INTERNET OF THINGS (IoT): UNRAVELING THE CONNECTED WORLD

SHIKHA DAS

Student
Cotton University
Guwahati, Assam, 781001

Abstract- **Internet of Things (IoT), coined by Kevin Ashton in 1999, connects physical devices and items worldwide using the internet to facilitate communication.**
This article explains the fundamentals of IoT, presenting an overview of the current status of it, covering recent advances, trends, and future prospects. It delves into upcoming technologies such as cloud computing, artificial intelligence, and block chain which are crucial in expanding IoT capabilities and tackling IoT issues. It also addresses the ethical and societal ramifications of mass IoT deployment, emphasizing the significance of responsible design, governance, and inclusion.
The article also discusses the various levels utilized in IoT as well as some fundamental terminologies associated with it. It is essentially an augmentation of the services offered by the Internet. Furthermore, the chapter discusses the architecture of the IoT.
Lastly, the article discusses the various challenges and difficulties faced in its implications and the potential solutions to make the use of IoT for the betterment of the world at large.

Keywords**: Internet of Things, RFID, WSN, IOT architecture, Internet of Things Technologies.**

1. Introduction:

The core idea of IoT is a world in which objects can communicate and their data can be processed to execute specified activities using machine learning. In the information age, the Internet of Things (IoT) is a popular technology that can gather different types of information in real time, realise the widespread connection between things and people, and perform the intelligent thinking, recognition, and management of things, processes, and information, as well as safeguarding the environment through various connection to networks. By allowing sensing devices to connect to the Web for data transfer and enabling smart verification, tracking, location, and monitoring, the Internet of Things (IoT) intends to deliver intelligent services and setups in a variety of circumstances.

2. Definitions and Historical background:

Although there are a number of definitions given by different researchers for the term " Internet of Things", the core idea of IoT, in all these definitions remain similar.
The Internet of Things (IoT) is a network of physical devices integrated with electronics, circuits, software, sensors, and network connections. It enables remote monitoring and management of the objects, such as different types of gadgets, instruments, cars, buildings etc., in order to integrate the physical world into computer-based systems with improved accuracy and efficiency. This integration of the physical world into computer-based systems enhances overall efficiency and effectiveness.
In 1991, Mark Weiser presented a contemporary picture of the IoT, and in 1999, Bill Joy's internet taxonomy incorporated device communication. Similar subjects were covered in Neil Gershenfeld's book "When Things Start to Think" from 1999. In the same year, Kevin Ashton created the phrase "Internet of Things" to describe a system of linked devices.
The Internet of Things (IoT), according to Kevin Ashton's initial idea, is a network of individually identifiable connected objects that uses radio-frequency identification (RFID) technology. The Internet of Things evolved in general as "dynamic global network infrastructure with self-configuring capabilities based on standards and communication protocols." However, no definition was provided at the time of its invention, and while most people agree that IoT comprises things and connection, the precise meaning of IoT is still up for debate. Although so many years have passed since the invention of IoT, it is still a developing technology which has yet to reach the general public's attention. Nonetheless, it has a remarkably extensive, if not distinguished, past.
If we analyze the Internet deeply, we may categorise its development into five periods:
1. The first periods is the Internet of Documents, which consists of document-based websites and electronic libraries.

2. The second period can be referred as the Internet of Commerce, which consists of sites for stock trading, e-banking, and e-commerce.
3. Web 2.0 can also be termed as the Internet of Applications, which is said to be the third period of the Internet.
4. Social networks or the Internet of People comes in the fourth period.
5. Finally, The Internet of Things is the fifth and the most recent period in the internet history, which is made up of linked devices and machinery.

In today's world, IoT is being used in our everyday life, in almost every aspect. With the rise of IoT, two major schools of thinking on IoT have emerged. The first is a reactive framework of ideas and cognition that sees IoT as an additional layer of digital interconnection on top of current structures and items. This viewpoint regards the Internet of Things as a controllable set of convergent advancements in service delivery, infrastructure, programmes, and governance mechanisms. The second is a proactive framework of ideas and thought that sees IoT as a seriously disruptive convergence that is uncontrollable with current tools, as it will redefine the understanding of what data and what clutter is from the supply chain on to 'apps'. Both techniques have the same difficulties. The difference will be in the methods and solutions.

