**Deisithani.S**

**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**

### Organizational applications

#### Medical and healthcare

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 Other consumer devices to encourage healthy living, such as connected scales or [wearable heart monitors](https://en.wikipedia.org/wiki/Wearable_technology), are also a possibility with the IoT. End-to-end health monitoring IoT platforms are also available for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements.

Advances in plastic and fabric electronics fabrication methods have enabled ultra-low cost, use-and-throw IoMT sensors. These sensors, along with the required [RFID](https://en.wikipedia.org/wiki/Radio-frequency_identification) electronics, can be fabricated on [paper](https://en.wikipedia.org/wiki/Paper) or [e-textiles](https://en.wikipedia.org/wiki/E-textiles) for wireless powered disposable sensing devices Applications have been established for [point-of-care medical diagnostics](https://en.wikipedia.org/wiki/Point-of-care_testing), where portability and low system-complexity is essential.

#### V2X communications

In [vehicular communication systems](https://en.wikipedia.org/wiki/Vehicular_communication_systems), [vehicle-to-everything](https://en.wikipedia.org/wiki/Vehicle-to-everything) communication (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](https://en.wikipedia.org/wiki/Autonomous_car) 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)[2]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-CoMAN-52) 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 consumption[]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-IoTEnergyKettle-33) and monitoring occupant behaviors
* The integration of smart devices in the built environment and how they might be used in future applications.

#### 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](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.

**Trends And Characteristics**

### Architecture

IoT system architecture, in its simplistic view, consists of three tiers: Tier 1: Devices, Tier 2: the [Edge](https://en.wikipedia.org/wiki/Edge_computing) [Gateway](https://en.wikipedia.org/wiki/Gateway_(telecommunications)#IoT_gateway), and Tier 3: the Cloud. Devices include networked things, such as the sensors and actuators found in IoT equipment, particularly those that use protocols such as [Modbus](https://en.wikipedia.org/wiki/Modbus), [Bluetooth](https://en.wikipedia.org/wiki/Bluetooth), [Zigbee](https://en.wikipedia.org/wiki/ZigBee" \o "ZigBee), or proprietary protocols, to connect to an Edge Gateway.[]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-:4-124) The Edge Gateway layer consists of sensor data aggregation systems called Edge Gateways that provide functionality, such as pre-processing of the data, securing connectivity to cloud, using systems such as WebSockets, the event hub, and, even in some cases, edge analytics or [fog computing](https://en.wikipedia.org/wiki/Fog_computing). Edge Gateway layer is also required to give a common view of the devices to the upper layers to facilitate in easier management. The final tier includes the cloud application built for IoT using the microservices architecture, which are usually polyglot and inherently secure in nature using HTTPS/[OAuth](https://en.wikipedia.org/wiki/OAuth" \o "OAuth). It includes various [database](https://en.wikipedia.org/wiki/Database) systems that store sensor data, such as time series databases or asset stores using backend data storage systems (e.g. Cassandra, PostgreSQL).[]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-:4-124) The cloud tier in most cloud-based IoT system features event queuing and messaging system that handles communication that transpires in all tiers Some experts classified the three-tiers in the IoT system as edge, platform, and enterprise and these are connected by proximity network, access network, and service network, respectively.

Building on the Internet of things, the [web of things](https://en.wikipedia.org/wiki/Web_of_things) is an architecture for the application layer of the Internet of things looking at the convergence of data from IoT devices into Web applications to create innovative use-cases. In order to program and control the flow of information in the Internet of things, a predicted architectural direction is being called [BPM Everywhere](https://en.wikipedia.org/wiki/BPM_Everywhere) which is a blending of traditional process management with process mining and special capabilities to automate the control of large numbers of coordinated devices.

