Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 1 (2023)

Application of Internet of Things

[1] Rajkumar Kaushik, [2] Rohan Sharma, [3] Rachita Sharma, [4] Nikita Chaturvedi

[1] Asst. Professor, Electrical Engineering
Arya Institute of Engineering and Technology, Jaipur
[2] Asst. Professor, Electrical Engineering
Arya Institute of Engineering, Technology and Management, Jaipur
[3] (Research Scholar), Computer Science Engineering
Arya Institute of Engineering and Technology, Jaipur
[4] (Research Scholar), Computer Science Engineering
Arya Institute of Engineering and Technology, Jaipur

Abstract: Today, there is a tremendous push towards modern technology throughout the world. Specialized companies, on the other hand, are experiencing a terrifying rush towards the Internet of objects, or the Internet of things, in information technology. This refers to the process of connecting objects to the Internet by installing hardware or software that gives them the intelligence to interact with one another and efficiently take part in all facets of daily life. To achieve their full potential, however, a number of obstacles and problems still need to be resolved, and they must be seen from a variety of angles. This review study's main objective is to give the reader a comprehensive analysis from a technological and sociological perspective.

Keywords: Internet of Things (IoT), Architecture of IOT, Sensors, Actuators, Challenges of IOT, Applications of IOT

1. Introduction

In 1999, Kevin Ashton first used the phrase "Internet of Things" (IoT) in a presentation to Proctor & Gamble. The networking of real objects with embedded electronics that can interact and sense what's going on around them is known as the Internet of Things or IoT for short. In the coming years, IoT-based technology will offer better quality services, therefore changing people's everyday routines. Improvements in electricity, gene treatments, healthcare, agriculture, smart cities, and smart homes are just a few areas where IoT is well-established. The term "Internet of Things" (IoT) refers to a network of embedded networked computing devices that are able to transmit and receive data. Realizing the Internet of Things' potential benefits, however, may be hampered by certain serious obstacles that it presents. Attention-grabbing tales regarding privacy concerns, surveillance concerns, and internet device hacking have already attracted the public's attention. There are still technical difficulties as well as fresh issues with politics, the law, and development.

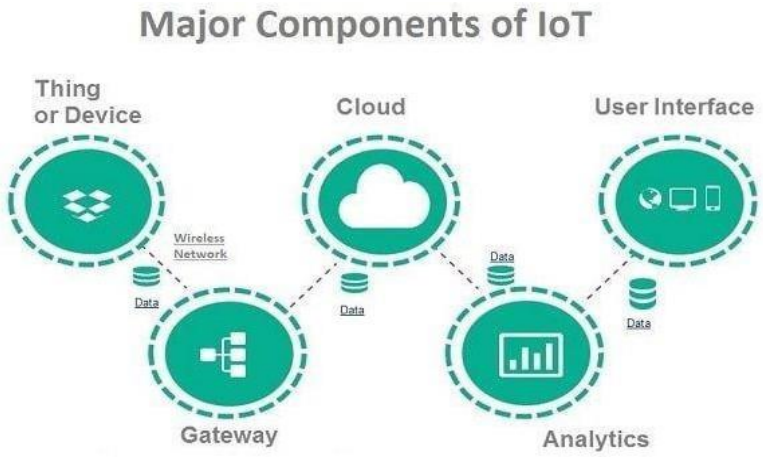

Fig 1: Internet of Things

2. Architecture of Iot

The devices, network architecture, and cloud technologies that enable inter-device communication make up the Internet ofThings architecture.

THREE LAYER ARCHITECTURE

1) Perception Layer - It is equipped with sensors to sense and collect environmental data. It detects certain physical characteristics or locates other intelligent items nearby. In addition, edge devices, sensors, and actuators that interactwith the environment are included. It can identify other intelligent objects or items in the environment based on specific spatial criteria.
2) Network Layer - It establishes connections with servers, network devices, and other smart objects. Sensor data processing and transmission are further characteristics of it.
3) Application Layer - It provides the user with services unique to their application. As an example, it describes several uses for the Internet of Things, such as "smart houses," "smart cities,"and"smarthealth."

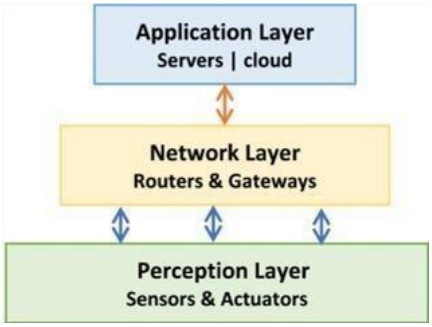

Fig 2: Three Layer ArchitectureFIVE LAYER ARCHITECTURE

The Internet of Things' well-recognized 5-layer architecture offers a disciplined method for designing and implementing IoT systems.

