Internet of things

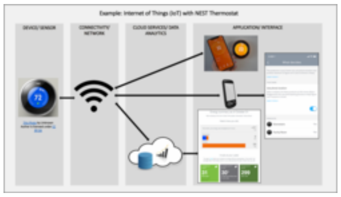
Example: Internet of Things (IoT) with NEST Thermostat
DEVICE/ SENSOR
CONNECTIVITY/ NETWORK
CLOUD SERVICES/ DATA ANALYTICS
APPLICATION/ INTERFACE
72

Figure 1: An example of how the Internet of Things is being utilized to connect a home thermostat.

The Internet of Things (IoT) describes physical objects that are embedded with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the internet or other communication networks. The IoT encompasses electronics, communication, and computer science engineering. “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, including ubiquitous computing, commodity sensors, increasingly powerful embedded systems, and machine learning. Traditional fields of embedded systems, wireless sensor networks, and control systems independently and collectively enable the Internet of Things.

While in the consumer market, IoT technology is most synonymous with “smart home”products—including devices and appliances like thermostats and smart speakers—the technology’s largest applications are in the business and industrial sectors. Commercial asset tracking and fleet management represent the largest single application of IoT, accounting for 22% of the total market, driven by the need to monitor mobile assets like vehicles and shipping containers. Other major applications include industrial monitoring, smart metering in utilities, and connected healthcare.

However, several concerns exist regarding the risks associated with the growth and diffusion of IoT technologies and products, particularly in the areas of privacy and security. Consequently, several industries, technology companies, and governments (or their branches, ministries, bureaus, departments, etc.) of many countries have taken multiple steps and implemented a variety of precautionary measures to address these concerns adequately and minimize safety risks, including the development and implementation of international and local standards, guidelines, and regulatory frameworks. Due to their interconnected nature, IoT devices are vulnerable to security breaches and privacy concerns. At the same time, the way these devices communicate wirelessly creates regulatory ambiguities, complicating jurisdictional boundaries of the data transfer.

Background

Around 1972, for its remote site use, Stanford Artificial Intelligence Laboratory developed a computer-controlled vending machine, adapted from a machine rented from Canteen Vending, which sold for cash or, through a computer terminal (Teletype Model 33 KSR), on credit. Amongst its products were beer, yogurt, and milk. It was named Prancing Pony, after the name of the room, which was named after an inn in J. R. R. Tolkien’s epic fantasy novel The Lord of the Rings. Each room at the Stanford Artificial Intelligence Laboratory was named after a Lord Of The Rings’fantasy world, known as Middle-earth. A successor version still operates in the Computer Science Department at Stanford, with updated hardware and software.

History

In 1982, an early concept of a network connected smart device was constructed as an Internet interface for sensors installed in the Carnegie Mellon University Computer Science Department’s departmental Coca-Cola vending machine, supplied by graduate student volunteers, provided a temperature model and an inventory status, inspired by the computer controlled vending machine in the Prancing Pony room at Stanford Artificial

Intelligence Laboratory. While it was initially accessible only on the CMU campus, it gained prominence as the first ARPANET-connected appliance.

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, such as Microsoft's at Work or Novell's NEST. The field gained momentum when Bill Joy envisioned device-to-device communication as part of his "Six Webs"framework, which was presented at the World Economic Forum in 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."

The term "Internet of things"was coined independently by Kevin Ashton of Procter & Gamble, later of Massachusetts Institute of Technology's Auto-ID Center, in 1999, despite preferring the phrase "Internet for things."At that point, he considered radio-frequency identification (RFID) an essential component of the Internet of things, as it would effectively enable computers to manage all individual things. The primary defining characteristic of the Internet of things has been considered its ability to embed short-range mobile transceivers in various gadgets and daily necessities, enabling new forms of communication between people and things, as well as between things themselves.

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 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

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

Consumers

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

IoT devices are part of the broader concept of home automation, which generally includes lighting, heating and air conditioning, media and security systems, and camera systems. Moreover, 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, also known as an automated home, could be based on a platform or hubs that control smart devices and appliances. For instance, using Apple's 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. These include the Amazon Echo, Google Home, Apple's HomePod, and Samsung's SmartThings Hub. In addition to the commercial systems, there are many non-proprietary, open source ecosystems, including Home Assistant, OpenHAB, and Domoticz.

