International Journal of Humanities Social Science and Management (IJHSSM)
Volume 2, Issue 1, pp: 93-99 www.ijhssm.org

Internet of things: Technology for the future

Ajay Lotheta
Asstt. Proff. UIT HPU Shimla-5.

Date of Submission: 05-04-2022 Date of Acceptance: 21-04-2022

Abstract: The IoT has become a prominent field of research. It is fast developing and has the potential to change our lives. The present paper studies the technical aspects of the IoT and the role it can play in our lives by various applications and the control on IoT. Much research needs to be done on the IoT and it is one of the important technology for the future.

I. INTRODUCTION

The **Internet of things** (**IoT**) describes physical objects (or groups of such objects) with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks. Internet of things has been considered a misnomer because devices do not need to be connected to the public internet, they only need to be connected to a network and be individually addressable.

The field has evolved due to the convergence of multiple technologies. Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), independently and collectively constitute the Internet of things. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", including devices and appliances (such as lighting fixtures, thermostats, home security systems, cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smart phones and smart speakers. IoT is also used in healthcare systems.

There are a number of concerns about the risks in the growth of IoT technologies and products, especially in the areas of privacy and security, and consequently, industry and governmental moves to address these concerns have begun, including the development of international and local standards, guidelines, and regulatory frameworks.

Historical Background:

The main concept of a network of smart devices was discussed as early as 1982, with a modified Coca-Cola vending machine at Carnegie Mellon University becoming the first ARPANET-connected appliance, able to report its inventory and whether newly loaded drinks were cold or not. Mark Weiser's 1991 paper on ubiquitous computing, "The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of the IOT. In 1994, Reza Raji described the concept in *IEEE Spectrum* as "[moving] small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories". Between 1993 and 1997, several companies proposed solutions like Microsoft's at Work or Novell's NEST. The field gained momentum when Bill Joy envisioned device-to-device communication as a part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999.

The concept of the "Internet of things" and the term itself, first appeared in a speech by Peter T. Lewis, to the Congressional Black Caucus Foundation 15th Annual Legislative Weekend in Washington, D.C, published in September 1985. According to Lewis, "The Internet of Things, or IoT, is the integration of people, processes and technology with connectable devices and sensors to enable remote monitoring, status, manipulation and evaluation of trends of such devices."

Defining the Internet of things as "simply the point in time when more 'things or objects' were connected to the Internet than people", Cisco Systems estimated that the IoT was "born" between 2008 and 2009, with the things/people ratio growing from 0.08 in 2003 to 1.84 in 2010.

Applications of IoT

The extensive set of applications for IoT devices is often divided into consumer, commercial, industrial, and infrastructure spaces.

A growing portion of IoT devices are created for consumer use, including connected vehicles, home automation, wearable technology, connected health, and appliances with remote monitoring capabilities.

Smart home

IoT devices are a part of the larger concept of home automation which can include lighting, heating and air conditioning, media and security systems and camera systems. Long-term benefits could include energy savings by automatically ensuring lights and electronics are turned off or by making the residents in the home aware of usage.

A smart home or automated home could be based on a platform or hubs that control smart devices and appliances. For instance, using apples homekit manufacturers can have their home products and accessories controlled by an application in ios devices such as the iphone and the apple watch. This could be a dedicated app or iOS native applications such as siri. This can be demonstrated in the case of Lenovo's Smart Home Essentials, which is a line of smart home devices that are controlled through Apple's Home app or Siri without the need for a Wi-Fi bridge. There are also dedicated smart home hubs that are offered as standalone platforms to connect different smart home products and these include the amazon home, Apple's homepod and Samsung's smart things hub. In addition to the commercial systems, there are many non-proprietary, open source ecosystems; including Home Assistant, OpenHAB and Domoticz.

Elder care

One key application of a smart home is to provide assistance to elderly people and people with disabilities. These home systems use assistive technology to accommodate an owner's specific disabilities. Voice control can assist users with sight and mobility limitations while alert systems can be connected directly to cochlear implants worn by hearing-impaired users. They can also be equipped with additional safety features. These features can include sensors that monitor for medical emergencies such as falls or seizures. Smart home technology applied in this way can provide users with more freedom and a higher quality of life.

The term "Enterprise IoT" refers to devices used in business and corporate settings. By 2019, it is estimated that the EIoT will account for 9.1 billion devices.

Medical and healthcare

The **Internet of Medical Things** (**IoMT**) is an application of the IoT for medical and health related purposes, data collection and analysis for research, and monitoring.The IoMT has been referenced as "Smart Healthcare" as the technology for creating a digitized healthcare system, connecting available medical resources and healthcare services.

IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids. Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses. A 2015 Goldman Sachs report indicated that healthcare IoT devices "can save the United States more than $300 billion in annual healthcare expenditures by increasing revenue and decreasing cost." Moreover, the use of mobile devices to support medical follow-up led to the creation of 'm-health', used analyzed health statistics."

Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people to regain lost mobility via therapy as well. These sensors create a network of intelligent sensors that are able to collect, process, transfer, and analyze valuable information in different environments, such as connecting in-home monitoring devices to hospital-based systems. End-to-end health monitoring IoT platforms are also available for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements.

As of 2018 IoMT was not only being applied in the clinical laboratory industry, but also in the healthcare and health insurance industries. IoMT in the healthcare industry is now permitting doctors, patients, and others, such as guardians of patients, nurses, families, and similar, to be part of a system, where patient records are saved in a database, allowing doctors and the rest of the medical staff to have access to patient information.[59] Moreover, IoT-based systems are patient-centered, which involves being flexible to the patient's medical conditions. IoMT in the insurance industry provides access to better and new

types of dynamic information. This includes sensor-based solutions such as biosensors, wearables, connected health devices, and mobile apps to track customer behavior. This can lead to more accurate underwriting and new pricing models.

The application of the IoT in healthcare plays a fundamental role in managing chronic diseases and in disease prevention and control. Remote monitoring is made possible through the connection of powerful wireless solutions. The connectivity enables health practitioners to capture patient's data and applying complex algorithms in health data analysis.

Transportation

Digital variable speed-limit sign

The IoT can assist in the integration of communications, control, and information processing across various transportation systems. Application of the IoT extends to all aspects of transportation systems (i.e. the vehicle, the infrastructure, and the driver or user). Dynamic interaction between these components of a transport system enables inter- and intra-vehicular communication, smart traffic control, smart parking, logistics and fleet managemant, vehicle control safety, and road assistance.

V2X communications

In vehicular communications systems (V2X), consists of three main components: vehicle to vehicle communication (V2V), vehicle to infrastructure communication (V2I) and vehicle to pedestrian communications (V2P). V2X is the first step to autonomous driving and connected road infrastructure.

Building and home automation

IoT devices can be used to monitor and control the mechanical, electrical and electronic systems used in various types of buildings (e.g., public and private, industrial, institutions, or residential) in home automation building automation systems. In this context, three main areas are being covered in literature:

- The integration of the Internet with building energy management systems in order to create energy-efficient and IOT-driven "smart buildings".
- The possible means of real-time monitoring for reducing energy consumption and monitoring occupant behaviors.
- The integration of smart devices in the built environment and how they might be used in future applications.

Also known as IIoT, industrial IoT devices acquire and analyze data from connected equipment, operational technology (OT), locations, and people. Combined with operational technology (OT) monitoring devices, IIoT helps regulate and monitor industrial systems. Also, the same implementation can be carried out for automated record updates of asset placement in industrial storage units as the size of the assets can vary from a small screw to the whole motor spare part, and misplacement of such assets can cause a percentile loss of manpower time and money.

Manufacturing

The IoT can connect various manufacturing devices equipped with sensing, identification, processing, communication, actuation, and networking capabilities. Network control and management of manufacturing equipmant and situation management, or manufacturing process control allow IoT to be used for industrial applications and smart manufacturing. IoT intelligent systems enable rapid manufacturing and optimization of new products, and rapid response to product demands.

Digital control systems to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IIoT. IoT can also be applied to asset management via predictive maintenance, statistical evaluation, and measurements to maximize reliability. Industrial management systems can be integrated with smart grids, enabling energy optimization. Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by networked sensors.

In addition to general manufacturing, IoT is also used for processes in the industrialization of construction.

Agriculture

There are numerous IoT applications in farming such as collecting data on temperature, rainfall, humidity, wind speed, pest infestation, and soil content. This data can be used to automate farming techniques, take informed decisions to improve quality and quantity, minimize risk and waste, and reduce the effort required to manage crops. For example, farmers can now monitor soil temperature and moisture from afar, and even apply IoT-acquired data to precision fertilization programs.[72] The overall goal is that data from sensors, coupled with the farmer's knowledge and

intuition about his or her farm, can help increase farm productivity, and also help reduce costs.

