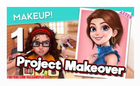
Benefits of rooting android 2020

Continue



Do you want to unlock the bootloader of your Android device? Then you need to enable OEM unlock option first. In this post, we'll talk about what OEM unlocking is and then show you how to enable it on your Android device. Android is known for its open-source nature and ability to break through OEM limitations. In terms of restrictions, device manufacturers often tend to limit the functionality of the operating system through a software switch to prevent external changes. This is recommended so that everyday users can maintain the integrity of their Android devices. But what if the user decides to intentionally change the preinstalled software? Well, the word "official" is not supported in most cases. This means that unlocking your Android device's bootloader will void your warranty. Just not in the case of OnePlus, or maybe Google itself. Now, if you're really interested in customizing your Android phone with third-party software, you need to unlock the bootloader first. However, to do this, you need to enable the “OEM Unlock” option in your phone settings. We'll cover all of that below. Contents What is OEM Unlocking? Android OEM Unlock is an option in your device's developer options that you must enable in order to unlock your bootloader. It was first introduced by Google in Android 5.0 Lollipop and is sometimes referred to as "OEM Unlock". Enabling this option will set the unlock_ability flag to 1, allowing the user to run the fastboot flashing unlock command to unlock the phone's bootloader. Once enabled, this option remains unchanged after reboots and factory resets until manually disabled. The option itself is usually hidden to prevent accidental access, just like "USB Debugging". It can also serve as a recovery process to revive your deviceDo you want to unlock the bootloader of your Android device? Then you need to enable OEM unlock option first. In this post, we are going to talk about what OEM unlock is and how to enable it on your Android device. Android is known for its open source and ability to push the limits set by the OEM. Speaking of limits: device manufacturers often try to limit the functionality of the operating system by changing the software in order to prevent external modifications. This is recommended to allow regular users to maintain the integrity of their Android devices. But what if the user intentionally messes with the preinstalled software? Well, the word "official" is not supported in most cases. This means that unlocking your Android device's bootloader will void your warranty. Just not in the case of OnePlus, or maybe Google itself. If you really want to customize your Android phone with third-party software, you need to unlock the bootloader first. But for that you need to enable "OEM Unlock" in your phone settings. We'll look at all of this below. Contents What is OEM Unlock? Android OEM Unlock is a setting in the device developer settings that needs to be enabled to unlock the bootloader. It was first introduced by Google in Android 5.0 Lollipop and is sometimes referred to as "OEM Unlock". Enabling this option will set the "unlock_ability" flag to "1", which allows the user to issue the "fastboot flashing unlock" command to unlock the phone's bootloader. Once enabled, this setting will remain constant during reboots and factory resets until manually disabled. The option itself is usually hidden to prevent accidental access, as is USB debugging. It can also be used as a recovery process to bring your device back to life.something is wrong with the software. Why do you need to enable OEM unlock? Before we even get into the instructions and enable OEM unlocking on Android, let's fully understand the pros and cons of unlocking the bootloader. Next, we will add what "OEM Unlock" actually is and why it is necessary. The standard process of installing a custom ROM, kernel or some famous mods like ViPER4Android etc. requires your device to be rooted. In most cases, rooting depends on a custom recovery like TWRP. In addition, you must have write access to the device partitions to install a custom recovery. A locked bootloader prevents this. This prevents existing partitions from being overwritten or modified. So, the first step to root your Android device is to unlock the bootloader. The image below will help you understand the process better if everything in the above paragraph sounds confusing. So what is a bootloader? â It is software that runs from the moment you turn on your Android phone. It is loaded with instructions for booting the operating system kernel and the OEM provides the user with the necessary permissions to modify or access the bootloader. Unlocked bootloader also allows you to flash factory images for Google Nexus/Pixel, Razer and other devices. An unlocked bootloader has its benefits, yes! But it also has some disadvantages. So before we dive into the instructions on how to enable OEM unlocking on Android, take a look at some of the general guidelines below. The main disadvantage is that in most cases you will lose the official warranty or support. Apart from some OEMs like OnePlus. Second, once you unlock the bootloader, your device will be wiped. This can prevent you from using DRM-protected features or apps like Netflix on your Android device. How to Enable OEM Unlocking on Android Devicesin fact, we're actually here today. We have divided the guide into three steps so you can easily follow the whole process. Step 1: Back up your Android device. It is highly recommended that you make a full backup of your device, including apps, messages, contacts, and internal storage. Activating OEM-only unlock will not delete the data stored on the device. You will probably proceed to unlock the bootloader, which will completely erase your data. You can follow our Android device backup guide. Step 2: Enable Android Developer Options As already mentioned, the option/toggle itself is hidden in the developer options menu by default. To enable OEM unlocking, you must first view/enable developer options in your phone's settings. Go to the app drawer and open "Settings". Scroll down and find the "System" section. If you're using an Android Nougat or earlier device, please search "About Phone" directly. Click on the "About phone" section. You will then see device information such as Android version, security patch level, etc. Search for "build number". Quickly tap the build number seven times. If you have set a PIN/Password, you will be prompted to enter it. Once you publish it, you will see a popup at the bottom of the screen saying "You are now a developer!". Return to the "System" section. On Android Nougat and earlier, just go back to the main settings. You will see a new section called Developer Options. Now you can follow the instructions below to enable OEM Unlock on Android. Step 3: Enable OEM Unlock (OEM Unlock) on Android. Go to "Settings" and click "System". Select Developer Options. Scroll down the options and look for "OEM Unlock". Just tap the switch next to it. If you have set a password/PIN, you will be prompted to enter it again. You will be asked to confirm the operation"TURN ON". So now you know what OEM unlock is and how to enable it on your Android device. You can then unlock the bootloader using the fastboot command. After unlocking, you can easily install TWRP recovery and root your phone with Magisk. That was easy now, wasn't it? We hope the article was able to explain the whole concept to you well. However, if you still have questions, please go to the comments below and ping us. Not to be confused with the web of things. An internet-like system that connects everyday physical objects The Internet of Things (IoT) describes physical objects (or groups of such objects) with sensors, processing capabilities, software and other technologies that connect to and communicate with other devices and systems over the internet or other networks. Communication.[1][2][3][4][5] The Internet of Things is considered wrong because devices are not allowed to be connected to the public internet, they just need to be connected to a network and a unicast address. The field has evolved through the convergence of multiple technologies, including ubiquitous computing, mass sensors, increasingly powerful embedded systems, and machine learning.[8] The traditional domains of embedded systems, wireless sensor networks, control systems, automation (including home automation and building automation) independently and collectively enable the Internet of Things.[9] In the consumer market, IoT technology is primarily synonymous with smart home products, including devices and devices (such as lights, thermostats, home security systems, cameras, and other household appliances) that support one or more ubiquitous ecosystems and can be controlled by devices that connected to this ecosystem, such as smartphones and smart speakers. IoT is also used in healthcare systems.[10] There are several concerns about the risks associated with the growth of IoT technologies and products, particularly in the countryprivacy and security, and as a result industry and government have taken steps to address these issues, including the development of international and domestic standards, guidelines and regulatory frameworks[11]. History The basic concept of a smart device network was discussed as early as 1982, when a redesigned Coca-Cola machine at Carnegie Mellon University became the first ARPANET-connected device[12] capable of counting its inventory and detecting whether new drinks had been added . reported. whether they were cold or not.[13] Mark Weiser's 1991 essay on ubiquitous computing, “21. century computer' together with academic institutions such as UbiComp and PerCom created the vision of today's IOT.[14][15] In 1994, Reza Raji described the concept in IEEE Spectrum as "[moving] small packets of data to large numbers of nodes to integrate and automate everything from home appliances to entire factories".[16] Between 1993 and 1997, several companies offered solutions such as Microsoft's at Work or Novell's NEST. The field gained momentum when Bill Joy introduced device-to-device communication as part of his "Six Webs" framework presented at the 1999 World Economic Forum in Davos.[17] The concept of the Internet of Things and the term itself first appeared in a speech by Peter T. Lewis before the Congressional Black Caucus Foundation's 15th Annual Legislative Weekend in Washington, D.C. which was published in September 1985.[18] According to Lewis, "The Internet of Things, or IoT, is the integration of people, processes, and technology with connectable devices and sensors that enable the remote monitoring, status, manipulation, and trends of such devices." The term "Internet of Things" was independently coined in 1999 by Kevin Ashton of Procter & Gamble, later the MIT Auto-ID Center[19], although he prefers the term "Internet of Things"[20]. At the time, he believed that radio frequency identification (RFID) was necessary for the Internet of Things[21] to enable this.govern all things.[22][23][24] The main theme of the Internet of Things is the incorporation of short-range mobile transceivers into various devices and everyday objects, which will enable new forms of communication between people and things and between things themselves.[25] In 2004, NetSilicon CEO Cornelius "Pete" Peterson predicted that "the next era of information technology will be dominated by [IoT] devices, and networked devices will increase in popularity and importance over time until they greatly surpass the world's many computers and workstations in use." Peterson believed that medical devices and industrial controls would become the dominant applications of the technology.[26] Cisco Systems defined the Internet of Things as "simply a time when more "things or objects" are connected to the Internet than people, Cisco Systems estimates that the Internet of Things was "born" between 2008 and 2009, with the ratio of things to people increasing from 0 .08 in 2003 to 1.84 in 2010.[27] Applications A large number of Internet of Things applications[28] are often categorized into consumer, commercial, industrial, and infrastructure domains.[29][30] Consumer applications Consumer applications are an increasing number of IoT devices have been developed, including connected devices h vehicles, home automation, wearable technology, connected health, and devices with remote monitoring capabilities.[31] Smart home IoT devices are part of a broader concept of home automation that may include lighting, heating and air conditioning, multimedia and security systems and camera systems.[32][33] Long-term benefits could include energy savings, nto the lighting. and electronics are automatically turned off or the occupants of the home are notified of use.[34] A smart home or automated home can be based on a platform or hubs [35] For example, with Apple HomeKit, manufacturers can control their home products and accessories via an app on iOS devices, e.g.and Apple Watch.[36][37] This can be a dedicated app or a native iOS app such as Siri.[38] This can be demonstrated with Lenovo Smart Home Essentials, a series of smart home devices that are controlled through the Apple Home app or Siri without the need for a Wi-Fi bridge.[38] There are also dedicated smart home hubs that are offered as standalone platforms for connecting various smart home products, including Amazon Echo, Google Home, Apple HomePod and Samsung SmartThings Hub. In addition to commercial systems, there are many non-proprietary open source ecosystems; including Home Assistant, OpenHAB and Domoticz. Elderly care One of the main applications of smart homes is to help the elderly and the disabled. These home systems use assistive technology to accommodate the owner's specific disability. Voice control can assist users with visual and mobility impairments, and public address systems can be connected directly to cochlear implants worn by users with hearing impairments.[43] They can also be equipped with additional safety features, including sensors that monitor for emergencies such as falls or seizures.[44] Smart home technology used in this way can provide users with greater freedom and a higher quality of life.[42] The term "enterprise IoT" refers to devices used in corporate and corporate environments. It is estimated that EIoT will include 9.1 billion devices by 2019.[29] Organizational applications Medicine and healthcare The Internet of Medical Things (IoMT) is an IoT application for medical and medical purposes, data collection and analysis for research and monitoring.[45][46][47][48][49] IoMT has been called "Smart Healthcare" [50] as a technology to create a digital healthcare system by linking available medical resources and healthcare services.[51][52] IoT devices can be used to provide remote health monitoring and emergency response.systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices that can control specialized implants such as B pacemakers, Fitbit electronic bracelets or advanced hearing aids. Some hospitals have started introducing "smart beds" that can detect when they are occupied and when the patient is trying to get up. It can also self-adjust to provide the patient with adequate compression and support without the need for manual intervention by caregivers.[45] A 2015 Goldman Sachs report noted that IoT devices in healthcare "could save the United States more than $300 billion in annual healthcare spending by increasing revenues and reducing costs." In addition, the use of mobile devices to support medical monitoring has led to "mHealth "creation through analysis of health statistics". [55] Special sensors can also be placed in living spaces to monitor the health and general well-being of seniors, while providing appropriate treatment and helping to recover what they have lost. mobility, including through therapy.[56] These sensors form an intelligent sensor network that can collect, process, transmit and analyze valuable information in various environments, including B. connecting home monitoring devices to hospital systems.[50] IoT also enables the use of other consumer devices that promote a healthy lifestyle, such as connected scales or wearable heart rate monitors.