One key application of a smart home is to assist the elderly and individuals 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 individuals with hearing impairments. They can also be equipped with additional safety features, including 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.

Organizations

The term "Enterprise IoT"refers to devices used in business and corporate settings.

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 are 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', which is used to analyze health statistics.

Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while ensuring that proper treatment is administered and assisting people in regaining 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, 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 radio-frequency identification electronics, can be fabricated on paper or e-textiles for wireless powered disposable sensing devices. Applications have been established for point-of-care medical diagnostics, where portability and low system complexity are considered essential.

As of 2018[update], IoMT was being applied in the clinical laboratory industry.

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 patients'data and apply complex algorithms in health data analysis.

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

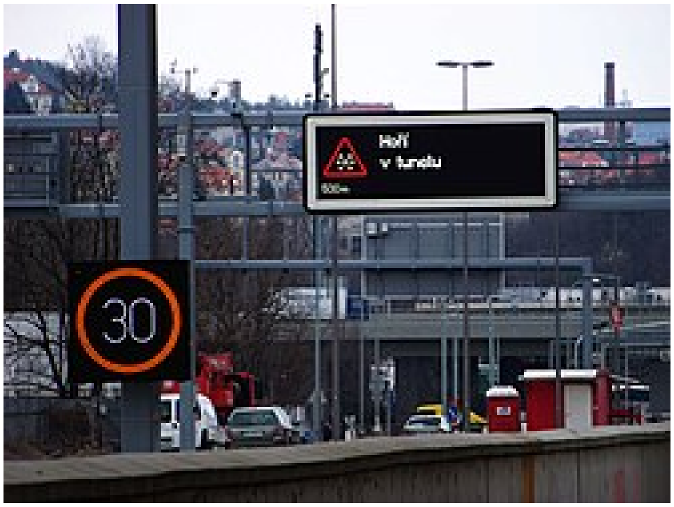

Figure 2: Digital variable speed-limit sign in the Czech Republic.

transport system enables inter- and intra-vehicular communication, smart traffic control, smart parking, electronic toll collection systems, logistics and fleet management, vehicle control, safety, and road assistance.

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

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 and building automation systems. In this context, three main areas are being covered in the literature:

- The integration of the Internet with building energy management systems 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.

Industrial

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. Additionally, 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.

The IoT can connect various manufacturing devices equipped with sensing, identification, processing, communication, actuation, and networking capabilities. Network control and management of manufacturing equipment, asset and situation management, or manufacturing process control enable IoT to be utilized 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, which aim to automate process controls, operator tools, and service information systems, alongside optimizing plant safety and security, fall within the purview of the IIoT. Furthermore, 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.

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, make 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 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.

IoT devices are in use to monitor 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 connected Android & Apple applications for example.

Infrastructure

Monitoring and controlling operations of sustainable urban and rural infrastructures like bridges, railway tracks and on- and offshore wind farms is a key application of the IoT. The IoT infrastructure can be used for monitoring any events or changes in structural conditions that can compromise safety and increase risk. The IoT can benefit the construction industry by cost-saving, time reduction, better quality workday, paperless workflow and increase in productivity. It can help in taking faster decisions and saving money in Real-Time Data Analytics. It can also be used for scheduling repair and maintenance activities efficiently, by coordinating tasks between different service providers and users of these facilities. IoT devices can also be used to control critical infrastructure like bridges to provide access to ships. The usage of IoT devices for monitoring and operating infrastructure is likely to significantly improve incident management and emergency response coordination, and quality of service, up-times and reduce costs of operation in all infrastructure-related areas. Even areas such as waste management can benefit.

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 fully equipped and wired smart city, is gradually being built,[when?] with approximately 70 percent of the business district completed as of June 2018[update]. A sizeable portion of the city, the first of its kind, is planned to be wired and automated to operate with little or no human intervention.

In 2014, another application was 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 and environmental monitoring. Additionally, city context information is used in this deployment, aiming to benefit merchants through a spark deals mechanism based on city behavior that aims at maximizing the impact of each notification.

