**Poonguzhali.R**

**INTERNET OF THINGS**

The **Internet of things** (**IoT**) describes physical objects (or groups of such objects) with [sensors](https://en.wikipedia.org/wiki/Sensor), processing ability, [software](https://en.wikipedia.org/wiki/Software), and other technologies that connect and exchange data with other devices and systems over the [Internet](https://en.wikipedia.org/wiki/Internet) or other communications networks. Internet of things has been considered a [misnomer](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/Technologies), including [ubiquitous computing](https://en.wikipedia.org/wiki/Ubiquitous_computing), [commodity](https://en.wikipedia.org/wiki/Commodity) [sensors](https://en.wikipedia.org/wiki/Sensors), increasingly powerful [embedded systems](https://en.wikipedia.org/wiki/Embedded_system), and [machine learning](https://en.wikipedia.org/wiki/Machine_learning). Traditional fields of [embedded systems](https://en.wikipedia.org/wiki/Embedded_system), [wireless sensor networks](https://en.wikipedia.org/wiki/Wireless_sensor_network), control systems, [automation](https://en.wikipedia.org/wiki/Automation) (including [home](https://en.wikipedia.org/wiki/Home_automation) and [building automation](https://en.wikipedia.org/wiki/Building_automation)), independently and collectively enable the Internet of thing. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "[smart home](https://en.wikipedia.org/wiki/Smart_home_technology)", including devices and [appliances](https://en.wikipedia.org/wiki/Home_appliance) (such as lighting fixtures, [thermostats](https://en.wikipedia.org/wiki/Thermostats), home [security systems](https://en.wikipedia.org/wiki/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 [smartphones](https://en.wikipedia.org/wiki/Smartphone) and [smart speakers](https://en.wikipedia.org/wiki/Smart_speaker). IoT is also used in [healthcare systems](https://en.wikipedia.org/wiki/Health_system).

There are number of concerns about the risks in the growth of IoT technologies and products, especially in the areas of [privacy](https://en.wikipedia.org/wiki/Digital_privacy) and [security](https://en.wikipedia.org/wiki/Digital_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.

History

In 2004 Cornelius "Pete" Peterson, CEO of NetSilicon, predicted that, "The next era of information technology will be dominated by [IoT] devices, and networked devices will ultimately gain in popularity and significance to the extent that they will far exceed the number of networked computers and workstations." Peterson believed that medical devices and industrial controls would become dominant applications of the technology.

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](https://en.wikipedia.org/wiki/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.

**Application**

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

### Consumer applications

A growing portion of IoT devices are created for consumer use, including connected vehicles, [home automation](https://en.wikipedia.org/wiki/Home_automation), [wearable technology](https://en.wikipedia.org/wiki/Wearable_technology), connected health, and appliances with remote monitoring capabilities.

#### Smart home

IoT devices are a part of the larger concept of [home automation](https://en.wikipedia.org/wiki/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.

### Organizational applications

#### 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](https://en.wikipedia.org/wiki/Remote_patient_monitoring) and [emergency notification systems](https://en.wikipedia.org/wiki/Emergency_notification_system). 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."

#### Transportation

[](https://en.wikipedia.org/wiki/File:Nov%C3%A1_Povltavsk%C3%A1,_Ho%C5%99%C3%AD_v_tunelu_(01).jpg)

The IoT can assist in the integration of communications, control, and information processing across various [transportation systems](https://en.wikipedia.org/wiki/Intelligent_transportation_system). Application of the IoT extends to all aspects of transportation systems (i.e. the vehiclethe infrastructure, and the driver or user). Dynamic interaction between these components of a transport system enables inter- and intra-vehicular communication, [smart traffic control](https://en.wikipedia.org/wiki/Smart_traffic_light), smart parking, [electronic toll collection systems](https://en.wikipedia.org/wiki/Electronic_toll_collection), [logistics](https://en.wikipedia.org/wiki/Logistics_management) and [fleet management](https://en.wikipedia.org/wiki/Fleet_management), [vehicle control](https://en.wikipedia.org/wiki/Autonomous_cruise_control_system), safety, and road assistance.

#### 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](https://en.wikipedia.org/wiki/Home_automation) and [building automation](https://en.wikipedia.org/wiki/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 consumptionand monitoring occupant behaviors.
* The integration of smart devices in the built environment and how they might be used in future applications.

### Industrial 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 loss of manpower time and money.

**Trends And Characteristics**

The IoT's major significant trend in recent years is the explosive growth of devices connected and controlled via the Internet. The wide range of applications for IoT technology mean that the specifics can be very different from one device to the next but there are basic characteristics shared by most.

The IoT creates opportunities for more direct integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions.

The number of IoT devices increased 31% year-over-year to 8.4 billion in the year 2017 and it is estimated that there will be 30 billion devices by 2020. The global market value of the IoT is projected to reach $7.1 trillion by 2020.

