THESIS TITLE
„Introduction in Internet of Things”

A Thesis presented to the Faculty of Sciences and Engineering Technologies
DEPARTMENT OF SYSTEMS ENGINEERING AND MANAGEMENT
Of
IICSE University
...a liberal arts education

Year Two Doctor of Philosophy PHD
in Systems Engineering and Management
Proposal Thesis

By
Dan Rîmniceanu
July 2023

CERTIFICATION OF APPROVAL

THESIS TITLE

„Introduction in Internet of Things**”**

By

Dan Rîmniceanu

VERIFIED STANFORD CENTER FOR PROFESSIONAL DEVELOPMENT OFFICIAL RECORD OF COMPLETION

STANFORD UNIVERSITY
Stanford Center for Professional Development
496 Lomita Mall, Durand Bdg., Stanford CA 94305

Record of Completion

06/Jun/2019
Page 1 of 1

Dan Rîmniceanu
s6
Bucharest, Bucuresti
061576 Romania

Account Number: X479322

Course No.	Title	Quarter	Completion Date	Grade	CEU(s)
XEE100 - 009	Introduction to Internet of Things	Spring 2018-19	06/Jun/2019	S	-

Paul Marca
Executive Director
Stanford Center For Professional Development
Stanford University

KEY TO RECORD OF COMPLETION ON FINAL PAGE

TABLE OF CONTENTS

Thank you.

IoT (Internet of Things) is an advanced automation and analytics system which exploits networking, sensing, big data, and artificial intelligence technology to deliver complete systems for a product or service. These systems allow greater transparency, control, and performance when applied to any industry or system.

IoT systems have applications across industries through their unique flexibility and ability to be suitable in any environment. They enhance data collection, automation, operations, and much more through smart devices and powerful enabling technology.

This tutorial aims to provide you with a thorough introduction to IoT. It introduces the key concepts of IoT, necessary in using and deploying IoT systems.

IoT systems allow users to achieve deeper automation, analysis, and integration within a system. They improve the reach of these areas and their accuracy. IoT utilizes existing and emerging technology for sensing, networking, and robotics.

IoT exploits recent advances in software, falling hardware prices, and modern attitudes towards technology. Its new and advanced elements bring major changes in the delivery of products, goods, and services; and the social, economic, and political impact of those changes.

IoT − Key Features

The most important features of IoT include artificial intelligence, connectivity, sensors, active engagement, and small device use. A brief review of these features is given below −

- **AI** − IoT essentially makes virtually anything “smart”, meaning it enhances every aspect of life with the power of data collection, artificial intelligence algorithms, and networks. This can mean something as simple as enhancing your refrigerator and cabinets to detect when milk and your favorite cereal run low, and to then place an order with your preferred grocer.

- **Connectivity** − New enabling technologies for networking, and specifically IoT networking, mean networks are no longer exclusively tied to major providers. Networks can exist on a much smaller and cheaper scale while still being practical. IoT creates these small networks between its system devices.

- **Sensors** − IoT loses its distinction without sensors. They act as defining instruments which transform IoT from a standard passive network of devices into an active system capable of real-world integration.

•**Active Engagement** − Much of today's interaction with connected technology happens through passive engagement. IoT introduces a new paradigm for active content, product, or service engagement.

•**Small Devices** − Devices, as predicted, have become smaller, cheaper, and more powerful over time. IoT exploits purpose-built small devices to deliver its precision, scalability, and versatility.

IoT − Advantages

The advantages of IoT span across every area of lifestyle and business. Here is a list of some of the advantages that IoT has to offer −

•**Improved Customer Engagement** − Current analytics suffer from blind-spots and significant flaws in accuracy; and as noted, engagement remains passive. IoT completely transforms this to achieve richer and more effective engagement with audiences.

•**Technology Optimization** − The same technologies and data which improve the customer experience also improve device use, and aid in more potent improvements to technology. IoT unlocks a world of critical functional and field data.
•**Reduced Waste** − IoT makes areas of improvement clear. Current analytics give us superficial insight, but IoT provides real-world information leading to more effective management of resources.

•**Enhanced Data Collection** − Modern data collection suffers from its limitations and its design for passive use. IoT breaks it out of those spaces, and places it exactly where humans really want to go to analyze our world. It allows an accurate picture of everything.

IoT − Disadvantages

Though IoT delivers an impressive set of benefits, it also presents a significant set of challenges. Here is a list of some its major issues −

•**Security** − IoT creates an ecosystem of constantly connected devices communicating over networks. The system offers little control despite any security measures. This leaves users exposed to various kinds of attackers.

•**Privacy** − The sophistication of IoT provides substantial personal data in extreme detail without the user's active participation.
•**Complexity** − Some find IoT systems complicated in terms of design, deployment, and maintenance given their use of multiple technologies and a large set of new enabling technologies.

•**Flexibility** − Many are concerned about the flexibility of an IoT system to integrate easily with another. They worry about finding themselves with several conflicting or locked systems.

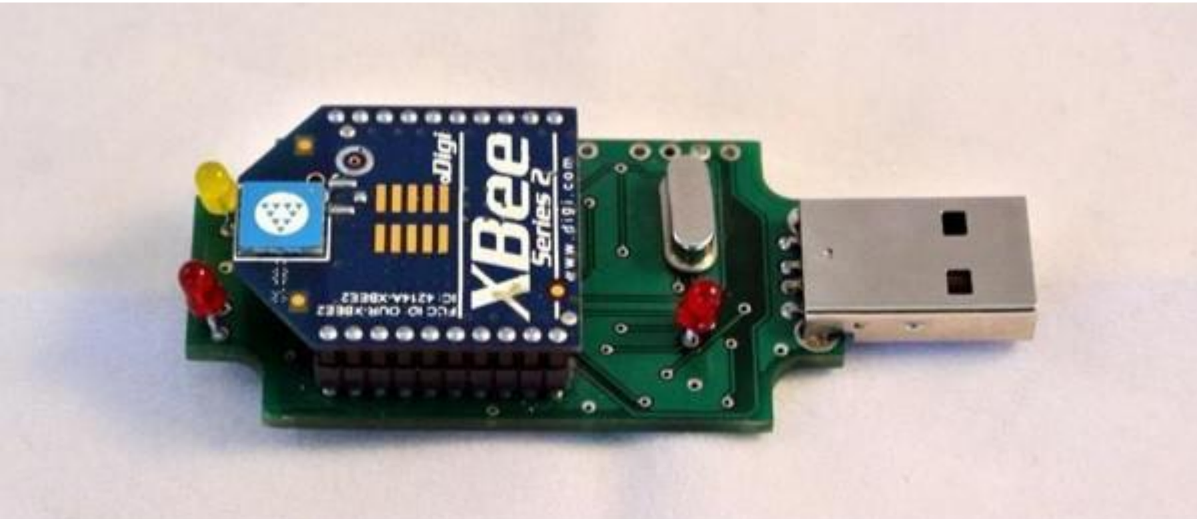
•**Compliance** − IoT, like any other technology in the realm of business, must comply with regulations. Its complexity makes the issue of compliance seem incredibly challenging when many consider standard software compliance a battle.