Other examples of large-scale deployments underway include the Sino-Singapore Guangzhou Knowledge City; work on improving air and water quality, reducing noise pollution, and increasing transportation efficiency in San Jose, California; and smart traffic management in western Singapore. Using its RPMA (Random Phase Multiple Access) technology, San Diego–based Ingenu has built a nationwide public network for low-bandwidth data transmissions using the same unlicensed 2.4 gigahertz spectrum as Wi-Fi. Ingenu's "Machine Network"covers more than a third of the US population across 35 major cities including San Diego and Dallas. French company, Sigfox, commenced building an Ultra Narrowband wireless data network in the San Francisco Bay Area in 2014, the first business to achieve such a deployment in the U.S. It subsequently announced it would set up a total of 4000 base stations to cover a total of 30 cities in the U.S. by the end of 2016, making it the largest IoT network coverage provider in the country thus far. Cisco also participates in smart cities projects. Cisco has deployed technologies for Smart Wi-Fi, Smart Safety & Security, Smart Lighting, Smart Parking, Smart Transports, Smart Bus Stops, Smart Kiosks, Remote Expert for Government Services (REGS) and Smart Education in the five km area in the city of Vijayawada, India.

Another example of a large deployment is the one completed by New York Waterways in New York City to connect all the city's vessels and be able to monitor them live 24/7. The network was designed and engineered by Fluidmesh Networks, a Chicago-based company developing wireless networks for critical applications. The NYWW network is currently providing coverage on the Hudson River, East River, and Upper New York Bay. With the wireless network in place, NY Waterway is able to take control of its fleet and passengers in a way that was not previously possible. New applications can include security, energy and fleet management, digital signage, public Wi-Fi, paperless ticketing and others.

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 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.

Another example of integrating the IoT is the concept of a "living lab."Living labs integrate and combine research and innovation processes, establishing within a public-private-people-partnership. Between 2006 and January 2024, there were over 440 living labs (though not all are currently active) that use the IoT to collaborate and share knowledge between stakeholders to co-create innovative and technological products. When companies intend to implement and develop IoT services for smart cities, they need to have economic incentives. The US government plays a key role in smart city projects; 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 US government provides tax incentives and affordable rent, improves public transport, 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 processes, and transaction costs.

Military

The Internet of Military Things (IoMT) is the application of IoT technologies in the military domain for the purposes of reconnaissance, surveillance, and other combat-related objectives. It is heavily influenced by the future prospects of warfare in an urban environment and involves the use of sensors, munitions, vehicles, robots, human-wearable biometrics, and other smart technology that is relevant on the battlefield.

One of the examples of IOT devices used in the military is the Xaver 1000 system. The Xaver 1000 was developed by Israel's Camero Tech, which is the latest in the company's line of "through-wall imaging systems."The Xaver line uses millimeter wave (MMW) radar, or radar in the range of 30-300 gigahertz. It is equipped with an AI-based life target tracking system as well as its own 3D 'sense-through-the-wall' technology.

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 enhances 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.

The Ocean of Things project is a 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 detects and tracks military and commercial vessels as part of a cloud-based network.

Product digitalization

There are several applications of smart or active packaging in which a QR code or NFC tag is affixed to 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.

Trends and characteristics

The IoT's major significant trend in recent years[when?] is the 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.

IoT Analytics reported there were 16.6 billion IoT devices connected in 2023. In 2020, the same firm projected there would be 30 billion devices connected by 2025. As of October, 2024, there are around 17 billion.

Intelligence

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) 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. An approach in this context is deep 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. By reinforcement learning approach, a learning agent can sense the environment's state (e.g., sensing home temperature), perform actions (e.g., turn HVAC on or off) and learn through the maximizing accumulated rewards it receives in long term.

IoT intelligence can be offered at three levels: IoT devices, Edge/Fog nodes, and cloud computing. The need for intelligent control and decision at each level depends on the time sensitiveness of the IoT application. For example, an autonomous vehicle's camera needs to make real-time obstacle detection to avoid an accident. This fast decision making would not be possible through transferring data from the vehicle to cloud instances and return the predictions back to the vehicle. Instead, all the operation should be performed locally in the vehicle. Integrating advanced machine learning algorithms including deep learning into IoT devices is an active research area to make smart objects closer to reality. Moreover, it is possible to get the most value out of IoT deployments through analyzing IoT data, extracting hidden information, and predicting control decisions. A wide variety of machine learning techniques have been used in IoT domain ranging from traditional methods such as regression, support vector machine, and random forest to advanced ones such as convolutional neural networks, LSTM, and variational autoencoder.

