WIKIPEDIA

Internet of things

The **Internet of things** (**IoT**) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.[1][2][3][4]

The definition of the Internet of things has evolved due to the convergence of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems.[1] Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of things. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", covering devices and appliances (such as lighting fixtures, thermostats, home security systems and 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 and smart speakers.
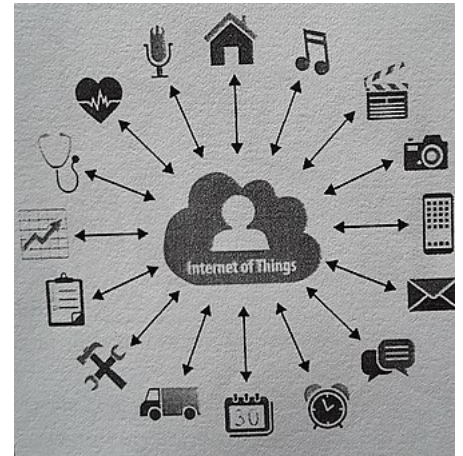
There are a number of serious concerns about dangers in the growth of IoT, especially in the areas of privacy and security, and consequently industry and governmental moves to address these concerns have begun.

Contents

History

Applications

Consumer applications

Smart home

Elder care

Organisational applications

Medical and healthcare

Transportation

V2X communications

Building and home automation

Industrial applications

Manufacturing

Agriculture

Infrastructure applications

Metropolitan scale deployments

Energy management

History

The main concept of a network of smart devices was discussed as early as 1982, with a modified Coca-Cola vending machine at Carnegie Mellon University becoming the first Internet-connected appliance,[5] able to report its inventory and whether newly loaded drinks were cold or not.[6] 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.[7][8] 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".[9] Between 1993 and 1997, several companies proposed solutions like Microsoft's at Work or Novell's NEST. The field gained momentum when Bill Joy envisioned device-to-device communication as a part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999.[10]

The term "Internet of things" was likely coined by Kevin Ashton of Procter & Gamble, later MIT's Auto-ID Center, in 1999,[11] though he prefers the phrase "Internet *for* things".[12] At that point, he viewed radio-frequency identification (RFID) as essential to the Internet of things,[13] which would allow computers to manage all individual things.[14][15][16]

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.[17]

The key driving force behind the Internet of things is the MOSFET (metal-oxide-semiconductor field-effect transistor, or MOS transistor),[18] which was originally invented by Mohamed M. Atalla and Dawon Kahng at Bell Labs in 1959.[19][20] The MOSFET is the basic building block of most modern electronics, including computers, smartphones, tablets and Internet services. MOSFET scaling miniaturization at a pace predicted by Dennard scaling and Moore's law has been the driving force behind technological advances in the electronics industry since the late 20th century. MOSFET scaling has been extended into the early 21st century with advances such as reducing power consumption, silicon-on-insulator (SOI) semiconductor device fabrication, and multi-core processor technology, leading up to the Internet of things, which is being driven by MOSFETs scaling down to nanoelectronic levels with reducing energy consumption.[21]

Applications

The extensive set of applications for IoT devices[22] is often divided into consumer, commercial, industrial, and infrastructure spaces.[23][24]

Consumer applications

A growing portion of IoT devices are created for consumer use, including connected vehicles, home automation, wearable technology, connected health, and appliances with remote monitoring capabilities.[25]

Smart home

IoT devices are a part of the larger concept of home automation, which can include lighting, heating and air conditioning, media and security systems.[26][27] Long-term benefits could include energy savings by automatically ensuring lights and electronics are turned off.

A smart home or automated home could be based on a platform or hubs that control smart devices and appliances.[28] 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.[29][30] This could be a dedicated app or iOS native applications such as Siri.[31] 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.[31] There are also dedicated smart home hubs that are offered as standalone platforms to connect different smart home products and these include the Amazon Echo, Google Home, Apple's HomePod, and Samsung's SmartThings Hub.[32] In addition to the commercial systems, there are many non-proprietary, open source ecosystems; including Home Assistant, OpenHAB and Domoticz.[33][34]

A Nest learning thermostat reporting on energy usage and local weather
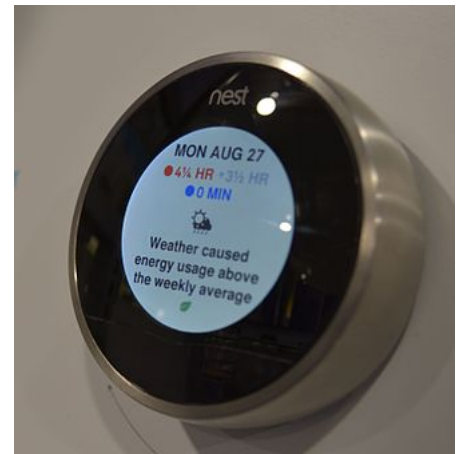
Elder care

One key application of a smart home is to provide assistance for those with disabilities and elderly individuals. These home systems use assistive technology to accommodate an owner's specific disabilities.[35] Voice control can assist users with sight and mobility limitations while alert systems can be connected directly to cochlear implants worn by hearing-impaired users.[36] They can also be equipped with additional safety features. These features can include sensors that monitor for medical emergencies such as falls or seizures.[37] Smart home technology applied in this way can provide users with more freedom and a higher quality of life.[35]

A Ring doorbell connected to the Internet

The term "Enterprise IoT" refers to devices used in business and corporate settings. By 2019, it is estimated that the EIoT will account for 9.1 billion devices.[23]

Organisational applications

An August Home smart lock connected to the Internet

Medical and healthcare

The **Internet of medical things (IoMT)** is an application of the IoT for medical and health related purposes, data collection and analysis for research, and monitoring.[38][39][40][41][42] The IoMT has been referenced as "Smart Healthcare",[43] as the technology for creating a digitized healthcare system, connecting available medical resources and healthcare services.[44]

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.[45] Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses.[38] 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."[46] Moreover, the use of mobile devices to support medical follow-up led to the creation of 'm-health', used analyzed health statistics." [47]

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 regain lost mobility via therapy as well.[48] 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.[43] Other consumer devices to encourage healthy living, such as connected scales or wearable heart monitors, are also a possibility with the IoT.[49] End-to-end health monitoring IoT platforms are also available for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements.[50]

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 electronics, can be fabricated on paper or e-textiles for wirelessly powered disposable sensing devices.[51] Applications have been established for point-of-care medical diagnostics, where portability and low system-complexity is essential.[52]

As of 2018 IoMT was not only being applied in the clinical laboratory industry,[40] but also in the healthcare and health insurance industries. IoMT in the healthcare industry is now permitting doctors, patients, and others, such as guardians of patients, nurses, families, and similar, to be part of a system, where patient records are saved in a database, allowing doctors and the rest of the medical staff to have access to patient information.[53] Moreover, IoT-based systems are patient-centered, which involves being flexible to the patient's medical conditions. 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 behaviour. This can lead to more accurate underwriting and new pricing models.[54]

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 patient's data and applying complex algorithms in health data analysis.[55]

Transportation

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,[56] the infrastructure, and the driver or user). Dynamic interaction between these components of a transport system enables inter- and intra-vehicular communication,[57] smart traffic control, smart parking, electronic toll collection systems, logistics and fleet management, vehicle control, safety, and road assistance.[45][58] In Logistics and Fleet Management, for example, an IoT platform can continuously monitor the location and conditions of cargo and assets via wireless sensors and send

specific alerts when management exceptions occur (delays, damages, thefts, etc.). This can only be possible with the IoT and its seamless connectivity among devices. Sensors such as GPS, Humidity, and Temperature send data to the IoT platform and then the data is analyzed and then sent to the users. This way, users can track the real-time status of vehicles and can make appropriate decisions. If combined with Machine Learning, then it also helps in reducing traffic accidents by introducing drowsiness alerts to drivers and providing self-driven cars too.

V2X communications

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 communications (V2P). V2X is the first step to autonomous driving and connected road infrastructure.

Digital variable speed-limit sign

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)[45] in home automation and building automation systems. In this context, three main areas are being covered in literature:[59]

- The integration of the Internet with building energy management systems in order to create energy efficient and IOT-driven "smart buildings".[59]
- The possible means of real-time monitoring for reducing energy consumption[60] and monitoring occupant behaviors.[59]
- The integration of smart devices in the built environment and how they might to know how to be used in future applications.[59]

Industrial applications

Also known as IIoT, industrial IoT devices acquire and analyze data from connected equipment, (OT) operational technology, locations and people. Combined with operational technology (OT) monitoring devices, IIoT helps regulate and monitor industrial systems.Also, the same implementation can be carried out for automated record updates of asset placement in industrial storage units as the size of the assets can vary from a small screw till the whole motor spare part and misplacement of such assets can cause a percentile loss of manpower time and money.

Manufacturing

The IoT can realize the seamless integration of various manufacturing devices equipped with sensing, identification, processing, communication, actuation, and networking capabilities. Based on such a highly integrated smart cyber-physical space, it opens the door to create whole new business and market opportunities for manufacturing.[61] Network control and management of manufacturing equipment, asset and situation management, or manufacturing process control bring the IoT within the realm of industrial applications and smart manufacturing as well.[62] The IoT intelligent systems enable rapid

manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply chain networks, by networking machinery, sensors and control systems together.[45]

Digital control systems to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IIoT.[63] But it also extends itself to asset management via predictive maintenance, statistical evaluation, and measurements to maximize reliability.[64] Industrial management systems can also be integrated with smart grids, enabling real-time energy optimization. Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by a large number of networked sensors.[45]

Industrial IoT (IIoT) in manufacturing could generate so much business value that it will eventually lead to the Fourth Industrial Revolution, also referred to as Industry 4.0. The potential for growth from implementing IIoT may generate $12 trillion of global GDP by 2030.[65]

Industrial big data analytics will play a vital role in manufacturing asset predictive maintenance, although that is not the only capability of industrial big data.[66] Cyber-physical systems (CPS) is the core technology of industrial big data and it will be an interface between human and the cyber world.

Agriculture

There are numerous IoT applications in farming[67] such as collecting data on temperature, rainfall, humidity, wind speed, pest infestation, and soil content. This data can be used to automate farming techniques, take informed decisions to improve quality and quantity, minimize risk and waste, and reduce 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.[68]

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 specific computer programs used in the process fall under the Azure Machine Learning and the Azure IoT Hub platforms.[69]

Infrastructure applications

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.[63] 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 save money with Real-Time Data Analytics. It can also be used for scheduling repair and maintenance activities in an efficient manner, by coordinating tasks between different service providers and users of these facilities.[45] IoT devices can also be used to control critical infrastructure like bridges to provide access to ships. Usage of IoT devices for monitoring and operating infrastructure is likely to improve incident management and emergency response coordination, and quality of service, up-times and reduce costs of operation in all infrastructure related areas.[70] Even areas such as waste management can benefit[71] from automation and optimization that could be brought in by the IoT.

Metropolitan scale deployments

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 of its kind fully equipped and wired smart city, is gradually being built, with approximately 70 percent of the business district completed as of June 2018. Much of the city is planned to be wired and automated, with little or no human intervention.[72][73]

Another application is a currently undergoing 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, environmental monitoring, digital city agenda, and more. City context information is used in this deployment so as to benefit merchants through a spark deals mechanism based on city behavior that aims at maximizing the impact of each notification.[74]

Other examples of large-scale deployments underway include the Sino-Singapore Guangzhou Knowledge City;[75] work on improving air and water quality, reducing noise pollution, and increasing transportation efficiency in San Jose, California;[76] and smart traffic management in western Singapore.[77] Using its RPMA (Random Phase Multiple Access) technology, San Diego-based Ingenu has built a nationwide public network[78] 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.[79] 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.[80][81] 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.[82][83] Cisco also participates in smart cities projects. Cisco has started deploying 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 Vijaywada.[84]

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.[85]

Energy management

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 energy consumption as a whole.[45] 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.).[45] 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.[86] 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.[45]

Environmental monitoring

Environmental monitoring applications of the IoT typically use sensors to assist in environmental protection[87] by monitoring air or water quality,[88] atmospheric or soil conditions,[89] and can even include areas like monitoring the movements of wildlife and their habitats.[90] 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.[45] It has been argued that the standardization IoT brings to wireless sensing will revolutionize this area.[91]

Living Lab

Another example of integrating the IoT is Living Lab which integrates and combines research and innovation process, establishing within a public-private-people-partnership.[92] There are currently 320 Living Labs that use the IoT to collaborate and share knowledge between stakeholders to co-create innovative and technological products. For companies to implement and develop IoT services for smart cities, they need to have incentives. The governments play key roles in smart cities projects as 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 government provides tax incentives and cheap rent, improves public transports, and offers an environment where start-up companies, creative industries, and multinationals may co-create, share common infrastructure and labor markets, and take advantages of locally embedded technologies, production process, and transaction costs.[92] The relationship between the technology developers and governments who manage city's assets, is key to provide open access of resources to users in an efficient way.