[57] IoT platforms for end-to-end healthcare monitoring are also available to prenatal and chronically ill patients to help manage healthcare resources and periodic medication orders.[58] Advances in plastic and fabric electronics manufacturing methods have enabled the use of extremely low-cost, reusable and disposable IoMT sensors. These sensors can be fabricated on paper or e-textiles along with the necessary RFID electronics for disposable wireless sensing devices. Point-of-care applications have been createdDiagnostics where portability and low system complexity are important.[60] As of 2018 [update] IoT is used not only in clinical laboratories[47], but also in healthcare and health insurance. The IoT in healthcare now allows doctors, patients, and others such as healthcare professionals to provide access to patient information.[61] In addition, IoT-based systems are patient-centric, which means they must be flexible to respond to the patient's health status. [link needed] IoMT provides access to better and new types of dynamic information in the insurance industry. This includes sensor solutions such as biosensors, wearable devices, connected medical devices and mobile apps to track customer behavior. This could lead to more accurate underwriting and new pricing models.[62] The use of the Internet of Things in healthcare plays a vital role in the management of chronic diseases, as well as disease prevention and control. Remote monitoring is possible by connecting high-performance radio solutions. Connectivity allows medical professionals to collect patient data and apply sophisticated algorithms in the analysis of medical data.[63] The IoT Digital Speed Limit Transport Sign can help integrate communication, control, and information processing into various transportation systems. IoT applications cover all aspects of transportation systems (e.g. vehicle,[64] infrastructure, and driver or user). The dynamic interaction between these components of the transport system enables communication between and within vehicles[65], intelligent traffic management, intelligent parking, electronic toll collection, logistics and fleet management, vehicle control, safety and roadside assistance[53] . [66] V2X communications Main article: V2X in automotive communicationsVehicle-to-vehicle (V2X) communication consists of three main components: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) communication, and vehicle-to-pedestrian (V2P) communication. V2X is the first step towards autonomous driving and connected road infrastructure. [cit] IoT devices for building and home automation can be used to monitor and control mechanical, electrical and electronic systems used in different types of buildings (e.g. public and private, industrial, institutional or private) [53] in home automation and building automation systems. In this regard, the literature addresses three main areas:[67] Integrating the Internet with building energy management systems to create energy-efficient IOT-enabled “smart buildings”[67]. Possible real-time monitoring means reducing energy consumption[34] and tracking passenger behavior[67]. Integration of smart devices into the built environment and the possibility of their use in the future[67]. Industrial applications Main article: Industrial Internet of Things Industrial Internet of Things, also known as IIoT, collect and analyze data from connected devices, operational technologies (OT), places, and people. Combined with operational technology (OT) monitoring devices, IIoT helps regulate and monitor industrial systems.[68] The same implementation can be done for automated updates of asset location records in industrial storage units, since assets can vary in size from a small screw to an entire engine spare part, and misplacing such assets can lead to loss of manpower. time and money. Manufacturing IoT can connect various manufacturing devices equipped with sensing, identification, processing, communication, control, and networking capabilities.[69] Network and plant management, asset and situation management, or production process management enable the use of IoT for industrial purposesand smart manufacturing.[70] Intelligent IoT systems enable the rapid production and optimization of new products and the rapid response to product requirements.[53] Digital control systems to automate process control, operator tools, and service information systems to optimize equipment safety are within the remit of the IIoT.[71] IoT can also be used in asset management with predictive maintenance, statistical analysis and measurement to increase reliability.[72] Industrial control systems can be integrated into smart grids to optimize energy consumption. Measurements, automated inspections, asset optimization, occupational health and safety management and other functions are performed by networked sensors.[53] In addition to general manufacturing, IoT is also used in the industrialization of construction.[73] Agriculture There are many applications of the IoT in agriculture[74], such as collecting data on temperature, precipitation, humidity, wind speed, pest infestation and soil content. This data can be used to automate farming methods, make informed decisions to improve quality and quantity, reduce risk and waste, and reduce crop management effort. For example, farmers can now remotely monitor soil temperature and moisture and even use IoT data for precision fertilization programs.[75] The overarching goal is that sensor data combined with the farmer's knowledge and intuition about his farm can help increase farm productivity and reduce costs. In August 2018, Toyota Tsusho partnered with Microsoft to develop fish farming tools using the Microsoft Azure suite of applications for water-related IoT technologies. The water pump mechanisms, developed in part by researchers at Kindai University, use artificial intelligence to count fish on the conveyor, analyze the number of fish, and infer water flow efficiency based on the data provided by the fish.Microsoft Research, which uses whitespace TV to connect farms, is now part of the Azure Marketplace.[78] Maritime IoT devices are used to monitor the environment and systems of boats and yachts[79]. Many recreational boats are left unattended for days in summer and months in winter, so these devices provide valuable early warnings of boat flooding, fire and deep battery discharge. The use of global online data networks such as Sigfox, combined with long life batteries and microelectronics, provides continuous monitoring of the engine room, bilge and batteries, as well as reporting to connected Android and Apple applications. Infrastructure Applications Monitoring and managing sustainable urban and rural infrastructure such as bridges, railways, onshore and offshore wind farms is one of the main applications of the Internet of Things[71]. The IoT infrastructure can be used to track any events or changes in structural conditions that could compromise security and increase risk. The Internet of Things has the potential to benefit the construction industry through cost savings, time savings, improved workday quality, paperless workflow, and increased productivity. It can help you make faster decisions and save money through real-time data analysis. It can also be used to efficiently plan repair and maintenance activities by coordinating tasks between different service providers and users of these facilities.[53] IoT devices can also be used to control critical infrastructure such as bridges to provide access to ships. The use of IoT devices to monitor and operate infrastructure is likely to improve incident management and crisis response coordination, as well as service quality, availability, and lower operating costs in all areas related to infrastructure[80]. Even areas such as waste management can benefit[81] from the automation and optimization that IoT can bring.internet of things enabling better management of cities and systems. For example, Songdo in South Korea, the first fully equipped and wired smart city of its kind, is gradually being built, with about 70 percent of the business district completed as of June 2018 [update]. Much of the city is planned to be wired and automated with little or no human intervention. Another application is currently under development in Santander, Spain. Two approaches were used for this implementation. The city of 180,000 has already seen 18,000 downloads of the city's smartphone app. The app is connected to 10,000 sensors that provide services like finding parking spaces, environmental monitoring, city digital program and more. This deployment leverages city context information for the benefit of marketers with a sparkling city behavior based trading engine designed to maximize the impact of each announcement. Other examples of large-scale implementation underway include the China-Singapore Knowledge City in Guangzhou[84]; work to improve air and water quality, reduce noise pollution and increase traffic efficiency in San Jose, California[85] and intelligent traffic management in western Singapore. Using its Random Phase Multiple Access (RPMA) technology, San Diego-based Ingenu has created a nationwide public network[87] for low-bandwidth data transmission using the same unlicensed 2.4 GHz band as Wi-Fi. Ingenu's "car network" covers more than a third of the US population in 35 major cities, including San Diego and Dallas.[88] French company Sigfox began building an ultra-narrowband wireless data network in the San Francisco Bay Area in 2014, the first company to achieve such deployment in the US. It then announced that it will deploy a total of 4,000 base stations covering a total of 30 US cities by the end of 2016, making it the largest IoT network coverage provider in the country to date. Ciscoparticipates in smart city projects. Cisco begins deploying Smart Wi-Fi, Smart Safety & Security, Smart Lighting, Smart Parking, Smart Transport, Smart Bus Stops, Smart Kiosk, Remote Expert for Government Services (REGS) and Smart Education Technologies in a five-kilometer zone in Vijaywada, India. [93] Another example of a major deployment is New York Waterways in New York to connect all ships in the city and provide 24/7 surveillance. The network was designed and developed by Fluidmesh Networks, a Chicago-based company that develops wireless networks for mission-critical applications. The NYWW network currently covers the Hudson, East River, and Upper New York Bay. Thanks to the wireless network, NY Waterway can control its fleet and passengers in a way that was not possible before. New applications may include security, energy and fleet management, digital signage, public Wi-Fi, paperless ticketing, and more.[94] Energy management A significant number of energy consuming devices (e.g. lighting, household appliances, motors, pumps, etc.) are already integrated with the Internet, so that they can not only communicate with energy suppliers to balance electricity production, but also help in balancing energy consumption to optimize if necessary. general[53] These devices offer remote user management or centralized management via a cloud interface, and include functions such as scheduling (e.g. remotely switching heating systems on and off, controlling furnaces, changing lighting conditions, etc.)[53]. Smart Grid is a tool-side IoT application; Systems collect and process information related to energy and power in order to improve the efficiency of energy generation and distribution.[95] Using Internet-connected AMI (Advanced Metering Infrastructure) devices, utilities not only collect data from end users, but also manage distribution automation devices such as transformers.[53] environmentIoT environmental monitoring applications typically use sensors that help protect the environment[96] by monitoring air or water quality[97], weather or soil conditions[98] and even include areas such as monitoring the movement of wildlife and their habitats be able. [99] The development of the limited resources of Internet-connected devices also means that other applications, such as B. earthquake or tsunami early warning systems, can also be used by rescue services to provide more effective help. The IoT devices in this application typically cover a large geographic area and can also be mobile.[53] It has been argued that the standardization that IoT will bring to wireless sensing will revolutionize the field.[100] Living Lab Another example of IoT integration is the Living Lab, which integrates and connects research and innovation processes and creates partnerships between the public and private sectors.[101] There are currently 320 Living Labs using the IoT to collaborate and share knowledge between stakeholders to jointly develop innovative and technological products. Enterprises should be encouraged to implement and develop IoT services for smart cities. Governments play a key role in smart city projects as policy changes will help cities adopt IoT that ensures resource efficiency, effectiveness and accuracy. For example, the government offers tax incentives and low rents, improves public transport and provides an environment where start-ups, creative industries and multinationals can create together, share common infrastructure and labor markets and take advantage of local technology. Production processes and transaction costs.[101] The relationship between technology developers and governments that manage city assets is key to successfully providing users with open access to resources. Military applications Main article: Internet of Military Things Internet of Military Thingsis a military application of IoT technologies for intelligence, surveillance, and other combat-related purposes. It is heavily influenced by the future prospects of urban warfare and includes the use of sensors, munitions, vehicles, robots, wearable biometrics and other smart technologies relevant to the battlefield.[102] Internet of Things on the Battlefield The Internet of Things on the Battlefield (IoBT) is a project initiated and led by the US Army Research Laboratory (ARL) that focuses on the fundamental sciences of the Internet of Things that enable the military. [103] In 2017, ARL established the Internet of Battlefield Things Collaborative Research Alliance (IoBT-CRA), a working partnership between industry, universities, and military scientists to advance the theoretical foundations of IoT technologies and their application to military operations.[104]]]][105] Ocean of Things Project Ocean of Things is a DARPA-led program to build the Internet of Things in large oceans to collect, monitor and analyze environmental and ship activity data. The project involves the deployment of approximately 50,000 floats containing a suite of passive sensors that autonomously detect and track military and commercial vessels in a cloud network.[106] Product Digitization There are several applications for smart or active packaging where a QR code or NFC tag is placed on the product or its packaging. The tag itself is passive, but contains a unique identifier (usually a URL) that allows the user to access digital content about the product via a smartphone.[107] Strictly speaking, such passive elements are not part of the IoT, but can be seen as a way to enable digital interaction.[108] The term "Internet of Packaging" was coined to describe applications that use unique identifiers to automate supply chains andwidely used by consumers to access digital content[109]. Authentication of unique identifiers, and thus of the product itself, is possible with a copy-sensitive digital watermark or a copy identification pattern that can be scanned by scanning a QR code[110], while NFC tags can encrypt communications[111]. Trends and Characteristics The most significant IoT trend in recent years is the explosive growth of Internet-connected and controllable devices.[112] The wide range of applications of IoT technologies means that the specifics can vary greatly from device to device, but there are basic characteristics that are common to most. The Internet of Things creates opportunities for more direct integration of the physical world with computer systems, resulting in increased efficiency, economic benefits, and reduced human effort. The number of IoT devices grew by 31% year-over-year to 8.4 billion in 2017[117]. and an estimated 30 billion by 2020.