### Complexity

In semi-open or closed loops (i.e. value chains, whenever a global finality can be settled) the IoT will often be considered and studied as a [complex system](https://en.wikipedia.org/wiki/Complex_system) due to the huge number of different links, interactions between autonomous actors, and its capacity to integrate new actors. At the overall stage (full open loop) it will likely be seen as a [chaotic](https://en.wikipedia.org/wiki/Chaos_theory) environment (since [systems](https://en.wikipedia.org/wiki/System) always have finality). As a practical approach, not all elements in the Internet of things run in a global, public space. Subsystems are often implemented to mitigate the risks of privacy, control and reliability. For example, domestic robotics (domotics) running inside a smart home might only share data within and be available via a [local network](https://en.wikipedia.org/wiki/Local_area_network).[[142]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-MargineanSDOMO16-142) Managing and controlling a high dynamic ad hoc IoT things/devices network is a tough task with the traditional networks architecture, Software Defined Networking (SDN) provides the agile dynamic solution that can cope with the special requirements of the diversity of innovative IoT applications

### Size considerations

The exact scale of the Internet of things is unknown, with quotes of billions or trillions often quoted at the beginning of IoT articles. In 2015 there were 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.[]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-faz.net-116) and around 12 billion in 2021. Therefore, facts about a thing, such as its location in time and space, have been less critical to track because the person processing the information can decide whether or not that information was important to the action being taken, and if so, add the missing information (or decide to not take the action). (Note that some things in the Internet of things will be sensors, and sensor location is usually important. The [GeoWeb](https://en.wikipedia.org/wiki/GeoWeb" \o "GeoWeb) and [Digital Earth](https://en.wikipedia.org/wiki/Digital_Earth) are promising applications that become possible when things can become organized and connected by location. However, the challenges that remain include the constraints of variable spatial scales, the need to handle massive amounts of data, and an indexing for fast search and neighbour operations. In the Internet of things, if things are able to take actions on their own initiative, this human-centric mediation role is eliminated. Thus, the time-space context that we as humans take for granted must be given a central role in this information ecosystem. Just as standards play a key role in the Internet and the Web, geo-spatial standards will play a key role in the Internet of things.

**Enabling Technologies For Iot**

### Application Layer

* ADRC defines an application layer protocol and supporting framework for implementing IoT applications.

### Short-range wireless

* [Bluetooth mesh networking](https://en.wikipedia.org/wiki/Bluetooth_mesh_networking) – Specification providing a mesh networking variant to [Bluetooth low energy](https://en.wikipedia.org/wiki/Bluetooth_low_energy) (BLE) with an increased number of nodes and standardized application layer (Models).
* [Light-Fidelity](https://en.wikipedia.org/wiki/Li-Fi) (Li-Fi) – Wireless communication technology similar to the Wi-Fi standard, but using [visible light communication](https://en.wikipedia.org/wiki/Visible_light_communication) for increased bandwidth.
* [Near-field communication](https://en.wikipedia.org/wiki/Near_field_communication) (NFC) – Communication protocols enabling two electronic devices to communicate within a 4 cm range.
* [Radio-frequency identification](https://en.wikipedia.org/wiki/Radio-frequency_identification) (RFID) – Technology using electromagnetic fields to read data stored in tags embedded in other items.
* [Wi-Fi](https://en.wikipedia.org/wiki/Wi-Fi) – Technology for [local area networking](https://en.wikipedia.org/wiki/Local_area_network) based on the [IEEE 802.11](https://en.wikipedia.org/wiki/IEEE_802.11) standard, where devices may communicate through a shared access point or directly between individual devices.
* [ZigBee](https://en.wikipedia.org/wiki/ZigBee) – Communication protocols for [personal area networking](https://en.wikipedia.org/wiki/Personal_area_network) based on the IEEE 802.15.4 standard, providing low power consumption, low data rate, low cost, and high throughput.
* [Z-Wave](https://en.wikipedia.org/wiki/Z-Wave) – [Wireless](https://en.wikipedia.org/wiki/Wireless) communications protocol used primarily for [home automation](https://en.wikipedia.org/wiki/Home_automation) and security applications.

### Medium-range wireless

* [LTE-Advanced](https://en.wikipedia.org/wiki/LTE_Advanced) – High-speed communication specification for mobile networks. Provides enhancements to the [LTE](https://en.wikipedia.org/wiki/LTE_(telecommunication)) standard with extended coverage, higher throughput, and lower latency.
* [5G](https://en.wikipedia.org/wiki/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. There are three features of 5G that are each considered to be useful for supporting particular elements of IoT: enhanced mobile broadband (eMBB), massive machine type communications (mMTC) and ultra-reliable low latency communications (URLLC).