3. IoT Architecture and Design:

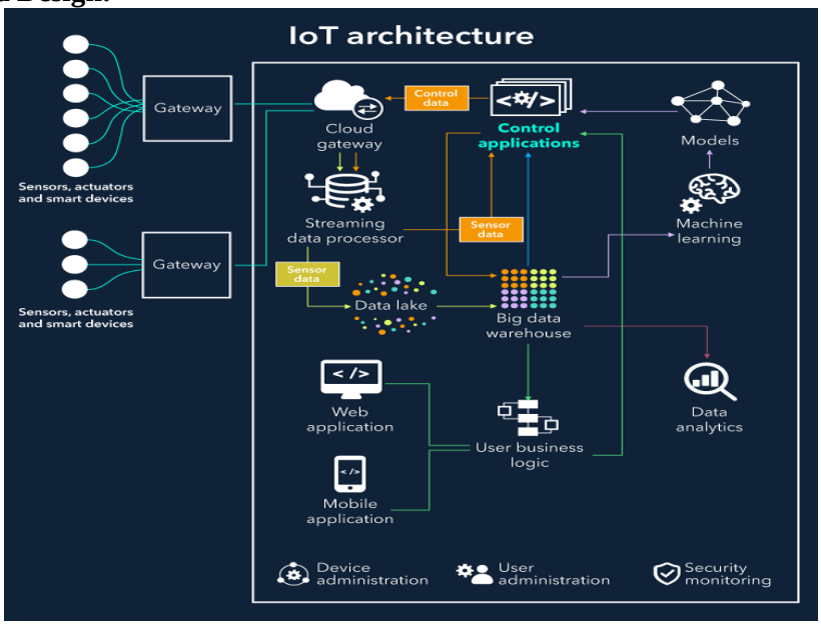

Fig: IoT architecture (image taken from google.com)

One of the basic issues with the IoT architecture is that it is a huge and expansive project. IoT is a concept that needs a variety of sensor, network, communications, and computing devices to function. In general, the Internet of Things architecture is made up of five significant levels that define all of the system's functionalities.

(a) The Sensing Layer
(b) The Network Layer
(c) The Middleware Layer
(d) The Application Layers
(e) The Business layer:

(a)The Sensing Layer: The sensing layer comprises of physical devices like sensors, RFID chips, barcodes, and other physical items connected to an IoT network, which may detect the temperature, humidity, speed, and position of items, among other things, It is the base of the IoT architecture. This is the IoT device layer that provides every item a physical meaning. The layer processes sensor data, converts it into digital signals, and transmits them to the Network Layer for further work.

(b)The Network Layer: The main objective of this layer is to receive valuable information in the form of digital signals from the Perception Layer and convey it over transmission mediums like Wi-Fi, Bluetooth, etc. to the processing systems in the Middleware Layer. The network layer is used as a transmission medium to transfer the information from the perception layer to the information processing system. Any wireless or cable technique may be used for this data transfer.

(c)The Middleware Layer: Middleware layer is the layer below the network layer. This layer's primary responsibility is to process the data obtained from the network layer. It includes tools like cloud computing and ubiquitous computing that provide speedy access to the database where every important data is stored. Using smart processing

tools, the information is processed, and a completely automated procedure is carried out depending on the information's processed outputs.
(d)The Application Layer: This layer uses the processed data for universal control of the devices. Based on the processed data, the layer utilises IoT applications for various types of industries. This layer is highly useful in the large-scale development of IoT networks. Smart homes, smart transportation, and smart planet are examples of IoT applications.
(e)The Business Layer: The business layer controls the IoT system, including apps and services. It visualizes information and data from the application layer, utilizing it to develop future aims and plans. This layer creates various business models for efficient company strategy.

4. Internet of Things Technologies:

The creation of a global system in the world of computing, where digital objects are able to be individually characterized, think, and communicate with other objects in order to gather information from which controlled actions are taken, necessitates an assortment of new and efficient technologies, which can be made possible only by the incorporation of various technologies that enable the identification and communication of the objects. This section covers the pertinent technologies that can aid in the widespread growth of the Internet of Things.

