**Sahira Banu.J**

**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.

#### Agriculture

There are numerous IoT applications in farming[[]](https://en.wikipedia.org/wiki/Internet_of_things" \l "cite_note-MeolaWhy16-73) 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. 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, [Toyota Tsusho](https://en.wikipedia.org/wiki/Toyota_Tsusho) began a partnership with [Microsoft](https://en.wikipedia.org/wiki/Microsoft) to create [fish farming](https://en.wikipedia.org/wiki/Fish_farming) tools using the [Microsoft Azure](https://en.wikipedia.org/wiki/Microsoft_Azure) application suite for IoT technologies related to water management. Developed in part by researchers from [Kindai University](https://en.wikipedia.org/wiki/Kindai_University" \o "Kindai University), the water pump mechanisms use [artificial intelligence](https://en.wikipedia.org/wiki/Artificial_intelligence) to count the number of fish on a [conveyor belt](https://en.wikipedia.org/wiki/Conveyor_belt), analyze the number of fish, and deduce the effectiveness of water flow from the data the fish provide.[[]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-75) 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.[[]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-78) 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](https://en.wikipedia.org/wiki/Sigfox" \o "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.

#### 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.

#### Internet of Battlefield Things

The **Internet of Battlefield Things** (**IoBT**) is a project initiated and executed by the [U.S. Army Research Laboratory (ARL)](https://en.wikipedia.org/wiki/United_States_Army_Research_Laboratory) 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)](https://en.wikipedia.org/wiki/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.

#### Ocean of Things

The **Ocean of Things** project is a [DARPA](https://en.wikipedia.org/wiki/DARPA)-led program designed to establish an Internet of things across large ocean areas for the purposes of collecting, monitoring, and analyzing environmental and vessel activity data. The project entails the deployment of about 50,000 floats that house a passive sensor suite that autonomously detect and track military and commercial vessels as part of a cloud-based network.

### Product digitalization

There are several applications of smart or [active packaging](https://en.wikipedia.org/wiki/Active_packaging) in which a [QR code](https://en.wikipedia.org/wiki/QR_code) or [NFC tag](https://en.wikipedia.org/wiki/NFC_tag) is affixed on a product or its packaging. The tag itself is passive, however, it contains a [unique identifier](https://en.wikipedia.org/wiki/Unique_identifier) (typically a [URL](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/Digital_watermark) or [copy detection pattern](https://en.wikipedia.org/wiki/Copy_detection_pattern) for scanning when scanning a QR code, while NFC tags can encrypt communication.

**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 IoT Challenges

1. Internet of things is multifaceted and complicated. One of the main factors that hindering people from adopting and use Internet of things (IoT) based products and services is its complexity. Installation and setup is a challenge to people, therefore, there is a need for IoT devices to mix match and configure themselves automatically to provide different services at different situation.
2. System security always a concern for any technology, and it is more crucial for SIoT as not only security of oneself need to be considered but also the mutual trust mechanism between collaborative IoT devices from time to time, from place to place.
3. Another critical challenge for SIoT is the accuracy and reliability of the sensors. At most of the circumstances, IoT sensors would need to respond in nanoseconds to avoid accidents, injury, and loss of life.

**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:

### Environmental sustainability impact

A concern regarding Internet-of-things technologies pertains to the environmental impacts of the manufacture, use, and eventual disposal of all these semiconductor-rich devices. Modern electronics are replete with a wide variety of heavy metals and rare-earth metals, as well as highly toxic synthetic chemicals. This makes them extremely difficult to properly recycle. Electronic components are often incinerated or placed in regular landfills. Furthermore, the human and environmental cost of mining the rare-earth metals that are integral to modern electronic components continues to grow. This leads to societal questions concerning the environmental impacts of IoT devices over their lifetime