[112] Intelligence Ambient intelligence and autonomous control are not part of the original IoT concept. Ambient intelligence and autonomous control also do not require web frameworks. However, there has been a shift in research (from companies such as Intel) to integrate the concepts of IoT and autonomous control, with early results in this direction seeing objects as the driving force behind autonomous IoT.[118] A promising approach in this regard is deep reinforcement, for which most IoT systems provide a dynamic and interactive environment[119]. Traditional machine learning algorithms such as supervised learning cannot train an agent (i.e. an IoT device) to behave intelligently in such an environment. Through reinforcement learning, a learning agent can sense the state of the environment (such as the temperature in the house), perform actions (such as turning heating, ventilation, and air conditioning on or off), and learn by maximizingthe rewards he receives in the long run. IoT intelligence can be offered at three levels: IoT devices, edge/fog nodes, and cloud computing.[120] The need for intelligent control and decision making at each level depends on the time sensitivity of the IoT application. For example, a camera in an autonomous vehicle must perform real-time obstacle detection to avoid an accident. This rapid decision-making would not be possible by transmitting data from the vehicle to cloud instances and sending predictions back to the vehicle. Instead, all operations must be performed locally in the vehicle. Integrating advanced machine learning algorithms, including deep learning, into IoT devices is an active research area to bring smart objects closer to reality. Additionally, it is possible to get the most out of IoT deployments by analyzing IoT data, extracting hidden information and predicting control decisions. A wide variety of machine learning techniques have been used in the IoT space, from traditional methods such as regression, support vector machines, and random forests to advanced techniques such as convolutional neural networks, LSTMs, and variational autoencoders.[121][120] In the future, the Internet of Things may be a non-deterministic and open network in which automatically organized or intelligent entities (web services, SOA components) and virtual objects (avatars) will be interoperable and able to act independently (own the chase). Goals or common goals) depending on the context, circumstances or environment. Autonomous behavior through the collection and reasoning of contextual information, as well as the ability of an object to detect environmental changes (damage affecting sensors) and take appropriate mitigation measures, is an important research trend[122] that is clearly needed to ensure the reliability of IoT technology. . . Today's IoT products and solutions on the market use different technologies to support such contextual automation, but moreForms of intelligence are required for sensor units and intelligent cyber-physical systems to be used in real-world settings. Architecture This section requires the attention of a technology expert. A particular problem is that the information is partly out of date, unclear and not quoted. He asks for more details, but not so technical that others don't understand. WikiProject technology can help you hire an expert. (July 2018) The simplified architecture of the IoT system consists of three tiers: Tier 1: Devices, Tier 2: Edge Gateway, and Tier 3: Cloud.[124] Devices include network elements such as sensors and actuators used in IoT hardware, particularly those that use protocols such as Modbus, Bluetooth, Zigbee, or proprietary protocols to connect to the Edge Gateway.[124] The Edge Gateway layer consists of sensor data collection systems called Edge Gateway, which provide features such as data pre-processing, cloud connection security, the use of systems such as WebSockets, an event hub, and in some cases even edge analytics. or fog calculations. The edge gateway layer is also needed to provide an overview of devices in higher layers for ease of management. The last tier is a cloud application built for IoT using a microservices architecture, typically multilingual and inherently secure over HTTPS/OAuth. This includes various database systems that store sensor data, such as time-series databases or function repositories using back-end storage systems (e.g. Cassandra, PostgreSQL). The cloud tier in most cloud IoT systems includes event queues and a messaging system that handles communication between all tiers.[125] Some experts have classified the three layers of the IoT system as edge, platform and enterprise, which are connected by proximity network, access network and service network, respectively.[126] Creation of the Internet of Things, the network of thingsan IoT application layer architecture that focuses on integrating data from IoT devices into web applications to create innovative use cases. For programming and information flow management in the Internet of Things, an architecture direction called BPM Everywhere is expected, which is a combination of traditional process management with intelligent process analysis and special capabilities to automate the management of a large number of coordinated devices. . [citation needed] The network architecture of the Internet of Things requires enormous scalability in the network domain to cope with the onslaught of devices.[127] IETF 6LoWPAN can be used to connect devices to IP networks. With the emergence of billions of devices[128] in the internet space, IPv6 will play an important role in managing the scalability of the network layer. The IETF Restricted Application Protocol, ZeroMQ and MQTT can enable simplified data transmission. In practice, many groups of IoT devices are hidden behind gateway nodes and may not have unique addresses. Additionally, most applications don't need to see everything that's connected because the data must first be connected at a higher level. Fog computing is a viable alternative to prevent such a large increase in traffic over the Internet.[129] The computing power of peripheral devices for data analysis and processing is extremely limited. Limited processing power is a key feature of IoT devices as their goal is to provide data about physical objects while remaining autonomous. High processing demands consume more battery power, which reduces the ability of the IoT to work. Scalability is easy as IoT devices simply deliver data over the Internet to a server with sufficient processing power.[130] Decentralized Internet of Things Decentralized Internet of Things or Decentralized Internet of Things is a modified Internet of Things. It uses fog computing to process and balance the requests of connected IoT devices to reduce cloud server load and improve responsivenessIoT applications such as patient vital sign monitoring, vehicle-to-vehicle communication during autonomous driving, and critical fault detection in industrial equipment.[131] Conventional IoT is connected via a mesh network and controlled by a central master node (centralized controller).[132] The root node decides how data is created, stored, and transmitted.[133] In contrast, decentralized IoT attempts to divide IoT systems into smaller divisions.[134] The root node grants subnodes partial decision-making rights according to a mutually agreed upon policy. Improved performance, especially for large IoT systems with millions of nodes.[136] Decentralized IoT attempts to solve the problem of limited bandwidth and the combination of battery-powered or wireless IoT devices with a lightweight

blockchain.[137][138][139] Detection of cyber attacks can be achieved through early detection and mitigation of edge nodes through traffic monitoring and estimation[140]. Complexity In semi-open or closed loops (i.e., and its ability to integrate new actors. At the general stage (fully open loop), it is likely to be perceived as a chaotic environment (since systems always have finiteness). From a practical point of view, not all elements of the IoT operate in a global public space. Subsystems are often implemented to mitigate privacy, control, and reliability risks. For example, home robots (home appliances) operating in a smart home can only communicate internally and be accessed via a local area network[142]] Highly Dynamic Network of Things/ management and control of special IoT devices is a difficult task with traditional network architecture.Software Defined Network (SDN) provides a flexible dynamic solution capable of meeting special diversification requirements.innovative IoT.Size Considerations The exact scope of the IoT is unknown, and early IoT articles often quote billions or trillions. In 2015, there were 83 million smart devices in homes. This number is expected to increase to 193 million devices by 2020.[33][145] Between 2016 and 2017, the number of devices connected to the internet increased by 31% to 8.4 billion[117]. Spatial Considerations In the IoT, the precise geographic location of things, as well as the precise geographic dimensions of things, can be critical.[146] Therefore, it was less important to include facts about the item, such as its position in time and space, since the information processor could decide whether that information was important to the action to be taken, and if so, add (or not decide) the missing information. take action). (Note that some things in the IoT will be sensors, and sensor location is usually important. [147]) GeoWeb and Digital Earth are promising applications that become possible when things can be organized and connected by location. However, remaining challenges include the limitations of different spatial scales, the need to process massive amounts of data, and indexing for fast searches and neighbor operations. In the Internet of Things, this human-centered intermediary role disappears when things can act on their own initiative. Therefore, the spatio-temporal connection that we humans take for granted must play a central role in this information ecosystem. Just as standards play a key role in the Internet and the Internet, geo-standards will play a key role in the Internet of Things.[148][149] Remote Cart Solution Many IoT devices have the potential to participate in this market. Jean-Louis Gasset (Apple's first alumni team and co-founder of BeOS) touched on this issue in a Monday note [150], predicting that the most likely problem will be thereis called the "remote cart" problem, where we will have hundreds of applications to connect to hundreds of devices that do not have common protocols to communicate with each other. To improve the user experience, some technology leaders are joining forces to create device-to-device communication standards to address this issue. Others focus on the concept of predictive device interaction, "where collected data is used to predict and trigger actions on specific devices", allowing them to work together. Social Internet of Things The Social Internet of Things (SIoT) is a new type of Internet of Things that focuses on the importance of social interactions and relationships between IoT devices.[152] SIoT is an example of how cross-domain IoT devices allow applications to interact and collaborate without human intervention to serve their owners with autonomous services,[153] and this can only be realized when both IoT technologies provide low-level architectural support. software and hardware engineering. Social network of IoT devices (not people) The IoT identifies a device with the identity of a community citizen and connects it to the Internet to provide services to users.[155] SIoT defines a social network for IoT devices to interact with each other for various purposes that serve people. How is SIoT different from IoT? SIoT differs from the original IoT in terms of collaboration. IoT is passive, it was created for specific purposes with existing IoT devices in a predefined system. SIoT is active, programmed and managed by artificial intelligence to fulfill unintended purposes by combining potential IoT devices from different systems for the benefit of its users.[157] How does SIOT work? IoT devices built for communication will broadcast their capabilities or functionality when discovering, navigating, and grouping other IoT devices on the same or nearby network for a useful set of services.actively helping its users in everyday life, especially in emergency situations. Examples of the Social Internet of Things Smart home technology based on the Internet of Things monitors the health of patients or the elderly, analyzes their physiological parameters, and in the event of a medical emergency informs nearby medical facilities.[159] In an emergency, an ambulance will be automatically called from the nearest available hospital with a collection point designated by the ward, the patient's medical data will be transferred to the ER and immediately displayed on the doctor's computer for further action [160] IoT sensors on vehicles, roads and traffic lights monitor the status vehicles and drivers, and warn when attention is required, and automatically coordinate their actions to ensure the normal functioning of autonomous driving. Unfortunately, in the event of an accident, the IoT camera will report help to the nearest hospital and police station.[161] Societal challenges of the Internet of Things The Internet of Things is multifaceted and complex.[162] One of the main factors preventing people from adopting and using Internet of Things (IoT) products and services is their complexity.[163] Installation and configuration is a complex human task, so IoT devices must adapt and automatically configure themselves to provide different services in different situations.[164] System security is always a concern of any technology and this is more important for SIoT as it is necessary from time to time to consider not only one's own security but also a mutual trust mechanism between cooperating IoT devices in different locations. [154] Another important issue for SIoT is sensor accuracy and reliability. In most cases, IoT sensors will need to respond within nanoseconds to prevent accidents, injury and loss of life.[154] Implementing technologies for the Internet of Things There are many technologies that enable the use of the Internet of Things. The network used for communication between IoT devices is crucial in this area.a role that several wireless or wired technologies can fulfill: [165][166][167] Targeting The original idea of Auto-ID-Center is based on RFID tags and unique identification using an electronic product code. This has evolved into objects that have an IP address or URI.[168] Instead, an alternative view from the world of the Semantic Web[169] focuses on all (not just electronic, smart, or RFID-enabled) addressing using existing naming protocols such as URIs. The objects themselves do not speak, but other agents can now speak to them, such as powerful centralized servers that act on behalf of their human owners.[170] Internet integration means that devices use the IP address as a unique identifier. Because IPv4 has a limited address space (4.3 billion different addresses allowed), IoT entities must use the next generation Internet Protocol (IPv6) to scale to the extremely large address space required. 