Internet of Things – Hardware

The hardware utilized in IoT systems includes devices for a remote dashboard, devices for control, servers, a routing or bridge device, and sensors. These devices manage key tasks and functions such as system activation, action specifications, security, communication, and detection to support-specific goals and actions.

IoT − Sensors

The most important hardware in IoT might be its sensors. These devices consist of energy modules, power management modules, RF modules, and sensing modules. RF modules manage communications through their signal processing, WiFi, ZigBee, Bluetooth, radio transceiver, duplexer, and BAW.



The sensing module manages sensing through assorted active and passive measurement devices. Here is a list of some of the measurement devices used in IoT −

S.No Devices

1. accelerometers temperature sensors

2. magnetometer proximity sensors s

3. gyroscopes image sensors acoustic

4. light sensors sensors

5. pressure gas RFID sensors

sensors
humidity
6. micro flow sensors
sensors

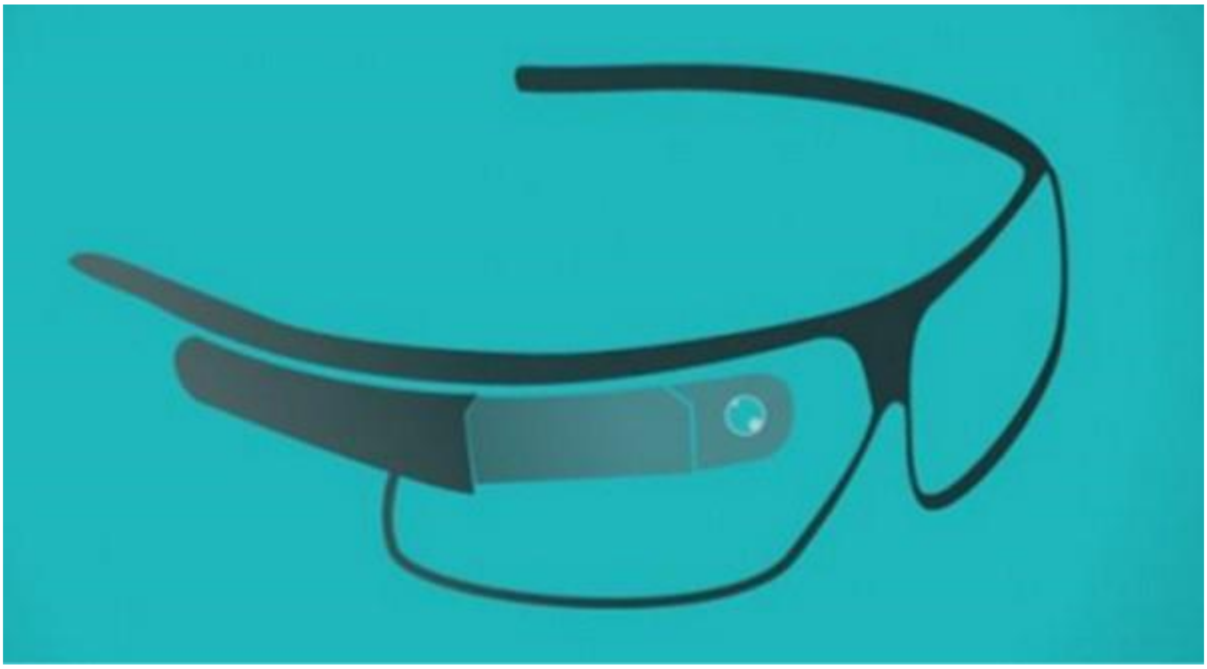
Wearable Electronics

Wearable electronic devices are small devices worn on the head, neck, arms, torso, and feet.

Smartwatches not only help us stay connected, but as a part of an IoT system, they allow access needed for improved productivity.

Current smart wearable devices include −

- **Head** − Helmets, glasses
- **Neck** − Jewelry, collars
- **Arm** − Watches, wristbands, rings
- **Torso** − Clothing, backpacks
- **Feet** − Socks, shoes



Smart glasses help us enjoy more of the media and services we value, and when part of an IoT system, they allow a new approach to productivity.

Standard Devices

The desktop, tablet, and cellphone remain integral parts of IoT as the command center and remotes.

•The **desktop** provides the user with the highest level of control over the system and its settings.

•The **tablet** provides access to the key features of the system in a way resembling the desktop, and also acts as a remote.
•The **cellphone** allows some essential settings modification and also provides remote functionality.

Other key connected devices include standard network devices like **routers** and **switches**.

Internet of Things – Software

IoT software addresses its key areas of networking and action through platforms, embedded systems, partner systems, and middleware. These individual and master applications are responsible for data collection, device integration, real-time analytics, and application and process extension within the IoT network. They exploit integration with critical business systems (e.g., ordering systems, robotics, scheduling, and more) in the execution of related tasks.

Data Collection

This software manages sensing, measurements, light data filtering, light data security, and aggregation of data. It uses certain protocols to aid sensors in connecting with real-time, machine-to-machine networks. Then it collects data from multiple devices and distributes it in accordance with settings. It also works in reverse by distributing data over devices. The system eventually transmits all collected data to a central server.

Device Integration

Software supporting integration binds (dependent relationships) all system devices to create the body of the IoT system. It ensures the necessary cooperation and stable networking between devices. These applications are the defining software technology of the IoT network because without them, it is not an IoT system. They manage the various applications, protocols, and limitations of each device to allow communication.

Real-Time Analytics

These applications take data or input from various devices and convert it into viable actions or clear patterns for human analysis. They analyze information based on various settings and designs in order to perform automation-related tasks or provide the data required by industry.

Application and Process Extension

These applications extend the reach of existing systems and software to allow a wider, more effective system. They integrate predefined devices for specific purposes such as allowing certain mobile devices or engineering instruments access. It supports improved productivity and more accurate data collection.

IoT software addresses its key areas of networking and action through platforms, embedded systems, partner systems, and middleware. These individual and master applications are responsible for data collection, device integration, real-time analytics, and application and process extension within the IoT network. They exploit integration with critical business systems (e.g., ordering systems, robotics, scheduling, and more) in the execution of related tasks.

Data Collection

This software manages sensing, measurements, light data filtering, light data security, and aggregation of data. It uses certain protocols to aid sensors in connecting with real-time, machine-to-machine networks. Then it collects data from multiple devices and distributes it in accordance with settings. It also works in reverse by distributing data over devices. The system eventually transmits all collected data to a central server.

Device Integration

Software supporting integration binds (dependent relationships) all system devices to create the body of the IoT system. It ensures the necessary cooperation and stable networking between devices. These applications are the defining software technology of the IoT network because without them, it is not an IoT system. They manage the various applications, protocols, and limitations of each device to allow communication.