Military applications

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.[93]

Internet of Battlefield Things

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 IoT that enhance the capabilities of Army soldiers.[94] 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.[95][96]

Ocean of Things

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 detect and track military and commercial vessels as part of a cloud-based network.[97]

Product digitisation

There are several applications of smart or active packaging in which a QR code or NFC tag is affixed on 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.[98] Strictly speaking, such passive items are not part of the Internet of Thing but they can be seen as enablers of digital interactions.[99] 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.[100] 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,[101] while NFC tags can encrypt communication.[102]

Trends and characteristics

The IoT's major significant trend in recent years is the explosive growth of devices connected and controlled by the Internet.[103] 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.[104][105][106][107]

Technology roadmap: Internet of things
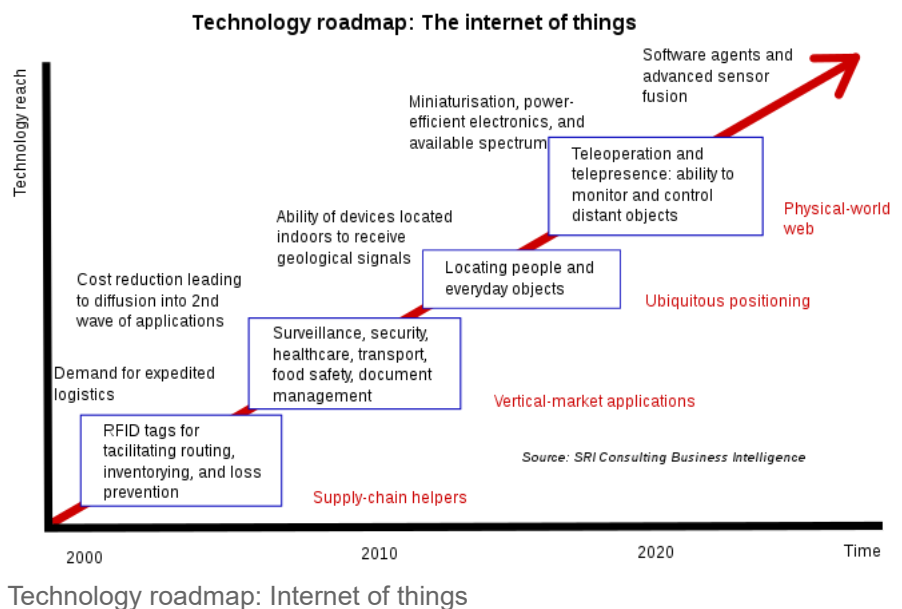
The number of IoT devices increased 31% year-over-year to 8.4 billion in the year 2017[108] and it is estimated that there will be 30 billion devices by 2020.[103] The global market value of IoT is projected to reach $7.1 trillion by 2020.[109]

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.[110] A promising approach in this context is deep reinforcement learning where most of IoT systems provide a dynamic and interactive environment.[111] 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.[112] 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.[113][112]

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,[114] 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.[115]

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.[116] Devices include networked things, such as the sensors and actuators found in IIoT equipment, particularly those that use protocols such as Modbus, Bluetooth, Zigbee, or proprietary protocols, to connect to an Edge Gateway.[116] The Edge Gateway 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.[116] 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 IIoT 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).[116] The cloud tier in most cloud-based IoT system features event queuing and messaging system that handles communication that transpires in all tiers.[117] Some experts classified the three-tiers in the IIoT system as edge, platform, and enterprise and these are connected by proximity network, access network, and service network, respectively.[118]

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.

Network architecture

The Internet of things requires huge scalability in the network space to handle the surge of devices.[119] IETF 6LoWPAN would be used to connect devices to IP networks. With billions of devices[120] 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 would provide lightweight data transport.

Fog computing is a viable alternative to prevent such large burst of data flow through Internet.[121] The edge devices' computation power to analyse 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.[122]

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[123] 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 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.[124] 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.[125]

Size considerations

The Internet of things would encode 50 to 100 trillion objects, and be able to follow the movement of those objects. Human beings in surveyed urban environments are each surrounded by 1000 to 5000 trackable objects.[126] In 2015 there were already 83 million smart devices in people's homes. This number is expected to grow to 193 million devices by 2020.[27]

The figure of online capable devices grew 31% from 2016 to 2017 to reach 8.4 billion.[108]

Space considerations

In the Internet of Things, the precise geographic location of a thing—and also the precise geographic dimensions of a thing—will be critical.[127] 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.[128]) The GeoWeb and 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 neighbor 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, geospatial standards will play a key role in the Internet of things.[129][130]

A solution to "basket of remotes"

Many IoT devices have a 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*,[131] 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.[131] 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.[132]

Enabling technologies for IoT

There are many technologies that enable the IoT. Crucial to the field is the network used to communicate between devices of an IoT installation, a role that several wireless or wired technologies may fulfill:[133][134][135]

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.[136] An alternative view, from the world of the Semantic Web[137] 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 centralized servers acting for their human owners.[138] 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.[139][140][141] Internet-of-things devices additionally will benefit from the stateless address auto-configuration present in IPv6,[142] as it reduces the configuration overhead on the hosts,[140] 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.[141]

Application Layer

- ADRC[143] 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 increased number of nodes and standardized application layer (Models).
- **Light-Fidelity** (Li-Fi) – 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.[144]

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.
- **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.

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.[145][146]

Short name	Long name	Standards under development	Other notes
Auto-ID Labs	Auto Identification Center	Networked RFID (radiofrequency identification) and emerging sensing technologies	
EPCglobal	Electronic Product code Technology	Standards for adoption of EPC (Electronic Product Code) technology	
FDA	U.S. Food and Drug Administration	UDI (Unique Device Identification) system for distinct identifiers for medical devices	
GS1	Global Standards One	Standards for UIDs ("unique" identifiers) and RFID of fast-moving consumer goods (consumer packaged goods), health care supplies, and other things The GS1 digital link standard,[147] first released in August 2018, allows the use QR Codes, GS1 Datamatrix, RFID and NFC to enable various types of business-to-business, as well as business-to-consumers interactions.	Parent organization comprises member organizations such as GS1 US
IEEE	Institute of Electrical and Electronics Engineers	Underlying communication technology standards such as IEEE 802.15.4, IEEE P1451-99 (IoT Harmonization), and IEEE P1931.1 (ROOF Computing).	
IETF	Internet Engineering Task Force	Standards that comprise TCP/IP (the Internet protocol suite)	
MTConnect Institute	—	MTConnect is a manufacturing industry standard for data exchange with machine tools and related industrial equipment. It is important to the IIoT subset of the IoT.	
O-DF	Open Data Format	O-DF is a standard published by the Internet of Things Work Group of The Open Group in 2014, which specifies a generic information model structure that is meant to be applicable for describing any "Thing", as well as for publishing, updating and querying information when used together with O-MI (Open Messaging Interface).	

Short name	Long name	Standards under development	Other notes
O-MI	Open Messaging Interface	O-MI is a standard published by the Internet of Things Work Group of The Open Group in 2014, which specifies a limited set of key operations needed in IoT systems, notably different kinds of subscription mechanisms based on the Observer pattern.	
OCF	Open Connectivity Foundation	Standards for simple devices using CoAP (Constrained Application Protocol)	OCF (Open Connectivity Foundation) supersedes OIC (Open Interconnect Consortium)
OMA	Open Mobile Alliance	OMA DM and OMA LWM2M for IoT device management, as well as GotAPI, which provides a secure framework for IoT applications	
XSF	XMPP Standards Foundation	Protocol extensions of XMPP (Extensible Messaging and Presence Protocol), the open standard of instant messaging	

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 organizations 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.[148]

Government regulation on IoT

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.[149] The other issues pertain to consumer choice and ownership of data[150] 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.[151][152][153] 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.[154]

Current regulatory environment:

A report published by the Federal Trade Commission (FTC) in January 2015 made the following three recommendations:[155]

- 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 "defence in depth" approach and encrypt data at each stage.[156]
- 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 minimization – 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.[157]

A resolution passed by the Senate in March 2015, is already being considered by the Congress.[158] 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, Senate Bill No. 327[159] 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.[160]

A recent report from the World Bank examines the challenges and opportunities in government adoption of IoT.[161] 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)

Criticism, problems and controversies

Platform fragmentation

The IoT suffers from platform fragmentation, lack of interoperability and common technical standards[162][163][164][165][166][167][168] 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.[1] For example, wireless connectivity for IoT devices can be done using Bluetooth, 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.[169]

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.[170][171][172] 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.[173][174]

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.[175]

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.[176] 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.[177]

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 conceptual panopticon described by Jeremy Bentham in the 18th Century.[178] The assertion was defended 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.[179] Foucault also argued that the discipline systems established in factories and school reflected Bentham's vision of panopticism.[179] 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.[180]

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.[181]

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."[182]

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."[183]

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."[184]

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."[185]

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.[186] However the British Computer Society is doubtful these principles were ever actually implemented.[187] 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.[187]

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.[188] These networks share data among sensor nodes that are sent to a distributed system for the analytics of the sensory data.[189]

Another challenge is the storage of this bulk data. Depending on the application, there could be high data acquisition requirements, which in turn lead to high storage requirements. Currently the Internet is already responsible for 5% of the total energy generated,[188] and a "daunting challenge to power" IoT devices to collect and even store data still remains.[190]

Security

Security is the biggest concern in adopting Internet of things technology,[191] with concerns that rapid development is happening without appropriate consideration of the profound security challenges involved[192] and the regulatory changes that might be necessary.[193][194]

Most of the technical security concerns are similar to those of conventional servers, workstations and smartphones,[195] and include weak authentication, forgetting to change default credentials, unencrypted messages sent between devices, SQL injections and poor handling of security updates.[196] 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[197] - and the low price and consumer focus of many devices makes a robust security patching system uncommon.[198]

Internet of Things devices also have access to new areas of data, and can often control physical devices,[199] 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,[200] cameras, and thermostats.[201] 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.[202] By 2008 security researchers had shown the ability to remotely control pacemakers without authority. Later hackers demonstrated remote control of insulin pumps[203] and implantable cardioverter defibrillators.[204]

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.[205] The Mirai Botnet had infected roughly 65,000 IoT devices within the first 20 hours.[206] Eventually the infections increased to around 200,000 to 300,000 infections.[206] Brazil, Colombia and Vietnam made up of 41.5% of the infections.[206] The Mirai Botnet had singled out specific IoT devices that consisted of DVRs, IP cameras, routers and printers.[206] Top vendors that contained the most infected devices were identified as Dahua, Huawei, ZTE, Cisco, ZyXEL and MikroTik.[206] 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.[207][208] These sorts of attacks have caused security experts to view IoT as a real threat to Internet services.[209]

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."[210] In general, the intelligence community views the Internet of things as a rich source of data.[211]

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"[212]

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.[213] As per the estimates from KBV Research,[214] the overall IoT security market[215] would grow at 27.9% rate during 2016–2022 as a result of growing infrastructural concerns and diversified usage of Internet of things.[216][217]

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.[218][193][194] 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 MiTM attack. However, various hardening approaches were proposed by many researchers to resolve the issue of SSH weak implementation and weak keys.[219]

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.[220] 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,[221] Apple's HomeKit,[222] and Amazon's Alexa,[223] 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".[220] 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.[220] 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."[224] 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.[224]

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."[225]

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.[226] 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 its lifetime.[227]

Although IoT devices can help in some cases to reduce the energy consumption of certain applications, the impact of having billions of devices connected and consuming power from batteries and from the grid will have a huge impact on energy consumption and CO_2 emissions. The technology developed by Omniflow [228] can house all kinds of DC powered IoT devices inside the protective shell that also integrates power generation from integrated vertical wind turbine and solar photovoltaic as well as energy storage using built-in batteries.