172][173] IoT devices also benefit from stateless address autoconfiguration in IPv6[174] as it reduces host configuration effort[172] and IETF 6LoWPAN header compression. The future of the Internet of Things will be largely impossible without IPv6 support; and thus the worldwide adoption of IPv6 in the coming years will be critical to the successful development of IoT in the future[173]. Application layer ADRC[175] defines the application layer protocol and support framework for implementing IoT applications. Bluetooth Short Range Wireless Mesh is a specification that integrates a Bluetooth Low Energy (BLE) mesh network with an increased number of nodes and a standardized application layer (models). Light fidelity (Li-Fi) is a wireless technology similar to the Wi-Fi standard, but uses visible light to increase throughput. Near field communicationCommunication protocols that allow two electronic devices to communicate within a radius of 4 cm. Radio Frequency Identification (RFID) • Technology that uses electromagnetic fields to read data stored on tags embedded in other objects. Wi-Fi - A LAN technology based on the IEEE 802.11 standard that allows devices to communicate through a common access point or directly between devices. ZigBee - IEEE 802.15.4-based personal network communication protocols that offer low power consumption, low data rate, low cost, and high throughput. Z-Wave – A wireless communication protocol primarily used in home automation and security applications Medium Wireless Range LTE-Advanced – A specification for high-speed communications in cellular networks. It offers improvements to the LTE standard with extended coverage, higher throughput and lower latency. 5G – 5G wireless networks can be used to meet the high communication needs of IoT and connect large numbers of IoT devices on the go.[176] 5G has three features, each considered useful for supporting specific elements of the Internet of Things: enhanced mobile broadband (eMBB), massive machine-type communications (mMTC), and ultra-reliable low-latency communications (URLLC).[177] Long Range Wireless Networks Low Power Wide Area Networks (LPWAN) • Wireless networks designed to enable communication over long distances at low data rates, reducing power consumption and transmission costs. Available LPWAN technologies and protocols: LoRaWan, Sigfox, NB-IoT, Weightless, RPMA. Very Small Aperture Terminal (VSAT) • Satellite communications technology that uses small parabolic antennas to transmit narrowband and broadband data. Wired Ethernet A universal networking standard that uses twisted pair cables and fiber optic connections in conjunction with hubs or switches. Power Line Communications (PLC) ■ A communications technology that transmits power and data over electrical wires. Such specificationsHomePlug or G.hn uses a PLC to connect IoT devices to the network. Standards and Standards Organizations This is a list of technical standards for the Internet of Things, most of which are open standards, and the standards organizations that are committed to their successful implementation. Short name Full name Development standards Other notes Auto-ID Good Auto-ID center RFID (radio frequency identification) network and new sensor technologies Connected home via IP Project Connected Home via IP Open Connected Home via IP (or Connected Home via IP project) -source , a free standard home automation connectivity project that provides interoperability between various smart home and Internet of Things (IoT) products and software [181]. The project is backed by large companies and, based on proven Internet design principles and protocols, aims to unify the currently fragmented systems.[182] EPCGlobal Electronic Product Code Technology EPC (Electronic Product Code) FDA Technology Implementation Standards US Food and Drug Administration UDI (Unique Device Identification System) Unique Medical Device Identifier System GS1 Global Standards Uniform UID (“Unique” Identifiers) and RFID Express Commodity Standards (Consumer goods), health goods and more The GS1 digital communications standard, first introduced in August 2018, enables the use of QR codes, GS1 Datamatrix, RFID and NFC to enable various types of interactions between businesses as well as between businesses. and consumers. The parent organization includes member organizations such as GS1 US IEEE Institute of Electrical and Electronics Engineers Core Standards Communication technology standards such as IEEE 802.15.4, IEEE P1451-99[184] (IoT Harmonization) and IEEE P1931.1 (ROOF Computing). IETF Working Group on Internet Designincluding TCP/IP (Internet Protocol Suite) MTConnect Institute – MTConnect is the industry standard for communicating with machine tools and associated industrial equipment. This is important for the IIoT subset of IoT. O-DF Open Data Format O-DF is a standard published in 2014 by the Open Group's Internet of Things Working Group that defines the general structure of the information model used to describe all "things" and to publish, update, and search for information is used - when used with O-MI (Open Messaging Interface). O-MI Open Messaging Interface O-MI is a standard published in 2014 by the Internet of Things Open Group that defines a limited set of key operations required in IoT systems, specifically different types of subscription mechanisms based on the Observer -Pattern based. . OCF Open Connectivity Foundation standards for simple devices using CoAP (Restricted Application Protocol) OCF (Open Connectivity Foundation) replaces OIC (Open Interconnect Consortium) OMA Open Mobile Alliance OMA DM and OMA LWM2M for IoT device management and GotAPI which is a secure framework for XSF provides IoT applications XMPP Standards Foundation Protocol extensions for XMPP (Extensible Messaging and Presence Protocol), an open standard for instant messaging W3C World Wide Web Consortium standards for interoperability between different protocols and IoT platforms such as Thing Description, Discovery, Scripting API and architecture explaining how they work together. W3C Web of Things website at Politics and Civic Engagement Some scholars and activists argue that the IoT could be used to create new models of civic engagement when device networks are used for user control and interoperable platforms are open. Professor and author Philip N. Howard writes that how the IoT works determines political life in both democratic and authoritarian regimesuse for civic engagement. To do so, they argue that any connected device should be able to reveal a list of "ultimate recipients" of its sensor data, and that individual citizens should be able to add new organizations to the list of recipients. Furthermore, they argue that civil society groups need to start developing IoT strategies to harness data and engage the public.[185] IoT government regulation One of the most important drivers of IoT is data. The success of the idea of connecting devices to increase their efficiency depends on the access, storage and processing of data. To this end, IoT companies 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 breaches and single vulnerabilities in many systems.[186] Other issues relate to consumer choices and data ownership[187] and how data is used. While still in its infancy, regulation and governance related to privacy, security and data ownership issues are evolving.[188][189][190] IoT regulation varies by country. Some examples of rights related to privacy and data collection are the US Privacy Act of 1974, the OECD Directive on the Protection of Privacy and Cross-Border Data Flows of 1980, and EU Directive 95/46/EC of 1995[191]. Current regulatory environment: A report published by the Federal Trade Commission (FTC) in January 2015 makes the following three recommendations: be safe at all times. Organizations should adopt a “defense in depth” approach and encrypt data at every stage.[193] Data Consent – Users should be able to choose what data they share with IoT companies, and users must be informed when their data is disclosed. Data minimization - IoT companiescollect only the data they need and only store the collected information for a limited period of time. However, the FTC has stopped issuing recommendations for now. According to the FTC's analysis, existing legislation, which consists of the FTC Act, the Fair Credit Reporting Act, and the Children's Online Privacy Act, as well as the development of consumer education and business consulting, participation in multi-stakeholder efforts, and advocacy for other federal states. , state and local government agencies are sufficient to protect consumers' rights.[194] The resolution adopted by the Senate in March 2015 is already under consideration in Congress.[195] This resolution recognized the need for a national policy on IoT and privacy, security and spectrum issues. To give the IoT ecosystem a boost, two out of four senators proposed the Internet of Things Innovation and Growth (DIGIT) Act in March 2016 to direct the Federal Spectrum Commission to connect IoT devices. . California Senate Act No. 327 [196], approved September 28, 2018, effective January 1, 2020. Measures appropriate to the nature and function of the device, appropriate to the information it collects, may contain or transmit, and designed to protect the device and all contained information from unauthorized access, destruction, use, modification or disclosure: “In fact, the IoT industry is defined by several car standards, as the biggest concerns about connected cars also relate to medical devices. In fact, the National Highway Traffic Safety Administration (NHTSA) is preparing cybersecurity guidelines and a database of best practices to make computer systems in motor vehicles safer. [197] AA World Bank report examines the challenges and opportunities associated with IoT adoption in government[198]. These include “IoT in government is still in its infancy” Underdeveloped policy and regulatory framework. Unclear business models despite a strong value proposition. A clear institutional and capacity gap in government AND the private sector The most successful pilots have common features (PPP, local, management) In early December 2021, the UK government introduced the Product Safety and Telecommunications Infrastructure (PST) Act, which is expected to be launched. comes into effect IoT Distributors, manufacturers and importers must meet certain requirements. Cyber security standards. The bill also aims to improve the security features of consumer IoT devices.[199] Criticisms, Issues and Controversies Platform Fragmentation The Internet of Things suffers from platform fragmentation, interoperability, and a lack of common technical standards[200][201][202][203][204][205][206][excessive references], The situation where IoT the diversity of devices, both in terms of hardware variations and differences in the software running on them, complicates the task of developing applications that work consistently across a variety of inconsistent technology ecosystems.[1] For example, wireless connectivity for IoT devices can be via Bluetooth, Zigbee, Z-Wave, LoRa, NB-IoT, Cat M1, as well as fully custom proprietary radios – each with their own advantages and disadvantages; and a unique support ecosystem.[207] The amorphous nature of IoT computing is also a security concern, as patches for bugs found in the operating system kernel often fail to reach users of older and cheaper devices.[208][209][210] The research group claims that more than 87% of active Android devices are vulnerable because vendors fail to support older devices with patches and updates.[211][212] privacy,and Control Professor and author Philip N. Howard writes that the Internet of Things offers tremendous potential for empowering citizens, improving government transparency and expanding access to information. However, Howard warns that the threat to privacy is enormous, as is the potential for social control and political manipulation.[213] Privacy concerns have led many to believe that big data infrastructures such as the Internet of Things and data mining are inherently incompatible with privacy.[214] The main challenges related to increasing digitization in the water, transport or energy sector are related to data protection and cybersecurity, which require an appropriate response from research and policy makers[215]. Author Adam Greenfield argues that IoT technologies are not only an invasion of public space, but are also being used to perpetuate normative behavior, citing a case where billboards with hidden cameras tracked the demographics of passers-by who stopped, to read an ad. The Internet of Things Council compared the IoT's proliferation of digital surveillance to the conceptual panopticon described by Jeremy Bentham in the 18th century.[216] The claim was defended by the works of French philosophers Michel Foucault and Gilles Deleuze. In Discipline and Punish: The Birth of the Prison, Foucault argues that the panopticon was central to the disciplinary society that developed during the Industrial Age.[217] Foucault also argued that the disciplinary systems established in factories and schools reflected Bentham's panoptic vision.[217] In his 1992 article Postscripts on the Societies of Control, Deleuze wrote that the society of discipline has become the society of control, with the computer replacing the panopticon as the tool of discipline and control, while retaining panopticon-like properties. [218] Peter Paul Verbeek, Professor of Philosophy of TechnologyThe University of Twente in the Netherlands writes that technology is already affecting moral decision-making, which in turn affects human agency, privacy and autonomy. He warns against seeing technology only as a human tool, and instead advocates seeing it as an active agent. Justin Brookman of the Center for Democracy and Technology expressed concern about the impact of the IoT on consumer privacy, saying, "There are people in commerce who are like, 'Oh, big data...okay, let's collect it all, let's keep it it.' forever, we're paying for someone to think about security later. The question is whether we want to create a political framework to contain it. [220] Tim O'Reilly believes there is a flaw in the way companies are marketing IoT devices to consumers and challenges the notion that IoT is about increasing efficiency by using all kinds of devices are brought online, and posits that "IoT is really a human enhancement other than when you have sensors and data to make decisions." WIRED editors also expressed concern, saying, "What you're going to lose is your privacy . It's actually worse. Not only are you losing your privacy, but you are also seeing the concept of privacy being rewritten right under your nose. “[222] The American Civil Liberties Union (ACLU) has expressed concern about the potential of the IoT to weaken people's control over their lives. The ACLU wrote: "It is simply impossible to predict how this enormous power, accumulating disproportionately in the hands of corporations seeking financial gain and governments seeking ever greater control, will be harnessed. The opportunity is Big Data and the Internet of Things will make it harder for us to manage our own control over life as we become more transparent to powerful corporations and government institutions that are increasingly hidden from us.[223] In response to growing concernsPrivacy and smart technology In 2007, the UK government announced that it would adhere to formal privacy principles when implementing a smart metering scheme. The program will replace traditional electricity meters with intelligent electricity meters that can track and control energy consumption more accurately.[224] However, the British Computer Society doubts that these principles have ever been implemented.[225] In 2009, the Dutch parliament rejected a similar smart metering scheme, citing privacy concerns. The Dutch program was later revised and adopted in 2011.[225] Data storage The challenge for IoT application providers is to clean, process and interpret the vast amount of data collected by sensors. A solution called wireless sensor networks[226] has been proposed for information analysis. These networks exchange data between sensor nodes, which are sent to a distributed system to analyze the sensor data.[227] Another problem is storing such a large amount of data. Depending on the application, the data acquisition requirements can be high, which in turn leads to high storage requirements. Currently, the internet already accounts for 5% of all energy generation[226] and remains the “difficult task” of powering IoT devices to collect and even store data[228]. Although data warehouses are a common problem for legacy systems, they are still a common problem in the adoption of IoT devices, especially in manufacturing. While IoT and IIoT devices can bring many benefits, storage media can present significant challenges without considering the principles of autonomy, transparency, and interoperability.