Real-Time Analytics

These applications take data or input from various devices and convert it into viable actions or clear patterns for human analysis. They analyze information based on various settings and designs in order to perform automation-related tasks or provide the data required by industry.

Application and Process Extension

These applications extend the reach of existing systems and software to allow a wider, more effective system. They integrate predefined devices for specific purposes such as allowing certain mobile devices or engineering instruments access. It supports improved productivity and more accurate data collection.

Internet of Things - Technology and Protocols

IoT primarily exploits standard protocols and networking technologies. However, the major enabling technologies and protocols of IoT are RFID, NFC, low-energy Bluetooth, low-energy wireless, low-energy radio protocols, LTE-A, and WiFi-Direct. These technologies support the specific networking functionality needed in an IoT system in contrast to a standard uniform network of common systems.

NFC and RFID

RFID (radio-frequency identification) and NFC (near-field communication) provide simple, lowenergy, and versatile options for identity and access tokens, connection bootstrapping, and payments.

- •RFID technology employs 2-way radio transmitter-receivers to identify and track tags associated with objects.

- •NFC consists of communication protocols for electronic devices, typically a mobile device and a standard device.

Low-Energy Bluetooth

This technology supports the low-power, long-use need of IoT function while exploiting a standard technology with native support across systems.

Low-Energy Wireless

This technology replaces the most power hungry aspect of an IoT system. Though sensors and other elements can power down over long periods, communication links (i.e., wireless) must remain in listening mode. Low-energy wireless not only reduces consumption, but also extends the life of the device through less use.

Radio Protocols

ZigBee, Z-Wave, and Thread are radio protocols for creating low-rate private area networks. These technologies are low-power, but offer high throughput unlike many similar options. This increases the power of small local device networks without the typical costs.

LTE-A

LTE-A, or LTE Advanced, delivers an important upgrade to LTE technology by increasing not only its coverage, but also reducing its latency and raising its throughput. It gives IoT a tremendous power through expanding its range, with its most significant applications being vehicle, UAV, and similar communication.

WiFi-Direct

WiFi-Direct eliminates the need for an access point. It allows P2P (peer-to-peer) connections with the speed of WiFi, but with lower latency. WiFi-Direct eliminates an element of a network that often bogs it down, and it does not compromise on speed or throughput.

Internet of Things - Common Uses

IoT has applications across all industries and markets. It spans user groups from those who want to reduce energy use in their home to large organizations who want to streamline their operations. It proves not just useful, but nearly critical in many industries as technology advances and we move towards the advanced automation imagined in the distant future.

Engineering, Industry, and Infrastructure

Applications of IoT in these areas include improving production, marketing, service delivery, and safety. IoT provides a strong means of monitoring various processes; and real transparency creates greater visibility for improvement opportunities.

The deep level of control afforded by IoT allows rapid and more action on those opportunities, which include events like obvious customer needs, nonconforming product, malfunctions in equipment, problems in the distribution network, and more.

Example

Joan runs a manufacturing facility that makes shields for manufacturing equipment. When regulations change for the composition and function of the shields, the new appropriate requirements are automatically programmed in production robotics, and engineers are alerted about their approval of the changes.

Government and Safety

IoT applied to government and safety allows improved law enforcement, defense, city planning, and economic management. The technology fills in the current gaps, corrects many current flaws, and expands the reach of these efforts. For example, IoT can help city planners have a clearer view of the impact of their design, and governments have a better idea of the local economy.

Example

Joan lives in a small city. She’s heard about a recent spike in crime in her area, and worries about coming home late at night.

Local law enforcement has been alerted about the new “hot” zone through system flags, and they’ve increases their presence. Area monitoring devices have detected suspicious behavior, and law enforcement has investigated these leads to prevent crimes.

Home and Office

In our daily lives, IoT provides a personalized experience from the home to the office to the organizations we frequently do business with. This improves our overall satisfaction, enhances productivity, and improves our health and safety. For example, IoT can help us customize our office space to optimize our work.

Example

Joan works in advertising. She enters her office, and it recognizes her face. It adjusts the lighting and temperature to her preference. It turns on her devices and opens applications to her last working points.

Her office door detected and recognized a colleague visiting her office multiple times before she arrived. Joan’s system opens this visitor’s messages automatically.

Health and Medicine

IoT pushes us towards our imagined future of medicine which exploits a highly integrated network of sophisticated medical devices. Today, IoT can dramatically enhance medical research, devices, care, and emergency care. The integration of all elements provides more accuracy, more attention to detail, faster reactions to events, and constant improvement while reducing the typical overhead of medical research and organizations.

Example

Joan is a nurse in an emergency room. A call has come in for a man wounded in an altercation. The system recognized the patient and pulls his records. On the scene, paramedic equipment captures critical information automatically sent to the receiving parties at the hospital. The system analyzes the new data and current records to deliver a guiding solution. The status of the patient is updated every second in the system during his transport. The system prompts Joan to approve system actions for medicine distribution and medical equipment preparation.

