Grenze International Journal of Engineering and Technology, June Issue

Internet of Things: Vision, Applications and Challenges

Hirdesh Sharma[1], Rishabh Gosain[2] and Prerna Sachdeva[3]
[1]Assistant Professor, Dept. of CSE, JIMS Engineering Management Technical Campus, (JEMTEC), Greater Noida, U.P., India,
Email: hirdesharma@gmail.com
[2-3]JIMS Engineering Management Technical Campus (JEMTEC), Greater Noida, U.P., India.
Email: rishabhgosain26@gmail.com, prernasachdeva68@gmail.com

***Abstract*— The Internet of Things (IoT) is defined as global physical network and virtual goods that have identities, characteristics, and personalities. Kevin Ashton coined the phrase "Internet of Things" in 1999 (Ashton, 2009). The next section discusses IoT concepts. It goes through the various levels used in IoT as well as some basic terms linked with it. It is simply an enhancement to the services provided by the Internet. The Internet of Things (IoT) promises to link anything in our surroundings via a common infrastructure, providing us not only power over the things surrounding us, but also keeping us informed of their status. The definitions, vision, applications, and issues of the Internet of Things are the topic of this research study. This article's major objective aims to offer a summary of the Internet of Things, structures, applications, and obstacles in our daily life.**

***Index Terms*— Internet of Things (IoT), detector, design, intelligent Farming, intelligent Grid, Student Tracking, future challenges, Security attacks and Privacy.**

I. INTRODUCTION

There has been a tidal change in human everyday lives as well as working conditions in businesses with the introduction of IT technology. The Internet of Things (IoT) is a network of physical devices and network connectivity that allows for data collecting and exchange. It refers to physical items such as detectors, computing energy, software, and additional technologies that let them to interact with and exchange information with others systems and devices over the web or different networks of communication. The name "Internet of Things" has been called deceptive since devices are not required to be connected to the open internet; rather, they need to be connected to a network and remain autonomously accessible. The Internet of items enables items to be detected and managed remotely utilizing existing network infrastructure, resulting in higher efficiency, quicker operations, lower error, theft prevention, and the inclusion of complex and adaptable organisational systems. The development of IoT involves several challenges, including infrastructure, connectivity, interfaces, rules, and standards.
The IoT ecosystem includes a wide range of objects/things that may be broken down into two categories:
i) Items with batteries that can be recharged: the vast majority are mobile devices (e.g., computers, tablets, and mobile phones).
ii) Items without batteries that can be recharged: in terms of movement, these items are fixed.
In general, IoT covers three major requirements:
The first is a shared understanding of its clients' and apps' circumstances.

Grenze ID: 01.GIJET.10.2.12

Second, the architecture of software and ubiquitous networks of communication will be used to cover and evaluate contextual information, followed by IoT analytics tools aimed at independent and smart behaviour.
The main objective of this article is to present an overview of IoT, including its definition, architecture, application, problems, and advantages and downsides.

II. Internet Of Things

The Internet of Things, as it is commonly referred as, is "an open and comprehensive network of intelligent items with the ability to organize themselves and share information, information, and resources, reacting and acting in response to circumstances and shifts in the environment."
The Internet of Things depicts a world in which practically everything may be joined and communicates with greater intelligence than ever previously.
When we examine the growth of the Internet, we may categorise it into five stages shown below:

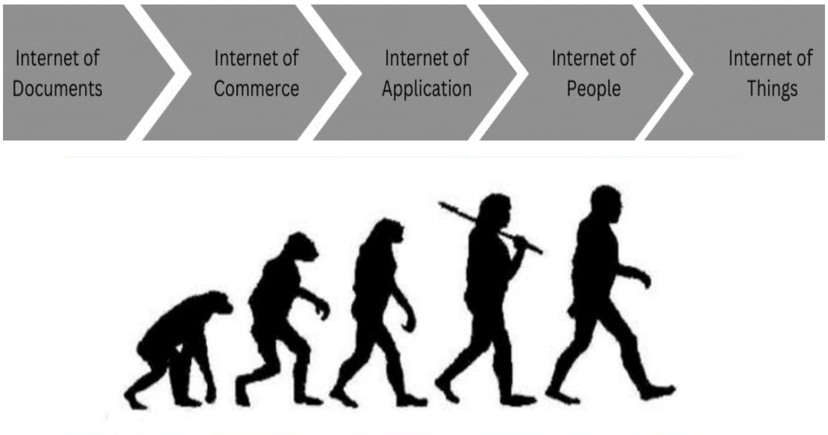

Fig.1 IOT five stages

When we examine the growth of the Internet, we may categorise it into five stages:
1. Document-based websites and e-libraries comprise the Internet of Documents.
2. Electronic commerce, online banking and trading in stocks websites comprise the Internet of Commerce.
3. Web 2.0 refers to the Internet of Applications.
4. People's Internet -- Social Media Networks.
5. IOT refers to interconnected items and equipment.