[229] The problems don't come from the device itself, but from the assets where the databases are the storage. These issues have typically been identified in manufacturing and in companies that have started and are participating in digital transformation.To get the most out of IoT devices and decision making, organizations must first overhaul their data storage methods. These challenges were identified by Keller (2021) in his study on the IT and application environment of I4.0 implementation at German M&E manufacturers. [229] Security Security is a major concern in the adoption of IoT technology[230] and there are concerns that rapid evolution is occurring without due consideration of the pervasive security challenges[231] and potential regulatory changes[232] involved . [233] Most technical security problems are similar to ordinary servers, workstations and smartphones.[234] These concerns include using weak authentication, forgetting to change default credentials, unencrypted messages sent between devices, SQL injection, man-to-man attacks, and poor handling of security updates.[235][236] However, many IoT devices have severe operating limitations in terms of the computing power available to them. Because of these limitations, they often cannot directly apply basic security measures such as implementing firewalls or using strong cryptography to encrypt communications with other devices,[237] and the low cost and consumer focus of many devices make a system of strong security patches uncommon. [237] 238] Instead of traditional vulnerabilities, bug injection attacks targeting IoT devices are on the rise. A bug injection attack is a physical attack on a device to intentionally inject bugs into a system to change its intended behavior. Random errors can occur due to ambient noise and electromagnetic fields. There are ideas derived from Control Flow Integrity (CFI) to prevent error injection attacks and restore the system to a healthy state before failure.[239] IoT devices also have access to new data areas and can often control physical data areasEven in 2014, many internet-connected devices could already be said to be "spying on people in their own homes", including televisions, kitchen appliances,[241] cameras and thermostats.[242] Computer-controlled devices in vehicles such as brakes, engine, locks, hood and trunk opening, horn, heater and dashboard have been shown to be vulnerable to intruders with access to the vehicle's electrical system. In some cases, car computer systems are connected to the Internet so they can be used remotely.[243] By 2008, security researchers had demonstrated the ability to remotely control pacemakers without authorization. Later, hackers demonstrated remote control of insulin pumps[244] and implantable cardioverter defibrillators[245]. Even poorly secured IoT devices that can be accessed over the Internet can be hacked and attack others. In 2016, a distributed denial-of-service attack using IoT devices with the Mirai malware disabled DNS providers and major websites.[246] The Mirai botnet infected approximately 65,000 IoT devices in the first 20 hours.[247] Eventually, the number of infections rose to around 200,000–300,000 cases.[247] Brazil, Colombia and Vietnam accounted for 41.5% of infections.[247] The Mirai botnet targeted specific IoT devices, including DVRs, IP cameras, routers, and printers.[247] Dahua, Huawei, ZTE, Cisco, ZyXEL and MikroTik were identified as the top manufacturers with the most infected devices.[247] In May 2017, Junad Ali, a computer scientist at Cloudflare, noted that IoT devices have inherent DDoS vulnerabilities due to poor implementation of the publish-subscribe pattern.[248][249] These types of attacks have led security professionals to view the IoT as a real threat to Internet services.[250] The U.S. National Intelligence Council said in an unclassified report that it would be difficult to "deny enemies of the United States, criminals and others access to networks of sensors and remotely controlled objects."Creators... An open marketplace for aggregated sensor data can serve commercial and security interests as well as help criminals and spies identify vulnerable targets. Thus, massively parallel fusion of sensors could undermine social cohesion if found to fundamentally violate the Fourth Amendment's guarantees against unreasonable searches.”[251] In general, the intelligence community views the Internet of Things as a rich source of data252.] On January 31, 2019, The Washington Post wrote an article about the security and ethical issues that can arise with doorbells and IoT cameras: “Last month, Ring was caught allowing its team in Ukraine to view and comment on certain user videos; the company says it only reviews public videos and videos from ring owners who give consent. Last week, a California family's Nest camera allowed a hacker to take control and broadcast audio alerts of fake missile attacks, not to mention the same information, when they used a weak password.” [253] There have been mixed responses to security concerns. The Internet of Things Security Foundation (IoTSF) was founded on September 23, 2015 with the mission of securing the Internet of Things by spreading knowledge and best practices. Its founding boards are made up of technology providers and telecommunications companies. In addition, major IT companies are constantly developing innovative solutions to secure IoT devices. In 2017, Mozilla launched Project Things, which allows IoT devices to be routed through a secure Web of Things gateway[254]. the security market[256] will grow by 27% between 2016 and 2022, up 0.9% due to growing infrastructure challenges and diversified IoT usage.[257][258] Government Some argue that domestic regulation is necessary to protect IoT devices and the wider Internet, as market incentives are insufficient to protect IoT devices.[259][232][233] Was found.due to the nature of most IoT development boards, they generate predictable and weak keys that make them easy to use in a man-in-the-middle attack. However, many researchers have proposed various hardening approaches to solve the problem of poor SSH implementation and weak keys.[260] IoT security in manufacturing presents a number of challenges and perspectives. In the EU and Germany, data protection is constantly mentioned in industrial and digital policies, especially in I4.0. However, there is a different approach to data security from a business perspective, which focuses on less data protection in the form of GDPR, as data collected from IoT devices in the manufacturing sector does not reflect personal data.[229] However, the research showed that manufacturing professionals are concerned about "data security to protect machine technology from international competitors with an ever-increasing desire for interoperability". IoT security systems are typically controlled by intelligent, event-driven applications that take as input data from sensors, user data, or other external triggers (from the Internet) and control one or more actuators to provide various forms of automation. Examples of sensors include smoke detectors, motion detectors, and contact sensors. Examples of actors include smart locks, smart sockets and door controls. Popular control platforms where third-party developers can create smart applications that communicate wirelessly with these sensors and actuators include Samsung SmartThings[262], Apple HomeKit[263], and Amazon Alexa[264]. A specific problem with IoT systems is that faulty applications, unexpected bad application interactions, or device/communication failures can lead to unsafe and dangerous physical conditions such as "opening the front door when no one is home" or "turning off the heat". when the temperature drops below 0 degrees Celsius and peopleat night."[261] Discovering the flaws that cause these conditions requires comprehensive insight into installed applications, component devices, their configurations, and more importantly, their interactions. Recently, researchers at the University of California Riverside developed IotSan, a new hands-on system that uses pattern checking as a basis for detecting defects at the "interaction level" by identifying events that could lead the system to an unsafe state.[261] They evaluated IotSan on the Samsung SmartThings platform. Out of 76 manually configured systems, IotSan detects 147 vulnerabilities (i.e. breaches of secure physical states/properties). solutions must build "anarchic scalability". “[265] The application of the concept of anarchic scalability can also be extended to physical systems (i.e. controlled real-world objects) by making those systems designed to accommodate uncertain future control. Thus, this hard anarchic scalability provides a way forward to fully exploit the potential of IoT solutions by selectively constraining physical systems to enable all forms of management without the risk of physical failure. [265] Computer scientist Michael Littman of Brown University has argued that successful implementation of the Internet of Things must consider its usefulness. interfaces as well as the technology itself. These interfaces not only need to be more user-friendly, but also better integrated: "If users have to learn different interfaces for their vacuum cleaners, locks, sprinklers, lights and coffee machines, it's hard to say that their lives have been made easier." [266] Impact on Environmental Sustainability Concerns related to Internet technologies are related to the production, use and ecological impact of any possible damage. ch of these semiconductors rich inToday's electronics are full of all kinds of heavy and rare earth metals, as well as highly toxic synthetic chemicals. This makes it difficult to process them properly. Electronic components are often incinerated or disposed of in conventional landfills. In addition, the human and environmental costs associated with the extraction of rare earth metals, an integral part of today's electronic components, continue to rise. This raises public questions about the environmental impact of IoT devices over their lifetime.[268] Deliberate obsolescence of devices The Electronic Frontier Foundation has raised concerns that companies may be using the technologies needed to support connected devices to deliberately disable or "jail down" their customers' devices by remotely updating software or disabling a service necessary for the device to function. . In one example, home automation devices sold with the promise of a "lifetime subscription" turned out to be worthless after Nest Labs bought Revolv and decided to shut down the central servers used by Revolv's devices. Because Nest is a company owned by Alphabet (Google's parent company), EFF says it sets "a terrible precedent for a company that wants to sell self-driving cars, medical devices and other high-end gadgets that could be critical to business." physical security”[270]. Owners should be able to redirect their devices to another server or collaborate on software improvements. However, doing so violates Section 1201 of the DMCA, which contains only a “local use” exception. This puts crafters who want to continue using their equipment into a legal gray area. EFF believes that consumers should avoid electronics and software where the wishes of the manufacturer are more important than their own.[270] Examples of post-market tampering include the Google Nest Revolv, disabling privacy settings on Android, disabling Sony Linux on the PlayStation 3, and enforcing end-user licensing agreements on the Wii U.[270] Confusing terminologyLonergan of Business Technology Age magazine called IoT-related terms a "terminological zoo". The lack of clear terminology is not "useful from a practical point of view" and "a source of confusion for the end user"[271]. An IoT company can work on anything related to sensor technology, networking, embedded systems, or analytics.[271] According to Lonergan, the term IoT was coined before smartphones, tablets and devices as we know them today, 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 Things (Supply Chain), Industrial Internet, Pervasive Computing, Pervasive Computing, Pervasive Computing, Cyber Physical Systems (CPS), Wireless Sensor Networks (WSN), Smart Objects, Digital Twins, Cyber Objects or Avatars[141].] interacting objects, machine-to-machine (M2M), ambient intelligence (AmI), operations technology (OT) and information technology (IT) [271]. For IoT, an industrial IoT subsector, the Industrial Internet Consortium Vocabulary Task Force created a "common and reusable glossary of terms"[272] to ensure "consistent terminology"[272][273] in publications produced by the Industrial Internet Consortium. Internet Consortium. IoT One has created a database of IoT terms that includes a new term alert[274] that alerts when a new term is published. As of March 2020 [update], this database collects 807 IoT-related terms while remaining "transparent and comprehensive". IoT Services Market First IEEE Computer Society TechIgnite Lack of Interoperability and Unclear Value Propositions Despite widespread confidence in the potential of the Internet of Things, industry leaders and consumers face barriers to wider adoption of IoT technologies. Mike Farley claimedthat IoT solutions, while appealing to early adopters, either lack interoperability or do not have a clear use case for the end user.[277] Ericsson's study of IoT adoption among Danish companies shows that many find it difficult to "determine exactly what the value of IoT is for them"[278]. Privacy and Security Issues For the Internet of Things, especially the consumer Internet of Things, information about the user's daily life is collected so that "things" around the user can work together to provide better services tailored to personal preferences.[279] If the collected information that describes the user in detail goes through multiple hops in the network due to different services, devices, and network integration, the information stored in the device is vulnerable to privacy breaches, which puts the nodes in the IoT network at risk. . [280] For example, on October 21, 2016, a multiple distributed denial of service (DDoS) attack on systems managed by domain name system provider Dyn caused several websites such as GitHub, Twitter, and others to become inaccessible. This attack is carried out using a botnet consisting of many IoT devices, including IP cameras, gateways, and even baby monitors.[281] Basically, the IoT system needs 4 security goals: (1) data privacy: unauthorized persons cannot access 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 the message; (4) data availability: transmitted and stored data must be available to authorized parties even in the event of Denial of Service (DOS) attacks[282]. Data protection regulations also require organizations to maintain “reasonable security.” California SB-327 Information Privacy: Connected Devices "According to this definition, the connected device manufacturer must equip the device with reasonableFeatures or functions appropriate to the nature and function of the device, consistent with the information it may collect, contain or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, alteration or Protect disclosure as stated [283] Because each organization's environment is unique, it can be difficult to demonstrate what constitutes “reasonable security” and the potential risks that may be associated with an organization. Oregon statute HB 2395 "also requires that a person manufactures, sells, or offers for sale a connected device] that the manufacturer must provide the connected device with appropriate security features that protect the connected device and the information that the connected device contains collects, contains and stores , or transmits] store, destroy, alter, use or disclose access by the consumer. Deny permission.”[284] According to antivirus vendor Kaspersky Lab, there were 639 million data breaches in IoT devices in 2020 and 1.5 billion lions in the first six months of 2021.