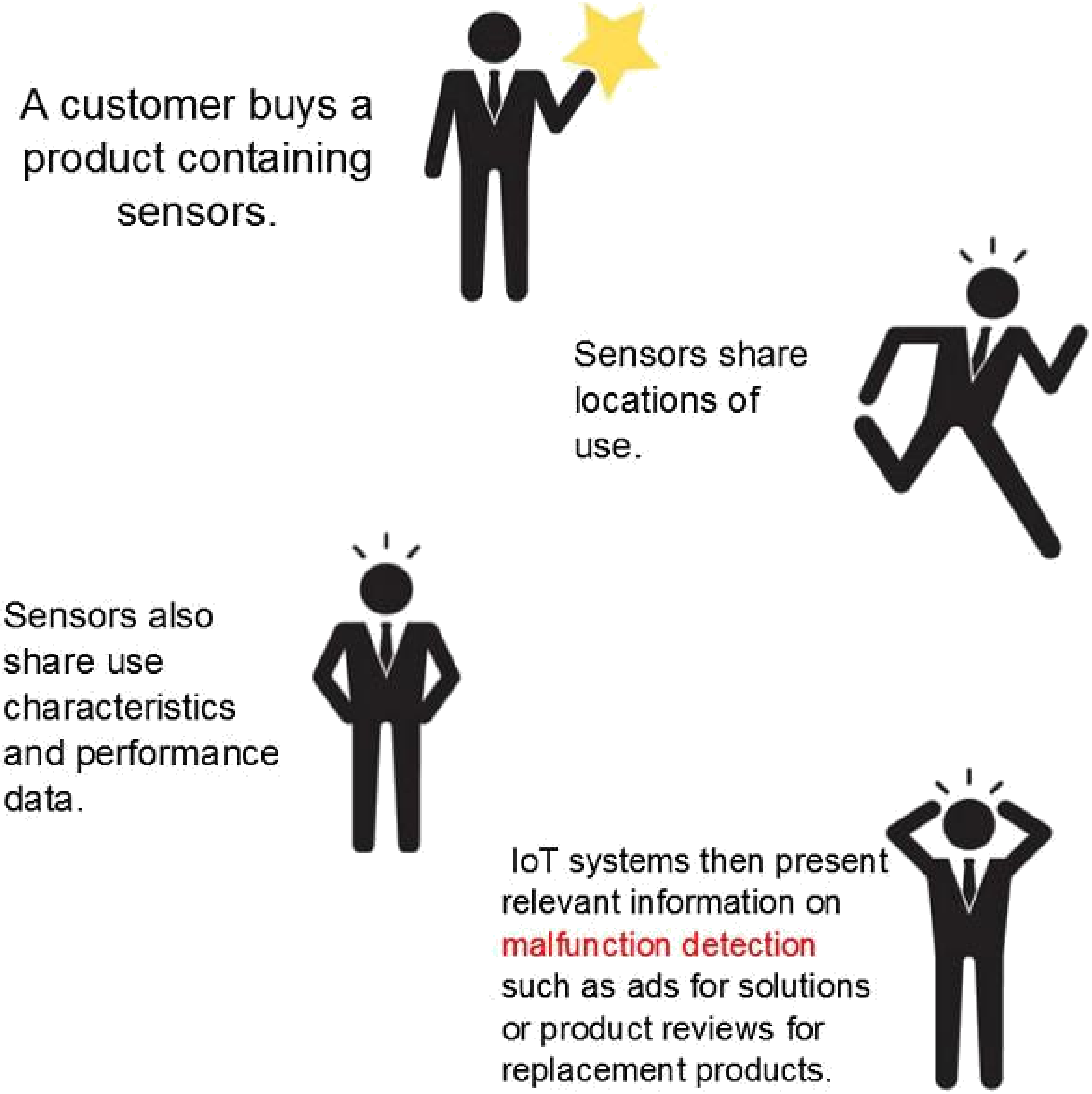
IoT - Media, Marketing, & Advertising

The applications of IoT in media and advertising involve a customized experience in which the system analyzes and responds to the needs and interests of each customer. This includes their general behavior patterns, buying habits, preferences, culture, and other characteristics.

Marketing and Content Delivery

IoT functions in a similar and deeper way to current technology, analytics, and big data. Existing technology collects specific data to produce related metrics and patterns over time, however, that data often lacks depth and accuracy. IoT improves this by observing more behaviors and analyzing them differently.

- This leads to more information and detail, which delivers more reliable metrics and patterns.
- It allows organizations to better analyze and respond to customer needs or preferences.
- It improves business productivity and strategy, and improves the consumer experience by only delivering relevant content and solutions.


A customer buys a product containing sensors.
Sensors share locations of use.
Sensors also share use characteristics and performance data.
IoT systems then present relevant information on malfunction detection such as ads for solutions or product reviews for replacement products.

Improved Advertising

Current advertising suffers from excess and poor targeting. Even with today's analytics, modern advertising fails. IoT promises different and personalized advertising rather than one-size-fitsall strategies. It transforms advertising from noise to a practical part of life because consumers interact with advertising through IoT rather than simply receiving it. This makes advertising more functional and useful to people searching the marketplace for solutions or wondering if those solutions exist.

IoT - Environmental Monitoring

The applications of IoT in environmental monitoring are broad − environmental protection, extreme weather monitoring, water safety, endangered species protection, commercial farming, and more. In these applications, sensors detect and measure every type of environmental change.

Air and Water Pollution

Current monitoring technology for air and water safety primarily uses manual labor along with advanced instruments, and lab processing. IoT improves on this technology by reducing the need for human labor, allowing frequent sampling, increasing the range of sampling and monitoring, allowing sophisticated testing on-site, and binding response efforts to detection systems. This allows us to prevent substantial contamination and related disasters.

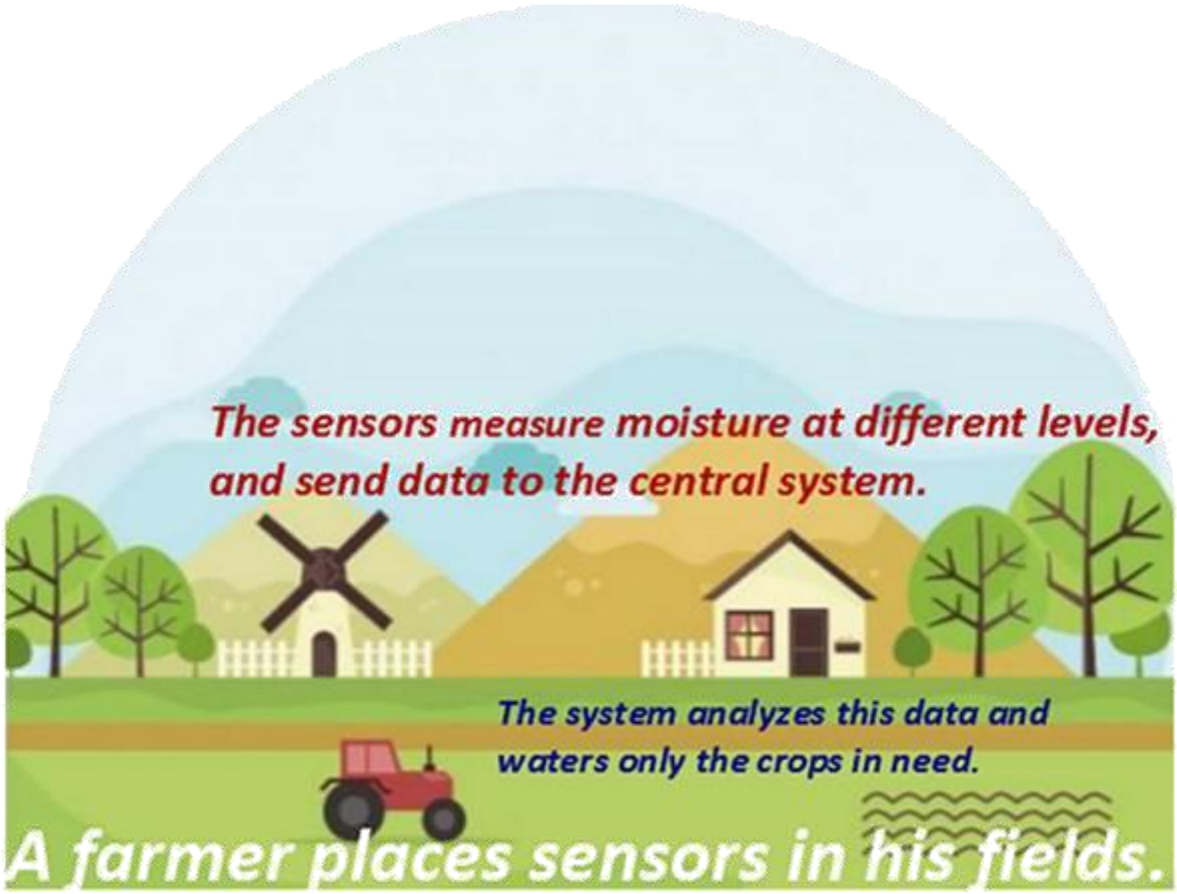
Extreme Weather

Though powerful, advanced systems currently in use allow deep monitoring, they suffer from using broad instruments, such as radar and satellites, rather than more granular solutions. Their instruments for smaller details lack the same accurate targeting of stronger technology.