IOT is the Internet's forthcoming generation , in which real-world objects may be accessed and recognized over the Internet. The meaning of IoT varies based on the technology used to implement it. In contrast, the concept of IoT is that elements in an IoT may be identifiable individually in digital representations. Anything connected to the Internet of Things (IoT) can transmit information and, if needed, process it using preset procedures. When things can sense and communicate with their surroundings, they are transformed into instruments for grasping and reacting to complexities.

III. Architecture Of IoT

The ability of devices in a network to interact with one another is a critical requirement of an IoT. The design of IoT architecture includes considerations for networking, communication, procedures, and other variables. Device extensibility, scaling and functionality must all be considered while creating IoT architecture. IoT design should be adaptive so that devices may interact and communicate with one another in real time.
IOT Architecture, consists of four layers given below in Table I .
They are:

- To feel the status of all accessible objects (things), the sensing layer is incorporated.
- The network layer, among other things, is the network infrastructure that enables wireless or wired connectivity.
- The service layer's objective is to develop and administer services that are demanded by clients or applications.
- The interfaces layer includes techniques for interacting with people or apps.

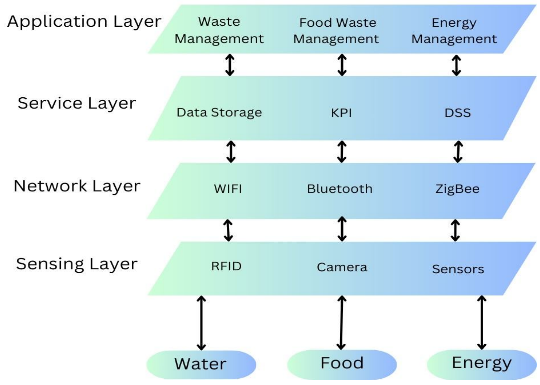

Fig.2 Architecture of IOT

TABLE I. LAYERS OF IOT

A. Sensing Layer	The initial layer of the IoT architecture is the sensor layer and it collects data from numerous sources. This layer is made up of actuators and sensors that are placed in the surroundings to collect data on humidity, temperature, sound, light, and other physical properties. These devices connect with the network layer via wired or wireless means. Sensors used in the field include sensor networks, embedded systems, RFID tags and readers, and other soft sensors. Each of these sensors includes data collection as well as identification and data storage (e.g., RFID tags). A unique identifier (UUID) is a 128-bit integer that is employed to uniquely identify an entity or item on the web. The following criteria should be considered while selecting an IoT sensor layer: • Cost, size, material usage, and energy consumption: gadgets should be designed to use as little resources as possible. • Deployment: Detecting things (RFID tags, detectors, etc.) can be installed once, incrementally, or at random, depending on the demands. • Communication: Sensors must be able to communicate in order for things to be accessible and retrievable.
B. Network Layer	This layer is in charge of transmitting sensor data to the next layer. It is in charge of facilitating connectivity and communication amongst IoT system devices, and it should provide a scalable, adaptable, based on standards global protocol for sending data from different devices. Gateways and routers serve as mediators between gadgets and the rest of the internet on this tier. For sharing of data and device service providing, a robust network is necessary. The following concerns should be addressed at the networking layer: • Fixed, wireless, and mobile networks are all managed through network management technology. • Data searching and processing technologies. • Privacy and security. Bluetooth, WiFi, Zigbee, and cellular networks like 4G and 5G are instances of the network technologies used in IoT.
C. Service Layer	This layer connects the Gateway - network layer with the application layer in a bidirectional manner. It is an inexpensive platform that allows reusable software and hardware. This layer's services operate straight on the network in order to discover novel services for a programme and dynamically obtain data about those services. The duties of the service layer are as follows:

	• Discovering a Service: Locating objects capable of providing the necessary service and data. • Service composition: It allows for the interaction of linked entities and outlines the links between them in order to provide the required service. • Service APIs: They serve as a bridge between the services that consumers demand.
D. Application Layer	It is in charge of creating user-friendly interfaces and functions that allow people to access and operate Internet of Things devices. This layer contains a number of software, application, and middleware services that enable various IoT devices and systems to connect and share data in real time. Furthermore, the application layer includes analytics along with processing capabilities for analysing and transforming data into actionable insights. Machine learning techniques, data visualisation tools, and other advanced analytics skills might all be combined. Among the industries that might profit from the applications are transportation, medical care, farming, logistics, administration, and retailing.