### 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.

### Confusing terminology

Kevin Lonergan at *Information Age*, a business technology magazine, has referred to the terms surrounding the IoT as a "terminology zoo". The lack of clear terminology is not "useful from a practical point of view" and a "source of confusion for the end user". A company operating in the IoT space could be working in anything related to sensor technology, networking, embedded systems, or analytics.[[270]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-Vitesse_Media_Plc-270) According to Lonergan, the term IoT was coined before smart phones, tablets, and devices as we know them today existed, and there is a long list of terms with varying degrees of overlap and [technological convergence](https://en.wikipedia.org/wiki/Technological_convergence): Internet of things, Internet of everything (IoE), Internet of goods (supply chain), industrial Internet, [pervasive computing](https://en.wikipedia.org/wiki/Pervasive_computing), pervasive sensing, [ubiquitous computing](https://en.wikipedia.org/wiki/Ubiquitous_computing), [cyber-physical systems](https://en.wikipedia.org/wiki/Cyber-physical_system) (CPS), [wireless sensor networks](https://en.wikipedia.org/wiki/Wireless_sensor_network) (WSN), [smart objects](https://en.wikipedia.org/wiki/Smart_object), [digital twin](https://en.wikipedia.org/wiki/Digital_twin), cyberobjects or avatars, cooperating objects, [machine to machine](https://en.wikipedia.org/wiki/Machine_to_machine) (M2M), ambient intelligence (AmI), [Operational technology](https://en.wikipedia.org/wiki/Operational_Technology) (OT), and [information technology](https://en.wikipedia.org/wiki/Information_technology) (IT). Regarding IIoT, an industrial sub-field of IoT, the [Industrial Internet Consortium](https://en.wikipedia.org/wiki/Industrial_Internet_Consortium)'s Vocabulary Task Group has created a "common and reusable vocabulary of terms"[[271]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-Technology_Working_Group-271) to ensure "consistent terminology" across publications issued by the Industrial Internet Consortium. IoT One has created an IoT Terms Database including a New Term Alert to be notified when a new term is published. As of March 2020, this database aggregates 807 IoT-related terms, while keeping material "transparent and comprehensive."

**Iot Adoption Barriers**

### Privacy and security concerns

As for IoT, especially in regards to consumer IoT, information about a user's daily routine is collected so that the “things” around the user can cooperate to provide better services that fulfill personal preference. When the collected information which describes a user in detail travels through multiple [hops](https://en.wikipedia.org/wiki/Hops) in a network, due to a diverse integration of services, devices and network, the information stored on a device is vulnerable to [privacy violation](https://en.wikipedia.org/wiki/Privacy_violation) by compromising nodes existing in an IoT network.

For example, on 21 October 2016, a multiple [distributed denial of service](https://en.wikipedia.org/wiki/Distributed_denial_of_service) (DDoS) attacks systems operated by [domain name system](https://en.wikipedia.org/wiki/Domain_name_system) provider Dyn, which caused the inaccessibility of several websites, such as [GitHub](https://en.wikipedia.org/wiki/GitHub" \o "GitHub), [Twitter](https://en.wikipedia.org/wiki/Twitter), and others. This attack is executed through a [botnet](https://en.wikipedia.org/wiki/Botnet) consisting of a large number of IoT devices including IP cameras, [gateways](https://en.wikipedia.org/wiki/Residential_gateway), and even baby monitors.

Fundamentally there are 4 security objectives that the IoT system requires: (1) data [confidentiality](https://en.wikipedia.org/wiki/Confidentiality): unauthorized parties cannot have access to the transmitted and stored data; (2) data [integrity](https://en.wikipedia.org/wiki/Integrity): intentional and unintentional [corruption](https://en.wikipedia.org/wiki/Corruption) of transmitted and stored data must be detected; (3) [non-repudiation](https://en.wikipedia.org/wiki/Non-repudiation): the sender cannot deny having sent a given message; (4) data availability: the transmitted and stored data should be available to authorized parties even with the [denial-of-service](https://en.wikipedia.org/wiki/Denial-of-service) (DOS) attacks.