New IoT advances promise more fine-grained data, better accuracy, and flexibility. Effective forecasting requires high detail and flexibility in range, instrument type, and deployment. This allows early detection and early responses to prevent loss of life and property.

Commercial Farming

Today's sophisticated commercial farms have exploited advanced technology and biotechnology for quite some time, however, IoT introduces more access to deeper automation and analysis.



Much of commercial farming, like weather monitoring, suffers from a lack of precision and requires human labor in the area of monitoring. Its automation also remains limited.

IoT allows operations to remove much of the human intervention in system function, farming analysis, and monitoring. Systems detect changes to crops, soil, environment, and more. They optimize standard processes through analysis of large, rich data collections. They also prevent health hazards (e.g., e. coli) from happening and allow better control.

IoT - Manufacturing Applications

Manufacturing technology currently in use exploits standard technology along with modern distribution and analytics. IoT introduces deeper integration and more powerful analytics. This opens the world of manufacturing in a way never seen before, as organizations become fullydeveloped for product delivery rather than a global network of suppliers, makers, and distributors loosely tied together.

Intelligent Product Enhancements

Much like IoT in content delivery, IoT in manufacturing allows richer insight in real-time. This dramatically reduces the time and resources devoted to this one area, which traditionally requires heavy market research before, during, and well after the products hit the market.

IoT also reduces the risks associated with launching new or modified products because it provides more reliable and detailed information. The information comes directly from market use and buyers rather than assorted sources of varied credibility.

Dynamic Response to Market Demands

Supplying the market requires maintaining a certain balance impacted by a number of factors such as economy state, sales performance, season, supplier status, manufacturing facility status, distribution status, and more. The expenses associated with supply present unique challenges given today's global partners. The associated potential or real losses can dramatically impact business and future decisions.

IoT manages these areas through ensuring fine details are managed more at the system level rather than through human evaluations and decisions. An IoT system can better assess and control the supply chain (with most products), whether demands are high or low.

Lower Costs, Optimized Resource Use, and Waste Reduction

IoT offers a replacement for traditional labor and tools in a production facility and in the overall chain which cuts many previously unavoidable costs; for example, maintenance checks or tests traditionally requiring human labor can be performed remotely with instruments and sensors of an IoT system.

IoT also enhances operation analytics to optimize resource use and labor, and eliminate various types of waste, e.g., energy and materials. It analyzes the entire process from the source point to its end, not just the process at one point in a particular facility, which allows improvement to have a more substantial impact. It essentially reduces waste throughout the network, and returns those savings throughout.

This XRS relay box connects all truck devices (e.g., diagnostics and driver cell) to the XRS fleet management supporting software, which allows data collection.

Improved Facility Safety

A typical facility suffers from a number of health and safety hazards due to risks posed by processes, equipment, and product handling. IoT aids in better control and visibility. Its monitoring extends throughout the network of devices for not only performance, but for dangerous malfunctions and usage. It aids (or performs) analysis and repair, or correction, of critical flaws.

Product Safety

Even the most sophisticated system cannot avoid malfunctions, nonconforming product, and other hazards finding their way to market. Sometimes these incidents have nothing to do with the manufacturing process, and result from unknown conflicts.

In manufacturing, IoT helps in avoiding recalls and controlling nonconforming or dangerous product distribution. Its high level of visibility, control, and integration can better contain any issues that appear.

Internet of Things - Energy Applications

The optimization qualities of IoT in manufacturing also apply to energy consumption. IoT allows a wide variety of energy control and monitoring functions, with applications in devices, commercial and residential energy use, and the energy source. Optimization results from the detailed analysis previously unavailable to most organizations and individuals.

Residential Energy

The rise of technology has driven energy costs up. Consumers search for ways to reduce or control consumption. IoT offers a sophisticated way to analyze and optimize use not only at device level, but throughout the entire system of the home. This can mean simple switching off or dimming of lights, or changing device settings and modifying multiple home settings to optimize energy use.

IoT can also discover problematic consumption from issues like older appliances, damaged appliances, or faulty system components. Traditionally, finding such problems required the use of often multiple professionals.

Commercial Energy

Energy waste can easily and quietly impact business in a major way, given the tremendous energy needs of even small organizations. Smaller organizations wrestle with balancing costs of business while delivering a product with typically smaller margins, and working with limited funding and technology. Larger organizations must monitor a massive, complex ecosystem of energy use that offers few simple, effective solutions for energy use management.

A smart-meter still requires a reader to visit the site. This automated meter reader makes visits unnecessary, and also allows energy companies to bill based on real-time data instead of estimates over time.

IoT simplifies the process of energy monitoring and management while maintaining a low cost and high level of precision. It addresses all points of an organization's consumption across devices. Its depth of analysis and control provides organizations with a strong means of managing their consumption for cost shaving and output optimization. IoT systems discover energy issues in the same way as functional issues in a complex business network, and provide solutions.

Reliability

The analytics and action delivered by IoT also help to ensure system reliability. Beyond consumption, IoT prevents system overloads or throttling. It also detects threats to system performance and stability, which protects against losses such as downtime, damaged equipment, and injuries.

Internet of Things - Healthcare Applications

IoT systems applied to healthcare enhance existing technology, and the general practice of medicine. They expand the reach of professionals within a facility and far beyond it. They increase both the accuracy and size of medical data through diverse data collection from large sets of real-world cases. They also improve the precision of medical care delivery through more sophisticated integration of the healthcare system.

Research

Much of current medical research relies on resources lacking critical real-world information. It uses controlled environments, volunteers, and essentially leftovers for medical examination. IoT opens the door to a wealth of valuable information through real-time field data, analysis, and testing.

IoT can deliver relevant data superior to standard analytics through integrated instruments capable of performing viable research. It also integrates into actual practice to provide more key information. This aids in healthcare by providing more reliable and practical data, and better leads; which yields better solutions and discovery of previously unknown issues.

It also allows researchers to avoid risks by gathering data without manufactured scenarios and human testing.

Devices

Current devices are rapidly improving in precision, power, and availability; however, they still offer less of these qualities than an IoT system integrating the right system effectively. IoT unlocks the potential of existing technology, and leads us toward new and better medical device solutions.

IoT closes gaps between equipment and the way we deliver healthcare by creating a logical system rather than a collection of tools. It then reveals patterns and missing elements in healthcare such as obvious necessary improvements or huge flaws.

The ClearProbe portable connected ultrasound device can use any computer anywhere as a supporting machine. The device sends all imaging records to the master system.