In August 2018, ToyotaTsusho began a partnership with Microsoft to create fish farming tools using the Microsoft Azure application suite for IoT technologies related to water management. Developed in part by researchers from Kindai University, the water pump mechanisms use artificial intelligence to count the number of fish on a conveyor belt, analyze the number of fish, and deduce the effectiveness of water flow from the data the fish provide. The FarmBeats project from Microsoft Research that uses TV white space to connect farms is also a part of the Azure Marketplace now.

Maritime

IoT devices are in use monitoring the environments and systems of boats and yachts. Many pleasure boats are left unattended for days in summer, and months in winter so such devices provide valuable early alerts of boat flooding, fire, and deep discharge of batteries. The use of global internet data networks such as Sigfox, combined with long-life batteries, and microelectronics allows the engine rooms, bilge, and batteries to be constantly monitored and reported to a connected Android & Apple applications for example.

Metropolitan scale deployments

There are several planned or ongoing large-scale deployments of the IoT, to enable better management of cities and systems. For example, Songdo, South Korea, the first of its kind fully equipped and wired smart city, is gradually being built, with approximately 70 percent of the business district completed as of June 2018. Much of the city is planned to be wired and automated, with little or no human intervention.

Another application is currently undergoing a project in Santander, Spain. For this deployment, two approaches have been adopted. This city of 180,000 inhabitants has already seen 18,000 downloads of its city smartphone app. The app is connected to 10,000 sensors that enable services like parking search, environmental monitoring, digital city agenda, and more. City context information is used in this deployment so as to benefit merchants through a spark deals mechanism based on city behavior that aims at maximizing the impact of each notification.

Energy management

Significant numbers of energy-consuming devices (e.g. lamps, household appliances, motors, pumps, etc.) already integrate Internet connectivity, which can allow them to communicate with utilities not only to balance power generation but also helps optimize the energy consumption as a whole. These devices allow for remote control by users, or central management via a cloud-based interface, and enable functions like scheduling (e.g., remotely powering on or off heating systems, controlling ovens, changing lighting conditions etc.). The smart grid is a utility-side IoT application; systems gather and act on energy and power-related information to improve the efficiency of the production and distribution of electricity. Using advanced metering infrastructure (AMI) Internet-connected devices, electric utilities not only collect data from end-users, but also manage distribution automation devices like transformers.

Environmental monitoring

Environmental monitoring applications of the IoT typically use sensors to assist in environmental protection by monitoring air or water quality, atmospheric or soil conditions, and can even include areas like monitoring the movements of wildlife and their habitats. Development of resource-constrained devices connected to the Internet also means that other applications like earthquake or tsunami early-warning systems can also be used by emergency services to provide more effective aid. IoT devices in this application typically span a large geographic area and can also be mobile. It has been argued that the standardization that IoT brings to wireless sensing will revolutionize this area.

Living Lab

Another example of integrating the IoT is Living Lab which integrates and combines research and innovation processes, establishing within a public-private-people-partnership. There are currently 320 Living Labs that use the IoT to collaborate and share knowledge between stakeholders to co-create innovative and technological products. For companies to implement and develop Ion services for smart cities, they need to have incentives. The governments play key roles in smart city projects as changes in policies will help cities to implement the IoT which provides effectiveness, efficiency, and accuracy of the resources that are being used. For instance, the government provides tax incentives and cheap rent, improves public transports, and offers an

environment where start-up companies, creative industries, and multinationals may co-create, share a common infrastructure and labor markets, and take advantage of locally embedded technologies, production process, and transaction costs. The relationship between the technology developers and governments who manage the city's assets, is key to provide open access to resources to users in an efficient way.

Internet of Battlefield Things

The **Internet of Battlefield Things** (**IoBT**) is a project initiated and executed by the U.S. Army Research Laboratory (ARL) that focuses on the basic science related to the IoT that enhance the capabilities of Army soldiers. In 2017, ARL launched the Internet of Battlefield Things Collaborative Research Alliance (IoBT-CRA), establishing a working collaboration between industry, university, and Army researchers to advance the theoretical foundations of IoT technologies and their applications to Army operations.

Product digitalization

There are several applications of smart or active packaging in which a QR code or NFC tag is affixed on a product or its packaging. The tag itself is passive, however, it contains a unique identifier (typically a URL) which enables a user to access digital content about the product via a smartphone. Strictly speaking, such passive items are not part of the Internet of things, but they can be seen as enablers of digital interactions. The term "Internet of Packaging" has been coined to describe applications in which unique identifiers are used, to automate supply chains, and are scanned on large scale by consumers to access digital content. Authentication of the unique identifiers, and thereby of the product itself, is possible via a copy-sensitive digital watermark or copy detection pattern for scanning when scanning a QR code, while NFC tags can encrypt communication.