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.[229] 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."[230]

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.[230]

Examples of post-sale manipulations include Google Nest Revolv, disabled privacy settings on Android, Sony disabling Linux on PlayStation 3, enforced EULA on Wii U.[230]

Confusing terminology

Kevin Lonergan at *Information Age*, a business technology magazine, has referred to the terms surrounding the IoT as a "terminology zoo".[231] The lack of clear terminology is not "useful from a practical point of view" and a "source of confusion for the end user".[231] A company operating in the IoT space could be working in anything related to sensor technology, networking, embedded systems, or analytics.[231] 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,[123] cooperating objects, machine to machine (M2M), ambient intelligence (AmI), Operational technology (OT), and information technology (IT).[231] 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"[232] to ensure "consistent terminology"[232][233] across publications issued by the

Industrial Internet Consortium. IoT One has created an IoT Terms Database including a New Term Alert[234] to be notified when a new term is published. As of March 2020, this database aggregates 807 IoT-related terms, while keeping material "transparent and comprehensive."[235][236]

IoT adoption barriers

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.[237] 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".[238]

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

Privacy and security concerns

As for 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.[239] 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.[240]

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.[241]

Fundamentally there are 4 security objectives that the IOT system requires:(1)data confidentiality: unauthorized 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 authorized parties even with the denial-of-service (DOS) attacks.[242]

Traditional governance structure

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."[238] 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."[238] 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",[238] or further action in regards to IoT "was pending

competitor moves, customer pull, or regulatory requirements."[238] 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"[243] and "to truly embrace the new business models the disruptive change opens up."[243] 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"[243] but ultimately failed to realize that "online photo sharing *was* the new business, not just a way to expand the printing business."[243]

Town of Internet of Things in Hangzhou, China

Business planning and models

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.[244][245]

Studies on IoT literature and projects show a disproportionate prominence of technology in the IoT projects, which are often driven by technological interventions rather than business model innovation.[246][247]

See also

- 5G
- Automotive security
- Big Data
- Cloud manufacturing
- Cyber-physical system
- Data Distribution Service
- Digital object memory
- Digital twin
- Edge computing
- Four-dimensional product
- Home automation
- Indoor positioning system
- Industry 4.0
- Internet of Military Things
- IoT Cloud
- Open Interconnect Consortium
- OpenWSN
- Quantified self
- Responsive computer-aided design
- Smart grid
- Web of things

References

1. Rouse, Margaret (2019). "internet of things (IoT)" (https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT). *IOT Agenda*. Retrieved 14 August 2019.

2. Brown, Eric (20 September 2016). "21 Open Source Projects for IoT" (http://www.linux.com/NEWS/21-OPEN-SOURCE-PROJECTS-IOT). *Linux.com*. Retrieved 23 October 2016.

3. "Internet of Things Global Standards Initiative" (http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx). *ITU*. Retrieved 26 June 2015.

4. Hendricks, Drew. "The Trouble with the Internet of Things" (http://data.london.gov.uk/blog/the-trouble-with-the-internet-of-things/). *London Datastore*. Greater London Authority. Retrieved 10 August 2015.

5. "The "Only" Coke Machine on the Internet" (https://www.cs.cmu.edu/~coke/history_long.txt). *Carnegie Mellon University*. Retrieved 10 November 2014.

6. "Internet of Things Done Wrong Stifles Innovation" (http://www.informationweek.com/strategic-cio/executive-insights-and-innovation/internet-of-things-done-wrong-stifles-innovation/a/d-id/1279157). *InformationWeek*. 7 July 2014. Retrieved 10 November 2014.

7. Mattern, Friedemann; Floerkemeier, Christian (2010). "From the Internet of Computer to the Internet of Things" (http://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf) (PDF). *Informatik-Spektrum*. **33** (2): 107–121. Bibcode:2009InfSp..32..496H (https://ui.adsabs.harvard.edu/abs/2009InfSp..32..496H). doi:10.1007/s00287-010-0417-7 (https://doi.org/10.1007%2Fs00287-010-0417-7). S2CID 29563772 (https://api.semanticscholar.org/CorpusID:29563772). Retrieved 3 February 2014.

8. Weiser, Mark (1991). "The Computer for the 21st Century" (https://web.archive.org/web/20150311220327/http://web.media.mit.edu/~anjchang/ti01/weiser-sciam91-ubicomp.pdf) (PDF). *Scientific American*. **265** (3): 94–104. Bibcode:1991SciAm.265c..94W (https://ui.adsabs.harvard.edu/abs/1991SciAm.265c..94W). doi:10.1038/scientificamerican0991-94 (https://doi.org/10.1038%2Fscientificamerican0991-94). Archived from the original (http://web.media.mit.edu/~anjchang/ti01/weiser-sciam91-ubicomp.pdf) (PDF) on 11 March 2015. Retrieved 5 November 2014.

9. Raji, R.S. (1994). "Smart networks for control". *IEEE Spectrum*. **31** (6): 49–55. doi:10.1109/6.284793 (https://doi.org/10.1109%2F6.284793). S2CID 42364553 (https://api.semanticscholar.org/CorpusID:42364553).

10. Pontin, Jason (29 September 2005). "ETC: Bill Joy's Six Webs" (http://www.technologyreview.com/view/404694/etc-bill-joys-six-webs/). *MIT Technology Review*. Retrieved 17 November 2013.

11. Ashton, K. (22 June 2009). "That 'Internet of Things' Thing" (http://www.rfidjournal.com/articles/view?4986). Retrieved 9 May 2017.

12. "Peter Day's World of Business" (http://downloads.bbc.co.uk/podcasts/radio/worldbiz/worldbiz_20150319-0730a.mp3). *BBC World Service*. BBC. Retrieved 4 October 2016.

13. Magrassi, P. (2 May 2002). "Why a Universal RFID Infrastructure Would Be a Good Thing" (https://www.gartner.com/doc/356347/universal-rfid-infrastructure-good-thing). *Gartner research report G00106518*.

14. Magrassi, P.; Berg, T (12 August 2002). "A World of Smart Objects" (http://www.gartner.com/DisplayDocument?id=366151). *Gartner research report R-17-2243*.

15. Commission of the European Communities (18 June 2009). "Internet of Things – An action plan for Europe" (http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf) (PDF). COM(2009) 278 final.

16. Wood, Alex (31 March 2015). "The internet of things is revolutionizing our lives, but standards are a must" (https://www.theguardian.com/media-network/2015/mar/31/the-internet-of-things-is-revolutionising-our-lives-but-standards-are-a-must). *The Guardian*.

17. Dave Evans (April 2011). "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything" (https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf) (PDF). *CISCO White Paper*.

18. Omura, Yasuhisa; Mallik, Abhijit; Matsuo, Naoto (2017). *MOS Devices for Low-Voltage and Low-Energy Applications* (https://books.google.com/books?id=yOjFDQAAQBAJ&pg=PA3). John Wiley & Sons. p. 3. ISBN 9781119107354.

19. "1960: Metal Oxide Semiconductor (MOS) Transistor Demonstrated" (https://www.computerhistory.org/siliconengine/metal-oxide-semiconductor-mos-transistor-demonstrated/). *The Silicon Engine: A Timeline of Semiconductors in Computers*. Computer History Museum. Retrieved 31 August 2019.

20. "The Foundation of Today's Digital World: The Triumph of the MOS Transistor" (https://www.youtube.com/watch?v=q6fBEjf9WPw). Computer History Museum. 13 July 2010. Retrieved 21 July 2019.

21. Omura, Yasuhisa; Mallik, Abhijit; Matsuo, Naoto (2017). *MOS Devices for Low-Voltage and Low-Energy Applications* (https://books.google.com/books?id=yOjFDQAAQBAJ). John Wiley & Sons. ISBN 9781119107354.

22. Vongsingthong, S.; Smanchat, S. (2014). "Internet of Things: A review of applications & technologies" (http://ird.sut.ac.th/e-journal/Journal/suwimonv/1403739/1403739.pdf) (PDF). *Suranaree Journal of Science and Technology*.

23. "The Enterprise Internet of Things Market" (http://www.businessinsider.com/the-enterprise-internet-of-things-market-2014-12). *Business Insider*. 25 February 2015. Retrieved 26 June 2015.

24. Perera, C.; Liu, C. H.; Jayawardena, S. (December 2015). "The Emerging Internet of Things Marketplace From an Industrial Perspective: A Survey". *IEEE Transactions on Emerging Topics in Computing*. **3** (4): 585–598. arXiv:1502.00134 (https://arxiv.org/abs/1502.00134). Bibcode:2015arXiv150200134P (https://ui.adsabs.harvard.edu/abs/2015arXiv150200134P). doi:10.1109/TETC.2015.2390034 (https://doi.org/10.1109%2FTETC.2015.2390034). ISSN 2168-6750 (https://www.worldcat.org/issn/2168-6750). S2CID 7329149 (https://api.semanticscholar.org/CorpusID:7329149).

25. "How IoT's are Changing the Fundamentals of "Retailing" " (http://trak.in/tags/business/2016/08/30/internet-of-things-iot-changing-fundamentals-of-retailing/). *Trak.in – Indian Business of Tech, Mobile & Startups*. 30 August 2016. Retrieved 2 June 2017.

26. Kang, Won Min; Moon, Seo Yeon; Park, Jong Hyuk (5 March 2017). "An enhanced security framework for home appliances in smart home". *Human-centric Computing and Information Sciences*. **7** (6). doi:10.1186/s13673-017-0087-4 (https://doi.org/10.1186%2Fs13673-017-0087-4).

27. "How IoT & smart home automation will change the way we live" (http://www.businessinsider.com/internet-of-things-smart-home-automation-2016-8). *Business Insider*. Retrieved 10 November 2017.

28. Greengard, Samuel (2015). *The Internet of Things*. Cambridge, MA: MIT Press. p. 90. ISBN 9780262527736.

29. Inc., Apple. "HomeKit – Apple Developer" (https://developer.apple.com/homekit/). *developer.apple.com*. Retrieved 19 September 2018.

30. Wollerton, Megan (3 June 2018). "Here's everything you need to know about Apple HomeKit" (https://www.cnet.com/news/apple-homekit-everything-you-need-to-know/). *CNET*. Retrieved 19 September 2018.

31. Lovejoy, Ben (31 August 2018). "HomeKit devices getting more affordable as Lenovo announces Smart Home Essentials line" (https://9to5mac.com/2018/08/31/cheap-homekit-bulbs-switches-camera/). *9to5Mac*. Retrieved 19 September 2018.

32. Prospero, Mike (12 September 2018). "Best Smart Home Hubs of 2018" (https://www.tomsguide.com/us/best-smart-home-hubs,review-3200.html). *Tom's Guide*. Retrieved 19 September 2018.

33. Chinchilla, Chris (26 November 2018). "What Smart Home IoT Platform Should You Use?" (https://hackernoon.com/what-smart-home-iot-platform-should-you-use-2554ea213df1). *Hacker Noon*. Retrieved 13 May 2019.

34. Baker, Jason (14 December 2017). "6 open source home automation tools" (https://opensource.com/tools/home-automation). *opensource.com*. Retrieved 13 May 2019.

35. Demiris, G; Hensel, K (2008). "Technologies for an Aging Society: A Systematic Review of 'Smart Home' Applications". *IMIA Yearbook of Medical Informatics 2008*. **17**: 33–40. doi:10.1055/s-0038-1638580 (https://doi.org/10.1055%2Fs-0038-1638580). PMID 18660873 (https://pubmed.ncbi.nlm.nih.gov/18660873). S2CID 7244183 (https://api.semanticscholar.org/CorpusID:7244183).

36. Aburukba, Raafat; Al-Ali, A. R.; Kandil, Nourhan; AbuDamis, Diala (10 May 2016). *Configurable ZigBee-based control system for people with multiple disabilities in smart homes*. pp. 1–5. doi:10.1109/ICCSII.2016.7462435 (https://doi.org/10.1109%2FICCSII.2016.7462435). ISBN 978-1-4673-8743-9. S2CID 16754386 (https://api.semanticscholar.org/CorpusID:16754386).