Care

Perhaps the greatest improvement IoT brings to healthcare is in the actual practice of medicine because it empowers healthcare professionals to better use their training and knowledge to solve problems. They utilize far better data and equipment, which gives them a window into blind spots and supports more swift, precise actions. Their decision-making is no longer limited by the disconnects of current systems, and bad data.

IoT also improves their professional development because they actually exercise their talent rather than spending too much time on administrative or manual tasks. Their organizational decisions also improve because technology provides a better vantage point.

Medical Information Distribution

One of the challenges of medical care is the distribution of accurate and current information to patients. Healthcare also struggles with guidance given the complexity of following guidance. IoT devices not only improve facilities and professional practice, but also health in the daily lives of individuals.

IoT devices give direct, 24/7 access to the patient in a less intrusive way than other options. They take healthcare out of facilities and into the home, office, or social space. They empower individuals in attending to their own health, and allow providers to deliver better and more granular care to patients. This results in fewer accidents from miscommunication, improved patient satisfaction, and better preventive care.

Emergency Care

The advanced automation and analytics of IoT allows more powerful emergency support services, which typically suffer from their limited resources and disconnect with the base facility. It provides a way to analyze an emergency in a more complete way from miles away. It also gives more providers access to the patient prior to their arrival. IoT gives providers critical information for delivering essential care on arrival. It also raises the level of care available to a patient received by emergency professionals. This reduces the associated losses, and improves emergency healthcare.

IoT - Building/Housing Applications

IoT applied to buildings and various structures allows us to automate routine residential and commercial tasks and needs in a way that dramatically improves living and working environments. This, as seen with manufacturing and energy applications, reduces costs, enhances safety, improves individual productivity, and enhances quality of life.

Environment and Conditioning

One of the greatest challenges in the engineering of buildings remains management of environment and conditions due to many factors at work. These factors include building materials, climate, building use, and more. Managing energy costs receives the most attention, but conditioning also impacts the durability and state of the structure.

IoT aids in improving structure design and managing existing structures through more accurate and complete data on buildings. It provides important engineering information such as how well a material performs as insulation in a particular design and environment.

Health and Safety

Buildings, even when constructed with care, can suffer from certain health and safety issues. These issues include poor performing materials, flaws that leave the building vulnerable to extreme weather, poor foundations, and more.

The Boss 220 smart plug allows the user to monitor, control, optimize, and automate all plug-in devices. Users employ their mobile device or desktop to view performance information and control devices from anywhere.

Current solutions lack the sophistication needed to detect minor issues before they become major issues, or emergencies. IoT offers a more reliable and complete solution by observing issues in a fine-grained way to control dangers and aid in preventing them; for example, it can measure changes in a system's state impacting fire safety rather than simply detecting smoke.

Productivity and Quality of Life

Beyond safety or energy concerns, most people desire certain comforts from housing or commercial spaces like specific lighting and temperature. IoT enhances these comforts by allowing faster and easier customizing.

Adjustments also apply to the area of productivity. They personalize spaces to create an optimized environment such as a smart office or kitchen prepared for a specific individual.

IoT - Transportation Applications

At every layer of transportation, IoT provides improved communication, control, and data distribution. These applications include personal vehicles, commercial vehicles, trains, UAVs, and other equipment. It extends throughout the entire system of all transportation elements such as traffic control, parking, fuel consumption, and more.

Rails and Mass Transit

Current systems deliver sophisticated integration and performance, however, they employ older technology and approaches to MRT. The improvements brought by IoT deliver more complete control and monitoring. This results in better management of overall performance, maintenance issues, maintenance, and improvements.

Mass transit options beyond standard MRT suffer from a lack of the integration necessary to transform them from an option to a dedicated service. IoT provides an inexpensive and advanced way to optimize performance and bring qualities of MRT to other transportation options like buses. This improves services and service delivery in the areas of scheduling, optimizing transport times, reliability, managing equipment issues, and responding to customer needs.

Road

The primary concerns of traffic are managing congestion, reducing accidents, and parking. IoT allows us to better observe and analyze the flow of traffic through devices at all traffic observation points. It aids in parking by making storage flow transparent when current methods offer little if any data.

This smart road sign receives data and modifications to better inform drivers and prevent congestion or accidents.

Accidents typically result from a number of factors, however, traffic management impacts their frequency. Construction sites, poor rerouting, and a lack of information about traffic status are all issues that lead to incidents. IoT provides solutions in the form of better information sharing with the public, and between various parties directly affecting road traffic.

Automobile

Many in the automotive industry envision a future for cars in which IoT technology makes cars “smart,” attractive options equal to MRT. IoT offers few significant improvements to personal vehicles. Most benefits come from better control over related infrastructure and the inherent flaws in automobile transport; however, IoT does improve personal vehicles as personal spaces. IoT brings the same improvements and customization to a vehicle as those in the home.

Commercial Transportation

Transportation benefits extend to business and manufacturing by optimizing the transport arm of organizations. It reduces and eliminates problems related to poor fleet management through better analytics and control such as monitoring idling, fuel consumption, travel conditions, and travel time between points. This results in product transportation operating more like an aligned service and less like a collection of contracted services.

Internet of Things - Education Applications

IoT in the classroom combines the benefits of IoT in content delivery, business, and healthcare. It customizes and enhances education by allowing optimization of all content and forms of delivery. It enables educators to give focus to individuals and their method. It also reduces costs and labor of education through automation of common tasks outside of the actual education process.

Education Organizations

Education organizations typically suffer from limited funding, labor issues, and poor attention to actual education. They, unlike other organizations, commonly lack or avoid analytics due to their funding issues and the belief that analytics do not apply to their industry.

IoT not only provides valuable insight, but it also democratizes that information through lowcost, low-power small devices, which still offer high performance. This technology aids in managing costs, improving the quality of education, professional development, and facility management improvement through rich examinations of key areas −

- Student response, performance, and behavior
- Instructor response, performance, and behavior
- Facility monitoring and maintenance
- Data from other facilities

Data informs them about ineffective strategies and actions, whether educational efforts or facility qualities. Removing these roadblocks makes them more effective.

Educators

Information provided by IoT empowers educators to deliver improved education. They have a window into the success of their strategies, their students' perspective, and other aspects of their performance. IoT relieves them of administrative and management duties, so they can focus on their mission. It automates manual and clerical labor, and facilitates supervising through features like system flags or controls to ensure students remain engaged.

A school in Richmond, California, embeds RFID chips in ID cards to track the presence of students. Even if students are not present for check-in, the system will track and log their presence on campus.

IoT provides instructors with easy access to powerful educational tools. Educators can use IoT to perform as a one-on-one instructor providing specific instructional designs for each pupil; for example, using data to determine the most effective supplements for each student, and autogenerating content from lesson materials on-demand for any student.

The application of technology improves the professional development of educators because they truly see what works, and learn to devise better strategies, rather than simply repeating old or ineffective methods.