[199] Traditional Governance Structure of Internet of Things City Hangzhou, China by Ericsson A study on IoT adoption among Danish companies found “a conflict between the IoT and traditional corporate governance structures as the IoT continues to experience both uncertainty and a lack of historical creates priority". [278] Of those surveyed, 60 percent said they “don't believe they have the organizational skills and three in four don't believe they have the processes necessary to embrace the power of the IoT.” [278] Test New Methods of Innovation Management The lack of digital leadership in the age of digital transformation is also hampering innovation and IoT adoption to the point where, faced with uncertainty, dow ji companies “were waiting for market momentum to kick in .or IoT tracking “in anticipation of competitor movements, customer requests, or regulatory requirements.” Photos”—failure to recognize “the disruptive forces affecting their industry”[285] and “the actual acceptance of new business models that are causing disruptive change.” [285] Scott Anthony wrote in the Harvard Business Review that Kodak "invented the digital camera, invested in technology, and even realized that photos would go online"[285] but ultimately failed to realize that "photo sharing in networks are something new. business, not just a way to expand a print business.”] Business Planning and Project Management According to a 2018 study, 70–75% of IoT deployments get stuck in the pilot or prototype phase and fail to scale, due in part to a lack of business planning. [286] [needs page] [287] While researchers, engineers, and managers around the world are constantly working to create and take advantage of IoT products, there are some shortcomings in managing, managing, and implementing such projects. . Despite the huge pace of development in the field of information and other assistive technologies, IoT is still a complex area, and the problem of managing IoT projects has not yet been solved. IoT projects must be carried out differently than simple and traditional IT, manufacturing or construction projects. As IoT projects have longer timelines, a lack of skilled resources, and few security/legal issues, there is a need for new tailor-made design processes. The following management practices are intended to improve the success of IoT projects: Separate R&D phase. Concept/prototype verification before the actual project starts. Project manager with interdisciplinary technical experience.Genre See also 5G Artificial Intelligence of Things Automotive Security Big Data Cloud Manufacturing Cyber-Physical System Data Distribution Service Digital Object Storage Digital Twin Edge Computing 4D Product Home Automation Indoor Positioning System Industry 4.0 IoT Cloud Simulation IoT Open Connection Consortium OpenWSN Quantified Self-Responsive Computer Design Smart Web of Things Thread (network protocol) Materia (default) Electric Dreams, a 1984 comedy film featuring a sentient (random) personal computer capable of controlling all of its human owner's home appliances and becoming a physical threat or even a rival to it. ^

ab Gillis, Alexander (2021). "What is the Internet of Things (IoT)?". IOT agenda. Retrieved 17 August 2021. ^ Brown, Eric (20 September 2016). "21 Open Source Projects for IoT". linux.com. Retrieved 23 October 2016. ^ "Global Standards Initiative for the Internet of Things". ITU. Retrieved June 26, 2015. ^ Hendricks, Drew. "The Internet of Things Problem". Data warehouse in London. Greater London authorities. Retrieved 10 August 2015. ^ Shafiq, Muhammad; Gu, Zhaoquan; Cheikhrouhou, Omar; Alhakami, Wajdi; Hamam, Habib (3 August 2022). "Rise of the 'Internet of Things': A Review and Open Research on the Challenges of Detecting and Preventing Internet of Things-Based Security Attacks". Wireless communication and mobile computing. 2022: e8669348. doi: 10.1155/2022/8669348. ISSN 1530-8669. ^ Internet of Things and Big Data Analytics for Next Generation Intelligence. Nilanjan Dey, Aboul Ella Hassanen, Chintan Bhatt, Amira Ashour and Suresh Chandra Satapathy. Ham, Switzerland. 2018. p. 440. ISBN 978-3-319-60435-0. OCLC 1001327784.{{Cit book}} : CS1 maint: other (link) ^ "Forecast: Internet of Things, Worldwide, 2013." Gardener. Retrieved March 3, 2022. ^ Hu, J.; Niu, H.; Carrasco, J.; Lennox, B.; Arvin, F., “Fault-Tolerant Cooperative Navigation of Networked UAV Swarms to Forest FiresAerospace Science and Technology, 2022. ^ Hu, J.; Lennox, B.; Arvin, F., "Robust formation control for networked robotic systems with negative imaginary dynamics", Automatica, 2022. ^ Laplante, Phillip A.; Kassab, Muhammad; Laplante, Nancy L.; Voas, Jeffrey M. (2018). "Building Caring Health Systems on the Internet of Things". IEEE Systems Journal. 12(3): 3030-3037. Bibcode: 2018ISysJ..12.3030L. doi:10.1109/JSYST.2017.2662602. ISSN 1932-8184. PMC 6506834. PMID 31080541. ^ "New York Internet of Things Strategy". www1.nyc.gov. Retrieved September 6, 2021. ^ "Only Coke Machine on the Internet". Carnegie Mellon University. Retrieved November 10, 2014. ^ "The broken internet of things is stifling innovation". information week. July 7, 2014 Retrieved November 10, 2014. ^ Mattern, Friedemann; Floerkemeier, Christian (2010). "From the Internet of Computers to the Internet of Things" (PDF). The spectrum of computer science. 33(2):107-121. Bibcode:2009InfSp..32..496H. doi:10.1007/s00287-010-0417-7. hdl:20.500.11850/159645. S2CID 29563772. Retrieved February 3, 2014. ^ Weiser, Mark (1991). "The 21st Century Computer" (PDF). American scientist. 265(3):94-104. Bibcode: 1991SciAm.265c..94W. doi:10.1038/scientificamerican0991-94. Archived from the original (PDF) on March 11, 2015. Retrieved November 5, 2014. ^ Raji, R.S. (1994). "Smart Grids for Control". IEEE spectrum. 31(6):49-55. doi:10.1109/6.284793. S2CID 42364553. ^ Pontin, Jason (September 29, 2005). "ETC: Bill Joy's Six Nets". MIT technology overview. Retrieved November 17, 2013. ^ "IOT HISTORY REPAIR". CHETAN SHARMA. March 14, 2016 Retrieved June 1, 2021. ^ Ashton, K. (June 22, 2009). "The 'Internet of Things' Thing". Retrieved May 9, 2017. ^ "Peter Day's Business World". BBC World Service. BBC. Retrieved October 4, 2016. ^ Magrassi, P. (May 2, 2002). "Why a universal RFID infrastructure would be a good thing". Gartner Research Report G00106518. Berg, T. (August 12, 2002). "One WorldSmart Objects. Gartner Research Report R-17-2243. Archived from the original on October 3, 2003. ^ Commission of the European Communities (June 18, 2009). "Internet of Things - An Action Plan for Europe" (PDF) COM(2009) 278 final ^ Wood, Alex (31 March 2015). "The Internet of Things is revolutionizing our lives, but standards are a must." The Guardian. ^ Stallings, William (2016). Modern Networking Essentials. : SDN, NFV, QoE, IoT and the Cloud Florence Agboma, Sofiene Jelassi Indianapolis, Indiana ISBN 978-0-13-417547-8 OCLC 927715441 "Internet of Things: How the next evolution of the Internet will change everything" (PDF). CISCO White Paper. ^ Vongsingthong, S.; Smanchat, S. (2014). The Internet of Things: An Overview of Applications and Technologies” (PDF). Suranaree Journal of Science and Technology. ^ a b "The Enterprise Internet of Things Market". Business informant. February 25, 2015 Retrieved June 26, 2015. ^ Perera, C.; Liu, CH; Jayawardena, S. (December 2015). "The Emerging IoT Market from an Industry Perspective: A Survey". IEEE Transactions on Emerging Topics in Computer Science. 3(4):585-598.arXiv:1502.00134. Bibcode: 2015arXiv150200134P. doi:10.1109/TETC.2015.2390034. ISSN 2168-6750. S2CID 7329149. ^ "How IoT is changing the foundations of 'retail'". Trak.in - Indian technology, mobile and startup company. August 30, 2016 Retrieved June 2, 2017. ^ Kang, won min; Moon, Seo Yeon; Park, Jong Hyuk (March 5, 2017). "Advanced Home Appliance Security Framework for Smart Home". Computer science and human-centered computing. 7 (6). doi:10.1186/s13673-017-0087-4. ^ a b "How IoT and smart home automation will change the way we live". Business informant. Retrieved November 10, 2017. ^ ab Jussi Karlgren; Lennart Fahlen; Anders Wallberg; Couple Hansson; lead steel; Jonas Soderberg; Karl-Petter Åkesson (2008). Smart social interfaceIncreased energy awareness in the household. Internet of Things Computer science lecture notes. Vol. 4952. Springer. pp. 263-275. arXiv:2106.15297. doi:10.1007/978-3-540-78731-0_17. ISBN 978-3-540-78730-3. S2CID 30983428. ^ Greengard, Samuel (2015). Internet of Things Cambridge, MA: MIT Press. p. 90. ISBN 9780262527736. ^ "HomeKit - Apple Developer". developer.apple.com. Retrieved September 19, 2018. ^ Wollerton, Megan (June 3, 2018). "Here's everything you need to know about Apple HomeKit." OVERHANG. Retrieved September 19, 2018. ^a b Lovejoy, Ben (August 31, 2018). "HomeKit devices are becoming more affordable as Lenovo announces the Smart Home Essentials line." 9 to 5 Macs. Retrieved September 19, 2018. ^ Prospero, Mike (September 12, 2018). "Best Smart Home Hubs 2018". Tom's guide. Retrieved September 19, 2018. ^ Chinchilla, Chris (November 26, 2018). "Which Smart Home IoT platform should you use?". Hacker south. Retrieved May 13, 2019. ^ Baker, Jason (December 14, 2017). "6 Open Source Home Automation Tools". opensource.com. Retrieved May 13, 2019. ^ ab Demiris, G; Hensel, K. (2008). "Technology 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. PMID 18660873. S2CID 7244183. ^ Aburukba, Raafat; Al Ali, AR; Kandil, Nurhan; AbuDamis, Diala (May 10, 2016). Configurable ZigBee-based control system for people with multiple disabilities in smart homes. pp. 1-5. doi:10.1109/ICCSII.2016.7462435. ISBN 978-1-4673-8743-9. S2CID 16754386. ^ Mulvenna, Maurice; Hutton, Anton; Marcin, Susanna; Todd, Stephen; Bond, Raymond; Moorhead, Anne (December 14, 2017). "Carers' views on the ethics of assistive technology used in home monitoring of people with dementia". neuroethics. 10(2): 255-266. doi:10.1007/s12152-017-9305-z. PMC 5486509. PMID 28725288. Ab da Costa, CA; Pasluosta, CF; Escofier, B; da Silva DB; da Rosa Righi, R (July 2018). "InternetHealth Matters: Towards Smart Vital Signs Monitoring in Hospital Wards. Artificial intelligence in medicine. 89:61–69. doi: 10.1016/j.artmed.2018.05.005. PMID 29871778. S2CID 46941758. ^ Engineer, A; Sternberg, E.M.; Najafi, B (21 Aug 2018) Interior Design to Mitigate Age-Related Physical and Cognitive Deficits and Promote Longevity in the Elderly: Gerontology Review 64(6):612-622 doi:10.1159/000491488. PMID 30130764 S2CID 52056959^a b Kricka, LJ (2019) "History of failures in laboratory medicine: What have we learned from predictions?". Clinical Chemistry and Laboratory Medicine 57(3):308–311 doi:10.1515/ cclm-2018-0518 PMID 29927745 S2CID 49354315 ^ Gatouillat, Arthur, Badr, Youakim, Massot, Bertrands: Internet of 2018 Review of recent papers dealing with cyber fiscal systems in Medicine” (PDF). IEEE Journal Internet of Things. 5(5):3810-3822. doi:10.1109/jiot.2018.2849014. ISSN 23 27-4662. S2CID 53440449. ^ Poplar, Eric (2016). The patient will now see you: the future of medicine is in your hands. Basic books. ISBN 978-0465040025. ^ ab Dey, Nilanjan; Hassanien, Aboul Ella; Bhatt, Chintan; Ashour, Amira S.; Satapathy, Suresh Chandra (2018). IoT and Big Data Analytics for Next Generation Intelligence (PDF) Springer International Publishing House. ISBN 978-3-319-60434-3. Retrieved 14 October 2018. ^ Pratap Singh, R.; Javaid, M.; Haleem, A.; Vaishya, R.; Ali, S. (2020). "The Internet of Medical Things (IoMT) for Orthopedics in the COVID-19 Pandemic: Roles, Challenges and Applications". Journal of Clinical Orthopedics and Trauma. 11(4):713-717. doi:10.1016/j.jcot.2020.05.011. PMC 7227564. PMID 32425428. ^ "Deloitte Center for Health Solutions" (PDF). Deloitte. ^ a b c d e f g hi j Ersue, M.; Romascanu, D.; Schoenwalder, J.; Sehgal, A. (May 2015). "Managing Networks with Constrained Devices: Use Cases". IETF Online Project. Wikimedia Commons has media related to Goldman SachsIn fact, the Internet of Things could save the US healthcare system $305 billion a year. Enable mobile blogging. Engage Mobile Solutions, LLC. June 23, 2016. Retrieved July 26, 2018. ^ World Health Organization. m Health. New horizons of health thanks to mobile technologies" (PDF). World Health Organization. Retrieved 3 January 2020^ Istepanyan, R.; Hu, S.; Philip, N.; Sungur, A. (2011). Potential of M-Health Internet of Things "m-IoT" for non-invasive glucose detection. Annual International Conference IEEE Engineering in Medicine and Biology Society 2011. Annual International Conference IEEE Engineering in Medicine and Biology Society. Society for Engineering Medicine and Biology IEEE. Annual international conference. Volume. 2011. S. 5264-6. doi: 10.1109/IEMBS.2011.6091302. ISBN 978-1-4577-1589-1. PMID 22255525. S2CID 995488. ↑ Swan, Melanie (November 8, 2012) "Sensory mania! Internet of Things, Wearable Devices, Objective Metrics, and Quantitative Self-Activity 2.0”, Journal of Sensor and Actuator Networks. 1(3): 217-253. doi: 10.3390/jsan1030217. ^ Taiwan Information Strategy, Internet Strategy and E-Strategy Information Guide, Terms, Contact. UPS, Inc. UNITED STATES. 2016. P. 79. ISBN 978-1514521021. ^ Grell, Mack; Dinser, bank; Le, Tao; Lauri, Alberto; Nunez Bajo, Estefania; Casimatis, Michael; Barandoon, Jandrine; Mayer, Stefan A.; Kass, Anthony E. G. (2019). “Autocatalytic metallization of fabrics with silicon ink for biosensors, batteries and energy harvesting. Advanced functional materials. 29 (1): 1804798. doi: 10.1002/adfm. 201804798. ISSN 1616-301X. PMC 7384005. of- Testing for Care - xPOCT. | HealthIT.gov. www.healthit.gov. Source 21.2020. ^ Amiot, Emmanuel. "Internet of Things. Breaking Traditional Business Models" (PDF). Oliver Wymann. Retrieved October 14, 2018. ↑ Vermesan, Ovidiu, and Peter Friess, eds. Internet of Things: Converged Technologies for Smart Environments and Integrated Ecosystems. River Publisher, 2013 . ^ Mahmoud, Khizir, Stadt, Graham E., Morsalin, Saidul, Hossain, MJ (February 2018)."Integrating Electric Vehicles and Driving into the Energy Internet".Overview of renewable and sustainable energy sources 82:4179-4203 doi:10.1016/j.rser.2017.11.004 ^ Xie, Xiao-Feng; Wang, Zong-Ching (2017). "An integrated decision support system in a car for driving at signalled Intersections: a Prototype of the Intelligent Internet of Things in Transportation". Transportation Research Board (TRB) Annual Meeting, Washington, DC, USA. ^ "Key Applications of Intelligent Internet of Things for Transportation Transformation". 20 September 2016 ^ a b c d Haase January; Alakhmad, Mahmoud; Nishi, Hiroaki; Plennigs, Yorn; Tsang, Kim Fung (2016). "IOT-Mediated Embedded Environment: A Brief Overview". 2016 14th IEEE International Conference on Industrial Informatics (INDIN). pp. 1065-1068. doi: 10.1109/INDIN.2016.7819322. ISBN 978-1-5090-2870-2. S2CID 5554635. ^ "Everything you need to know about the Internet of Things and the Industrial Internet of Things". Retrieved July 5, 2022. ↑ Yang, Chen; Shen, Weiming; Wang, Xianbin (January 2018). "Internet of Things in Manufacturing: Key Issues and Potential Applications". IEEE Systems, Journal of Humans and Cybernetics. 4(1):6-15. doi: 10.1109/MSMC.2017.2702391. S2CID 42651835. ^ Savery, S.; Abreu, G.; Sottile, F.; Pastrone, K.; Spirito, M.; Behrens, F. (June 23–26, 2014). "M2M Technologies: Opportunities for the Pervasive Internet of Things". European Conference on Networks and Communications (EUCNC2014). ^ b Gubbi, Jayawardhana; Buya, Rajkumar; Marusich, Slaven; Palaniswami, Marimutu (24 February 2013). Internet of Things (IoT): vision, architectural elements anddirections". Future Generation Computing Systems. 29(7): 1645–1660. arXiv: 1207.0203. doi: 10.1016/j.future.2013.01.010. S2CIDÂ 204982032. W2982032. 