37. Mulvenna, Maurice; Hutton, Anton; Martin, Suzanne; Todd, Stephen; Bond, Raymond; Moorhead, Anne (14 December 2017). "Views of Caregivers on the Ethics of Assistive Technology Used for Home Surveillance of People Living with Dementia" (https://link.springer.com/content/pdf/10.1007%2Fs12152-017-9305-z.pdf) (PDF). *Neuroethics*. **10** (2): 255–266. doi:10.1007/s12152-017-9305-z (https://doi.org/10.1007%2Fs12152-017-9305-z). PMC 5486509 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5486509). PMID 28725288 (https://pubmed.ncbi.nlm.nih.gov/28725288).

38. da Costa, CA; Pasluosta, CF; Eskofier, B; da Silva, DB; da Rosa Righi, R (July 2018). "Internet of Health Things: Toward intelligent vital signs monitoring in hospital wards". *Artificial Intelligence in Medicine*. **89**: 61–69. doi:10.1016/j.artmed.2018.05.005 (https://doi.org/10.1016%2Fj.artmed.2018.05.005). PMID 29871778 (https://pubmed.ncbi.nlm.nih.gov/29871778).

39. Engineer, A; Sternberg, EM; Najafi, B (21 August 2018). "Designing Interiors to Mitigate Physical and Cognitive Deficits Related to Aging and to Promote Longevity in Older Adults: A Review". *Gerontology*. **64** (6): 612–622. doi:10.1159/000491488 (https://doi.org/10.1159%2F000491488). PMID 30130764 (https://pubmed.ncbi.nlm.nih.gov/30130764). S2CID 52056959 (https://api.semanticscholar.org/CorpusID:52056959).

40. Kricka, LJ (2019). "History of disruptions in laboratory medicine: what have we learned from predictions?". *Clinical Chemistry and Laboratory Medicine*. **57** (3): 308–311. doi:10.1515/cclm-2018-0518 (https://doi.org/10.1515%2Fcclm-2018-0518). PMID 29927745 (https://pubmed.ncbi.nlm.nih.gov/29927745). S2CID 49354315 (https://api.semanticscholar.org/CorpusID:49354315).

41. Gatouillat, Arthur; Badr, Youakim; Massot, Bertrand; Sejdic, Ervin (2018). "Internet of Medical Things: A Review of Recent Contributions Dealing with Cyber-Physical Systems in Medicine" (https://hal.archives-ouvertes.fr/hal-01836236/file/ieee-iot-j.pdf) (PDF). *IEEE Internet of Things Journal*. **5** (5): 3810–3822. doi:10.1109/jiot.2018.2849014 (https://doi.org/10.1109%2Fjiot.2018.2849014). ISSN 2327-4662 (https://www.worldcat.org/issn/2327-4662).

42. Topol, Eric (2016). *The Patient Will See You Now: The Future of Medicine Is in Your Hands*. Basic Books. ISBN 978-0465040025.

43. Dey, Nilanjan; Hassanien, Aboul Ella; Bhatt, Chintan; Ashour, Amira S.; Satapathy, Suresh Chandra (2018). *Internet of things and big data analytics toward next-generation intelligence* (http://shsalmani.ir/wp-content/uploads/2017/09/Internet-of-Things-and-Big-Data-Analytics-Toward-Next-Generation-Intelligence.pdf) (PDF). Springer International Publishing. ISBN 978-3-319-60434-3. Retrieved 14 October 2018.

44. "Deloitte Centre for Health Solutions" (https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/life-sciences-health-care/deloitte-uk-connected-health.pdf) (PDF). *Deloitte*.

45. Ersue, M.; Romascanu, D.; Schoenwaelder, J.; Sehgal, A. (4 July 2014). "Management of Networks with Constrained Devices: Use Cases". *IETF Internet Draft*.

46. "Goldman Sachs Report: How the Internet of Things Can Save the American Healthcare System $305 Billion Annually" (https://www.engagemobile.com/goldman-sachs-report-how-the-internet-of-things-can-save-the-american-healthcare-system-305-billion-annually/). *Engage Mobile Blog*. Engage Mobile Solutions, LLC. 23 June 2016. Retrieved 26 July 2018.

47. World Health Organization. "mHealth. New horizons for health through mobile technologies" (https://www.who.int/goe/publications/goe_mhealth_web.pdf) (PDF). *World Health Organization*. Retrieved 3 January 2020.

48. Istepanian, R.; Hu, S.; Philip, N.; Sungoor, A. (2011). "The potential of Internet of m-health Things "m-IoT" for non-invasive glucose level sensing" (https://dspace.lboro.ac.uk/2134/22172). *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. **2011**. pp. 5264–6. doi:10.1109/IEMBS.2011.6091302 (https://doi.org/10.1109%2FIEMBS.2011.6091302). ISBN 978-1-4577-1589-1. PMID 22255525 (https://pubmed.ncbi.nlm.nih.gov/22255525). S2CID 995488 (https://api.semanticscholar.org/CorpusID:995488).

49. Swan, Melanie (8 November 2012). "Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0". *Journal of Sensor and Actuator Networks*. **1** (3): 217–253. doi:10.3390/jsan1030217 (https://doi.org/10.3390%2Fjsan1030217).

50. *Taiwan Information Strategy, Internet and E-commerce Development Handbook - Strategic Information, Regulations, Contacts*. IBP, Inc. USA. 2016. p. 79. ISBN 978-1514521021.

51. Grell, Max; Dincer, Can; Le, Thao; Lauri, Alberto; Nunez Bajo, Estefania; Kasimatis, Michael; Barandun, Giandrin; Maier, Stefan A.; Cass, Anthony E. G. (2019). "Autocatalytic Metallization of Fabrics Using Si Ink, for Biosensors, Batteries and Energy Harvesting". *Advanced Functional Materials*. **29**: 1804798. doi:10.1002/adfm.201804798 (https://doi.org/10.1002%2Fadfm.201804798). ISSN 1616-301X (https://www.worldcat.org/issn/1616-301X).

52. Dincer, Can; Bruch, Richard; Kling, André; Dittrich, Petra S.; Urban, Gerald A. (1 August 2017). "Multiplexed Point-of-Care Testing – xPOCT" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5538621). *Trends in Biotechnology*. **35** (8): 728–742. doi:10.1016/j.tibtech.2017.03.013 (https://doi.org/10.1016%2Fj.tibtech.2017.03.013). ISSN 0167-7799 (https://www.worldcat.org/issn/0167-7799). PMC 5538621 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5538621). PMID 28456344 (https://pubmed.ncbi.nlm.nih.gov/28456344).

53. "What is HIE? | HealthIT.gov" (https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/what-hie). *www.healthit.gov*. Retrieved 21 January 2020.

54. Amiot, Emmanuel. "The Internet of Things. Disrupting Traditional Business Models" (https://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/jun/2015_OliverWyman_Internet-of-Things.pdf) (PDF). *Oliver Wyman*. Retrieved 14 October 2018.

55. Vermesan, Ovidiu, and Peter Friess, eds. Internet of things: converging technologies for smart environments and integrated ecosystems. River Publisher, 2013. https://www.researchgate.net/publication/272943881

56. Mahmud, Khizir; Town, Graham E.; Morsalin, Sayidul; Hossain, M.J. (February 2018). "Integration of electric vehicles and management in the internet of energy". *Renewable and Sustainable Energy Reviews*. **82**: 4179–4203. doi:10.1016/j.rser.2017.11.004 (https://doi.org/10.1016%2Fj.rser.2017.11.004).

57. Xie, Xiao-Feng; Wang, Zun-Jing (2017). "Integrated in-vehicle decision support system for driving at signalized intersections: A prototype of smart IoT in transportation" (https://trid.trb.org/view.aspx?id=1437314). *Transportation Research Board (TRB) Annual Meeting, Washington, DC, USA*.

58. "Key Applications of the Smart IoT to Transform Transportation" (http://www.wiomax.com/what-can-the-smart-iot-transform-transportation-and-smart-cities/). 20 September 2016.

59. Haase, Jan; Alahmad, Mahmoud; Nishi, Hiroaki; Ploennigs, Joern; Tsang, Kim Fung (2016). "The IOT mediated built environment: A brief survey". *2016 IEEE 14th International Conference on Industrial Informatics (INDIN)*. pp. 1065–1068. doi:10.1109/INDIN.2016.7819322 (https://doi.org/10.1109%2FINDIN.2016.7819322). ISBN 978-1-5090-2870-2. S2CID 5554635 (https://api.semanticscholar.org/CorpusID:5554635).

60. Jussi Karlgren; Lennart Fahlén; Anders Wallberg; Pär Hansson; Olov Ståhl; Jonas Söderberg; Karl-Petter Åkesson (2008). *Socially Intelligent Interfaces for Increased Energy Awareness in the Home. The Internet of Things. Lecture Notes in Computer Science*. **4952**. Springer. pp. 263–275. doi:10.1007/978-3-540-78731-0_17 (https://doi.org/10.1007%2F978-3-540-78731-0_17). ISBN 978-3-540-78730-3. S2CID 30983428 (https://api.semanticscholar.org/CorpusID:30983428).

61. Yang, Chen; Shen, Weiming; Wang, Xianbin (January 2018). "The Internet of Things in Manufacturing: Key Issues and Potential Applications". *IEEE Systems, Man, and Cybernetics Magazine*. **4** (1): 6–15. doi:10.1109/MSMC.2017.2702391 (https://doi.org/10.1109%2FMSMC.2017.2702391). S2CID 42651835 (https://api.semanticscholar.org/CorpusID:42651835).

62. Severi, S.; Abreu, G.; Sottile, F.; Pastrone, C.; Spirito, M.; Berens, F. (23–26 June 2014). "M2M Technologies: Enablers for a Pervasive Internet of Things" (https://www.academia.edu/6866526). *The European Conference on Networks and Communications (EUCNC2014)*.

63. Gubbi, Jayavardhana; Buyya, Rajkumar; Marusic, Slaven; Palaniswami, Marimuthu (24 February 2013). "Internet of Things (IoT): A vision, architectural elements, and future directions". *Future Generation Computer Systems*. **29** (7): 1645–1660. arXiv:1207.0203 (https://arxiv.org/abs/1207.0203). doi:10.1016/j.future.2013.01.010 (https://doi.org/10.1016%2Fj.future.2013.01.010). S2CID 204982032 (https://api.semanticscholar.org/CorpusID:204982032).

64. Tan, Lu; Wang, Neng (20–22 August 2010). *Future Internet: The Internet of Things*. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). **5**. pp. 376–380. doi:10.1109/ICACTE.2010.5579543 (https://doi.org/10.1109%2FICACTE.2010.5579543). ISBN 978-1-4244-6539-2.

65. Daugherty, Paul; Negm, Walid; Banerjee, Prith; Alter, Allan. "Driving Unconventional Growth through the Industrial Internet of Things" (https://www.accenture.com/mz-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Driving-Unconventional-Growth-through-IIoT.pdf) (PDF). *Accenture*. Retrieved 17 March 2016.

66. "Industrial Internet Insights Report" (https://www.accenture.com/us-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Industrial-Internet-Changing-Competitive-Landscape-Industries.pdf) (PDF). *Accenture*. Retrieved 17 March 2016.

67. Meola, A. (20 December 2016). "Why IoT, big data & smart farming are the future of agriculture" (https://www.businessinsider.com/internet-of-things-smart-agriculture-2016-10). *Business Insider*. Insider, Inc. Retrieved 26 July 2018.

68. Zhang, Q. (2015). *Precision Agriculture Technology for Crop Farming* (https://books.google.com/books?id=vHi9CgAAQBAJ&pg=PAPA249). CRC Press. pp. 249–58. ISBN 9781482251081.

69. "Google goes bilingual, Facebook fleshes out translation and TensorFlow is dope ~ And, Microsoft is assisting fish farmers in Japan" (https://www.theregister.co.uk/2018/09/01/ai_roundup_310818/).

70. Chui, Michael; Löffler, Markus; Roberts, Roger. "The Internet of Things" (http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things). *McKinsey Quarterly*. McKinsey & Company. Retrieved 10 July 2014.

71. "Smart Trash" (http://postscapes.com/smart-trash). *Postscapes*. Retrieved 10 July 2014.