IoT also enhances the knowledge base used to devise education standards and practices. Education research suffers from accuracy issues and a general lack of data. IoT introduces large high quality, real-world datasets into the foundation of educational design. This comes from IoT's unique ability to collect enormous amounts of varied data anywhere.

Personalized Education

IoT facilitates the customization of education to give every student access to what they need. Each student can control their experience and participate in instructional design, and much of this happens passively. The student simply utilizes the system, and performance data primarily shapes their design. This combined with organizational and educator optimization delivers highly effective education while reducing costs.

Internet of Things - Government Applications

IoT supports the development of smart nations and smart cities. This includes enhancement of infrastructure previously discussed (e.g., healthcare, energy, transportation, etc.), defense, and also the engineering and maintenance of communities.

City Planning and Management

Governing bodies and engineers can use IoT to analyze the often complex aspects of city planning and management. IoT simplifies examining various factors such as population growth, zoning, mapping, water supply, transportation patterns, food supply, social services, and land use. It gathers detailed data in these areas and produces more valuable and accurate information than current analytics given its ability to actually “live” with people in a city.


BOTTLES CANS PAPER
RECYCLING ONLY
BigBelly
SOLAR COMPACTOR

Smart trashcans in New York tell garbage collectors when they need to be emptied. They optimize trash service by ensuring drivers only make necessary stops, and drivers modify their route to reduce fuel consumption.

In the area of management, IoT supports cities through its implementation in major services and infrastructure such as transportation and healthcare. It also aids in other key areas like water control, waste management, and emergency management. Its real-time and detailed information facilitate more prompt decisions in contrast to the traditional process plagued by information lag, which can be critical in emergency management.

Standard state services are also improved by IoT, which can automate otherwise slow processes and trim unnecessary state expenses; for example, it can automate motor vehicle services for testing, permits, and licensing.

IoT also aids in urban improvement by skipping tests or poor research, and providing functional data for how the city can be optimized. This leads to faster and more meaningful changes.

Creating Jobs

IoT offers thorough economic analysis. It makes previous blind spots visible and supports better economic monitoring and modeling. It analyzes industry and the marketplace to spot opportunities for growth and barriers.

National Defense

National threats prove diverse and complicated. IoT augments armed forces systems and services, and offers the sophistication necessary to manage the landscape of national defense. It supports better protection of borders through inexpensive, high performance devices for rich control and observation.

IoT automates the protection tasks typically spread across several departments and countless individuals. It achieves this while improving accuracy and speed.

IoT - Law Enforcement Applications

IoT enhances law enforcement organizations and practice, and improves the justice system. The technology boosts transparency, distributes critical data, and removes human intervention where it proves unnecessary.

Policing

Law enforcement can be challenging. IoT acts as an instrument of law enforcement which reduces manual labor and subjective decisions through better data, information sharing, and advanced automation. IoT systems shave costs by reducing human labor in certain areas such as certain traffic violations.

IoT aids in creating better solutions to problems by using technology in the place of force; for example, light in-person investigations of suspicious activities can be replaced with remote observation, logged footage of violations, and electronic ticketing. It also reduces corruption by removing human control and opinion for some violations.

This dart planted in a truck gate prevents dangerous car chases. A patrol car launches the tracking dart which pierces the vehicle. Then the main system receives all data needed to locate the vehicle.

Court System

Current court systems utilize traditional technology and resources. They generally do not exploit modern analytics or automation outside of minor legal tasks. IoT brings superior analytics, better evidence, and optimized processes to court systems which accelerate processes, eliminate excessive procedures, manage corruption, reduce costs, and improve satisfaction.

In the criminal court system, this can result in a more effective and fair system. In routine court services, it introduces automation similar to that of common government office services; for example, IoT can automate forming an LLC.

IoT combined with new regulations can remove lawyers from many common legal tasks or reduce the need for their involvement. This reduces costs and accelerates many processes which often require months of traversing legal procedures and bureaucracy.

Internet of Things - Consumer Applications

Consumers benefit personally and professionally from the optimization and data analysis of IoT. IoT technology behaves like a team of personal assistants, advisors, and security. It enhances the way we live, work, and play.

Home

IoT takes the place of a full staff −

•**Butler −** IoT waits for you to return home, and ensures your home remains fully prepared. It monitors your supplies, family, and the state of your home. It takes actions to resolve any issues that appear.

•**Chef −** An IoT kitchen prepares meals or simply aids you in preparing them.

•**Nanny −** IoT can somewhat act as a guardian by controlling access, providing supplies, and alerting the proper individuals in an emergency.

•**Gardner −** The same IoT systems of a farm easily work for home landscaping.

•**Repairman −** Smart systems perform key maintenance and repairs, and also request them.

•**Security Guard −** IoT watches over you 24/7. It can observe suspicious individuals miles away, and recognize the potential of minor equipment problems to become disasters well before they do.

This smart, connected stove from Whirlpool allows two different heat settings on the same surface, remote monitoring, and remote control.

Work

A smart office or other workspace combines customization of the work environment with smart tools. IoT learns about you, your job, and the way you work to deliver an optimized environment. This results in practical accommodations like adjusting the room temperature, but also more advanced benefits like modifying your schedule and the tools you use to increase your output and reduce your work time. IoT acts as a manager and consultant capable of seeing what you cannot.

Play

IoT learns as much about you personally as it does professionally. This enables the technology to support leisure −

- **Culture and Night Life −** IoT can analyze your real-world activities and response to guide you in finding more of the things and places you enjoy such as recommending restaurants and events based on your preferences and experiences.

- **Vacations −** Planning and saving for vacations proves difficult for some, and many utilize agencies, which can be replaced by IoT.
- **Products and Services −** IoT offers better analysis of the products you like and need than current analytics based on its deeper access. It integrates with key information like your finances to recommend great solutions.

Internet of Things – Thingworx

Thingworx is a platform for the rapid development
devices. Its set of integrated IoT development and deployment of smart, connected production, and other aspects of IoT development. tools support connectivity, analysis,

It offers Vuforia for implementing augmented reality development, and Kepware for industrial connectivity. KEPServerEX provides a single point for data distribution, and facilitates interoperability when partnered with a ThingWorx agent.