1. Perception Layer - This layer is made up of sensors, actuators, and other hardware for gathering data from the realworld. Because it offers raw data that is utilized to automate processes and make well-informed judgments, the perception layer is essential to the Internet of Things. Devices from the perception layer include cameras, GPS receivers, motion detectors, and temperature sensors.
2. Network Layer - In an Internet of Things system, the network layer connects the devices and allows data to move between them and the cloud. The protocols, gateways, and wired and wireless networks that are used to transport data between devices are all included at this layer. Devices at the network layer include switches, routers, and gateways.
3. Processing Layer - Data generated by Internet of Things devices must be processed and stored by the data layer. The technologies at this layer for data processing, storage, and analysis are utilized to handle the enormous volumes of data produced by Internet of Things devices. Big data platforms like Hadoop and Spark, databases, and cloud storage are a few examples of data layer technology.
4. Application Layer - The user interface and apps that let end users engage with IoT systems are provided by the application layer. The dashboards, APIs, and mobile and web apps that are used to access and work with IoT data are included in this layer.
5. Application layer technologies include things like web apps, mobile apps, and APIs that are used to interface withdata from the Internet of Things.
6. Business Layer - The business layer is in charge of creating the rules and business logic that control

how an Internet of Things system behaves. This layer contains analytics tools, rules engines, and business processes for analyzing data from IoT devices and making choices.

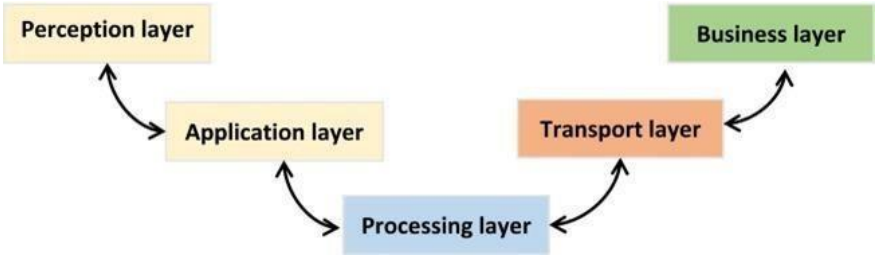

Fig 3: Five Layer Architecture

3. Sensors and Actuators

SENSORS

Actuators and sensors are two of the IoT's fundamental components. One or more sensors are required in many Internet of Things applications in order to gather data and system information. Alternatively, the sensors collect the information that will be sent over the network to the actuators that drive the machinery. For example, humidity sensors supply information to regulate irrigation systems, traffic sensors supply information to regulate traffic signals, and occupancy sensors provide information to regulate the interiors of buildings. After the data is processed, the triggers may receive directives that have an impact on the system as a whole. IoT solutions are made possible by sensors and actuators across all IoT vertical fields, including smart transportation, smart cities, and smart farming. Medical Sensors -With the aim of improving the efficiency, safety, and operational simplicity of medical equipment, the Internet of Things is becoming increasingly significant in the field of medical technology. With several applications based on smart sensors that track a patient's health whether he is not in the hospital or when he is by himself, the Internet of Things is growing the medical industry. Following that, they can provide the patient, family, or doctor prompt feedback. They have medical sensors installed that can detect and diagnose a number of characteristics, including blood pressure, body temperature, blood sugar levels, heart rate, and breathing rate. The goal of the Internet of Things is to create a new gadget that will be more advanced than wearable smart gadgets. This device will be able to identify places that are adhered to the skin, such as tattoos, which are inexpensive, flexible, and disposable. Rubber housing is used in the electrical fitting. For a few days, the patient is supposed to wear these in order to continuously monitor a vital health laboratory.

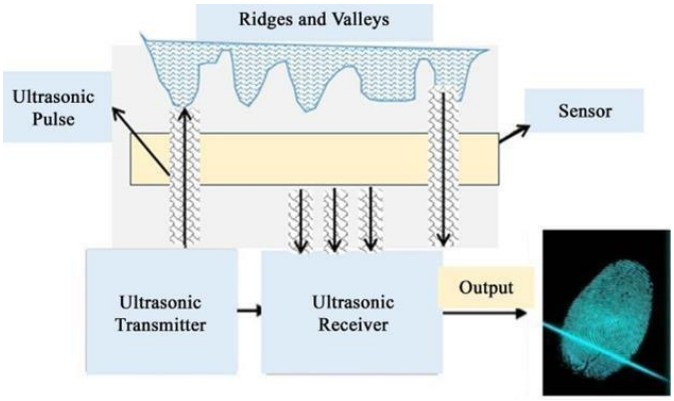

Fig 4: Medical Sensors

Physical Sensors - Sensors for air pressure, temperature, for usage in more specialized applications, as well as touch integration possible. It is possible to add more sensors, like gas concentration and radiation sensors, to certain mobile work environments to improve the user's perception and enable automated information

gathering.

