries and cells with the potential to support IoT systems over an extended period of time are the focus of a number of upcoming research solutions. Designing low-power processors and hardware, as well as low-power computation methods, energy harvesting, algorithms, alternative energy sources and others are all areas of study in this field.

→ Connectivity: - Strong connectivity is necessary for IoT sensors to collect and transfer data, but this is not always the case. Connectivity can become a real problem, especially when the devices are located in remote areas. Connectivity plays a vital role in the project's success where multiple cloud servers, physical devices, and applications must be connected.

For IoT devices, local connectivity is equally important. For instance, long-range connections will not work well for Bluetooth-connected devices.

→ Interoperability: - Numerous manufacturers offer a variety of IoT devices, each of which can be used for a wide range of purposes. For these devices to work together, they need to communicate with one another as they come from different manufacturers and serve different purposes. Researchers are actively working to make it possible for devices to automatically accomplish common objectives in light of the growing number of devices and the absence of universal standards.

→ Security: - IoT is vulnerable to threats from bots and malicious attackers due to the growing number of devices and the absence of robust and unified security standards. Even though encryption seems like a good solution in this situation, many of these devices don't have the storage and computing power to support complicated mathematical operations like encryption does. For security, some manufacturers include a built-in password, which can be useful for a short time in certain limited circumstances. However, attackers have sufficient resources to crack these default passwords, putting the entire system at risk. Although these low-power devices eventually connect to remote platforms like a server, fog, or cloud, IoT is not limited to low-power devices. Accessing the organization or the distant framework by compromising the low-power gadgets is a reality in the present-day mechanical domain. Attacks like phishing, flooding, denial of service, and man-in-the-middle attacks, among others, can easily set off a chain of anomalies that could bring down an entire network or business. Hardware-level security, processor/chip-level security, physically unclonable functions (PUFs), network security, cryptography, block chains, crypto-currency, encryption, and other topics are typical areas of study in this field.

→ Device size :- IoT devices are typically designed with the goal of improving user experience at a low cost. Additionally, these small devices usually have wireless communication antennae and unique IDs. The minimal expense and size make it hard to consolidate handling power and capacity in the device. Adding a battery also raises concerns about available space. Finally, operational capability, battery power, and storage capacity of these devices are constrained. Nano and microelectronics, photonics, device fabrication, and the upcoming quantum computing paradigm are typical areas of research in this IoT subfield.

→ Communication range :- IoT has received some powerful new solutions as a result of addressing some of its most significant challenges, which have arisen as a result of IoT's expansive scope and reach. Because of its usefulness, IoT solutions have been implemented in both areas with adequate connectivity and areas, particularly remote ones, with very little connectivity. Each of these scenarios has its own set of difficulties that must be dealt with

separately. Due to the presence of other powerful wireless solutions operating at the same frequency spectrum, low-power wireless IoT solutions frequently encounter interference and noise in urban areas. In contrast, the network infrastructure necessary to provide these solutions with basic Internet access is frequently lacking when IoT solutions are implemented in remote locations like forests and rural areas. Prime examples for a powerful yet cost-effective solution emerging as a result of the communication demand—supply gap in IoT is the rise of IoT in enabling backhaul network access, providing communication coverage to such areas through signal relaying,

→ Quality Control: - Alongside talented experts, the interest for equipment has likewise increased. Manufacturers frequently rush the process in an effort to meet this demand, resulting in a lack of testing and updates. Devices that haven't been thoroughly tested often end up being unreliable and pose a security risk. Automating device management is also hampered by this. Numerous organizations battle to automate updates and these devices need to be updated with manual access. In addition to being a security risk, this adds to the overhead costs, slows down the process, and causes bottlenecks.

→ Reliability and Hardware :- A robust and secure infrastructure is necessary for any IoT project to be successful, as we have previously discussed. The physical devices may vary depending on the industry and businesses, but their quality, upkeep, dependability, and efficiency are crucial.

Let's take, for instance, sensors. Many people believe that inexpensive sensors can be found easily and work well. However, reliable and long-lasting sensors rarely come cheap. The data that is gathered from sensitive sensors like pH or gas sensors can be unreliable if they are not regularly and thoroughly maintained.

Before beginning the project, it is necessary to take into account the fact that the overall hardware requirements do not always align with the resources that are readily available.

II. Conclusion

More than 100 nations are connected to a network that exchanges data or information over a shared platform according to the most recent research. For instance: sharing of news and opinions via the Internet. On December 31, 2011, a statistical world study estimated that there were approximately 2, 267, 233, 742 Internet users globally. This shows that 32.7% of the complete population of this world is utilizing Internet services. This clearly gives us an idea that it is going to be the most used technology in the coming future.

The Internet of Things promises to provide a quality change in a people's life sooner rather than later through broadly distributed and locally intelligent organization of smart gadgets. This papers provides an overview about how this technology have emerged and the most accepted 4-layer architecture. It also focuses on the applications of Internet of Things (IoT) in the three main domains of Agriculture, Vehicles, Healthcare and explores the challenges associated with it.

References

[1]. Ayushi Sharma (2016). A Study on Internet of Things https://www.academia.edu/88953482/A_Study_on_Internet_of_Things

[2]. Internet of Things - Wikipedia https://en.wikipedia.org/wiki/Internet_of_things#References

[3]. Internet of Things (IoT): Definitions, Challenges, and Recent Research Directions – By ZoZo Hassan, Hashram Arafat Ali, Mahmoud M. badawy https://www.researchgate.net/publication/320532203_Internet_of_Things_IoT_Definitions_Challenges_and_Recent_Research_Directions

[4]. Adeniran Ezekiel (2017). Term paper- Internet of Things https://www.academia.edu/35994766/TERM_PAPER_INTERNET_OF_THINGS

[5]. Internet of things (IoT): technologies, applications, challenges and solutions- Edited by B.K. Tripathy, J.K.Anuradha https://www.pdfdrive.com/internet-of-things-iot-technologies-applications-challenges-and-solutions-d158467863.html

[6]. Preeti Kulkarni- Top 8 challenges in IoT development and how to overcome them. https://bytebeam.io/blog/top-8-challenges-in-iot-development/

[7]. Sudip Misra, Anandarup Mukherjee, Arjit Roy- INTRODUCTION TO IOT (2021)

[8]. Pradyumna Gokhale, Omkar Bhat, Sagar Bhat – Introduction to IoT https://www.researchgate.net/publication/330114646_Introduction_to_IOT