72. Poon, L. (22 June 2018). "Sleepy in Songdo, Korea's Smartest City" (https://www.citylab.com/life/2018/06/sleepy-in-songdo-koreas-smartest-city/561374/). *CityLab*. Atlantic Monthly Group. Retrieved 26 July 2018.

73. M. Wijerathna Basnayaka, Chathuranga. "Internet of Things for Smart Cities" (https://www.researchgate.net/publication/340917038). *SLTC*. Retrieved 26 June 2019.

74. Rico, Juan (22–24 April 2014). "Going beyond monitoring and actuating in large scale smart cities". *NFC & Proximity Solutions – WIMA Monaco*.

75. "A vision for a city today, a city of vision tomorrow" (http://www.ssgkc.com). *Sino-Singapore Guangzhou Knowledge City*. Retrieved 11 July 2014.

76. "San Jose Implements Intel Technology for a Smarter City" (http://newsroom.intel.com/community/intel_newsroom/blog/2014/06/11/san-jose-implements-intel-technology-for-a-smarter-city). *Intel Newsroom*. Retrieved 11 July 2014.

77. "Western Singapore becomes test-bed for smart city solutions" (http://singapore.coconuts.co/2014/06/19/western-singapore-becomes-test-bed-smart-city-solutions). *Coconuts Singapore*. 19 June 2014. Retrieved 11 July 2014.

78. Higginbotham, Stacey. "A group of wireless execs aim to build a nationwide network for the Internet of things" (http://fortune.com/2015/09/11/ingenu-machine-network/). *Fortune.com*. Retrieved 8 June 2019.

79. Freeman, Mike (9 September 2015). "On-Ramp Wireless becomes Ingenu, launches nationwide IoT network" (https://www.sandiegouniontribune.com/business/technology/sdut-on-ramp-verizon-ingenu-internet-of-things-att-2015sep09-story.html). *SanDiegoUnionTribune.com*. Retrieved 8 June 2019.

80. Lipsky, Jessica. "IoT Clash Over 900 MHz Options" (http://www.eetimes.com/document.asp?doc_id=1326599). *EETimes*. Retrieved 15 May 2015.

81. Alleven, Monica. "Sigfox launches IoT network in 10 UK cities" (http://www.fiercewireless.com/tech/story/sigfox-launches-iot-network-10-uk-cities/2014-12-13). *Fierce Wireless Tech*. Retrieved 13 May 2015.

82. Merritt, Rick. "13 Views of IoT World" (http://www.eetimes.com/document.asp?doc_id=1326596). *EETimes*. Retrieved 15 May 2015.

83. Fitchard, Kevin (20 May 2014). "Sigfox brings its internet of things network to San Francisco" (https://gigaom.com/2014/05/20/sigfox-brings-its-internet-of-things-network-to-san-francisco/). *Gigaom*. Retrieved 15 May 2015.

84. Ujaley, Mohd (25 July 2018). "Cisco To Invest in Fiber Grid, IoT, Smart Cities in Andhra Pradesh" (https://www.expresscomputer.in/news/cisco-to-invest-in-fiber-grid-iot-smart-cities-in-andhra-pradesh/16750/). ProQuest 1774166769 (https://search.proquest.com/docview/1774166769).

85. "STE Security Innovation Awards Honorable Mention: The End of the Disconnect" (http://www.securityinfowatch.com/article/10840006/ste-security-innovation-awards-honorable-mention-the-end-of-the-disconnect). *securityinfowatch.com*. Retrieved 12 August 2015.

86. Parello, J.; Claise, B.; Schoening, B.; Quittek, J. (28 April 2014). "Energy Management Framework" (http://tools.ietf.org/html/draft-ietf-eman-framework-19). *IETF Internet Draft <draft-ietf-eman-framework-19>*.

87. Davies, Nicola. "How the Internet of Things will enable 'smart buildings' " (http://www.extremetech.com/extreme/209715-how-the-internet-of-things-will-enable-smart-buildings). *Extreme Tech*.

88. "Molluscan eye" (http://molluscan-eye.epoc.u-bordeaux1.fr/index.php?rubrique=accueil&lang=en/). Retrieved 26 June 2015.

89. Li, Shixing; Wang, Hong; Xu, Tao; Zhou, Guiping (2011). *Application Study on Internet of Things in Environment Protection Field* (http://ir.sia.cn/handle/173321/10234). *Lecture Notes in Electrical Engineering Volume* (Submitted manuscript). Lecture Notes in Electrical Engineering. **133**. pp. 99–106. doi:10.1007/978-3-642-25992-0_13 (https://doi.org/10.1007%2F978-3-642-25992-0_13). ISBN 978-3-642-25991-3.

90. "Use case: Sensitive wildlife monitoring" (https://web.archive.org/web/20140714124750/http://fit-equipex.fr/use-cases/23-use-case-sensitive-wildlife-monitoring). *FIT French Project*. Archived from the original (http://fit-equipex.fr/use-cases/23-use-case-sensitive-wildlife-monitoring) on 14 July 2014. Retrieved 10 July 2014.

91. Hart, Jane K.; Martinez, Kirk (1 May 2015). "Toward an environmental Internet of Things". *Earth & Space Science*. **2** (5): 194–200. Bibcode:2015E&SS....2..194H (https://ui.adsabs.harvard.edu/abs/2015E&SS....2..194H). doi:10.1002/2014EA000044 (https://doi.org/10.1002%2F2014EA000044).

92. Scuotto, Veronica; Ferraris, Alberto; Bresciani, Stefano (4 April 2016). "Internet of Things". *Business Process Management Journal*. **22** (2): 357–367. doi:10.1108/bpmj-05-2015-0074 (https://doi.org/10.1108%2Fbpmj-05-2015-0074). ISSN 1463-7154 (https://www.worldcat.org/issn/1463-7154).

93. Cameron, Lori. "Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT" (https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt). *IEEE Computer Society*. Retrieved 31 October 2019.

94. "Army Takes on Wicked Problems With the Internet of Battlefield Things" (https://www.meritalk.com/articles/army-takes-on-wicked-problems-with-the-internet-of-battlefield-things/). *MeriTalk*. 30 January 2018. Retrieved 31 October 2019.

95. Gudeman, Kim (6 October 2017). "Next-Generation Internet of Battle things (IoBT) Aims to Help Keep Troops and Civilians Safe" (https://ece.illinois.edu/newsroom/article/23747). *ECE Illinois*. Retrieved 31 October 2019.

96. "Internet of Battlefield Things (IOBT)" (https://www.arl.army.mil/www/default.cfm?page=3050). *CCDC Army Research Laboratory*. Retrieved 31 October 2019.

97. "DARPA Floats a Proposal for the Ocean of Things" (https://www.meritalk.com/articles/darpa-floats-a-proposal-for-the-ocean-of-things/). *MeriTalk*. 3 January 2018. Retrieved 31 October 2019.

98. "How to make smart packaging even smarter" (https://www.packagingdigest.com/smart-packaging/how-to-make-smart-packaging-even-smarter-2018-06-04). *Packaging Digest*. 4 June 2018. Retrieved 28 April 2020.

99. foodnavigator-asia.com. "Connecting with consumers: The benefits - and dangers - of smart packaging for the F&B industry" (https://www.foodnavigator-asia.com/Article/2019/06/18/Connecting-with-consumers-The-benefits-and-dangers-of-smart-packaging-for-the-F-B-industry). *foodnavigator-asia.com*. Retrieved 28 April 2020.

00. confectionerynews.com. "Which smart packaging technologies are readily available in 2018" (https://www.confectionerynews.com/Article/2018/07/18/Which-smart-packaging-technologies-are-readily-available-in-2018). *confectionerynews.com*. Retrieved 28 April 2020.

01. Chen, Changsheng; Li, Mulin; Ferreira, Anselmo; Huang, Jiwu; Cai, Rizhao (2020). "A Copy-Proof Scheme Based on the Spectral and Spatial Barcoding Channel Models". *IEEE Transactions on Information Forensics and Security*. **15**: 1056–1071. doi:10.1109/tifs.2019.2934861 (https://doi.org/10.1109%2Ftifs.2019.2934861). ISSN 1556-6013 (https://www.worldcat.org/issn/1556-6013).

02. "MIT unveils battery-free crypto tag for anti-counterfeit" (https://www.securingindustry.com/electronics-and-industrial/mit-unveils-battery-free-crypto-tag-for-anti-counterfeit/s105/a11381/). *www.securingindustry.com*. 26 February 2020. Retrieved 28 April 2020.

03. Nordrum, Amy (18 August 2016). "Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated" (https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated). *IEEE Spectrum*.

04. Vermesan, Ovidiu; Friess, Peter (2013). *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems* (http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf) (PDF). Aalborg, Denmark: River Publishers. ISBN 978-87-92982-96-4.

05. Santucci, Gérald. "The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects" (http://cordis.europa.eu/fp7/ict/enet/documents/publications/iot-between-the-internet-revolution.pdf) (PDF). *European Commission Community Research and Development Information Service*. Retrieved 23 October 2016.

06. Mattern, Friedemann; Floerkemeier, Christian. "From the Internet of Computers to the Internet of Things" (http://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf) (PDF). *ETH Zurich*. Retrieved 23 October 2016.

07. Lindner, Tim (13 July 2015). "The Supply Chain: Changing at the Speed of Technology" (http://connectedworld.com/the-supply-chain-changing-at-the-speed-of-technology/). *Connected World*. Retrieved 18 September 2015.

08. Köhn, Rüdiger. "Online-Kriminalität: Konzerne verbünden sich gegen Hacker" (https://www.faz.net/aktuell/wirtschaft/diginomics/grosse-internationale-allianz-gegen-cyber-attacken-15451953-p2.html?printPagedArticle=true#pageIndex_1). *Faz.net*.

09. Hsu, Chin-Lung; Lin, Judy Chuan-Chuan (2016). "An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives". *Computers in Human Behavior*. **62**: 516–527. doi:10.1016/j.chb.2016.04.023 (https://doi.org/10.1016%2Fj.chb.2016.04.023).

10. "Smarter Things: The Autonomous IoT" (http://gdruk.com/smarter-things-autonomous-iot/). *GDR Blog*. GDR Creative Intelligence. 5 January 2018. Retrieved 26 July 2018.

11. Levine, Sergey; Finn, Chelsea; Darrell, Trevor; Abbeel, Pieter (2016). "End-to-End Training of Deep Visuomotor Policies" (http://www.jmlr.org/papers/volume17/15-522/15-522.pdf) (PDF). *The Journal of Machine Learning Research*. **17** (1): 1334–1373. arXiv:1504.00702 (https://arxiv.org/abs/1504.00702). Bibcode:2015arXiv150400702L (https://ui.adsabs.harvard.edu/abs/2015arXiv150400702L).

12. Mohammadi, Mehdi; Al-Fuqaha, Ala; Sorour, Sameh; Guizani, Mohsen (2018). "Deep Learning for IoT Big Data and Streaming Analytics: A Survey". *IEEE Communications Surveys & Tutorials*. **20** (4): 2923–2960. arXiv:1712.04301 (https://arxiv.org/abs/1712.04301). doi:10.1109/COMST.2018.2844341 (https://doi.org/10.1109%2FCOMST.2018.2844341). S2CID 9461213 (https://api.semanticscholar.org/CorpusID:9461213).

13. Mahdavinejad, Mohammad Saeid; Rezvan, Mohammadreza; Barekatain, Mohammadamin; Adibi, Peyman; Barnaghi, Payam; Sheth, Amit P. (2018). "Machine learning for internet of things data analysis: A survey". *Digital Communications and Networks*. **4** (3): 161–175. arXiv:1802.06305 (https://arxiv.org/abs/1802.06305). Bibcode:2018arXiv180206305S (https://ui.adsabs.harvard.edu/abs/2018arXiv180206305S). doi:10.1016/j.dcan.2017.10.002 (https://doi.org/10.1016%2Fj.dcan.2017.10.002). S2CID 2666574 (https://api.semanticscholar.org/CorpusID:2666574).

14. Alippi, C. (2014). *Intelligence for Embedded Systems* (https://www.springer.com/engineering/electronics/book/978-3-319-05277-9). Springer Verlag. ISBN 978-3-319-05278-6.