4.1 RFID: Radio Frequency Identification

The main technique which is used to make the things individually identifiable is RFID. RFID is a wireless system consisting of tags and readers, with readers emitting radio waves and receiving signals from the RFID tag. Depending on the use case, it is a transmitter microchip and may be either active or passive. Because they are powered by a battery, active tags are constantly on and data signals are send out continuously from these, whereas passive tags turn on only when they are triggered. Active tags have more practical uses then the passive tags. The RFID system, when activated by the production of any suitable signal, transmit information about the item, including its identity, the location, and other details. The radio frequencies used to transmit the data signals are subsequently handed over to the processors for data analysis.

4.2: WSN: Wireless Sensor Network

WSN is a critical component of the Internet of Things and is regarded as the building block of the IoT. A WSN is a bi-directional, multiple-hop wireless sensor network made up of nodes disseminated throughout a sensor field, and each of the nodes is connected to one or more gauges that can gather object related data like relative humidity, heat, speed of wind, etc. and then transmit it to the processing devices. Sensors communicate in a multi-hop fashion, consisting of transmitters, antennas, microcontrollers, and interface circuits. They operate as sensing units and have a power source, which is either a battery or energy-harvesting device.

A WSN consists of hardware components like sensor interface, processing units, transceiver units, and power supply. Most applications use ad hoc nodes in the communication stack. WSN middleware combines SOA and cyber infrastructure, enabling applications to be composed using SOA architectural design. Secure data aggregation is essential for accurate sensor data collection.

4.3 The Cloud Computing

The cloud is an intelligent computing system that connects millions of devices, enabling efficient data analysis and storage. It connects multiple servers on a single platform, enabling resource sharing and access from any location, at any time and allowing for seamless access to data. IoT relies heavily on cloud computing, which consolidates servers, analyzes data, and provides storage space. However, the full potential of this technology is yet to be realized. Research is being conducted to explore how cloud computing combined with smart devices with millions of sensors could benefit IoT development on a large scale.

4.4 The Internet Protocol (IP):

Internet Protocol (IP) is the primary communications protocol on the Internet, created in the 1970s. It is used for transporting datagrams across network borders. IPv4 and IPv6 are the two current variants, with IP addresses defined differently. IPv4 addresses are commonly referred to as "IP addresses" due to their widespread use. Class A, B, and C are commonly used, out of all five classes. IPv6 is the modern version. IP addresses are made up of binary values and there are four different types of IP addresses: Public, Private, Static and Dynamic.

4.5 Electronic Product Code (EPC):

The Electronic Product Code (EPC) is a 64-bit or 98-bit code that is electronically encoded on an RFID tag designed to enhance the EPC barcode system. EPC codes are capable of storing information such as the kind of EPC, the product's unique serial number, specifications, manufacturer information, and so on. EPC, established in 1999 by MIT's AutoID center, is standardised by the EPCglobal Organisation. The EPCglobal Network, consisting of four parts, Object Naming Service (ONS), EPC Discovery Service (EPCDS), EPC Information Services (EPCIS), and EPC Security Services (EPCSS), enables the exchange of RFID data.