Radio Frequency Identification (RFID) - RFID stands for Radio Frequency Identification. It is a type of radio communication in which an item, animal, or human is uniquely identified through electromagnetic or electrostatic coupling in the radio frequency region of the electromagnetic spectrum. Usage applications for RFID technology include shipping, retail sales, manufacturing, healthcare, and home usage.

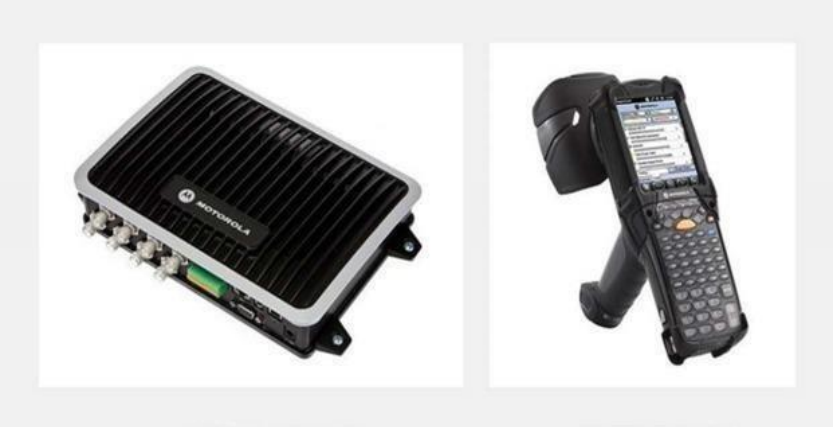

Fig 5: Radio Frequency Identification

Touch screen Sensors - Touching the screen modifies the signals coming from the smart phone's touchscreen, which has an electric current flowing through it constantly. The gadget has this modification as an input. In its most basic form, the touch screen is used for writing and tapping, and it handles basic input and output functions. There are three main methods to use the touch screen for interaction.

1) The main use of a touch screen is tapping or touching, which is characterized as clicking anywhere on the screen to open, close, or type a character.
2) Multi-touch, which allows you to tap the screen with multiple fingers at once, is mainly used in gaming applications. Drawing a certain pattern on a touch screen is referred to as a gesture. One finger may be used for drag and drop, or several fingers can be used to precisely resize and adjust the camera zoom while editing images.

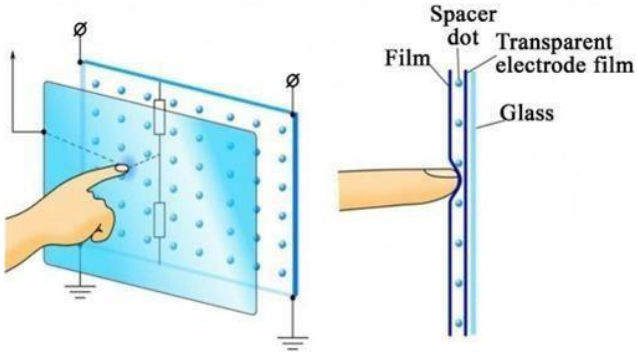

Fig 6: Touch screen Sensors

ACTUATORS -

Actuators are mechanical or electromechanical devices that can be powered by electricity, hand power, ordifferent fluids like air, hydraulic, etc. to give regulated and occasionally limited motions or positions. Power is transformed into linear movements By linear actuators, which are frequently employed in hydraulic and electrical positioning applications. A hydraulic actuator is composed of a cylinder or fluid drive that uses hydraulic power to facilitate mechanical action. An output from a mechanical movement can be oscillatory, rotational, or linear in motion. In the same way that compressing a fluid is nearly difficult, a hydraulic actuator

can apply significant force. This approach's restricted acceleration is a drawback. Electrical energy is used by electric actuators. There are several methods in which the electric actuator can supply operational power or torque.