### Long-range wireless

* [Low-power wide-area networking](https://en.wikipedia.org/wiki/LPWAN) (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](https://en.wikipedia.org/wiki/Lorawan" \o "Lorawan), Sigfox, [NB-IoT](https://en.wikipedia.org/wiki/NB-IoT), Weightless, RPMA.
* [Very small aperture terminal](https://en.wikipedia.org/wiki/Very-small-aperture_terminal) (VSAT) – [Satellite](https://en.wikipedia.org/wiki/Satellite) communication technology using small [dish antennas](https://en.wikipedia.org/wiki/Parabolic_antenna) for [narrowband](https://en.wikipedia.org/wiki/Narrowband) and [broadband](https://en.wikipedia.org/wiki/Broadband) data.

**Iot Adoption Barriers**

### Platform fragmentation

The IoT suffers from [platform fragmentation](https://en.wikipedia.org/wiki/Platform_fragmentation), lack of interoperability and common [technical standards](https://en.wikipedia.org/wiki/Technical_standard) a situation where the variety of IoT devices, in terms of both hardware variations and differences in the software running on them, makes the task of developing applications that work consistently between different inconsistent technology [ecosystems](https://en.wikipedia.org/wiki/Ecosystem) hard.[[1]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-Linux_Things-1) For example, wireless connectivity for IoT devices can be done using [Bluetooth](https://en.wikipedia.org/wiki/Bluetooth), [Zigbee](https://en.wikipedia.org/wiki/Zigbee" \o "Zigbee), [Z-Wave](https://en.wikipedia.org/wiki/Z-Wave), [LoRa](https://en.wikipedia.org/wiki/LoRa" \o "LoRa), [NB-IoT](https://en.wikipedia.org/wiki/Narrowband_IoT), [Cat M1](https://en.wikipedia.org/wiki/Cat-M1) as well as completely custom proprietary radios – each with its own advantages and disadvantages; and unique support ecosystem.

The IoT's [amorphous computing](https://en.wikipedia.org/wiki/Amorphous_computing) nature is also a problem for security, since patches to bugs found in the core operating system often do not reach users of older and lower-price devices. One set of researchers say that the failure of vendors to support older devices with patches and updates leaves more than 87% of active Android devices vulnerable

### Security

Security is the biggest concern in adopting Internet of things technology, with concerns that rapid development is happening without appropriate consideration of the profound security challenges involved[]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-230) and the regulatory changes that might be necessary.

Most of the technical security concerns are similar to those of conventional servers, workstations and smartphones These concerns include using weak authentication, forgetting to change default credentials, unencrypted messages sent between devices, [SQL injections](https://en.wikipedia.org/wiki/SQL_injection), [Man-in-the-middle attacks](https://en.wikipedia.org/wiki/Man-in-the-middle_attack), and poor handling of security updates However, many IoT devices have severe operational limitations on the computational power available to them. These constraints often make them unable to directly use basic security measures such as implementing firewalls or using strong cryptosystems to encrypt their communications with other devices[]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-236) - and the low price and consumer focus of many devices makes a robust security patching system uncommon

Rather than conventional security vulnerabilities, fault injection attacks are on the rise and targeting IoT devices. A fault injection attack is a physical attack on a device to purposefully introduce faults in the system to change the intended behavior. Faults might happen unintentionally by environmental noises and electromagnetic fields. There are ideas stemmed from control-flow integrity (CFI) to prevent fault injection attacks and system recovery to a healthy state before the fault.[[](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-238)

### Design

Given widespread recognition of the evolving nature of the design and management of the Internet of things, sustainable and secure deployment of IoT solutions must design for "anarchic scalability." Application of the concept of anarchic scalability can be extended to physical systems (i.e. controlled real-world objects), by virtue of those systems being designed to account for uncertain management futures. This hard anarchic scalability thus provides a pathway forward to fully realize the potential of Internet-of-things solutions by selectively constraining physical systems to allow for all management regimes without risking physical failure