4.6 Wi-Fi (Wireless Fidelity):
Wireless Fidelity (Wi-Fi) is a networking technology that connects computers and devices through wireless signals. Vic Hayes, the father of Wireless Fidelity, created the prototype in 1991. WaveLAN, the first wireless solution, introduced 1 to 2 Mbps transfer rates. Today, high-speed Wireless Local Area Network (WLAN) access is widely available in homes, workplaces, and public spaces. Wi-Fi has become the default in devices like laptops, notebooks, and mobiles due to its integration with CE products. Wireless APs (access points) have transformed entire towns into Wi-Fi corridors, increasing its popularity.
4.7 Bluetooth:
Bluetooth, or Bluetooth wireless technology, is an affordable, short-range radio technology that overcomes the necessity of separate cords connecting devices such as laptop computers, smartphones, PDAs, cameras, and printers. It transmits at less than 1 Mbps and using the IEEE 802.15.1 protocol. It has an efficient range of 10 to 100 metres. Bluetooth, developed by Ericson Mobile Communication Company in 1994, is used to create Personal Area Networks (PAN) and Piconets, which communicate data between 2-8 devices at the same time. Piconets can include text, images, video, or audio. Over 1000 firms are part of the Bluetooth Special Interest Group, including Intel, Cisco, HP, Aruba, Ericson, IBM, Motorola, Toshiba etc.
4.8 Artificial Intelligence:
Artificial intelligence is a topic that, in its most basic form, combines computer science and substantial datasets to facilitate problem-solving. Additionally, it includes the branches of artificial intelligence known as deep learning and machine learning, which are commonly addressed together. Artificial intelligence responds to human presence in technological surroundings, enabling smooth day-to-day activities. Ambient intelligence allows technology to access latent intelligence and data in networked devices, improving user experience and overall efficiency.
4.9 Near Field Communication:
Near Field Communication (NFC) is a short-range wireless technology. It is a technology that connects devices when they are touched together or within a few centimetres of each other. It enables authentication, physical access, information transfer, and the establishment of wireless networks by leveraging existing ecosystems and standards based on radio frequency ID tags. It was actually designed to transmit files between phones through Android Beam. NFC is used in modern applications such as Google Nearby Share to deploy wireless services over faster networks such as Bluetooth or Wi-Fi direct. NFC technology streamlines business dealings, facilitates the sharing of digital content, and links electronic devices all over the world. It requires a 4 cm operating distance and works at 13.56 MHz. NFC offers up to 10 cm of long-distance capability as an addition to Bluetooth and 802.11. It doesn't need a clear line of sight, and features an easy-to-use joining mechanism. The first companies to develop NFC were Philips and Sony.
4.10 Nano Technology:
This technology creates smaller and enhanced versions of related items. Nano-scale devices, constructed from nano components, can function as sensors and actuators, reducing energy consumption in systems. This new networking system, known as the Internet of Nano-Things, defines a new paradigm for communication and networking.

5. Practical applications of IoT in day to day life:
Many everyday apps are intelligent but lack the ability to connect and share essential information. This leads to the creation of creative applications that improve our lives. Some of these applications, like Google's automobile, utilize the Internet of Things to provide real-time traffic, highway conditions, and weather information. These applications will undoubtedly enhance our quality of life. In this chapter, let us discuss some of these applications which can ease our day to day life using IoT.
5.1 Efficient Traffic Monitoring System:
A traffic monitoring system based on IoT technology is critical for better transportation and travel experiences. This technology detects motor vehicles and other traffic factors automatically, decreasing congestion and enhancing the travel experience. It has features such as theft detection, traffic and accident reporting, and decreased pollution. Smart cities may enable pedestrian and vehicle path deviations, preserve energy through weather-adaptive traffic lights, and give accessible parking places. These innovative solutions can improve the travel experience while also reducing environmental pollutants by utilising IoT technology.
5.2 Smart Homes:
IoT provides remote home automation for controlling appliances, checking utility metres, tracking energy use, and determining water and resource overloads. Burglaries can be avoided with a reliable encroachment surveillance system. Gardening sensors keep an eye on the light, temperature, humidity, and wetness to ensure that plants are watered properly. These characteristics guarantee effective house management while preventing congestion.
5.3 Smart Monitoring of Environment:
The Internet of Things offers improved natural disaster predictions and air pollution monitoring, resulting in safer and more effective environmental management.
5.4 Improvised Agriculture:

IoT automates agricultural activities by monitoring variables such as light, humidity, and soil nutrition, therefore improving green housing and increasing yield. Proper irrigation and fertilisation enhance water quality while lowering fertiliser consumption.

5.5 Futuristic Healthcare:

Smart bendable gadgets containing RFID tags will be used by futuristic hospitals to monitor patients' health indicators such as pulse, blood pressure, and temperature. For medical crises, drone ambulances are currently available, allowing doctors to follow patients and offer immediate care until ambulances arrive. These technologies will enable healthcare providers to monitor patients' vital signs and provide prompt medical care.

5.6 Smart Retailing and Management:

IoT and RFID offer retailers significant benefits, enabling efficient stock management, identifying theft, and tracking inventory. Merchants can maintain records, place orders, and develop sales charts and graphs for effective order management. It also helps in maintaining the stock of goods so that the seller may never run out of stock.

6. Major issues and Challenges of IoT:

The incorporation of IoT-based systems into all parts of human life, as well as the numerous technologies involved in transferring information between embedded devices, made it complicated and created a number of concerns and obstacles. In the sophisticated smart tech society, these concerns are also a difficulty for IoT developers. As technology advances, so do the difficulties and need for sophisticated IoT systems. As a result, IoT developers must anticipate new difficulties and give solutions to them.