15. Delicato, F.C.; Al-Anbuky, A.; Wang, K., eds. (2018). *Smart Cyber-Physical Systems: towards Pervasive Intelligence systems* (https://www.journals.elsevier.com/future-generation-computer-systems/call-for-papers/smart-cyber-physical-systems-towards-pervasive-intelligence). *Future Generation Computer Systems*. Elsevier. Retrieved 26 July 2018.

16. Traukina, Alena; Thomas, Jayant; Tyagi, Prashant; Reddipalli, Kishore (29 September 2018). *Industrial Internet Application Development: Simplify IIoT development using the elasticity of Public Cloud and Native Cloud Services* (https://www.amazon.com/Industrial-Internet-Application-Development-development-ebook/dp/B075V92JW7/) (1st ed.). Packt Publishing. p. 18.

17. Hassan, Qusay; Khan, Atta; Madani, Sajjad (2018). *Internet of Things: Challenges, Advances, and Applications*. Boca Raton, Florida: CRC Press. p. 198. ISBN 9781498778510.

18. Chauhuri, Abhik (2018). *Internet of Things, for Things, and by Things*. Boca Raton, Florida: CRC Press. ISBN 9781138710443.

19. Pal, Arpan (May–June 2015). "Internet of Things: Making the Hype a Reality" (http://www.computer.org/cms/Computer.org/ComputingNow/issues/2015/07/mit2015030002.pdf) (PDF). *IT Pro*. **17** (3): 2–4. doi:10.1109/MITP.2015.36 (https://doi.org/10.1109%2FMITP.2015.36). Retrieved 10 April 2016.

20. "Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015" (http://www.gartner.com/newsroom/id/3165317). *Gartner*. 10 November 2015. Retrieved 21 April 2016.

21. Reza Arkian, Hamid (2017). "MIST: Fog-based Data Analytics Scheme with Cost-Efficient Resource Provisioning for IoT Crowdsensing Applications". *Journal of Network and Computer Applications*. **82**: 152–165. doi:10.1016/j.jnca.2017.01.012 (https://doi.org/10.1016%2Fj.jnca.2017.01.012).

22. "IoT The outer Edge Computing" (https://www.techthrive.co.za/techtalk/iot-the-outer-edge-computing/). June 2019. Retrieved 3 June 2019.

23. Gautier, Philippe; Gonzalez, Laurent (2011). *L'Internet des Objets... Internet, mais en mieux* (http://excerpts.numilog.com/books/9782124653164.pdf) (PDF). Foreword by Gérald Santucci (European commission), postword by Daniel Kaplan (FING) and Michel Volle. Paris: AFNOR editions. ISBN 978-2-12-465316-4.

24. Marginean, M.-T.; Lu, C. (2016). "sDOMO communication protocol for home robotic systems in the context of the internet of things" (https://books.google.com/books?id=OGItDQAAQBAJ&pg=PAPA151). *Computer Science, Technology And Application*. World Scientific. pp. 151–60. ISBN 9789813200432.

25. Rowayda, A. Sadek (May 2018). "– An Agile Internet of Things (IoT) based Software Defined Network (SDN) Architecture". *Egyptian Computer Science Journal*.

26. Waldner, Jean-Baptiste (2007). *Nanoinformatique et intelligence ambiante. Inventer l'Ordinateur du XXIeme Siècle*. London: Hermes Science. p. 254. ISBN 978-2-7462-1516-0.

27. "OGC SensorThings API standard specification" (https://portal.opengeospatial.org/files/?artifact_id=6 4146). *OGC*. Retrieved 15 February 2016.

28. "OGC Sensor Web Enablement: Overview And High Level Architecture" (http://portal.opengeospatia l.org/files/?artifact_id=25562). *OGC*. Retrieved 15 February 2016.

29. Minteer, A. (2017). "Chapter 9: Applying Geospatial Analytics to IoT Data" (https://books.google.com/ books?id=FedDDwAAQBAJ&pg=PAPA230). *Analytics for the Internet of Things (IoT)*. Packt Publishing. pp. 230–57. ISBN 9781787127579.

30. van der Zee, E.; Scholten, H. (2014). "Spatial Dimensions of Big Data: Application of Geographical Concepts and Spatial Technology to the Internet of Things" (https://books.google.com/books?id=tEC 5BQAAQBAJ&pg=PAPA160). In Bessis, N.; Dobre, C. (eds.). *Big Data and Internet of Things: A Roadmap for Smart Environments*. Springer. pp. 137–68. ISBN 9783319050294.

31. Gassée, J.-L. (12 January 2014). "Internet of Things: The "Basket of Remotes" Problem" (http://www. mondaynote.com/2014/01/12/internet-of-things-the-basket-of-remotes-problem/). *Monday Note*. Retrieved 26 June 2015.

32. de Sousa, M. (2015). "Chapter 10: Integrating with Muzzley" (https://books.google.com/books?id=CF tICgAAQBAJ&pg=PAPA163). *Internet of Things with Intel Galileo*. Packt Publishing. p. 163. ISBN 9781782174912.

33. Want, Roy; Schilit, Bill N.; Jenson, Scott (2015). "Enabling the Internet of Things". *Computer*. **48**: 28–35. doi:10.1109/MC.2015.12 (https://doi.org/10.1109%2FMC.2015.12). S2CID 17384656 (https://api. semanticscholar.org/CorpusID:17384656).

34. "The Internet of Things: a jumbled mess or a jumbled mess?" (https://www.theregister.co.uk/2015/05/ 14/the_internet_of_things_a_jumbled_mess_or_a_jumbled_mess/). *The Register*. Retrieved 5 June 2016.

35. "Can we talk? Internet of Things vendors face a communications 'mess' " (http://www.computerworld. com/article/2488373/emerging-technology/can-we-talk--internet-of-things-vendors-face-a-communica tions--mess-.html). *Computerworld*. 18 April 2014. Retrieved 5 June 2016.

36. Hassan, Q.F. (2018). *Internet of Things A to Z: Technologies and Applications* (https://books.google.c om/books?id=YmpaDwAAQBAJ&pg=PAPA27). John Wiley & Sons. pp. 27–8. ISBN 9781119456759.

37. Dan Brickley et al., c. 2001

38. Sheng, M.; Qun, Y.; Yao, L.; Benatallah, B. (2017). *Managing the Web of Things: Linking the Real World to the Web* (https://books.google.com/books?id=q0PQDAAAQBAJ&pg=PAPA256). Morgan Kaufmann. pp. 256–8. ISBN 9780128097656.

39. Waldner, Jean-Baptiste (2008). *Nanocomputers and Swarm Intelligence*. London: ISTE. pp. 227–231. ISBN 978-1-84704-002-2.

40. Kushalnagar, N.; Montenegro, G.; Schumacher, C. (August 2007). *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals* (http s://tools.ietf.org/html/rfc4919). IETF. doi:10.17487/RFC4919 (https://doi.org/10.17487%2FRFC4919). RFC 4919 (https://tools.ietf.org/html/rfc4919).

41. Sun, Charles C. (1 May 2014). "Stop using Internet Protocol Version 4!" (http://www.computerworld.c om/article/2488886/networking/stop-using-internet-protocol-version-4-.html). *Computerworld*.

42. Thomson, S.; Narten, T.; Jinmei, T. (September 2007). *IPv6 Stateless Address Autoconfiguration* (htt ps://tools.ietf.org/html/rfc4862). IETF. doi:10.17487/RFC4862 (https://doi.org/10.17487%2FRFC486 2). RFC 4862 (https://tools.ietf.org/html/rfc4862).

43. Xped Limited, ADRC Overview", from Wikipedia

44. Alsulami, M. M.; Akkari, N. (April 2018). "The role of 5G wireless networks in the internet-of- things (IoT)". *2018 1st International Conference on Computer Applications Information Security (ICCAIS)*: 1–8. doi:10.1109/CAIS.2018.8471687 (https://doi.org/10.1109%2FCAIS.2018.8471687). ISBN 978-1-5386-4427-0.

45. Jing, J.; Li, H. (2012). "Research on the Relevant Standards of Internet of Things" (https://books.goo gle.com/books?id=VAG7BQAAQBAJ&pg=PAPA627). In Wang, Y.; Zhang, X. (eds.). *Internet of Things: International Workshop, IOT 2012*. Springer. pp. 627–32. ISBN 9783642324277.

46. Mahmood, Z. (2018). *Connected Environments for the Internet of Things: Challenges and Solutions* (https://books.google.com/books?id=dKVFDwAAQBAJ&pg=PAPA89). Springer. pp. 89–90. ISBN 9783319701028.

47. "Digital Link - Standards | GS1" (https://www.gs1.org/standards/gs1-digital-link). *www.gs1.org*. 12 November 2018. Retrieved 28 April 2020.

48. Howard, Philip N. (1 June 2015). "The Internet of Things is Posed to Change Democracy Itself" (htt p://www.politico.com/agenda/story/2015/06/philip-howard-on-iot-transformation-000099). *Politico*. Retrieved 8 August 2017.

49. Thompson, Kirsten; Mattalo, Brandon (24 November 2015). "The Internet of Things: Guidance, Regulation and the Canadian Approach" (http://www.canadiancybersecuritylaw.com/2015/11/the-inte rnet-of-things-guidance-regulation-and-the-canadian-approach/). *CyberLex*. Retrieved 23 October 2016.

50. "The Question of Who Owns the Data Is About to Get a Lot Trickier" (http://fortune.com/2016/04/06/ who-owns-the-data/). *Fortune*. 6 April 2016. Retrieved 23 October 2016.

51. Weber, R.H.; Weber, R. (2010). *Internet of Things: Legal Perspectives* (https://books.google.com/boo ks?id=9adAAAAAQBAJ&pg=PAPA59). Springer Science & Business Media. pp. 59–64. ISBN 9783642117107.

52. Hassan, Q.F. (2018). *Internet of Things A to Z: Technologies and Applications* (https://books.google.c om/books?id=YmpaDwAAQBAJ&pg=PAPA41). John Wiley & Sons. pp. 41–4. ISBN 9781119456759.

53. Hassan, Q.F.; Khan, A. ur R.; Madani, S.A. (2017). *Internet of Things: Challenges, Advances, and Applications* (https://books.google.com/books?id=iGpQDwAAQBAJ&pg=PAPA41). CRC Press. pp. 41–2. ISBN 9781498778534.

54. Lopez, Javier; Rios, Ruben; Bao, Feng; Wang, Guilin (2017). "Evolving privacy: From sensors to the Internet of Things". *Future Generation Computer Systems*. **75**: 46–57. doi:10.1016/j.future.2017.04.045 (https://doi.org/10.1016%2Fj.future.2017.04.045).

55. "The 'Internet of Things': Legal Challenges in an Ultra-connected World" (http://www.mhc.ie/latest/blo g/the-internet-of-things-legal-challenges-in-an-ultra-connected-world). *Mason Hayes & Curran*. 22 January 2016. Retrieved 23 October 2016.

56. Brown, Ian (2015). "Regulation and the Internet of Things" (https://www.itu.int/en/ITU-D/Conferences/ GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf) (PDF). *Oxford Internet Institute*. Retrieved 23 October 2016.

57. "FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks" (https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-inter net-things-urges-companies-adopt-best-practices). *Federal Trade Commission*. 27 January 2015. Retrieved 23 October 2016.

58. Lawson, Stephen (2 March 2016). "IoT users could win with a new bill in the US Senate" (https://ww w.techbarrista.com/iot-users-could-win-with-a-new-bill-in-the-us-senate/). *Tech Barrista*. Retrieved 9 December 2019.

59. "California Legislative Information – SB-327 Information privacy: connected devices" (https://leginfo.l egislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327).

60. Pittman, F. Paul (2 February 2016). "Legal Developments in Connected Car Arena Provide Glimpse of Privacy and Data Security Regulation in Internet of Things" (http://www.lexology.com/library/detail. aspx?g=fd6bc26e-dd20-4c4f-897a-5d62484d37ba). *Lexology*. Retrieved 23 October 2016.

61. Rasit, Yuce, Mehmet; Claus, Beisswenger, Stefan; Mangalam, Srikanth; Das, Prasanna, Lal; Martin, Lukac (2 November 2017). "Internet of things : the new government to business platform – a review of opportunities, practices, and challenges" (http://documents.worldbank.org/curated/en/6100815096 89089303/Internet-of-things-the-new-government-to-business-platform-a-review-of-opportunities-pra ctices-and-challenges): 1–112.