IV. APPLICATION OF IOT

Below in Table II are shown application of IOT:

TABLE II. APPLICATION OF IOT

A. Temperature Monitoring	Human body temperature is employed in numerous diagnostic techniques as an indicator of homeostasis maintenance. A shift in body temperature can also serve as an early Some ailments, such as trauma and sepsis, have warning signs. Improvements in IoT-based technology, on the other hand, have provided a variety of answers to this problem. Another research used sensors that are wearable and lightweight to measure the body temperature of neonates in real time.
B. Oxygen Saturation Monitoring	Pulse oximetry is a simple technique for determining saturation that has the potential to be an essential metric in healthcare analysis. The non-invasive therapy overcomes the drawbacks of the old approach and enables real-time monitoring. Furthermore, gathered data may be delivered to a server via different communication methods such as Zigbee or Wi-Fi. Another study discovered an alarm system that might alert patients if their saturation of oxygen falls below a crucial level. The Blynk server was used to link a pulse oximeter and a WLAN router to the system.
C. Mood Monitoring	Mood monitoring is utilised to keep one's mental health in check by giving important information about an individual's emotional state. It also aids healthcare providers in the treatment of stress, sadness, and bipolar disorder are examples of mental illnesses. Stress may now be detected in advance by employing pulse rate and a powerful machine learning technique. It is also worth noting that stress analysis can help in the development of a system based on the Internet of Things capable of preventing an accident. When a driver enters a subconscious state, the technology switches off the vehicle's dc motor.
D. Iot For Smart Home/Building	In today's fast-paced world, smart homes are increasingly becoming a need. In a smart home, many household items may to communicate, you must be connected to the internet. The air conditioner, windows, doors, lights, clothes washer, and fridge in a smart house may all be controlled manually. The Internet of Things in conjunction with a wireless sensor network can give a smart solution for constructing energy management. Using a laptop or a smartphone, we may receive energy information and building control systems.
E. Iot For Smart Farming	IoT-based smart farming systems that use networked sensors may help monitor agricultural fields, sunlight, humidity, temperature, rain forecast, and moisture in the soil. IoT may also be used to automate irrigation systems. Smart farming benefits include increased efficiency in companies through process automation, increased quality of goods and volume, enhanced factory control, climate monitoring, and management of crops.

V. CHALLENGES

A. Smart Grid Challenges

Smart grids have a self-healing characteristic that distinguishes them from traditional grids. In the event of a device or network failure, which is one of the smart grid implementation issues, an alternate source of communication should be provided for service continuity and real-time automation. In a smart grid, a vast number of devices with varying power consumptions, operating times, application software, and wireless protocols are connected over the Internet. It is critical to provide efficient processing without any complexity or data loss for dependable smart grid operation and interoperability of smart devices. Interoperability of IoT systems and devices is both a difficulty and a requirement for effective heterogeneous system deployment. Cyber security of a smart grid communication network is also a significant concern.

B. Vulnerability To Network Attacks

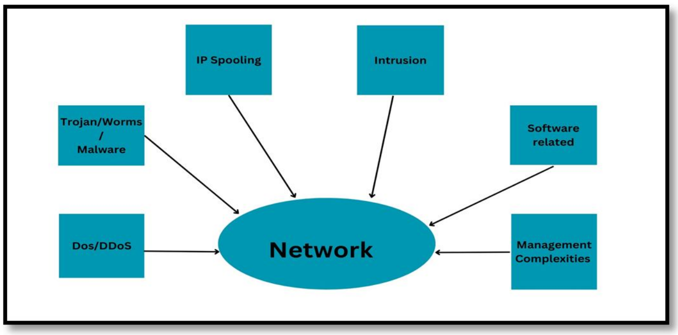

Fig. 4 Challenges

Vulnerability to network attacks refers to a network, system, or device's susceptibility to being penetrated or misused by cyber criminals. This might be caused by flaws in the network architecture, unfixed software, bad handling of passwords, or a lack of adequate security practises. It is critical to adopt robust security measures such as firewalls, encryption, and frequent software upgrades to limit exposure to network assaults, as well as educate users on safe internet practises. Because IoT devices rely on networks, they are vulnerable to assaults such as denial-of-service (DoS).