In the future, the Internet of things may be a non-deterministic and open network in which auto-organized or intelligent entities (web services, SOA components) and virtual objects (avatars) will be interoperable and able to act independently (pursuing their own objectives or shared ones) depending on the context, circumstances or environments. Autonomous behavior through the collection and reasoning of context information as well as the object's ability to detect changes in the environment (faults affecting sensors) and introduce suitable mitigation measures constitutes a major research trend, clearly needed to provide credibility to the IoT technology. Modern IoT products and solutions in the marketplace use a variety of different technologies to support such context-aware automation, but more sophisticated forms of intelligence are requested to permit sensor units and intelligent cyber-physical systems to be deployed in real environments.

Architecture

IoT system architecture, in its simplistic view, consists of three tiers: Tier 1: Devices, Tier 2: the Edge 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, Bluetooth, Zigbee, or proprietary protocols, to connect to an Edge Gateway. 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. 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. It includes various database systems that store sensor data, such as time series databases or asset stores using backend data storage systems (e.g. Cassandra, PostgreSQL). 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 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 which is a blending of traditional process management with process mining and special capabilities to automate the control of large numbers of coordinated devices.[citation needed]

The Internet of things requires huge scalability in the network space to handle the surge of devices. IETF 6LoWPAN can be used to connect devices to IP networks. With billions of devices being added to the Internet space, IPv6 will play a major role in handling the network layer scalability. IETF's Constrained Application Protocol, ZeroMQ, and MQTT can provide lightweight data transport. In practice many groups of IoT devices are hidden behind gateway nodes and may not have unique addresses. Also the vision of everything-interconnected is not needed for most applications as it is mainly the data which need interconnecting at a higher layer.[citation needed]

Fog computing is a viable alternative to prevent such a large burst of data flow through the Internet. The edge devices'computation power to analyze 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 Internet of things, or decentralized IoT, is a modified IoT which 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. Performance is improved, especially for huge IoT systems with millions of nodes.

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.

Some approached to decentralized IoT attempts to address the limited bandwidth and hashing capacity of battery powered or wireless IoT devices via blockchain.

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 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 environment (since systems always have finality). As a practical approach, not all elements on 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. 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. In 2023, the number of connected IoT devices will reach 16.6 billion.

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

Space considerations

In the Internet of things, the precise geographic location of a thing—and also the precise geographic dimensions of a thing—can be critical. 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 on the Internet of things will be sensors, and sensor location is usually important.) The GeoWeb and Digital Earth are 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. On 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 on the Internet and the Web, geo-spatial standards will play a key role on the Internet of things.

A solution to "basket of remotes"

Many IoT devices have the potential to take a piece of this market. Jean-Louis Gassée (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.

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.

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.

IoT devices built-in with sociability will broadcast their abilities or functionalities, and at the same time discovers, shares information, monitors, navigates and groups with other IoT devices in the same or nearby network realizing SIoT and facilitating useful service compositions in order to help its users proactively in every day’s life especially during emergency.

1. IoT-based smart home technology monitors health data of patients or aging adults by analyzing their physiological parameters and prompt the nearby health facilities when emergency medical services needed. In case emergency, automatically, ambulance of a nearest available hospital will be called with pickup location provided, ward assigned, patient’s health data will be transmitted to the emergency department, and display on the doctor’s computer immediately for further action.

2. IoT sensors on the vehicles, road and traffic lights monitor the conditions of the vehicles and drivers and alert when attention needed and also coordinate themselves automatically to ensure autonomous driving is working normally. Unfortunately if an accident happens, IoT camera will inform the nearest hospital and police station for help.

3. 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.

4. 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.

5. 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

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 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).
- Li-Fi (light fidelity) –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.
- Zigbee –Communication protocols for personal area networking–based on the IEEE 802.15.4 standard, providing low power consumption, low data rate, low cost, and high throughput.
- 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. 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).
- LoRa: Range up to 3 miles (4.8 km) in urban areas, and up to 10 miles (16 km) or more in rural areas (line of sight).
- DASH7: Range of up to 2 km.

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, MIoTy, IEEE 802.11ah
- 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.