2 ^ Neng, Lu, August 2010). Future. Internet: Internet of Things 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE) Volume 5 Pages 376-380 doi: 10.1109/ICACTE.2010.5579543 ISBN 978-1-4244-6539-2 S2CID 40587 ^ "Industrial Construction on Campus" (PDF). Autodesk. ^ Meola, A. (20 December 2016). Why IoT, Big Data and Smart Agriculture are the Future of Agriculture. business insider. Insider Inc. 26.2018. July ^ Zhang, K. (2015). Precision Agriculture Technology for Crop Production. C.R.C. Press. pp. 249–58. ISBN 9781482251081. Japan." Register. ^ Vasisht, Deepak; Kapetanovic, Zerina; Won, Chonho; Yin, Xinxin; Chandra, Ranveer; Sinha, Sudipta; Kapoor, Ashish; Sudarshan, Madhusudhan; Farms (2Beats1,7). : IoT Platform for Data-Driven Agriculture, pp. 515-529. p. ISBN 978-1-931971-37-9 ^ "FarmBeats: AI, Edge and IoT for Agriculture" Microsoft Research Retrieved 28 June 2021. ^ "Moni thetor IoT can turn your boat into a smart boat" Yachting World 9 March 2020 Retrieved 10 July 2014 Postscapes Retrieved 10 July 2014 ^ Poon, L. (22 June 2018) "Sleepy in Songdo, Korea's Smartest City" MontlyLab Atlantic City Group Retrieved July 26, 2018 Rico, Juan (April 22-24, 2014) "Beyond Monitoring and Control in Big Smart Cities" NFC and Contactless Solutions â WIMA Monaco ^ "Visible Today's City, Tomorrow's City Vision". China-Singapore Knowledge City Guangzhou. Retrieved 11 July 2014 ^ "San Jose Adopts Intel Technologycity. Intel Newsroom. Retrieved July 11, 2014. Fortune.com. Retrieved June 8, 2019. ^ Freeman, Mike (September 9, 2015). "On-Ramp Wireless Becomes Ingen, Launches Nationwide IoT Network". San DiegoUnionTribune.com. Retrieved June 8, 2019. ^ Lipska, Jessica. "IoT Clash Over 900 MHz Options". EETimes. Retrieved May 15, 2015. References "Sigfox launches IoT network in 10 UK cities". Fierce wireless technology. Retrieved May 13, 2015. Merritt, Rick. "13 views of the IoT world". EETimes. Retrieved May 15, 2015. ↑ Fitchard, Kevin (May 20, 2014). "Sigfox Moves Its IoT Network to San Francisco". gigahoms. Retrieved May 15, 2015. ↑ Ujaley, Mohd (July 25, 2018). "Cisco Invests in Fiber Networks, IoT, Smart Cities in Andhra Pradesh". ProQuest 1774166769. ^ "ST Honorable Mention E Security Innovation Awards: The End of Connection". securityinfowatch.com. Retrieved August 12, 2015. ↑ Parello, J.; Claes, B.; Schoening, B.; Quittek, J. (April 28, 2014). "Energy Management System". IETF online project. "How the Internet of Things enables smart buildings". Extreme technique. ^ "Will's Eye". Retrieved June 26, 2015. References Wang, Hong; Xu, Tao; Zhou, Guiping (2011). Research on the use of the Internet of Things in the field of environmental protection (submitted material). Electrical engineering lecture notes. St. page 133 99–106. doi:10.1007/978-3-642-25992-0_13. ISBN 978-3-642-25991-3. ^ "Use Case: Sensitive Wildlife Tracking". French FIT project. Archived from the original on July 14, 2014. Retrieved July 10, 2014. ↑ Hart, Jane K.; Martinez, Kirk (May 1, 2015). "Towards an environmentally friendly Internet of Things". Earth and space science. 2(5): 194–200. Bibcode: 2015E&SS...2..194H. doi:10.1002/2014EA000044. BibliographyVeronica; Ferrari, Alberto; Bresciani, Stefano (April 4, 2016). "Internet of Things". Journal of Business Process Management. 22(2):357-367. doi:10.1108/bpmj-05-2015-0074. ISSN 1463-7154. "The Internet of Things Meets the Military and the Battlefield: Bridging Hardware and Biometric Wearables for IoMT and IoBT". IEEE Computer Society. Retrieved 31 October 2019. MeriTalk. On January 30, 2018. Retrieved 31 October 2019. ↑ Gudeman, Kim (October 6, 2017). "The next-generation Internet of Things (IoBT) is designed to help keep soldiers and civilians safe." ECE Illinois. Retrieved 31 October 2019. ^ "Internet of Things on the Battlefield (IOBT)". CCDC Military Research Laboratory. Retrieved 31 October 2019. ^ "DARPA Unveils Ocean of Things Offer". MeriTalk. January 3, 2018. Retrieved October 31, 2019. ^ "How to make smart packaging even smarter". package inspection. June 4, 2018. Retrieved April 28, 2020. ^ "Communicating with consumers: the benefits and threats of smart packaging for the food and beverage industry". foodnavigator-asia.com. Retrieved 28 April 2020. ^ "What Smart Packaging Technologies Are Coming in 2018" . . bakerynews.com. Retrieved 28 April 2020. ^ Chen, Changsheng; Li, Mullin; Ferreira, Anselmo; Huang Jiwu; Cai, Rizhao (2020). "A Copy Protection Scheme Based on Spectral and Spatial Barcode Channel Models". IEEE Transactions on Computer Forensics and Security. 15:1056-1071. doi:10.1109/tifs.2019.2934861. ISSN 1556-6013. S2CID 201903693. ^ "MIT Introduces Batteryless Anti-Forgery Cryptosign." www.securingindustry.com. February 26, 2020 Retrieved April 28, 2020. ^ ab Nordrum, Amy (August 18, 2016). "The popular IoT prediction of 50 billion devices by 2020 is outdated." IEEE Spectrum. ^ Vermechan, Ovid; Chipp, Pete (2013). The Internet of Things: Converged Technologies for Smart Environments and Integrated Ecosystems (PDF). Aalborg, Denmark: River Publishers.^ Santucci, Gerald. "The Internet of Things: Between the Internet Revolution and the Metamorphosis of Objects" (PDF). European Commission Public Research and Development Information Service. Retrieved October 23, 2016. Flerkemeier, Christian. "From the Internet of Computers to the Internet of Things" (PDF). ETH Zurich. Retrieved October 23, 2016. Go to Lindner, Tim (13 July 2015). "Supply Chain: Changing at the Speed of Technology". connected world. Retrieved September 18, 2015. ^ a b Köhn, Rüdiger. Online Crime: Corporations Unite Against Hackers. Phase no. ^ "Smart Things: The Autonomous Internet of Things". GDR blog. The creative intelligence of the GDR. January 5, 2018. Retrieved July 26, 2018. ↑ Levin, Sergey; Finn, Chelsea; Darrell, Trevor; Abbel, Peter (2016). "Complete Training in Deep Visual Motor Principles" (PDF). Journal of Machine Learning Research. 17(1):1334-1373. archive: 1504.00702. Bibcode: 2015arXiv150400702L. ^ b Mohammadi, Mehdi; Al-Fuqaha, Cave; Sorur, Samekh; Guisani, Mohsen (2018). "Deep Learning for Big Data IoT and Streaming Analytics: A Review". IEEE Communications Surveys and Tutorials. 20(4):2923-2960. archive: 1712.04301. doi: 10.1109/COMST.2018.2844341. S2CID 9461213. ^ Mahdavinejad, Mohammad Said; Rezvan, Mohammadreza; Barekatayn, Mohammadamin; Adibi, Payman; Barnagi, Payam; Sheth, Amit P. (2018). "Machine Learning for Internet of Things Data Analysis: A Review". Digital Communications and Networks. 4(3):161-175. archive: 1802.06305. Bib code: 2018arXiv180206305S. doi:10.1016/j.dcan.2017.10.002. S2CID 2666574. ^ Alippi, K. (2014). Intelligence for embedded systems. Springer-Verlag. ISBN 978-3-319-05278-6. ^ Delicato, F.C.; Al-Anbuki, A.; Wang, K., ed. (2018). Intelligent Cyber-Physical Systems: Towards Comprehensive Intelligent Systems. New generation computer systems. Elsevier. Retrieved July 26, 2018. ^ a b c d Traukina, Alena; Thomas, Jayant; Tyagi, Prashant; Reddipally, Kishore (September 29, 2018).Web Application Development: Simplifying IIoT Development Using the Flexibility of Public Cloud and Cloud Native Services (1st ed.). Publish the package. Page 18^ Hasan, Qusay; Chan, Ata; Madani, Sajjad (2018). The Internet of Things: Challenges, Advances, and Applications. Boca Raton, FL: CRC Press. page 198 ISBN 9781498778510. ^ Chauhuri, Abhik (2018). Internet of things, for things and through things. Boca Raton, FL: CRC Press. ISBN 9781138710443. ^ Pal, Arpan (May–June 2015). "The Internet of Things: Making Noise a Reality" (PDF). computer specialist. 17(3):2-4. doi:10.1109/MITP.2015.36. Retrieved April 10, 2016. Gardener. November 10, 2015. Archived from the original on November 12, 2015. Retrieved April 21, 2016. ↑ Reza Arkian, Hamid (2017). "MIST: A Fog-Based Data Analysis Scheme with Inexpensive Resource Provisioning for IoT Applications". Network and Desktop Applications Magazine. 82:152-165. doi:10.1016/j.jnca.2017.01.012. ^ "Outer IoT Edge Computing". June 2019. Retrieved June 3, 2019. {{quote-journal}} : quote journal requires |journal= (help) ^ Cui, Laizhong; Yang, Shu; Chen, Ziteng; Lord, Yi; Ming John; Xu, Mingwei (May 2020). "A Decentralized and Trusted Edge Computing Platform for IoT". IEEE Journal Internet of Things. 7(5):3910-3922. doi:10.1109/JIOT.2019.2951619. ISSN 2327-4662. S2CID 209097962. ^ Nguyen, Tien-Dung; Huh, Eui-Nam; Jo, Minyu (June 2019). "A Decentralized and Transformed Platform for Content-Oriented Network-Based Service Delivery and Discovery in Mobile Edge Computing for IoT Devices." IEEE Journal Internet of Things. 6(3): 4162-4175. doi:10.1109/JIOT.2018.2875489. ISSN 2327-4662. S2CID 69250756. ^ Xiong, Zehui; Zhang, Yang; Luong, Nguyen Cong; Nijato, Dusit; Wang, Ping; Guizani, Nadra (January 2020). “The Best of Both Worlds: A Whole Blockchain Data Management ArchitectureIEEE networks. 34(1): 166-173. doi: 10.1109/MNET.001.1900095. ISSN 1558-156X. S2CID 211050783. Singer, Jeremy; Michala, Anna Lito (June 2021). "Task Distribution Optimization for Edge Microclusters in Smart Cities". 22. IEEE International Symposium on Wireless, Mobile, and Multimedia (WoWMoM), 2021: 341-347. doi: 10.1109/WoWMoM51794.2021.00062. ISBN 978-1-6654-2263-5. S2CID 235780952. ^ Guo, Hongzhi; Liu, Jiajia; Qin, Huilin (January 2018). "Mobile Device Offloading for Collaborative Edge Computing for IoT in Fiber Optic Networks". IEEE networks. 32(1):66-71. doi: 10.1109/MNET.2018.1700139. ISSN 1558-156X. S2CID 12479631. Bradai, Abbas; Bukhari, Syed Hashim Raza; Kuang, Pham Chang An; Ahmed, Olfa Ben; Atri, Mohamed (December 1, 2020). "Overview of Machine Learning in the Internet of Things: Algorithms, Strategies and Applications". internet of things 12:100314.doi:10.1016/j.iot.2020.100314. ISSN 2542-6605. S2CID 228876304. ^ Cherupalli, Sumant Reddy; God, Srinivas; Podili, Prashant; Kataoka, Kotaro (January 2021). "Lightweight and Scalable DAG-based Distributed Ledger for IoT Data Integrity Checking". International Conference on Information Networks (ICOIN) 2021: 267–272. doi: 10.1109/ICOIN50884.2021.9334000. ISBN 978-1-7281-9101-0. S2CID 231825899. ^ Fan, Xinxin; tea, qi; Xu, Lei; Guo, Dong (October 6, 2020). "DIAM-IoT: A Decentralized Identity and Access Management Framework for the Internet of Things". Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure. BKI 20. Taipei, Taiwan: Computer Machinery Association: 186–191. doi: 10.1145/3384943.3409436. ISBN 978-1-4503-7610-5. S2CID 222142832. ^ Durand, Arnaud; Gremo, Pascal; Pasquier, Jacques (October 22, 2017). "Decentralized Trust and Authentication Web for the Internet of Things". Proceedings of the 7th International Conference on the Internet of Things. Internet of Things '17. linz,Computer Engineering Association: 1-2. doi: 10.1145/3131542.3140263. ISBN 978-1-4503-5318-2. S2CID 3645848. ^ Rathor, Shailendra; Wook Kwon, Byun; Park, Jong Hyuk (October 1, 2019). "BlockSecIoTNet: A Blockchain-Based Decentralized Security Architecture for IoT Networks". Journal of Network and Desktop Applications. 143: 167-177. doi: 10.1016/j.jnca.2019.06.019. ISSN 1084-8045. S2CID 198365021. ^ ab Gauthier, Philippe; González, Laurent (2011). L'Internet des Objects... Internet, mais en mieux (PDF). Foreword by Gérald Santucci (European Commission), MEPs Daniel Kaplan (FING) and Michel Volle. Paris: Edition AFNOR. ISBN 978-2-12-465316-4. ^ Marginin, M.T.-T; Lu, C. (2016). "sDOMO communication protocol for home robotic systems in the context of the Internet of Things". Computer Science, Technology and Applications. Scientific world. 151-60. p. ISBN 9789813200432. ^ Montazerolghaem, Ahmadreza (2021). Software-defined multimedia IoT: energy-efficient and sustainable resource management. IEEE Journal Internet of Things. 9(3): 2432–2442. doi:10.1109/JIOT.2021.3095237. ISSN 2327-4662. S2CID 237801052. ^ Rowayda, A. Sadek (May 2018). "An Agile Software-Based Architecture of the Internet of Things (IoT) (SDN)" (PDF). Egyptian Journal of Informatics. ^ Montazerolghem, Ahmadreza; Yaghmaee, Mohammad Hossein (April 2020). "Software-defined IoT with load balancing and QoS support". IEEE Journal Internet of Things. 7(4): 3323–3337. doi:10.1109/JIOT.2020.2967081. ISSN 2327-4662. S2CID 214551067. ^ "OGC SensorThings API Standard Specification". OGC. Retrieved 15 February 2016. ^ "Enable OGC Sensor over the Internet: High Level Overview and Architecture". OGC. Retrieved 15 February 2016. ↑ Minteer, A. (2017). Chapter 9: Applying Geospatial Analytics to IoT Data. Analytics for the Internet of Things (IoT). Packt Publishing. 230–57. p. ISBN 9781787127579. ^ van der Zee, E.; Scholten, H. (2014). "Spatial dimensionsBig Data: Applying Geographical Concepts and Spatial Technologies to the Internet of Things. Bessis, N.; Dobre, K. (ed.). Big Data and the Internet of Things: A Blueprint for an Intelligent Environment. Springer. Pages 137-68. ISBN 9783319050294. ^ ab Gassee, J.-L. (January 12, 2014). "The Internet of Things: The Trash Problem". Monday note. Retrieved June 26, 2015. ^ de Sousa, M. (2015) "Chapter 10: Muzzley Integration". Internet of Things with Intel Galileo. Packt Publishing. page 163 ISBN 9781782174912. IoT enabling data exchange between applications. 2018 IEEE International Conference on Cloud Engineering (IC2E) Orlando, FL: IEEE: 346–350. doi: 10.1109/IC2E.2018.00068. ISBN-1-97 5386-500 8-0. S2CID 21720322. ^ a b c Afzal, Bilal; Umair, Muhammad; Asadullah Shah, Ghalib; Ahmed, Ejaz (March 2019). "Enabling IoT Platforms for Social IoT Applications: Vision, Feature Mapping and Challenges". Next generation computer systems. 92:718–731. doi:10.1016/j.future.2017.12.002. S2CID 57379503. ^ Bhatia, Munich; Sud, Sandeep K. (June 2020). "Quantum Computing-Based Network Optimization for IoT Applications". IEEE Journal of the Internet of Things. 7 (6): 5590–5598.doi:10.1109/JIOT.2020.2979887. ISSN 2327-4662. S2CID 215845606. ^ Cheng, Wai Huen; Ileladewa, Adeoye Abiodun; Tan, Take Bun (Jan 2019). "Personalized Recommendation System for the Social Internet of Things (SIoT)". International Conference on Green and Human Information Technology 2019 (ICGHIT): 24-29 doi:10.1109/ICGHIT.2019.00013. ISBN 978-1-7281-0627-4. S2CID 204702019. ^ Atzori, Luigi; Hiera, Antonio; Morabito, Giacomo; Nitti, Michele (November 14, 2012). “Social Internet of Things (SIoT) âsocial networks meet the internet of things: concept, architecture and characterization of networks. Computer Networks. 56 (16): 3594-3608. doi: 10.1016/j.comnet.2012.07.010. ISSN 1389-1286. ^ Khelloufi; Ning, Huansh Dhelim, Sahraoui; Qiu, Tie; Ma, Jianhua; Huang, Runhe; Atzori, Luigi (February 1, 2021). "Social Relationship Based Service Recommendation System for SIoT Devices". IEEE Journal of the Internet of Things. 8(3): 1859–1870. doi: 10.1109/JIOT.2020.3016659. ISSN 2327-4662. S2CID 226476576. , Switzerland: IEEE: 1-6 doi: 10.1109/GIOTS.2017.8016215. ISBN 978-1-823-47-07-07-523-7-0 ^ Udawant, Omkar; Thombare, Nikhil; Chauhan, Devanand; Hadke, Akasha; Waghole, Dattatray (December 2017). "Smart ambulance system using IoT". 2017 International Conference on Big Data, Internet of Things and Data Science (BID). Pune, India: IEEE: 171–176. doi: 10.1109/BID. 2017.8336593. I SBN 978-1-5090-6593-6. S2CID 4865714. ^ Saleem, Yasir; Crespi, Noel; Rehmani, Mubashir Hussain; Copeland, Rebecca; Hussein, Dina; Bertin, Emmanuel (December 2016). "Using the Social Internet of Things for Recommendation Services". 3rd IEEE 2016 World Forum on the Internet of Things (WF-IoT). Reston, Virginia, USA: IEEE: 359–364. doi:10.1109/WF-IoT.2016.7845500. ISBN 978-1-5090-4130-5. S2CID 206866361. ^ Andrade, Rossana M.C.; Arago, Belmondo R.; Oliveira, Pedro Almir M.; May, Marcio E. F.; Viana, Windson; Nogueira, Tales P. (April 2021). "Comprehensive infrastructure for self-adaptive IoT systems". Information and software technologies. 132: 106505. doi: 10.1016/j.infsof.2020.106505. S2CID 231731945. ^ Farahbakhsh, Bahareh;