4. Iot Difficulties and Challenges

The use of the Internet of Things (IoT) in daily life has increased, and the different technologies required to transport data across embedded devices have made it complicated and fraught with difficulties. A few topics are covered below:

1) Security - IoT devices and services with inadequate security can serve as possible points of entry for cyber attacks and leave user data vulnerable to theft due to inadequate data flow protection [30]. Because Internet of Things devices are interconnected, any device with inadequate security that is connected to the Internet has the potential to impact Internet security and resilience on a global scale. Other factors that contribute to this challenge include the widespread use of IoT devices that are uniform in nature, the capacity of some devices to establish connections with other devices on their own, and the possibility of deploying these devices in unsecure environments.
2) Privacy - Policies that protect people's right to privacy across a wide range of expectations are necessary for the Internet of Things to reach its full potential. IoT users can benefit greatly from the data flows and user privacy that IoT devices offer, yet worries about privacy and other risks may prevent IoT from being fully adopted. Thus, keeping users' trust in the Internet, connected devices, and related services depends on respecting their right to privacy and protecting their expectations about it.
3) Lawfulness and Coherence - In addition to exacerbating already-existing legal concerns around the Internet, the usage of IoT devices creates a host of new regulatory and legal difficulties. Becausethey are distrustful of IoT devices, the majority of Internet of Things users appear to support laws and rules that pertain to safety, privacy, and data protection. This issue needs to be considered in order to maintain and improve public trust regarding the use of IoT devices and systems.

Application of Iot

- Agriculture - The demand for agricultural goods is rising due to the growing global population. However,the human resource necessary for agricultural growth is unstable due to the exodus of young people to large cities. Automating agricultural procedures and meeting the need for food may be greatly aided by IoT andother technologies.
- Manufacturing - The industrial industries are placed in a more technologically advanced environment thanks to the Internet of Things. It can manage stocks, streamline the manufacturing flow, and automaticallytrack development cycles.
- Transportation - Through enhanced communication and information dissemination, IoT applications facilitate the integration of personal and commercial vehicles. It provides advantages including route optimization, vehicle tracking, weather monitoring, distance coverage, and more in addition to facilitatingthe connection of goods and customers.
- Hospitality - Many hotels include central controls for heating, ventilation, and air conditioning. Additiontypical are greeting cards and television controls. Additionally, staff members receive alerts from Internet of Things devices on the state of different equipment. Because of this, experts are able to repair importantequipment before they significantly lose function.
- Traffic Monitoring - Intelligent traffic monitoring facilitates urban expansion and better decision-making. Real-time traffic data is gathered, processed, and analyzed by an Internet of Things-based system to deliver updates on accidents and gridlock. Early warning alerts also reduce travel time during rush hours.

5. Conclusion

Our everyday lives have undergone several technological changes as a result of IoT, which, via a

variety of applications and technologies, has helped make life easier and more pleasant. Attacks may be launched against the IOT framework at every level. As such, there are several security risks and prerequisites that must be addressed. By having a divisive debate that weighs the advantages of IoT against its possible drawbacks, solutions to optimize itsbenefits and minimize its hazards will ultimately not be identified. The issues associated with IoT are not exclusive to developed nations; rather, determining the best course of action will need the educated engagement, communication, and cooperation of a wide variety of stakeholders. Organizations may lower the risk of cyber- attacks and safeguard sensitive data and IoT systems by making security a top priority. Defending against cyber attacks and unauthorized access to the Internet of Things devices and the sensitive data they gather and send. For security reasons, the benefits are incalculable, but research and analysis a reliable.

References

[1] "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications" by Jayavardhana Gubbi et al. (Published in the IEEE Communication Surveys & Tutorials)
[2] "The Fourth Industrial Revolution: The Internet of Things" by World Economic Forum
[3] "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions" by Jayavardhana Gubbi et al. (Published in the Future Generation Computer Systems journal)
[4] "The Internet of Things: Opportunities and Challenges" by Nuno Pereira and Marcelo R. Nascimento
[5] "Understanding the Internet of Things: Definition, Potentials, and Socio-Economic Benefits" by Ovidiu Vermesan and Peter Friess
[6] "Interoperability in the Internet of Things: A Survey" by Antonio Guerrieri et al. (Published in the MDPI Future Internet journal)
[7] "The Internet of Things Ecosystem: The Concept, Structure, and Implementation" by Zoraida Frias et al.
[8] "Challenges and Opportunities in the Internet of Things (IoT): A Review" by Vikash Jain and Sandeep Kumar
[9] "The Rise of the Internet of Things in the Digital Business Era" by R. Khan et al. (Published in the Procedia Computer Science journal)
[10] "Security and Privacy in the Internet of Things: Current State and Future Challenges" by Roman Lesner et al. (Published in the IEEE Security & Privacy journal)
[11] "Internet of Things (IoT): A Bibliometric Analysis of Scientific and Technological Production" by Isabel Ramos et al. (Published in the MDPI Sensors journal)
[12] "The Internet of Things (IoT): Applications, investments, and challenges for enterprises" by Theresa Johnson and Dorothy Monekosso
[13] "A Survey on Internet of Things: Security and Privacy Issues" by Wenyan Li et al. (Published in the IEEE Internet of Things Journal)
[14] "The Internet of Things (IoT) for Environmental Monitoring" by K. Chakraborty and J. A. Jethwa (Published in the Springer Wireless Personal Communications journal)