Comparison of technologies by layer

Different technologies have different roles in a protocol stack. Below is a simplified[notes 1] presentation of the roles of several popular communication technologies in IoT applications:

Standards and standards organizations

This is a list of technical standards for the IoT, most of which are open standards, and the standards organizations that aspire to successfully setting them.

Politics and civic engagement

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

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 develop. 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.

Current regulatory environment:

A report published by the Federal Trade Commission (FTC) in January 2015 made the following three recommendations:

- Data security –At the time of designing IoT companies should ensure that data collection, storage and processing would be secure at all times. Companies should adopt a "defense in depth"approach and encrypt data at each stage.
- Data consent –users should have a choice as to what data they share with IoT companies and the users must be informed if their data gets exposed.
- Data minimisation –IoT companies should collect only the data they need and retain the collected information only for a limited time.

However, the FTC stopped at just making recommendations for now. According to an FTC analysis, the existing framework, consisting of the FTC Act, the Fair Credit Reporting Act, and the Children's Online Privacy Protection Act, along with developing consumer education and business guidance, participation in multi-stakeholder efforts and advocacy to other agencies at the federal, state and local level, is sufficient to protect consumer rights.

A resolution passed by the Senate in March 2015, is already being considered by the Congress. This resolution recognized the need for formulating a National Policy on IoT and the matter of privacy, security and spectrum. Furthermore, to provide an impetus to the IoT ecosystem, in March 2016, a bipartisan group of four Senators proposed a bill, The Developing Innovation and Growing the Internet of Things (DIGIT) Act, to direct the Federal Communications Commission to assess the need for more spectrum to connect IoT devices.

Approved on 28 September 2018, California Senate Bill No. 327 goes into effect on 1 January 2020. The bill requires "a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure,"

Several standards for the IoT industry are actually being established relating to automobiles because most concerns arising from use of connected cars apply to healthcare devices as well. In fact, the National Highway Traffic Safety Administration (NHTSA) is preparing cybersecurity guidelines and a database of best practices to make automotive computer systems more secure.

A recent report from the World Bank examines the challenges and opportunities in government adoption of IoT. These include –

- Still early days for the IoT in government
- Underdeveloped policy and regulatory frameworks
- Unclear business models, despite strong value proposition
- Clear institutional and capacity gap in government AND the private sector
- Inconsistent data valuation and management
- Infrastructure a major barrier
- Government as an enabler
- Most successful pilots share common characteristics (public-private partnership, local, leadership)

In early December 2021, the U.K. government introduced the Product Security and Telecommunications Infrastructure bill (PST), an effort to legislate IoT distributors, manufacturers, and importers to meet certain cybersecurity standards. The bill also seeks to improve the security credentials of consumer IoT devices.

Criticism, problems and controversies

Platform fragmentation

The IoT suffers from platform fragmentation, lack of interoperability and common technical standards[excessive citations] 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 hard. For example, wireless connectivity for IoT devices can be done using Bluetooth, Wi-Fi, Wi-Fi HaLow, Zigbee, Z-Wave, LoRa, NB-IoT, 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 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 says that the failure of vendors to support older devices with patches and updates leaves more than 87% of active Android devices vulnerable.

Privacy, autonomy, and control

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. 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 infrastructures such as the

Internet of things and 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 which necessitate an adequate response from research and policymakers alike.

Writer 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 due to the Internet of things to the concept of the panopticon described by Jeremy Bentham in the 18th century. The assertion is supported by the works of French philosophers Michel Foucault and Gilles Deleuze. In Discipline and Punish: The Birth of the Prison, Foucault asserts that the panopticon was a central element of the discipline society developed during the Industrial Era. Foucault also argued that the discipline systems established in factories and school reflected Bentham's vision of 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 replacing the panopticon as an instrument of discipline and control while still maintaining the qualities similar to that of panopticism.

Peter-Paul Verbeek, a professor of philosophy of technology at the University of Twente, Netherlands, writes that technology already influences our moral decision making, which in turn affects human agency, privacy and autonomy. He cautions against viewing technology merely as a human tool and advocates instead to consider it as an active agent.