62. Wieland, Ken (25 February 2016). "IoT experts fret over fragmentation" (http://www.mobileworldlive.c om/mwc16-articles/iot-experts-fret-over-fragmentation/). *Mobile World*.

63. Wallace, Michael (19 February 2016). "Fragmentation is the enemy of the Internet of Things" (https:// www.qualcomm.com/news/onq/2016/02/19/fragmentation-enemy-internet-things). *Qualcomm.com*.

64. Bauer, Harald; Patel, Mark; Veira, Jan (October 2015). "Internet of Things: Opportunities and challenges for semiconductor companies" (http://www.mckinsey.com/industries/semiconductors/our-i nsights/internet-of-things-opportunities-and-challenges-for-semiconductor-companies). *McKinsey & Co*.

65. Ardiri, Aaron (8 July 2014). "Will fragmentation of standards only hinder the true potential of the IoT industry?" (https://evothings.com/will-fragmentation-of-standards-only-hinder-the-true-potential-of-the -iot-industry/). *evothings.com*.

66. "IOT Brings Fragmentation in Platform" (http://www.arm.com/zh/files/event/ATF2015SZ_A6_Thunder soft.pdf) (PDF). *arm.com*.

67. Raggett, Dave (27 April 2016). "Countering Fragmentation with the Web of Things: Interoperability across IoT platforms" (https://www.w3.org/Talks/2016/04-27-countering-fragmentation.pdf) (PDF). *W3C*.

68. Kovach, Steve (30 July 2013). "Android Fragmentation Report" (http://www.businessinsider.com/andr oid-fragmentation-report-2013-7). *Business Insider*. Retrieved 19 October 2013.

69. "Ultimate Guide to Internet of Things (IoT) Connectivity" (https://www.argenox.com/library/iot/ultimate -guide-iot-connectivity/).

70. Piedad, Floyd N. "Will Android fragmentation spoil its IoT appeal?" (http://techbeacon.com/will-androi d-fragmentation-spoil-its-iot-appeal). *TechBeacon*.

71. Franceschi-Bicchierai, Lorenzo (29 July 2015). "Goodbye, Android" (http://motherboard.vice.com/rea d/goodbye-android). *Motherboard*. Vice.

72. Kingsley-Hughes, Adrian. "The toxic hellstew survival guide" (https://www.zdnet.com/article/the-andr oid-toxic-hellstew-survival-guide/). *ZDnet*. Retrieved 2 August 2015.

73. Tung, Liam (13 October 2015). "Android security a 'market for lemons' that leaves 87 percent vulnerable" (https://www.zdnet.com/article/android-security-a-market-for-lemons-that-leaves-87-perc ent-insecure/). *ZDNet*. Retrieved 14 October 2015.

74. Thomas, Daniel R.; Beresford, Alastair R.; Rice, Andrew (2015). *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices – SPSM '15* (https://ww w.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf) (PDF). *Computer Laboratory, University of Cambridge*. pp. 87–98. doi:10.1145/2808117.2808118 (https://doi.org/10.1145%2F2808117.2808118). ISBN 9781450338196. S2CID 14832327 (https://api. semanticscholar.org/CorpusID:14832327). Retrieved 14 October 2015.

75. Howard, Philip N. (2015). *Pax Technica: How the internet of things May Set Us Free, Or Lock Us Up*. New Haven, CT: Yale University Press. ISBN 978-0-30019-947-5.

76. McEwan, Adrian (2014). "Designing the Internet of Things" (http://madsg.com/wp-content/uploads/20 15/12/Designing_the_Internet_of_Things.pdf) (PDF). Retrieved 1 June 2016.

77. Moy de Vitry, Matthew; Schneider, Mariane; Wani, Omar; Liliane, Manny; Leitao, João P.; Eggimann, Sven (2019). "Smart urban water systems: what could possibly go wrong?". *Environmental Research Letters*. **14** (8): 081001. Bibcode:2019ERL....14h1001M (https://ui.adsabs.harvard.edu/abs/2019ER L....14h1001M). doi:10.1088/1748-9326/ab3761 (https://doi.org/10.1088%2F1748-9326%2Fab3761).

78. "Panopticon as a metaphor for the internet of things" (http://www.theinternetofthings.eu/sites/default/files/Rob%20van%20Kranenburg/Panopticon%20as%20metaphor%20for%20the%20IoT_GS%20Dec2011.pdf) (PDF). *The Council of the Internet of Things*. Retrieved 6 June 2016.

79. "Foucault" (https://ccle.ucla.edu/pluginfile.php/1330126/mod_resource/content/0/foucault.pdf) (PDF). UCLA.

80. "Deleuze – 1992 – Postscript on the Societies of Control" (https://ccle.ucla.edu/pluginfile.php/1330127/mod_resource/content/0/Deleuze%20-%201992%20-%20Postscript%20on%20the%20Societies%20of%20Control.pdf) (PDF). UCLA.

81. Verbeek, Peter-Paul (2011). *Moralizing Technology: Understanding and Designing the Morality of Things* (https://archive.org/details/moralizingtechno0000verb). Chicago: The University of Chicago Press. ISBN 978-0-22685-291-1.

82. Cardwell, Diane (18 February 2014). "At Newark Airport, the Lights Are On, and They're Watching You" (https://www.nytimes.com/2014/02/18/business/at-newark-airport-the-lights-are-on-and-theyre-watching-you.html). *The New York Times*.

83. Hardy, Quentin (4 February 2015). "Tim O'Reilly Explains the Internet of Things" (http://bits.blogs.nytimes.com/2015/02/04/tim-oreilly-explains-the-internet-of-things/). *The New York Times*.

84. Webb, Geoff (5 February 2015). "Say Goodbye to Privacy" (https://www.wired.com/2015/02/say-goodbye-to-privacy/). *WIRED*. Retrieved 15 February 2015.

85. Crump, Catherine; Harwood, Matthew (25 March 2014). "The Net Closes Around Us" (http://www.tomdispatch.com/post/175822/tomgram%3A_crump_and_harwood%2C_the_net_closes_around_us/). *TomDispatch*.

86. Brown, Ian (12 February 2013). "Britain's Smart Meter Programme: A Case Study in Privacy by Design". *International Review of Law, Computers & Technology*. **28** (2): 172–184. doi:10.1080/13600869.2013.801580 (https://doi.org/10.1080%2F13600869.2013.801580). S2CID 62756630 (https://api.semanticscholar.org/CorpusID:62756630). SSRN 2215646 (https://ssrn.com/abstract=2215646).

87. "The Societal Impact of the Internet of Things" (https://www.bcs.org/upload/pdf/societal-impact-report-feb13.pdf) (PDF). *British Computer Society*. 14 February 2013. Retrieved 23 October 2016.

88. Gubbi, Jayavardhana; Buyya, Rajkumar; Marusic, Slaven; Palaniswami, Marimuthu (1 September 2013). "Internet of Things (IoT): A vision, architectural elements, and future directions". *Future Generation Computer Systems*. Including Special sections: Cyber-enabled Distributed Computing for Ubiquitous Cloud and Network Services & Cloud Computing and Scientific Applications – Big Data, Scalable Analytics, and Beyond. **29** (7): 1645–1660. arXiv:1207.0203 (https://arxiv.org/abs/1207.0203). doi:10.1016/j.future.2013.01.010 (https://doi.org/10.1016%2Fj.future.2013.01.010). S2CID 204982032 (https://api.semanticscholar.org/CorpusID:204982032).

89. Acharjya, D.P.; Ahmed, N.S.S. (2017). "Recognizing Attacks in Wireless Sensor Network in View of Internet of Things" (https://books.google.com/books?id=4UW4DgAAQBAJ&pg=PA149). In Acharjya, D.P.; Geetha, M.K. (eds.). *Internet of Things: Novel Advances and Envisioned Applications*. Springer. pp. 149–50. ISBN 9783319534725.

90. Hussain, A. (June 2017). "Energy Consumption of Wireless IoT Nodes" (https://brage.bibsys.no/xmlui/bitstream/handle/11250/2458157/17677_FULLTEXT.pdf?sequence=1) (PDF). Norwegian University of Science and Technology. Retrieved 26 July 2018.

91. "We Asked Executives About The Internet of Things And Their Answers Reveal That Security Remains A Huge Concern" (http://www.businessinsider.in/We-Asked-Executives-About-The-Internet-Of-Things-And-Their-Answers-Reveal-That-Security-Remains-A-Huge-Concern/articleshow/45959921.cms). *Business Insider*. Retrieved 26 June 2015.

92. Singh, Jatinder; Pasquier, Thomas; Bacon, Jean; Ko, Hajoon; Eyers, David (2015). "Twenty Cloud Security Considerations for Supporting the Internet of Things" (https://www.repository.cam.ac.uk/handle/1810/250441). *IEEE Internet of Things Journal*. **3** (3): 1. doi:10.1109/JIOT.2015.2460333 (https://doi.org/10.1109%2FJIOT.2015.2460333). S2CID 4732406 (https://api.semanticscholar.org/CorpusID:4732406).

93. Clearfield, Chris. "Why The FTC Can't Regulate The Internet of Things" (https://www.forbes.com/site s/chrisclearfield/2013/09/18/why-the-ftc-cant-regulate-the-internet-of-things/). *Forbes*. Retrieved 26 June 2015.

94. Feamster, Nick (18 February 2017). "Mitigating the Increasing Risks of an Insecure Internet of Things" (https://freedom-to-tinker.com/2017/02/18/mitigating-the-increasing-risks-of-an-insecure-inter net-of-things/). Freedom to Tinker. Retrieved 8 August 2017.

95. Li, S. (2017). "Chapter 1: Introduction: Securing the Internet of Things" (https://books.google.com/bo oks?id=uW1_CwAAQBAJ&pg=PAPA1). In Li, S.; Xu, L.D. (eds.). *Securing the Internet of Things*. Syngress. p. 4. ISBN 9780128045053.

96. Bastos, D.; Shackleton, M.; El-Moussa, F. (2018). "Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments". *Living in the Internet of Things: Cybersecurity of the IoT - 2018*. pp. 30 (7 pp.). doi:10.1049/cp.2018.0030 (https://doi.org/10.1049%2Fcp.2018.003 0). ISBN 9781785618437.

97. Liu, Ximeng; Yang, Yang; Choo, Kim-Kwang Raymond; Wang, Huaqun (24 September 2018). "Security and Privacy Challenges for Internet-of-Things and Fog Computing". *Wireless Communications and Mobile Computing*. **2018**: 1–3. doi:10.1155/2018/9373961 (https://doi.org/10.11 55%2F2018%2F9373961). ISSN 1530-8669 (https://www.worldcat.org/issn/1530-8669).

98. Morrissey, Janet (22 January 2019). "In the Rush to Join the Smart Home Crowd, Buyers Should Beware" (https://www.nytimes.com/2019/01/22/business/smart-home-buyers-security-risks.html). *The New York Times*. ISSN 0362-4331 (https://www.worldcat.org/issn/0362-4331). Retrieved 26 February 2020.

99. Clearfield, Christopher (26 June 2013). "Rethinking Security for the Internet of Things" (http://blogs.h br.org/2013/06/rethinking-security-for-the-in). *Harvard Business Review Blog*.

00. Witkovski, Adriano; Santin, Altair; Abreu, Vilmar; Marynowski, Joao (2014). "An IdM and Key-Based Authentication Method for Providing Single Sign-On in IoT" (https://www.researchgate.net/publicatio n/294889554). *2015 IEEE Global Communications Conference (GLOBECOM)*. pp. 1–6. doi:10.1109/GLOCOM.2014.7417597 (https://doi.org/10.1109%2FGLOCOM.2014.7417597). ISBN 978-1-4799-5952-5. S2CID 8108114 (https://api.semanticscholar.org/CorpusID:8108114).

01. Steinberg, Joseph (27 January 2014). "These Devices May Be Spying on You (Even in Your Own Home)" (https://www.forbes.com/sites/josephsteinberg/2014/01/27/these-devices-may-be-spying-on-you-even-in-your-own-home/). *Forbes*. Retrieved 27 May 2014.

02. Greenberg, Andy (21 July 2015). "Hackers Remotely Kill a Jeep on the Highway—With Me in It" (http s://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/). *Wired*. Retrieved 21 July 2015.