C. Data Management

Data management is critical to the IOT. In a world of networked gadgets constantly exchanging various types of information, the amount of produced data is enormous and the procedures involved in its administration become crucial.

D. Security

Security is a critical component of the Internet and a major worry for IoT. The number of IoT devices expands from millions to tens of billions over time. The possibility to exploit safety weaknesses, such as those present in low-cost or poorly manufactured equipment, develops as the number of linked devices grows. Data streams that are incomplete raise the threat of data theft, putting the safety and health of individuals at risk. Many IoT designs will also contain clusters of linked or adjacently comparable devices. Because of this uniformity, the potential effect of any one security issue is multiplied by the total amount of devices that share the same characteristics.

E. Scalability

Various new smart products or gadgets are constantly being added to the network. As a result, IoT should be capable of addressing, managing information, and providing service management in both local and large-scale settings. Scalability refers to a healthcare technology's capacity to adjust to environmental changes. A more scalable system runs smoothly and effectively, leveraging all available resources. As an outcome, it is necessary to build a device that is more scalable. This improves a system's efficiency for both present and future needs.

VI. ADVANTAGES AND DISADVANTAGES

Below in Table III are shown advantages and disadvantages of IOT:

TABLE III. ADVANTAGES AND DISADVANTAGES

Advantages	Disadvantages
Conserve Time: We save a significant amount of time by removing human effort. One of the key benefits of utilising an IoT platform is the ability to save time.	**Problem With Security:** Networks connect and interact with IoT systems. As an outcome, despite all safety precautions, the system provides little control and is vulnerable to a wide range of network assaults.
Enhanced Security: An interconnected system can aid in the smarter control of cities and homes via smartphones.	**Privacy Issues:** The IoT technology provides extensive personal information without the user's active participation.
Effective Resource Utilisation: Understanding how each thing works and how it operates can help us improve the way we utilise and evaluate natural resources.	**A Rise In Unemployment:** Inexperienced workers, like skilled people, face job loss and contribute to high rates of unemployment.
Useful For Safety Concerns: It is vital for safety since it identifies possible risks and alerts people to them.	**Intricacy Of The System:** The massive technology to IoT system is difficult to design, construct, manage, and enable.
Useful In The Medical Field: Without the need for a doctor's visit, medical attention may be delivered with greater efficiency and in real time.	**An Intense Dependence On The Web:** They rely entirely on the internet and cannot operate without it.

VII. CONCLUSION

In recent years, IoT has grown substantially, and a myriad of supporting technologies have been introduced. The IOT has emerged as the upcoming Internet trends.

We examined the IoT area, taking into account its architecture, applications, advantages, disadvantages, and obstacles. IoT has progressively introduced a sea of technical developments into everyday life using various technologies and apps, which in return helps to make our lives easier and more interesting. The challenges presented will form the basis of future advancement and research goals in the next years. IoT is still in its early stages. As sensor capabilities develop, one may create a strong IoT model, and therefore entire automated processes is possible with the help of IoT within a decade or two. Ultimately, The future of IoT is bright, but enormous volumes of data have made detection, interactions, the controller, and knowledge creation more challenging, yet its expansion will continue.

REFERENCES

[1] Internet of Things (IoT): A Literature Review Somayya Madakam, R. Ramaswamy, Siddharth Tripathi IT Applications Group, National Institute of Industrial Engineering (NITIE), Vihar Lake, Mumbai, India Email: somu4smart@gmail.com, ramaswamy2008@gmail.com, siddharth.iiita@gmail.com Received January 2015.

[2] IARJSET ISSN (Online) 2393-8021 ISSN (Print) 2394-1588 International Advanced Research Journal in Science, Engineering and Technology ISO 3297:2007 Certified Vol. 5, Issue 1, January 2018 Copyright to IARJSET DOI 10.17148/IARJSET.2018.517 41 Introduction to IOT Pradyumna Gokhale1 , Omkar Bhat2 , Sagar Bhat3 IT Dept., Smt. Kashibai Navale College of Engineering1-3.