Justin Brookman, of the Center for Democracy and Technology, expressed concern regarding the impact of the IoT on consumer privacy, saying that "There are some people in the commercial space who say, 'Oh, big data –well, let's collect everything, keep it around forever, we'll pay for somebody to think about security later.'The question is whether we want to have some sort of policy framework in place to limit that."

Tim O'Reilly believes that the way companies sell the IoT devices on consumers are misplaced, disputing the notion that the IoT is about gaining efficiency from putting all kinds of devices online and postulating that the "IoT is really about human augmentation. The applications are profoundly different when you have sensors and data driving the decision-making."

Editorials at WIRED have also expressed concern, one stating "What you're about to lose is your privacy. Actually, it's worse than that. You aren't just going to lose your privacy, you're going to have to watch the very concept of privacy be rewritten under your nose."

The American Civil Liberties Union (ACLU) expressed concern regarding the ability of IoT to erode people' s control over their own lives. The ACLU wrote that "There's simply no way to forecast how these immense powers –disproportionately accumulating in the hands of corporations seeking financial advantage and governments craving ever more control –will be used. Chances are big data and the Internet of Things will make it harder for us to control our own lives, as we grow increasingly transparent to powerful corporations and government institutions that are becoming more opaque to us."

In response to rising concerns about privacy and smart technology, in 2007 the British Government stated it would follow formal Privacy by Design principles when implementing their smart metering program. The program would lead to replacement of traditional power meters with smart power meters, which could track and manage energy usage more accurately. However the British Computer Society is doubtful these principles were ever actually implemented. In 2009 the Dutch Parliament rejected a similar smart metering program, basing their decision on privacy concerns. The Dutch program later revised and passed in 2011.

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. In 2013, the Internet was estimated to be responsible for consuming 5% of the total energy produced, 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 and data 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.

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 and the regulatory changes that might be necessary. The rapid development of the Internet of Things (IoT) has allowed billions of devices to connect to the network. Due to too many connected devices and the limitation of communication security technology, various security issues gradually appear in the IoT.

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, man-in-the-middle attacks, 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 - 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.

Internet of things devices also have access to new areas of data, and can often control physical devices, so that even by 2014 it was possible to say that many Internet-connected appliances could already "spy on people in their own homes"including televisions, kitchen appliances, cameras, and thermostats. Computer-controlled devices in automobiles such as brakes, engine, locks, hood and trunk releases, horn, heat, and dashboard have been shown to be vulnerable to attackers who have access to the on-board network. In some cases, vehicle computer systems are Internet-connected, allowing them to be exploited remotely. By 2008 security researchers had shown the ability to remotely control pacemakers without authority. Later hackers demonstrated remote control of insulin pumps and implantable cardioverter defibrillators.

Poorly secured Internet-accessible IoT devices can also be subverted to attack others. In 2016, a distributed denial of service attack powered by Internet of things devices running the Mirai malware took down a DNS provider and major web sites. The Mirai Botnet had infected roughly 65,000 IoT devices within the first 20 hours. Eventually the infections increased to around 200,000 to 300,000 infections. Brazil, Colombia and Vietnam made up of 41.5% of the infections. The Mirai Botnet had singled out specific IoT devices that consisted of DVRs, IP cameras, routers and printers. Top vendors that contained the most infected devices were identified as Dahua, Huawei, ZTE, Cisco, ZyXEL and MikroTik. In May 2017, Junade Ali, a computer scientist at Cloudflare noted that native DDoS vulnerabilities exist in IoT devices due to a poor implementation of the Publish–subscribe pattern. These sorts of attacks have caused security experts to view IoT as a real threat to Internet services.

The U.S. National Intelligence Council in an unclassified report maintains that it would be hard to deny "access to networks of sensors and remotely-controlled objects by enemies of the United States, criminals, and mischief makers...An open market for aggregated sensor data could serve the interests of commerce and security no less than it helps criminals and spies identify vulnerable targets. Thus, massively parallel sensor fusion may undermine social cohesion, if it proves to be fundamentally incompatible with Fourth-Amendment guarantees against unreasonable search."In general, the intelligence community views the Internet of things as a rich source of data.

On 31 January 2019, The Washington Post wrote an article regarding the security and ethical challenges that can occur with IoT doorbells and cameras: "Last month, Ring got caught allowing its team in Ukraine to view and annotate certain user videos; the company says it only looks at publicly shared videos and those from Ring owners who provide consent. Just last week, a California family's Nest camera let a hacker take over and broadcast fake audio warnings about a missile attack, not to mention peer in on them, when they used a weak password."