Network architecture

The Internet of things requires huge scalability in the network space to handle the surge of devices. IETF 6LoWPAN would be used to connect devices to IP networks. With billions of devices[126] being added to the Internet space, will play a major role in handling the network layer scalability. IETF's Constrained Application Protocol, ZeroMQ, and MQTT would provide lightweight data transport.

Fog computing is a viable alternative to prevent such a large burst of data flow through the Internet. The edge devices' computation power to analyse and process data is extremely limited. Limited processing power is a key attribute of IoT devices as their purpose is to supply data about physical objects while remaining autonomous. Heavy processing requirements use more battery power harming IoT's ability to operate. Scalability is easy because IoT devices simply supply data through the internet to a server with sufficient processing power.

Decentralized IoT

Decentralized Internet of things, or decentralized IoT, is a modified IoT. It utilizes Fog Computing to handle and balance requests of connected IoT devices in order to reduce loading on the cloud servers, and improve responsiveness for latency-sensitive IoT applications like vital signs monitoring of patients, vehicle-to-vehicle communication of autonomous driving, and critical failure detection of industrial devices.

Conventional IoT is connected via a mesh network and led by a major head node (centralized controller). The head node decides how a data is created, stored, and transmitted. In contrast, decentralized IoT attempts to divide IoT systems into smaller divisions. The head node authorizes partial decision making power to lower level sub-nodes under mutual agreed policy. Performance is improved, especially for huge IoT systems with millions of nodes.

Decentralized IoT attempts to address the limited bandwidth and hashing capacity of battery-powered or wireless IoT devices via lightweight blockchain.

Cyberattack identification can be done through early detection and mitigation at the edge nodes with traffic monitoring and evaluation.

The Internet of things would encode 50 to 100 trillion objects, and be able to follow the movement of those objects. Human beings in surveyed urban environments are each surrounded by 1000 to 5000 trackable objects.] In 2015 there were already 83 million smart devices in people's homes. This number is expected to grow to 193 million devices by 2020.

The figure of online capable devices grew 31% from 2016 to 2017 to reach 8.4 billion.

Enabling technologies for IoT

There are many technologies that enable the IoT. Crucial to the field is the network used to communicate between devices of an IoT installation,

a role that several wireless or wired technologies may fulfill

Addressability

The original idea of the Auto-ID Center is based on RFID-tags and distinct identification through the Electronic Product Code. This has evolved into objects having an IP address or URI. An alternative view, from the world of the Semantic Web focuses instead on making all things (not just those electronic, smart, or RFID-enabled) addressable by the existing naming protocols, such as URI. The objects themselves do not converse, but they may now be referred to by other agents, such as powerful centralised servers acting for their human owners. Integration with the Internet implies that devices will use an IP address as a distinct identifier. Due to the limited address space of IPv4 (which allows for 4.3 billion different addresses), objects in the IoT will have to use the next generation of the Internet protocol (IPv6) to scale to the extremely large address space required. Internet-of-things devices additionally will benefit from the stateless address auto-configuration present in IPv6, as it reduces the configuration overhead on the hosts, and the IETF 6LoWPAN header compression. To a large extent, the future of the Internet of things will not be possible without the support of IPv6; and consequently, the global adoption of IPv6 in the coming years will be critical for the successful development of the IoT in the future.

Application Layer

- ADRC[174] defines an application layer protocol and supporting framework for implementing IoT applications.

Short-range wireless

- Bluetooth mesh networking – Specification providing a mesh networking variant to Bluetooth low energy (BLE) with an increased number of nodes and standardized application layer (Models).
- Light-Fidelity (Li-Fi) – Wireless communication technology similar to the Wi-Fi standard, but using visible light communication for increased bandwidth.
- Near-field communication (NFC) – Communication protocols enabling two electronic devices to communicate within a 4 cm range.
- Radio-frequency identification (RFID) – Technology using electromagnetic fields to read data stored in tags embedded in other items.
- Wi-Fi – Technology for local area networking based on the IEEE 802.11 standard, where devices may communicate through a shared access point or directly between individual devices.
- Z-Wave – Wireless communications protocol used primarily for home automation and security applications

Medium-range wireless

- LTE-Advanced – High-speed communication specification for mobile networks. Provides enhancements to the LTE standard with extended coverage, higher throughput, and lower latency.
- 5G - 5G wireless networks can be used to achieve the high communication requirements of the IoT and connect a large number of IoT devices, even when they are on the move.