[3] Study of IoT: Understanding IoT Architecture, Applications, Issues and Challenges Soumyalatha, Shruti G Hegde Assistant Professor, Department of Computer Science and Engineering Brindavan College of Engineering, Bangalore-63, India soumyanaveen.u@gmail.com, shruti601@gmail.com

[4] IoT-Based Applications in Healthcare Devices Bikash Pradhan , 1 Saugat Bhattacharyya , 2 and Kunal Pal 1 1 Department of Biotechnology and Medical Engineering, National Institute of Technology, Rourkela 769008, India 2 School of Computing,Engineering & Intelligent System, Ulster University, Londonderry, UK

[5] A Review Paper on Internet of Things(IoT) and its Applications Mrs. Sarika A. Korade1, Dr. Vinit Kotak2, Mrs. Asha Durafe3 1Student, Dept. of Electronics Engineering, SAKEC, Chembur, Mumbai, Maharashtra, India 2Professor, Dept. of Electronics Engineering, SAKEC, Chembur, Mumbai, Maharashtra, India 3Professor, Dept. of Electronics Engineering, SAKEC, Chembur, Mumbai, Maharashtra, India

[6] Solution Integration Approach using IoT in Education System Suja P Mathews#1,Dr.Raju R Gondkar*2 1 Assistant Professor, Dept. of MCA,JyotiNivas College, Bangalore,India 2 HOD, Department of Management Studies and Research, Nagarjuna Institute of Technology, Bangalore, India
[7] IoT Application, A Survey Harika Devi Kotha1*, V Mnssvkr Gupta 2 1Assistant Professor, Department of ECE, IFHE-FST, Hyderabad. India 2Assistant Professor, Department of CSE, SRKR Engineering College, Bhimavaram, India *Email: harikadevikotha@gmail.com
[8] IoT Challenges Rob van Kranenburg1* and Alex Bassi
[9] Shancang Li & Li Da Xu & Shanshan Zhao, “The internet of things: a survey”, Published online: 26 April 2014,Springer Science+Business Media New York 2014
[10] Antonio J. Jara, Miguel A. Zamora and Antonio F. G. Skarmeta, “An architecture based on Internet of Things to support mobility and security in medical environments”, University of Murcia, Computer Science Faculty, Murcia, Spain 2010.
[11] Jayavardhana Gubbia, Rajkumar Buyyab, Slaven Marusic a, Marimuthu Palaniswami, ― Internet of Things (IoT): A vision, architectural elements, and future directions”, Future Generation Computer Systems, Elsevier,2013.
[12] Aggarwal, R. and Lal Das, M. (2012) RFID Security in the Context of “Internet of Things”. First International Conference on Security of Internet of Things, Kerala, 17-19 August 2012, 51-56. http://dx.doi.org/10.1145/2490428.249043
[13] Dr. Ovidiu Vermesan SINTEF, Norway, FriessEU, Belgium, “Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems”, river publishers’ series in communications, 2013.
[14] RakeshRoshan ,Abhay Kr. Ray , “Challenges and Risk to Implement IOT in Smart Homes: An Indian Perspective”, IJCA(0975 – 8887) Volume 153 – No3, November 2016,16.
[15] AkshayGapchup, AnkitWani, DurveshGapchup, and ShashankJadhav, “Health Care Systems Using Internet of Things “,IJIRCCE Pune, India,Vol.-4,Issue-12,December2016.
[16] Jayavardhana, G., Rajkumar, B., Marusic, S. and Palaniswami, M. (2013) Internet of Things: A Vision, Architectural Elements, and Future Directions. Future Generation.
[17] Sun, C. (2012) Application of RFID Technology for Logistics on Internet of Things
[18] S Mandal , "Internet of Things (part 1)," Introduction ,[Online], source : http://www.csharpcorner.com/uploadfile/f88748/internet-of-things-iot-anintroduction/ , 2015
[19] Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: vision, applications and research challenges,” Ad Hoc Networks, vol.10, no.7, pp.1497-1516, 2012.
[20] Karen Rose, Scott Eldridge, Internet of Things: An Issues and Challenges of Internet Society (ISOC), 2015.
[21] IoT - Challenges and Opportunities in Indian Market”, COMSNET, Bangalore India January.
[22] SurendraDhote, “Internet of Things (IoT) Market in India”,April 24, 2017.