**Roselin Juliyat.L**

**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.

#### Manufacturing

The IoT can connect various manufacturing devices equipped with sensing, identification, processing, communication, actuation, and networking capabilities. Network control and management of [manufacturing equipment](https://en.wikipedia.org/wiki/Reconfigurable_Manufacturing_System), [asset](https://en.wikipedia.org/wiki/Asset_management) and situation management, or manufacturing [process control](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/Digital_control) to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the [IIoT](https://en.wikipedia.org/wiki/Industrial_internet_of_things" \o "Industrial internet of things).[]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-IoT-Survey-70) IoT can also be applied to asset management via [predictive maintenance](https://en.wikipedia.org/wiki/Predictive_maintenance), [statistical evaluation](https://en.wikipedia.org/wiki/Statistical_model), and measurements to maximize reliability. Industrial management systems can be integrated with [smart grids](https://en.wikipedia.org/wiki/Smart_grid), 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. 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 The FarmBeats projec from Microsoft Research that uses TV white space to connect farms is also a part of the Azure Marketplace now.

#### 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**

### Intentional obsolescence of devices[[edit](https://en.wikipedia.org/w/index.php?title=Internet_of_things&action=edit&section=55" \o "Edit section: Intentional obsolescence of devices)]

The [Electronic Frontier Foundation](https://en.wikipedia.org/wiki/Electronic_Frontier_Foundation) has raised concerns that companies can use the technologies necessary to support connected devices to intentionally disable or "[brick](https://en.wikipedia.org/wiki/Brick_(electronics))" their customers' devices via a remote software update or by disabling a service necessary to the operation of the device. In one example, [home automation](https://en.wikipedia.org/wiki/Home_automation) devices sold with the promise of a "Lifetime Subscription" were rendered useless after [Nest Labs](https://en.wikipedia.org/wiki/Nest_Labs) acquired Revolv and made the decision to shut down the central servers the Revolv devices had used to operate.[[268]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-268) As Nest is a company owned by [Alphabet](https://en.wikipedia.org/wiki/Alphabet_Inc.) ([Google's](https://en.wikipedia.org/wiki/Google) parent company), the EFF argues this sets a "terrible precedent for a company with ambitions to sell self-driving cars, medical devices, and other high-end gadgets that may be essential to a person's livelihood or physical safety."[[269]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-effrem-269)

Owners should be free to point their devices to a different server or collaborate on improved software. But such action violates the United States [DMCA](https://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act) section 1201, which only has an exemption for "local use". This forces tinkerers who want to keep using their own equipment into a legal grey area. EFF thinks buyers should refuse electronics and software that prioritize the manufacturer's wishes above their own.[[269]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-effrem-269)

Examples of post-sale manipulations include [Google Nest](https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Google) Revolv, disabled privacy settings on [Android](https://en.wikipedia.org/wiki/Android_(operating_system)), Sony disabling [Linux](https://en.wikipedia.org/wiki/Linux) on [PlayStation 3](https://en.wikipedia.org/wiki/PlayStation_3), enforced [EULA](https://en.wikipedia.org/wiki/End-user_license_agreement) on [Wii U](https://en.wikipedia.org/wiki/Wii_U)

### A solution to "basket of remotes"

Many IoT devices have the potential to take a piece of this market. [Jean-Louis Gassée](https://en.wikipedia.org/wiki/Jean-Louis_Gass%C3%A9e) (Apple initial alumni team, and BeOS co-founder) has addressed this topic in an article on *Monday Note* where he predicts that the most likely problem will be what he calls the "basket of remotes" problem, where we'll have hundreds of applications to interface with hundreds of devices that don't share protocols for speaking with one another. For improved user interaction, some technology leaders are joining forces to create standards for communication between devices to solve this problem. Others are turning to the concept of predictive interaction of devices, "where collected data is used to predict and trigger actions on the specific devices" while making them work together.

### 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.

#### How SIoT different from IoT?

SIoT is different from the original IoT in terms of the collaboration characteristics. IoT is passive, it was set to serve for dedicated purposes with existing IoT devices in predetermined system. SIoT is active, it was programmed and managed by AI to serve for unplanned purposes with mix and match of potential IoT devices from different systems that benefit its users.