There have been a range of responses to concerns over security. The Internet of Things Security Foundation (IoTSF) was launched on 23 September 2015 with a mission to secure the Internet of things by promoting knowledge and best practice. Its founding board is made from technology providers and telecommunications companies. In addition, large IT companies are continually developing innovative solutions to ensure the security of IoT devices. In 2017, Mozilla launched Project Things, which allows to route IoT devices through a safe Web of Things gateway. As per the estimates from KBV Research, the overall IoT security market would grow at 27.9% rate during 2016–2022 as a result of growing infrastructural concerns and diversified usage of Internet of things.

Governmental regulation is argued by some to be necessary to secure IoT devices and the wider Internet – as market incentives to secure IoT devices is insufficient. It was found that due to the nature of most of the IoT development boards, they generate predictable and weak keys which make it easy to be utilized by man-in-the-middle attack. However, various hardening approaches were proposed by many researchers to resolve the issue of SSH weak implementation and weak keys.

IoT security within the field of manufacturing presents different challenges, and varying perspectives. Within the EU and Germany, data protection is constantly referenced throughout manufacturing and digital policy particularly that of I4.0. However, the attitude towards data security differs from the enterprise perspective whereas there is an emphasis on less data protection in the form of GDPR as the data being collected from IoT devices in the manufacturing sector does not display personal details. Yet, research has indicated that manufacturing experts are concerned about "data security for protecting machine technology from international competitors with the ever-greater push for interconnectivity".

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).

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.

Brown University computer scientist Michael Littman has argued that successful execution of the Internet of things requires consideration of the interface’s usability as well as the technology itself. These interfaces need to be not only more user-friendly but also better integrated: “If users need to learn different interfaces for their vacuums, their locks, their sprinklers, their lights, and their coffeemakers, it’s tough to say that their lives have been made any easier.”

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.

Intentional obsolescence of devices

The Electronic Frontier Foundation has raised concerns that companies can use the technologies necessary to support connected devices to intentionally disable or “brick”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 devices sold with the promise of a “Lifetime Subscription”were rendered useless after 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 (Google’s 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 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 Revolv, disabled privacy settings on Android, Sony disabling Linux on PlayStation 3, and enforced EULA on Wii U.

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. 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: Internet of things, Internet of everything (IoE), Internet of goods (supply chain), industrial Internet, pervasive computing, pervasive sensing, ubiquitous computing, cyber-physical systems (CPS), wireless sensor networks (WSN), smart objects, digital twin, cyberobjects or avatars, cooperating objects, machine to machine (M2M), ambient intelligence (AmI), Operational technology (OT), and information technology (IT). Regarding IIoT, an industrial sub-field of IoT, the Industrial Internet Consortium's Vocabulary Task Group has created a “common and reusable vocabulary of terms”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[update], this database aggregates 807 IoT-related terms, while keeping material “transparent and comprehensive”.

Adoption barriers

Figure 3: GE Digital CEO William Ruh speaking about GE's attempts to gain a foothold in the market for IoT services at the first IEEE Computer Society TechIgnite conference

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 that while IoT solutions appeal to 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”.

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 in a network, due to a diverse integration of services, devices and network, the information stored on a device is vulnerable to privacy violation by compromising nodes existing in an IoT network.

For example, on 21 October 2016, a multiple distributed denial of service (DDoS) attacks systems operated by domain name system provider Dyn, which caused the inaccessibility of several websites, such as GitHub, Twitter, and others. This attack is executed through a botnet consisting of a large number of IoT devices including IP cameras, gateways, and even baby monitors.

Fundamentally there are 4 security objectives that the IoT system requires: (1) data confidentiality: unauthorised parties cannot have access to the transmitted and stored data; (2) data integrity: intentional and unintentional corruption of transmitted and stored data must be detected; (3) non-repudiation: the sender cannot deny having sent a given message; (4) data availability: the transmitted and stored data should be available to authorised parties even with the denial-of-service (DOS) attacks.