### Intelligence

[Ambient intelligence](https://en.wikipedia.org/wiki/Ambient_intelligence) and autonomous control are not part of the original concept of the Internet of things. Ambient intelligence and autonomous control do not necessarily require Internet structures, either. However, there is a shift in research (by companies such as [Intel](https://en.wikipedia.org/wiki/Intel)) to integrate the concepts of the IoT and autonomous control, with initial outcomes towards this direction considering objects as the driving force for autonomous IoT. A promising approach in this context is [deep reinforcement learning](https://en.wikipedia.org/wiki/Reinforcement_learning) where most of IoT systems provide a dynamic and interactive environment. Training an agent (i.e., IoT device) to behave smartly in such an environment cannot be addressed by conventional machine learning algorithms such as [supervised learning](https://en.wikipedia.org/wiki/Supervised_learning). By reinforcement learning approach, a learning agent can sense the environment's state (e.g., sensing home temperature), perform actions (e.g., turn [HVAC](https://en.wikipedia.org/wiki/HVAC) on or off) and learn through the maximizing accumulated rewards it receives in long term.

### Social Internet of things

Social Internet of things (SIoT) is a new kind of IoT that focuses the importance of social interaction and relationship between IoT devices. SIoT is a pattern of how cross-domain IoT devices enabling application to application communication and collaboration without human intervention in order to serve their owners with autonomous services, and this only can be realized when gained low-level architecture support from both IoT software and hardware engineering.

#### Social Network for IoT Devices (Not Human)

IoT defines a device with an identity like a citizen in a community, and connect them to the internet to provide services to its users sIot defines a social network for IoT devices only to interact with each other for different goals that to serve human.

**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](https://en.wikipedia.org/wiki/Auto-ID_Labs) is based on RFID-tags and distinct identification through the [Electronic Product Code](https://en.wikipedia.org/wiki/Electronic_Product_Code). This has evolved into objects having an IP address or [URI](https://en.wikipedia.org/wiki/Uniform_resource_identifier). An alternative view, from the world of the [Semantic Web](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/IP_address) as a distinct identifier. Due to the [limited address space](https://en.wikipedia.org/wiki/IPv4_address_exhaustion) of [IPv4](https://en.wikipedia.org/wiki/IPv4) (which allows for 4.3 billion different addresses), objects in the IoT will have to use [the next generation](https://en.wikipedia.org/wiki/IPv6) of the Internet protocol ([IPv6](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/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.

### Data storage

A challenge for producers of IoT applications is to [clean](https://en.wikipedia.org/wiki/Data_cleansing), 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.

Data silos, although a common challenge of legacy systems, still commonly occur with the implementation of IoT devices, particularly within manufacturing. As there are a lot of benefits to be gained from IoT and IIoT devices, the means in which the data is stored can present serious challenges without the principles of autonomy, transparency, and interoperability being considered. The challenges do not occur by the device itself, but the means in which databases are warehouses are set-up. These challenges were commonly identified in manufactures and enterprises which have begun upon digital transformation, and are part of the digital foundation, indicating that in order to receive the optimal benefits from IoT devices and for decision making, enterprises will have to first re-align their data storing methods. These challenges were identified by Keller (2021) when investigating the IT and application landscape of I4.0 implementation within German M&E manufactures.

### Safety

IoT systems are typically controlled by event-driven smart apps that take as input either sensed data, user inputs, or other external triggers (from the Internet) and command one or more actuators towards providing different forms of automation. Examples of sensors include smoke detectors, motion sensors, and contact sensors. Examples of actuators include smart locks, smart power outlets, and door controls. Popular control platforms on which third-party developers can build smart apps that interact wirelessly with these sensors and actuators include Samsung's SmartThings, Apple's HomeKit, and Amazon's Alexa, among others.

A problem specific to IoT systems is that buggy apps, unforeseen bad app interactions, or device/communication failures, can cause unsafe and dangerous physical states, e.g., "unlock the entrance door when no one is at home" or "turn off the heater when the temperature is below 0 degrees Celsius and people are sleeping at night". Detecting flaws that lead to such states, requires a holistic view of installed apps, component devices, their configurations, and more importantly, how they interact. Recently, researchers from the University of California Riverside have proposed IotSan, a novel practical system that uses model checking as a building block to reveal "interaction-level" flaws by identifying events that can lead the system to unsafe states They have evaluated IotSan on the Samsung SmartThings platform. From 76 manually configured systems, IotSan detects 147 vulnerabilities (i.e., violations of safe physical states/properties).

Iot Adoption Barriers

[](https://en.wikipedia.org/wiki/File:WilliamRuhAtIEEETechIgnite2017.jpg)

### Lack of interoperability and unclear value propositions

Despite a shared belief in the potential of the IoT, industry leaders and consumers are facing barriers to adopt IoT technology more widely. Mike Farley argued in [Forbes](https://en.wikipedia.org/wiki/Forbes) that while IoT solutions appeal to [early adopters](https://en.wikipedia.org/wiki/Early_adopters), they either lack interoperability or a clear use case for end-users. A study by Ericsson regarding the adoption of IoT among Danish companies suggests that many struggle "to pinpoint exactly where the value of IoT lies for them".