Fanian, Ali; Manshaei, Mohammad Hossein (March 2021). "TGSM: Towards trusted group-based service management for social IoT". Internet of Things. 13: 100312. doi: 10.1016/j.iot.2020.100312. ISSN 2542-6605.^ Iqbal, Muhammad Azhar; Hussain, Sayyad; Xing, Huanlai; Imran, Muhammad (February 2021). Deploying the Internet of Things: Fundamentals, Design, and Applications (1st ed.). Wylie. doi: 10.1002/9781119701460.ch9. ISBN 978-1-119-70125-5. S2CID 240696468. ^ You want, Roy; Shilit, Bill N.; Jenson, Scott (2015). "Enable Internet of Things." Computer. 48:28-35. doi: 10.1109/MC.2015.12. S2CID 17384656. ^ "Internet of Things: Clutter or Clutter?". Register. Retrieved June 5, 2016 ^ "Can we talk? IoT providers are dealing with "chaos" in communication. computer world. April 18, 2014 Retrieved June 5, 2016 (2018). Internet of things from A to Z: technologies and applications. John Wylie & Sons. pp. 27-8. ISBN 9781119456759 ^ Dan Brickley et al., c. 2001 ^ Sheng, M.; Kuhn, Yu.; Yao, L.; Benatalla, B. (2017). Network of Things Management: connecting the real world to the network. Morgan Kaufman. pp. 256-8. ISBN 9780128097656. ^ Waldner, Jean-Baptiste (2008). Nanocomputers and swarm intelligence. London: ISTE. pp. 227-231. ISBN 978-1-84704-002-2. ^b Kushalnagar, N.; Montenegro, G.; Schumacher, K. (August 2007). IPv6 in low-power wireless personal area networks (6LoWPAN): overview, assumptions, problem description and goals. IETF. doi: 10.17487/RFC4919. RFC 4919. ^ ab Sun, Charles S. (May 1, 2014). "Stop using internet protocol version 4!". computer world. Narten, T.; Jinmei, T. (September 2007). Automatic configuration of stateless IPv6 addresses. IETF. doi: 10.17487/RFC4862. RFC 4862. ^ Xped Limited, ADRC Review", from Wikipedia ^ Alsulami, MM; Akkari, N. (April 2018). "The role of 5G wireless networks in the Internet of Things (IoT)". 2018 1st International Conference on Information Security in Computer Applications (ICCAIS): 1–8. doi: 10.1109/CAIS.2018.8471687. ISBN 978-1-5386-4427-0. S2CID 52897932. ^ "5G Internet of Things". July 2022. ↑ Jing, J.; Lee, H. (2012). "LearnInternet of Things standards. W Wang, Y.; Zhang, X. (Ed.). Internet of Things: International Workshop, IOT 2012. Springer. pp. 627-32 ISBN 9783642324277. ^ Mahmood, Z. (2018). Connected Experiences for the Internet of Things: Challenges and Solutions. Sweater. Pages 89-90. ISBN 9783319701028. ^ "IP-Home Connected Project". Google Developers Blog. Retrieved September 16, 2020. Carrie. "Apple, Amazon, Google and others want to create a new standard for smart home technology." CNET. Retrieved 24 December 2019. ↑ Strategy, Moor Insights i. Green IoT? Forbes. Retrieved 3 September 2020 ^ "Digital Link - Standards | GS1". www.gs1.org. On November 12, 2018. Retrieved 28 April 2020. Howard, Philip N. (June 1, 2015) "The Internet of Things Must Change Democracy Itself" Politico Retrieved August 8, 2017 ^ Thompson , Kirsten; Mattalo, Brandon (November 24, 2015). Canadian Regulation and Approach". Cyberlex. Retrieved 23 October 2016. (2010). The Internet of Things: Legal Perspectives. Springer Science & Business Media. Pages 59–64. ISBN 9783642117107. ^ Hassan, Q. F. (2018). The Internet of Things from A to Z: Technologies and Applications John Wiley & Sons, pp. 41-44 ISBN 9781119456759 ^ Hassan, K. F., R. Madani, S. A. (2017) The Internet of Things: Challenges, Advances, and Applications CRC Pr. Es. pp. 41–2 ISBN 9781498778534 ^ Lopez, Javier; Rios, Ruben; Bao, Feng; Wang, Guilin (2017). "Evolving Privacy: From Sensors to the Internet of Things". Next Generation Computing. 75: 46–57 doi:10.1016/j.future.2017.04.045 ^ "Internet of Things": Legalin an ultra-connected world. Mason Hayes & Curran. 22 January 2016. Retrieved 23 October 2016. ^ Brown, Ian (2015). "Regulation and the Internet of Things" (PDF). Oxford Internet Institute. Retrieved October 23, 2016 ^ "FTC IoT report urges companies to adopt best practices to address consumer privacy and security risks." Federal Trade Commission, January 27, 2015. Retrieved October 23, 2016. ^ Lawson, Stephen (March 2, 2016). "IoT users could win with a new bill in the US Senate." Tech Barrista. Retrieved December 9, 2019. “Legal developments in the connected car arena provide insight into privacy and data security laws in Matters.” Lexicon. Retrieved October 23, 2016. ^ Rasit, Yuce, Mehmet; Claus, Beisswenger, Stefan; Mangalam, Srikanth; That, Prasanna, Lal; Martin, Lukac (2017, November 2). "Internet of Things: A New Governance Platform for Enterprise - An Overview of Opportunities, Practices and Challenges": 1-112. {{quote journal}}: |journal= must be quoted (help) ^ a b Page, Carly (4/4/2021 Dec). "Is the UK Government's new IoT cybersecurity law appropriate?". TechCrunch. Retrieved December 4, 2021. ^ Wieland, Ken (February 25, 2016). "IoT pros worry about fragmentation." Mobile World ^ Wallace, Michael (19 February 2016). "Fragmentation is the enemy of the Internet of Things." Stuff: Opportunities and Challenges for Semiconductor Companies". McKinsey & Co. ^ Ardiri, Aaron (July 8, 2014). "Will fragmentation of standards only impede the true potential of the IoT industry?" evothings.com. PDF).arm. com. ↑ Raggett, Dave (27 April 2016). etu-Web: Interoperability of IoT platforms" (PDF). W3C. ^ Kovach, Steve (July 30, 2013).Fragmentation Report". business insider. Retrieved October 19, 2013 ^ "The Complete Guide to Connecting to the Internet of Things (IoT)". Lorenzo (July 29, 2015). Goodbye Android. Motherboard. Deputy. Android security is a lemon market. ', leaving 87 percent vulnerable." ZDNet. Retrieved October 14, 2015. ↑ Thomas, Daniel R.; Beresford, Alastair R.; Rees, Andrew (2015). Proceedings of the Fifth Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM '15 (PDF). Computer Lab at the University of Cambridge. s. 87–98. doi: 10.1145/2808117.2808118. ISBN 9781450338196. S2CID 14832327 . ↑ Howard, Philip N. (2015). Retrieved October 14, 2015. Pax Technica: how the Internet of Things can set us free or lock us up. New Haven, CT: Y bet University Press. ISBN 978-0-30019-947-5. ^ McEwan, Adrian (2014). "Designing the Internet of Things" (PDF). Retrieved 1 June 2016 ^ My de Vitry, Matthew; Schneider, Marian; Vani, Omar; Lillian, Manny; Leitao, Joe P.; Egimans, Sven (2019). "Smart Urban Water Systems: What Can Go Wrong?". Letters on ecological research. 14 (8): 081001. Bibcode: 2019ERL....14x1001M. doi: 10.1088/1748-9326/ab3761. ^ "Panopticon as a Metaphor for the Internet of Things" (PDF). Internet of Things Council. Accessed 6 June 2016 ^ ab "Foucault" (PDF). University of California at Los Angeles. Bibliography of the University of California, Los Angeles. ^ Verbeek, Peter-Paul (2011). Moralizing technologies: understanding and building the morality of things. Chicago: University of Chicago Press. ISBN 978-0-22685-291-1. ^ Cardwell, Diana (February 18, 2014). "The lights are on at Newark Airport and they're watching you." New York Times. ↑ Hardy, Quentin (February 4, 2015). "Tim O'ReillyThe Internet of Things". The New York Times. ^ Webb, Jeff (February 5, 2015). "Say Goodbye to Privacy." WIRED. Retrieved February 15, 2015. The Web is Closing Around Us." TomDispatch. ^ Brown, Ian (12 . February 2013). "The UK Smart Meter Scheme: A Case Study of Privacy by Design". International Review of Law, Computing and Technology. 28 (2): 172â 184. doi: 10.1080/13600869.2013.801580. S2CID 62756630. SSRN 2215646. ^ a b "The Impact of the Internet of Things on Society" (PDF). October, Gubbi, 23 February 0113 British Computer Society. Jayavardhana; Buyya, Rajkumar; Marušič, Slaven; Palaniswami, Marimuthu (1 September 2013). "The Internet of Things (IoT): vision, architectural elements, and future directions". Next Generation Computing Systems. Includes special sections: Enabling Cybercrime. Distributed Computing for Ubiquitous Cloud and Web Services, Cloud and Scientific Applications - Big Data, SC Analytics, and More. 29(7) : 1645–1660. arXiv:1207.0203. doi:10.1016/j.future.2013.01.010. S2CID 204982032. ^ Achar jya, D.P.; Ahmed, N.S.S. (2017). "Attack detection in a wireless sensor network with an Internet of Things view". In Acharjya, D.P.; Geeta, M.K. (ed.). The Internet of Things: New Advances and Expected Applications. Jumper. 149–50. p. ISBN 9783319534725. ^ Hussain, A. (June 2017). "Power consumption of wireless IoT nodes" (PDF). Norwegian University of Science and Technology. Retrieved 26 July 2018. ^ a b c d Keller, Matthias (2021). "Integration of I4.0 strategy and policy in the German manufacturing industry". KU Leuven, WWU, TalTech. ^ "We asked CEOs about the Internet of Things, and their responses show that security is still a big concern." Business Informer. Retrieved 26 June 2015. ↑ Singh, Jatinder; Pasquier, Thomas; Bacon, Jean; What, Hajoon; Ayers, David (2015). "Twenty Cloud Security Considerations for IoT Support". IEEEdiary of things. 3(3):1.doi:10.1109/JIOT.2015.2460333. S2CID 4732406. ^ ab Clearfield, Chris. "Why the FTC Can't Regulate the Internet of Things". forbes Retrieved 26 June 2015. ↑ a b Fimster, Nick (18 February 2017). "Reducing the Growing Risks of an Insecure Internet of Things". freedom for creativity. Retrieved August 8, 2017. ^ Lee, S. (2017). "Chapter 1: Getting Started: Securing the Internet of Things". W. Lee, S.; Xu, L.D. (Ed.). Security in the Internet of Things. Syngress. p. 4. ISBN 9780128045053. Shackleton, M.; El Moussa, F. (2018). "The Internet of Things: Exploring Technologies and Security Threats in Smart Homes and Urban Environments". Living in the Internet of Things: Cybersecurity of the Internet of Things - 2018. p. 30 (7 p.). doi: 10.1049/cp.2018.0030. ISBN 9781785618437. Aliwat, Zibuda; Harus, Saad; Bentaleb, Abdelhak; Refufi, Allaua (September 2019). "Security Review of the Internet of Things". Wireless personal connection. 108(1): 325-344. doi:10.1007/s11277-019-06405-y. ISSN 0929-6212. S2CID 150181134. ^ Liu, Ximen; Jan, Jan; Chu, Kim Kwang Raymond; Wang, Huaqun (September 24, 2018). "Security and Privacy Issues for IoT and Fog Computing". Wireless communication and mobile computers. 2018: 1-3 doi: 10.1155/2018/9373961. ISSN 1530-8669. ^ Morrissey, Janet (22 January 2019). "Buyers should be wary of joining the smart home crowd." New York Times. ISSN 0362-4331. Retrieved 26 February 2020 ^ Ahmadi, Mohsen; Kiai, Panthea; Emamdoust, Navid (2021). SN4KE: Practical Binary Level Mutation Testing (PDF) (MSc). NDSS Symposium 2021. ↑ Clearfield, Christopher (26 June 2013). "Rethinking IoT security". Harvard Business Review blog. ^ Witkowski, Adriano; Santin, Altair; Abreu, Wilmar; Marinovski, João (2014). "IdM and Key-Based Authentication Technique to Enable Single Sign-On in the Internet of Things". 2015 IEEE Global Communications Conference (GLOBECOM). pp. 1-6.ISBN 978-1-4799-5952-5. S2CID 8108114. ↑ Steinberg, Joseph (January 27, 2014). “These devices can spy on you (even in your own home).” Forbes. ^ Retrieved May 27, 2014. ↑ Greenberg, Andy (July 21, 2015). "Hackers remotely kill highway jeep - with me in it". Wire. Retrieved July 21, 2015. ↑ Scientific American, April 2015, p. 68. ↑ Lucas, George (June 2015). Cyber-Physical Attacks An invisible threat is on the rise. Oxford, UK: Butterworth-Heinemann (Elsevier). p. 65 ISBN 9780128012901. ↑ Wolfe, Nicky (October 26, 2016). According to experts, the DDoS attack that disrupted the Internet was the largest attack of its kind in history. Goalie. ^ a b c e f Antonakakis, Manos; April, Tim; Bailey, Michael; Bernhardt, Matt; Burstein, Eli; Cochran, James; Durumeric, Zakir; Halderman, J. Alex; Invernici, Luka (August 18, 2017). Understanding the Mirai Botnet (PDF). Usniks. ISBN 978-1-931971-40-9. Retrieved May 13, 2018. ^ "Antipatterns" that turned IoT into Internet of Crap/Boing Boing. boingboing.net. May 3, 2017. ↑ Ali, Junade (May 2, 2017). "IoT security anti-pattern". Cloudflare blog. ↑ Schneier, Bruce (October 6, 2016). "We must save the Internet from the Internet of Things." Motherboard. ^ "2025 Global Breakthrough Technology Trends". (PDF). National Intelligence Council (NIC). April 2008 p. 27 ^ Ackerman, Spencer (March 15, 2012). "CIA chief: We'll spy on you using the dishwasher". WIRE. Retrieved June 26, 2015. ^ "The Bells Have Eyes: The Privacy Battle Rages Over Home Security Cameras". Washington Post. Retrieved February 3, 2019. Mozilla Hacks is a blog for web developers. ^ "Step Into Innovation". ^ "Global IoT security market to reach $29.2 billion by 2022". ^ Branch, Mark (September 23, 2015). "Smart devices to improve security". BBC news. ^ "Executive Committee". Internet of Things Security Foundation. ↑ Schneier, Bruce (February 1, 2017). "Security and^ 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, ISBN 978-3-030-30522-2, S2CID 202550425^a bc Nguyen, Dang Tu; Song, Chengyu, V Edward, J Zhiyanth; Berta;; McDaniel, Patrick (2018). IoTSan: Strengthening the Security of IoT Systems Proceedings of the 14th International Conference on Emerging Network EXperiments and Technologies (CONEXT '18) Heraklion, Greece arXiv:1810.09551.doi:10.123141/38480141/38480141/38480141/3 arXiv:1810.095 SmartThings.com.^ "HomeKit â Apple Developers".developer.apple.com. Bibliography developer.amazon.com.^ab Fielding, Roy Thomas (2000)."Architectural Styles and Designing Web Software Architectures" (PDF).University of California, Irvine.^ Littman, Michael; Kortchmar, Samuel (June 11, 2014). "The path to a programmable shed". Retrieved June 14, 2014. ^ Finley, Klint (May 6, 2014). "The Internet of Things could flood our environment with gadgets." Wired. "Chapter 11: Responsible IoT Design" In Rowland C, Goodman E, Charlier M et al. (eds.) Connected Product Design: UX for IoT Stuff for Consumers O'Reilly Media pp 457-64 ISBN 9781449372569 ^ Gilbert, Arlo (April 3, 2016) "When Tony Fadell sold me a can of hummus. Retrieved April 7, 2016. ^ a b c Walsh, Kit (April 5, 2016). "Nest reminds customers that ownership is not what it used to be." Frontier Foundation. Retrieved April 7, 2016. ^ a b c d "Taming the zoo of IoT terminology: What bed Does it all mean?". information age. Vitesse Media Sp. July 30, 2015. ^ a b "Technology Working Group". Industrial Internet Consortium. Retrieved March 21, 2017. ^ "Dictionary Technical Report". Industrial Internet Consortium. Retrieved March 21, 2017. ^Sense." IoT One. Retrieved 21 March 2017. ^ "IoT Terms Database". IoT One. Retrieved 21 March 2017. ^ "Quick Start Guide". IoT One. Retrieved 26 July 2018. ^ "Why the Internet of things is slow for consumers". Forbes. Retrieved 24 March 2017. ^ a b c d e "Everyone. Thing. Related. Study on 'Internet of Things' Adoption by Danish Companies' (PDF). Ericsson. Retrieved 2 May 2020 Cheng Yi, Wang, Chia Wei, Xu, Chia-Wei, Chen, Chong-Kuan, Shi, Shiuping (2014) "IoT Security: Current Issues and Research Opportunities" 7th International Conference IEEE on Service Oriented Computing and Applications, 2014 , pp. 230–234. doi: 10.1109/SOCA.2014.58. ISBN 978-1-4799-6833-6. S2CID 18445510. ^ Khan, Minhaj Ahmad; Salah, Khaled (2018). Blockchain Solutions and Open Problems". Next Generation Computing Systems, 82:395-411, doi:10.1016/j.future.2017.11.022, references Jia, Yang, Pan, Annie, Zhang, Yuqing, Liu, Peng (2019), Security and Privacy Impact of New IoT Features: New Threats, Existing Solutions, and Challenges to Address IEEE Journal Internet of Things 6(2):1606–1616. ar XIV: 1802.03110. doi: 10.1109/JIOT.2018.2847733. Bibliography Padaki, Sagar (2016). "Issues with data security and privacy when implementing IoT solutions". IEEE 2016 International Conference on the Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) as well as IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). pp. 410-415. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.97. ISBN 978-1-5090-5880-8. S2CID 34661195. ^ "California Regulatory Information". ^ "Oregon Legislature". ↑ a b c d Anthony, Scott (15 July 2016). "Breakthrough innovation: Kodak's downfall wasn't about technology". Harvard Business Review. Harvard Business Publishing. Retrieved March 30, 2017. ^ "World Economic Forum: Scaling is the Next Driver of Economic Growth".Industrial Revolution Technologies in Manufacturing” (PDF). World Economic Forum. January 2018, page 4. ^ at 11:15 am Cat Hall 23 May 2017 “Three-quarters of IoT projects fail, says Cisco.” www. theregister.co.uk Retrieved 29 January 2020. ^ Prasher, W. S.; Onu, Steven (September 15, 2020). "The Internet of Things (IoT) Revolution: Overcoming Governance Challenges". Journal of Contemporary Project Management. 8(2). , D.P.; Gita, M.K., editors (2017). The Internet of Things: New Advances and Expected Applications. Springer, pp. 311. ISBN 9783319534725. Internet of Things. singer. page 154 ISBN 9780128045053. Rowland, C., Goodman, E., Charlier, M., et al., eds. (2015). Related Product Development: UX for Consumer IoT. . O'Reilly Media. pp. 726 ISBN 9781449372569. Thomas, Jayant; Traukina, Alena (2018). Industrial Internet Application Development: Simplify IIoT development with the flexibility of the public cloud and your own cloud services. Publishing package. page 25 ISBN 978-1788298599. Stevenson, W. David (2018). A Smarter Future: How Your Business Can Benefit from the Internet of Things and Capture the Internet Economy. The Harper Collins Handbook. page 250 ISBN 9780814439777. Retrieved from " title=Internet_of_things&oldid=10372