Long-range wireless

- Low-power wide-area networking (LPWAN) – Wireless networks designed to allow long-range communication at a low data rate, reducing power and cost for transmission. Available LPWAN technologies and protocols: LoRaWan, Sigfox, NB-IoT, Weightless, RPMA.
- Very small aperture terminal (VSAT) – Satellite communication technology using small dish antennas for narrowband and broadband data.

Wired

- Ethernet – General purpose networking standard using twisted pair and fiber optic links in conjunction with hubs or switches.
- Power-line communication (PLC) – Communication technology using electrical wiring to carry power and data. Specifications such as HomePlug or G.hn utilize PLC for networking IoT devices.

Some scholars and activists argue that the IoT can be used to create new models of civic engagement if device networks can be open to user control and inter-operable platforms. Philip N. Howard, a professor and author, writes that political life in both democracies and authoritarian regimes will be shaped by the way the IoT will be used for civic engagement. For that to happen, he argues that any connected device should be able to divulge a list of the "ultimate beneficiaries" of its sensor data and that individual citizens should be able to add new organisations to the beneficiary list. In addition, he argues that civil society groups need to start developing their IoT strategy for making use of data and engaging with the public.

Government regulation on IoT

One of the key drivers of the IoT is data. The success of the idea of connecting devices to make them more efficient is dependent upon access to and storage & processing of data. For this purpose, companies working on the IoT collect data from multiple sources and store it in their cloud network for further processing. This leaves the door wide open for privacy and security dangers and single point vulnerability of multiple systems. The other issues pertain to consumer choice and ownership of data and how it is used. Though still in their infancy, regulations and governance regarding these issues of privacy, security, and data ownership continue to develope IoT regulation depends on the country. Some examples of legislation that is relevant to privacy and data collection are: the US Privacy Act of 1974, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980, and the EU Directive 95/46/EC of 1995.

Data storage

A challenge for producers of IoT applications is to clean, process and interpret the vast amount of data which is gathered by the sensors. There is a solution proposed for the analytics of the information referred to as Wireless Sensor Networks. These networks share data among sensor nodes that are sent to a distributed system for the analytics of the sensory data.[]

Another challenge is the storage of this bulk data. Depending on the application, there could be high data acquisition requirements, which in turn lead to high storage requirements. Currently the Internet is already responsible for 5% of the total energy generated, and a "daunting challenge to power" IoT devices to collect and even store data still remains.

II. CONCLUSION :

The internet is the fast developing technology that is poised to grow rapidly and transform our lives in housing, urban facilities, transportation and smart homes and offices. As the more focus is given to it it will continue to grow and scope of research and utility in this field are enormous as it is a technology for the future.

REFERENCES :

[1]. Gillis, Alexander (2021). "What is internet of things (IoT)?". IOT Agenda. Retrieved 17 August 2021.
[2]. Brown, Eric (20 September 2016). "21 Open Source Projects for IoT". Linux.com. Retrieved 23 October 2016.
[3]. "Internet of Things Global Standards Initiative". ITU. Retrieved 26 June 2015.
[4]. Hendricks, Drew. "The Trouble with the Internet of Things". London Datastore. Greater London Authority. Retrieved 10 August 2015.
[5]. Internet of things and big data analytics toward next-generation intelligence. Nilanjan Dey, Aboul Ella Hassanien, Chintan Bhatt, Amira Ashour, Suresh Chandra Satapathy. Cham, Switzerland. 2018. p. 440. ISBN 978-3-319-60435-0. OCLC 1001327784.
[6]. "Forecast: The Internet of Things, Worldwide, 2013". Gartner. Retrieved 3 March 2022.
[7]. Hu, J.; Niu, H.; Carrasco, J.; Lennox, B.; Arvin, F., "Fault-tolerant cooperative navigation of networked UAV swarms for forest fire monitoring" Aerospace Science and Technology, 2022.
[8]. Hu, J.; Lennox, B.; Arvin, F., "Robust formation control for networked robotic systems using Negative Imaginary dynamics" Automatica, 2022.
[9]. Laplante, Phillip A.; Kassab, Mohamad; Laplante, Nancy L.; Voas, Jeffrey M. (2018). "Building Caring Healthcare Systems in the Internet of Things". IEEE Systems Journal. **12** (3): 3030–3037. Bibcode:2018ISysJ..12.3030L. doi:10.1109/JSYST.2017.2662602. ISSN 1932-8184. PMC 6506834. PMID 31080541.
[10]. "The New York City Internet of Things Strategy". www1.nyc.gov. Retrieved 6 September 2021.