Information privacy regulations also require organisations to practice “reasonable security”. California's SB-327 Information privacy: connected devices “would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorised access, destruction, use, modification, or disclosure, as specified". As each organisation's environment is unique, it can prove challenging to demonstrate what "reasonable security"is and what potential risks could be involved for the business. Oregon's HB2395 also "requires [a person that manufactures, sells or offers to sell connected device] manufacturer to equip connected device with reasonable security features that protect connected device and information that connected device [collects, contains, stores or transmits] stores from access, destruction, modification, use or disclosure that consumer does not authorise."

According to antivirus provider Kaspersky, there were 639 million data breaches of IoT devices in 2020 and 1.5 billion breaches in the first six months of 2021.

One method of overcoming the barrier of safety issues is the introduction of standards and certification of devices. In 2024, two voluntary and non-competing programs were proposed and launched in the United States: the US Cyber Trust Mark from The Federal Communications Commission and CSA's IoT Device Security Specification from the Connectivity Standards Alliance. The programs incorporate international expertise, with the CSA mark recognized by the Singapore Cybersecurity Agency. Compliance means that IoT devices can resist hacking, control hijacking and theft of confidential data.

Traditional governance structure

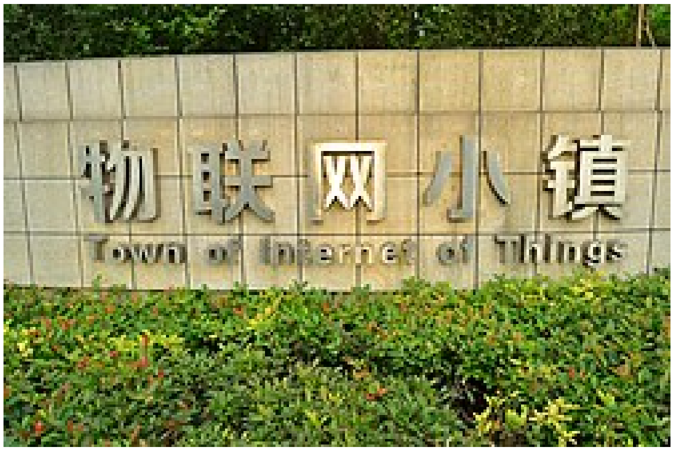

Figure 4: Town of Internet of Things in Hangzhou, China

A study issued by Ericsson regarding the adoption of Internet of things among Danish companies identified a "clash between IoT and companies'traditional governance structures, as IoT still presents both uncertainties and a lack of historical precedence."Among the respondents interviewed, 60 percent stated that they "do not believe they have the organizational capabilities, and three of four do not believe they have the processes needed, to capture the IoT opportunity."This has led to a need to understand organizational culture in order to facilitate organizational design processes and to test new innovation management practices. A lack of digital leadership in the age of digital transformation has also stifled innovation and IoT adoption to a degree that many companies, in the face of uncertainty, "were waiting for the market dynamics to play out", or further action in regards to IoT "was pending competitor moves, customer pull, or regulatory requirements". Some of these companies risk being "kodaked"–"Kodak was a market leader until digital disruption eclipsed film photography with digital photos"–failing to "see the disruptive forces affecting their industry"and "to truly embrace the new business models the disruptive change opens up". Scott Anthony has written in Harvard Business Review that Kodak "created a digital camera, invested in the technology, and even understood that photos would be shared online"but ultimately failed to realize that "online photo sharing was the new business, not just a way to expand the printing business."

Business planning and project management

According to 2018 study, 70–75% of IoT deployments were stuck in the pilot or prototype stage, unable to reach scale due in part to a lack of business planning.[page needed]

Even though scientists, engineers, and managers across the world are continuously working to create and exploit the benefits of IoT products, there are some flaws in the governance, management and implementation of such projects. Despite tremendous forward momentum in the field of information and other underlying technologies, IoT still remains a complex area and the problem of how IoT projects are managed still needs to be addressed. IoT projects must be run differently than simple and traditional IT, manufacturing or construction projects. Because IoT projects have longer project timelines, a lack of skilled resources and several security/legal issues, there is a need for new and specifically designed project processes. The following management techniques should improve the success rate of IoT projects:

- A separate research and development phase
- A Proof-of-Concept/Prototype before the actual project begins
- Project managers with interdisciplinary technical knowledge
- Universally defined business and technical jargon