**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.

### Privacy, autonomy, and control

[Philip N. Howard](https://en.wikipedia.org/wiki/Philip_N._Howard), a professor and author, writes that the Internet of things offers immense potential for empowering citizens, making government transparent, and broadening [information access](https://en.wikipedia.org/wiki/Information_access). Howard cautions, however, that privacy threats are enormous, as is the potential for social control and political manipulation.

Concerns about privacy have led many to consider the possibility that [big data](https://en.wikipedia.org/wiki/Big_data) infrastructures such as the Internet of things and [data mining](https://en.wikipedia.org/wiki/Data_mining) are inherently incompatible with privacy. Key challenges of increased digitalization in the water, transport or energy sector are related to privacy and [cybersecurity](https://en.wikipedia.org/wiki/Cybersecurity" \o "Cybersecurity) which necessitate an adequate response from research and policymakers alike.

Writer [Adam Greenfield](https://en.wikipedia.org/wiki/Adam_Greenfield) claims that IoT technologies are not only an invasion of public space but are also being used to perpetuate normative behavior, citing an instance of billboards with hidden cameras that tracked the demographics of passersby who stopped to read the advertisement.

The Internet of Things Council compared the increased prevalence of [digital surveillance](https://en.wikipedia.org/wiki/Surveillance) due to the Internet of things to the conceptual [panopticon](https://en.wikipedia.org/wiki/Panopticon" \o "Panopticon) described by [Jeremy Bentham](https://en.wikipedia.org/wiki/Jeremy_Bentham) in the 18th Century. The assertion was defended by the works of French philosophers [Michel Foucault](https://en.wikipedia.org/wiki/Michel_Foucault) and [Gilles Deleuze](https://en.wikipedia.org/wiki/Gilles_Deleuze). In [*Discipline and Punish: The Birth of the Prison*](https://en.wikipedia.org/wiki/Discipline_and_Punish) Foucault asserts that the panopticon was a central element of the discipline society developed during the [Industrial Era](https://en.wikipedia.org/wiki/Industrial_Era). Foucault also argued that the discipline systems established in factories and school reflected Bentham's vision of [panopticism](https://en.wikipedia.org/wiki/Panopticism" \o "Panopticism) In his 1992 paper "Postscripts on the Societies of Control," Deleuze wrote that the discipline society had transitioned into a control society, with the [computer](https://en.wikipedia.org/wiki/Computer) replacing the [panopticon](https://en.wikipedia.org/wiki/Panopticon" \o "Panopticon) as an instrument of discipline and control while still maintaining the qualities similar to that of panopticism.[[]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-217)

### 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".

### Intentional obsolescence of devices

The [Electronic Frontier Foundation](https://en.wikipedia.org/wiki/Electronic_Frontier_Foundation) has raised concerns that companies can use the technologies necessary to support connected devices to intentionally disable or "[brick](https://en.wikipedia.org/wiki/Brick_(electronics))" their customers' devices via a remote software update or by disabling a service necessary to the operation of the device. In one example, [home automation](https://en.wikipedia.org/wiki/Home_automation) devices sold with the promise of a "Lifetime Subscription" were rendered useless after [Nest Labs](https://en.wikipedia.org/wiki/Nest_Labs) acquired Revolv and made the decision to shut down the central servers the Revolv devices had used to operate. As Nest is a company owned by [Alphabet](https://en.wikipedia.org/wiki/Alphabet_Inc.) ([Google's](https://en.wikipedia.org/wiki/Google) parent company), the EFF argues this sets a "terrible precedent for a company with ambitions to sell self-driving cars, medical devices, and other high-end gadgets that may be essential to a person's livelihood or physical safety.

Owners should be free to point their devices to a different server or collaborate on improved software. But such action violates the United States [DMCA](https://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act) section 1201, which only has an exemption for "local use". This forces tinkerers who want to keep using their own equipment into a legal grey area. EFF thinks buyers should refuse electronics and software that prioritize the manufacturer's wishes above their own

Examples of post-sale manipulations include [Google Nest](https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Google) Revolv, disabled privacy settings on [Android](https://en.wikipedia.org/wiki/Android_(operating_system)), Sony disabling [Linux](https://en.wikipedia.org/wiki/Linux) on [PlayStation 3](https://en.wikipedia.org/wiki/PlayStation_3), enforced [EULA](https://en.wikipedia.org/wiki/End-user_license_agreement) on [Wii U](https://en.wikipedia.org/wiki/Wii_U)