03. *Scientific American*, April 2015, p.68.

04. Loukas, George (June 2015). *Cyber-Physical Attacks A growing invisible threat* (http://dl.acm.org/cita tion.cfm?id=2818550). Oxford, UK: Butterworh-Heinemann (Elsevier). p. 65. ISBN 9780128012901.

05. Woolf, Nicky (26 October 2016). "DDoS attack that disrupted internet was largest of its kind in history, experts say" (https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-bot net). *The Guardian*.

06. Antonakakis, Manos; April, Tim; Bailey, Michael; Bernhard, Matt; Bursztein, Elie; Cochran, Jaime; Durumeric, Zakir; Halderman, J. Alex; Invernizzi, Luca (18 August 2017). *Understanding the Mirai Botnet* (https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf) (PDF). *Usenix*. ISBN 978-1-931971-40-9. Retrieved 13 May 2018.

07. "The "anti-patterns" that turned the IoT into the Internet of Shit / Boing Boing" (https://boingboing.net/ 2017/05/03/bad-design-thinking.html). *boingboing.net*. 3 May 2017.

08. Ali, Junade (2 May 2017). "IoT Security Anti-Patterns" (https://blog.cloudflare.com/iot-security-anti-pa tterns/). *Cloudflare Blog*.

09. Schneier, Bruce (6 October 2016). "We Need to Save the Internet from the Internet of Things" (http s://www.schneier.com/essays/archives/2016/10/we_need_to_save_the_.html). *Motherboard*.

10. "Disruptive Technologies Global Trends 2025" (https://fas.org/irp/nic/disruptive.pdf) (PDF). *National Intelligence Council (NIC)*. April 2008. p. 27.

11. Ackerman, Spencer (15 March 2012). "CIA Chief: We'll Spy on You Through Your Dishwasher" (https://www.wired.com/dangerroom/2012/03/petraeus-tv-remote/). *WIRED*. Retrieved 26 June 2015.

12. https://www.facebook.com/geoffreyfowler. "The doorbells have eyes: The privacy battle brewing over home security cameras" (https://www.washingtonpost.com/technology/2019/01/31/doorbells-have-eyes-privacy-battle-brewing-over-home-security-cameras/). *Washington Post*. Retrieved 3 February 2019.

13. "Building the Web of Things – Mozilla Hacks – the Web developer blog" (https://hacks.mozilla.org/2017/06/building-the-web-of-things). *Mozilla Hacks – the Web developer blog*.

14. "The Step Towards Innovation" (https://kbvresearch.com/).

15. "Global IoT Security Market to reach a market size of $29.2 billion by 2022" (https://kbvresearch.com/global-iot-security-market/).

16. Ward, Mark (23 September 2015). "Smart devices to get security tune-up" (https://www.bbc.co.uk/news/technology-34324247). *BBC News*.

17. "Executive Steering Board" (https://iotsecurityfoundation.org/executive-steering-board/). *IoT Security Foundation*.

18. Schneier, Bruce (1 February 2017). "Security and the Internet of Things" (https://www.schneier.com/blog/archives/2017/02/security_and_th.html).

19. Alfandi, Omar; Hasan, Musaab; Balbahaith, Zayed (2019), "Assessment and Hardening of IoT Development Boards", *Lecture Notes in Computer Science*, Springer International Publishing, pp. 27–39, doi:10.1007/978-3-030-30523-9_3 (https://doi.org/10.1007%2F978-3-030-30523-9_3), ISBN 978-3-030-30522-2

20. Nguyen, Dang Tu; Song, Chengyu; Qian, Zhiyun; V. Krishnamurthy, Srikanth; J. M. Colbert, Edward; McDaniel, Patrick (2018). *IoTSan: Fortifying the Safety of IoT Systems*. Proc. of the 14th International Conference on emerging Networking EXperiments and Technologies (CoNEXT '18). Heraklion, Greece. arXiv:1810.09551 (https://arxiv.org/abs/1810.09551). doi:10.1145/3281411.3281440 (https://doi.org/10.1145%2F3281411.3281440). arXiv:1810.09551.

21. "SmartThings" (https://www.smartthings.com/). *SmartThings.com*.

22. "HomeKit – Apple Developer" (https://developer.apple.com/homekit/). *developer.apple.com*.

23. "Amazon Alexa" (https://developer.amazon.com/alexa). *developer.amazon.com*.

24. Fielding, Roy Thomas (2000). "Architectural Styles and the Design of Network-based Software Architectures" (https://www.ics.uci.edu/~fielding/pubs/dissertation/fielding_dissertation.pdf) (PDF). *University of California, Irvine*.

25. Littman, Michael; Kortchmar, Samuel (11 June 2014). "The Path to a Programmable World" (http://footnote1.com/the-path-to-a-programmable-world/). *Footnote*. Retrieved 14 June 2014.

26. Finley, Klint (6 May 2014). "The Internet of Things Could Drown Our Environment in Gadgets" (https://www.wired.com/2014/06/green-iot/). *Wired*.

27. Light, A.; Rowland, C. (2015). "Chapter 11: Responsible IoT Design" (https://books.google.com/books?id=PP1xCQAAQBAJ&pg=PASA10-PA69). In Rowland, C.; Goodman, E.; Charlier, M.; et al. (eds.). *Designing Connected Products: UX for the Consumer Internet of Things*. O'Reilly Media. pp. 457–64. ISBN 9781449372569.

28. http://omniflow.io

29. Gilbert, Arlo (3 April 2016). "The time that Tony Fadell sold me a container of hummus" (https://medium.com/@arlogilbert/the-time-that-tony-fadell-sold-me-a-container-of-hummus-cb0941c762c1). Retrieved 7 April 2016.

30. Walsh, Kit (5 April 2016). "Nest Reminds Customers That Ownership Isn't What It Used to Be" (https://www.eff.org/deeplinks/2016/04/nest-reminds-customers-ownership-isnt-what-it-used-be). *Electronic Frontier Foundation*. Retrieved 7 April 2016.

31. "Taming the IoT terminology zoo: what does it all mean?" (http://www.information-age.com/taming-iot-terminology-zoo-what-does-it-all-mean-123459907/). *Information Age*. Vitesse Media Plc. 30 July 2015.

32. "Technology Working Group" (http://www.iiconsortium.org/wc-technology.htm). The Industrial Internet Consortium. Retrieved 21 March 2017.

33. "Vocabulary Technical Report" (http://www.iiconsortium.org/vocab/index.htm). The Industrial Internet Consortium. Retrieved 21 March 2017.

34. "Acceleration Sensing" (http://www.iotone.com/term/acceleration-sensing/t19). IoT One. Retrieved 21 March 2017.

35. "IoT Terms Database" (http://www.iotone.com/terms). IoT One. Retrieved 21 March 2017.

36. "Quick Guide" (https://www.iotone.com/quick-guide). *IoT ONE*. Retrieved 26 July 2018.

37. "Why The Consumer Internet of Things Is Stalling" (https://www.forbes.com/sites/ciocentral/2016/09/13/why-the-consumer-internet-of-things-is-stalling/). *Forbes*. Retrieved 24 March 2017.

38. "Every. Thing. Connected. A study of the adoption of 'Internet of Things' among Danish companies" (https://www.ericsson.com/49928a/assets/local/news/2015/11/every-thing-connected.pdf) (PDF). Ericsson. Retrieved 2 May 2020.

39. Zhang, Zhi-Kai; Cho, Michael Cheng Yi; Wang, Chia-Wei; Hsu, Chia-Wei; Chen, Chong-Kuan; Shieh, Shiuhpyng (2014). "IoT Security: Ongoing Challenges and Research Opportunities". *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*. pp. 230–234. doi:10.1109/SOCA.2014.58 (https://doi.org/10.1109%2FSOCA.2014.58). ISBN 978-1-4799-6833-6. S2CID 18445510 (https://api.semanticscholar.org/CorpusID:18445510).

40. Khan, Minhaj Ahmad; Salah, Khaled (2018). "IoT security: Review, blockchain solutions, and open challenges". *Future Generation Computer Systems*. **82**: 395–411. doi:10.1016/j.future.2017.11.022 (https://doi.org/10.1016%2Fj.future.2017.11.022).

41. Zhou, Wei; Jia, Yan; Peng, Anni; Zhang, Yuqing; Liu, Peng (2019). "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to be Solved". *IEEE Internet of Things Journal*. **6** (2): 1606–1616. arXiv:1802.03110 (https://arxiv.org/abs/1802.03110). doi:10.1109/JIOT.2018.2847733 (https://doi.org/10.1109%2FJIOT.2018.2847733). S2CID 31057653 (https://api.semanticscholar.org/CorpusID:31057653).

42. Supriya, S.; Padaki, Sagar (2016). "Data Security and Privacy Challenges in Adopting Solutions for IOT". *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. pp. 410–415. doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2016.97 (https://doi.org/10.1109%2FiThings-GreenCom-CPSCom-SmartData.2016.97). ISBN 978-1-5090-5880-8. S2CID 34661195 (https://api.semanticscholar.org/CorpusID:34661195).

43. Anthony, Scott (15 July 2016). "Disruptive Innovation: Kodak's Downfall Wasn't About Technology" (https://hbr.org/2016/07/kodaks-downfall-wasnt-about-technology). *Harvard Business Review*. Harvard Business Publishing. Retrieved 30 March 2017.

44. "World Economic Forum: The Next Economic Growth Engine – Scaling Fourth Industrial Revolution Technologies in Production" (http://www3.weforum.org/docs/WEF_Technology_and_Innovation_The_Next_Economic_Growth_Engine.pdf) (PDF). *World Economic Forum*. January 2018. p. 4.

45. at 11:15, Kat Hall 23 May 2017. "Three-quarters of IoT projects are failing, says Cisco" (https://www.theregister.co.uk/2017/05/23/threequarters_of_iot_projects_are_failing/). *www.theregister.co.uk*. Retrieved 29 January 2020.

46. Solaimani, Sam; Keijzer-Broers, Wally; Bouwman, Harry (1 May 2015). "What we do – and don't – know about the Smart Home: An analysis of the Smart Home literature". *Indoor and Built Environment*. **24** (3): 370–383. doi:10.1177/1420326X13516350 (https://doi.org/10.1177%2F1420326X13516350). ISSN 1420-326X (https://www.worldcat.org/issn/1420-326X). S2CID 59443602 (https://api.semanticscholar.org/CorpusID:59443602).

47. Westerlund, Mika; Leminen, Seppo; Rajahonka, Mervi (2014). "Designing Business Models for the Internet of Things". *Technology Innovation Management Review*. **4** (7): 5–14. doi:10.22215/timreview/807 (https://doi.org/10.22215%2Ftimreview%2F807). ISSN 1927-0321 (http s://www.worldcat.org/issn/1927-0321).

Bibliography

- The Internet of Things (https://www.britannica.com/EBchecked/topic/2032782) at the *Encyclopædia Britannica*
- Acharjya, D.P.; Geetha, M.K., eds. (2017). *Internet of Things: Novel Advances and Envisioned Applications* (https://books.google.com/books?id=4UW4DgAAQBAJ&pg=PA1). Springer. p. 311. ISBN 9783319534725.
- Li, S.; Xu, L.D., eds. (2017). *Securing the Internet of Things* (https://books.google.com/books?id=uW 1_CwAAQBAJ&pg=PAPA1). Syngress. p. 154. ISBN 9780128045053.
- Rowland, C.; Goodman, E.; Charlier, M.; et al., eds. (2015). *Designing Connected Products: UX for the Consumer Internet of Things* (https://books.google.com/books?id=PP1xCQAAQBAJ). O'Reilly Media. p. 726. ISBN 9781449372569.
- Thomas, Jayant; Traukina, Alena (2018). *Industrial Internet Application Development: Simplify IIoT development using the elasticity of Public Cloud and Native Cloud Services* (https://www.amazon.co m/Industrial-Internet-Application-Development-development-ebook/dp/B075V92JW7/). Packt Publishing. p. 25. ISBN 978-1788298599.
- Stephenson, W. David. (2018). *The Future Is Smart: how your company can capitalize on the Internet of Things--and win in a connected economy* (https://www.harpercollinsleadership.com/97808 14439777/the-future-is-smart/). HarperCollins Leadership. p. 250. ISBN 9780814439777.