6.1 Concerns about security and privacy

Security and privacy are crucial challenges in IoT systems due to threats, cyber assaults, hazards, and loopholes in the system. Device-level privacy is a result of inadequate authorization, unsecured software, firmware, web interfaces, and insufficient transport layer encryption. To develop trust in IoT systems, security procedures must be implemented at every tier of architecture. Secure Socket Layer (SSL) and Datagram Transport Layer Security (DTLS) are cryptographic protocols used to ensure security in IoT systems between transport and application layers. IoT applications require various solutions to ensure secure communication between devices and avoid security vulnerabilities. Wireless technology increases vulnerability, so it's crucial to identify harmful behaviors and self-redress. Privacy is essential for consumer security, and maintaining authorization and authentication over a secure network is essential for trusted interactions. However, various privacy policies for multiple items within the IoT system can be challenging. As a result, before transferring data, each device must verify the privacy rules of other objects.

6.2 Interoperability and standardization concerns

The ability to communicate data between various IoT devices and platforms without relying on software or hardware is referred to as interoperability. This is because IoT technology and solutions are so different. IoT systems include a variety of characteristics to improve interoperability and communication across a heterogeneous ecosystem. Researchers have approved a variety of interoperability handling approaches, including adapters, gateways, virtual networks, overlays, and service-oriented architectures. While these solutions reduce the stress on IoT systems, there are still issues that need to be addressed in the future.

6.3 Legal, ethical, and regulatory rights

IoT developers must consider ethics, legislation, and regulatory rights to ensure the quality and safety of IoT systems and devices. These laws and regulations aim to uphold moral standards and deter unauthorized usage. However, IoT development has also created moral and legal dilemmas, such as data usability, security, and privacy protection. Many IoT users support government rules and laws on data protection, privacy, and safety due to their lack of confidence in IoT devices. These problems must be taken into account by the IoT developers, which is crucial for maintaining public trust in IoT usage.

6.4 Scalability, accessibility, and dependability

Scalability is the capacity to expand a system's capabilities without sacrificing its usability. Supporting a wide range of devices with different memory, processing, storage, and communication creates challenges for IoT. Availability is yet another crucial aspect to take into account. In the IoT layered structure, scalability and availability should be implemented synchronously. IoT solutions that are cloud-based exhibit scalability and offer adequate support.

6.5 Quality of Service

Quality of service (QoS) is an important statistic for Internet of Things (IoT) systems, architecture, and devices. It evaluates these systems' efficacy, efficiency, and performance. Dependability, affordability, energy use, safety, accessibility, and service length are all important QoS factors. These criteria must be met by an intelligent IoT ecosystem, and QoS metrics must be established to ensure dependability.

7. Conclusion:

The Internet of Things is redefining how we engage with technology and the real world in the digital universe. It has the enormous potential to transform industries, increase productivity, and enhance quality of life. However, the difficulties and moral ramifications of its acceptance should seriously be taken into account. In order to realise the full potential of the IoT for a connected and intelligent future, it is crucial to promote cooperation, creativity, and a shared vision. All in all, the Internet of Things is more than just a futuristic concept. It is already in place and has an influence on more than simply technical advancement.

REFERENCES:

1. Kumar, Sachin., Tiwari, Prayag., & Zymbler, Mikhail. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big Data*. volume 6, Article number: 111. https://doi.org/10.1186/s40537-019-0268-2
2. Farooq, M.U., et. al.(2015) A Review on Internet of Things (IoT). *International Journal of Computer Applications* (0975 8887). Volume 113 - No. 1.
3. Ali, Zainab H., Ali, Hesham A. & Badawy, Mahmoud M.(2015). Internet of Things (IoT): Definitions, Challenges and Recent Research Directions. *International Journal of Computer Applications* (0975 – 8887) Volume 128 – No.1
4. Sfar AR, Zied C, Challal Y.(2017) A systematic and cognitive vision for IoT security: a case study of military live simulation and security challenges. International conference on smart, monitored and controlled cities (SM2C), Sfax, Tunisia, 17–19 Feb. 2017. https://doi.org/10.1109/sm2c.2017.8071828.
5. Borgia, E.(2014). The Internet of Things vision: Key features, applications, and open issues. Computer Communications, 54, 1-31, http://doi.org/10.1016/j.comcom.2014.09.008