Components

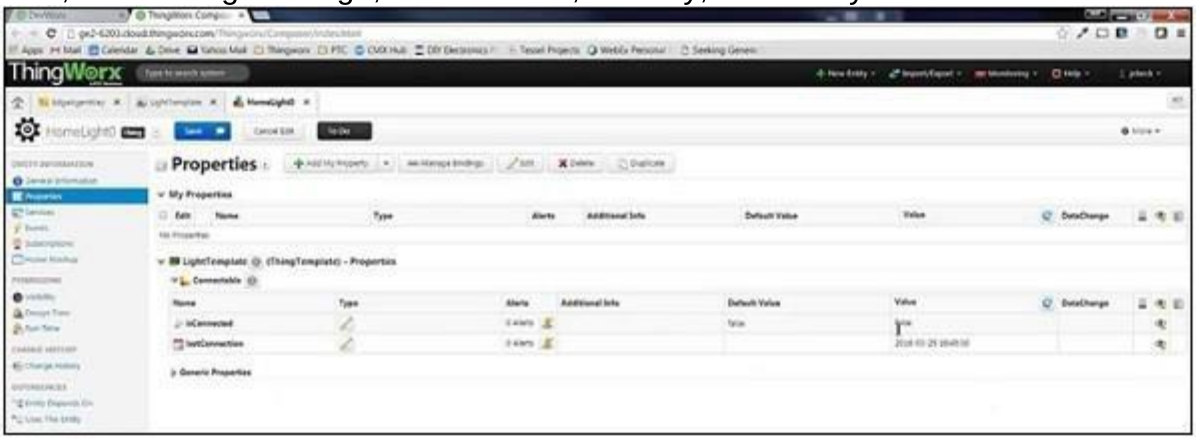
Thingworx offers several key tools for building applications. These tools include the Composer, the Mashup Builder, storage, a search engine, collaboration, and connectivity. The Composer provides a modeling environment for design testing. The Mashup Builder delivers easy dashboard building through common components (or widgets); for example, buttons, lists, wikis, gauges, and etc.

Thingworx uses a search engine known as SQUEAL, meaning Search, Query, and Analysis. Users employ SQUEAL in analyzing and filtering data, and searching records.

Interface

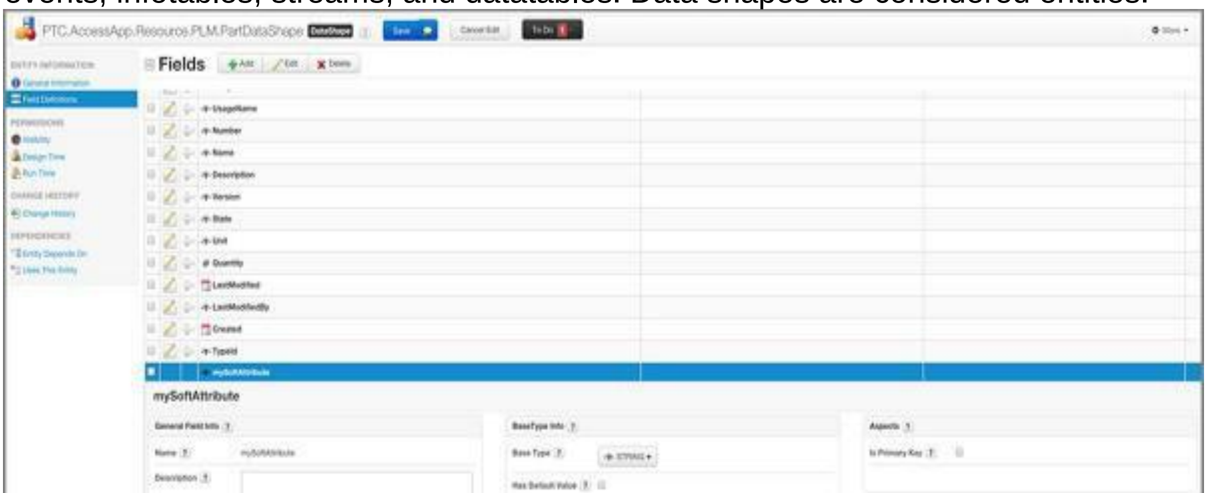
The ThingWorx platform uses certain terms you must familiarize yourself with. In the main screen's top menu, you search for **entities** or create them. “Entity” refers to something created in ThingWorx. You can also import/export files and perform various operations on them.

In the left menu, you find entity groups, which are used to produce models and visualize data; and manage storage, collaboration, security, and the system.



When you select the Modeling category in the menu, you begin the process by creating an entity. The entity can be any physical device or software element, and it produces an event on changes to its property values; for example, a sensor detects a temperature change. You can set **events** to trigger actions through a subscription which makes decisions based on device changes.

Data Shapes consist of one or more fields. They describe the data structure of custom events, infotables, streams, and datatables. Data shapes are considered entities.



Thing Templates and **Thing Shapes** allow developers to avoid repeating device property definitions in large IoT systems. Developers create Thing Templates to allow new devices to inherit properties. They use Thing Shapes to define Templates, properties, or execute services.

Note a Thing only inherits properties, services, events, and other qualities from a single template, however, Things and templates can inherit properties from multiple Thing Shapes.

Development

ThingWorx actually requires very little programming. Users connect devices, establish a data source, establish device behaviors, and build an interface without any coding. It also offers scalability appropriate for both hobbyist projects and industrial applications.

Cisco Virtualized Packet Core (VPC) is a technology providing all core services for 4G, 3G, 2G, WiFi, and small cell networks. It delivers networking functionality as virtualized services to allow greater scalability and faster deployment of new services at a reduced cost. It distributes and manages packet core functions across all resources, whether virtual or physical. Its key features include packet core service consolidation, dynamic scaling, and system agility.

Its technology supports IoT by offering network function virtualization, SDN (software-defined networking), and rapid networked system deployment. This proves critical because its virtualization and SDN support low-power, high flow networking, and the simple deployment of a wide variety of small devices. It eliminates many of the finer details of IoT systems, and conflicts, through consolidating into a single system and single technology for connecting and integrating all elements.

Use Case : Smart Transportation

Rail transportation provides a viable example of the power of VPC. The problems VPC solves relate to safety, mobility, efficiency, and service improvement −

- Rail applications use their own purpose-built networks, and suffer from interoperability issues; for example, trackside personnel cannot always communicate with local police due to different technologies.
- Determining if passengers need extra time to board remains a mostly manual task.
- Data updates, like schedules, remain manual.
- Each piece of equipment, e.g., a surveillance camera, requires its own network and power source.

A smart MRT sign in New York

VPC improves service by introducing direct communication over a standard network, more and automated monitoring, automatic data updates through smart signs, and native IP networks for all devices along with PoE (Power over Ethernet) technology. This results in passengers who feel safer, and enjoy a better quality service.

GE (General Electric) Predix is a software platform for data collection from industrial instruments. It provides a cloud-based PaaS (platform as a service), which enables industrial-grade analytics for operations optimization and performance management. It connects data, individuals, and equipment in a standard way.

Predix was designed to target factories, and give their ecosystems the same simple and productive function as operating systems that transformed mobile phones. It began as a tool for General Electric's internal IoT, specifically created to monitor products sold.

Ge Predix Partnered with Microsoft Azure

Microsoft's Azure is a cloud computing platform and supporting infrastructure. It provides PaaS and IaaS, and assorted tools for building systems. Predix, recently made available on Azure, exploits a host of extra features like AI, advanced data visualization, and natural language technology. Microsoft plans to eventually integrate Predix with its Azure IoT suite and Cortana Intelligence suite, and also their well-established business applications. Azure will also allow users to build applications using Predix data. Note AWS and Oracle also support Predix.

Developer Kits

GE offers inexpensive developer kits consisting of general components and an Intel Edison processor module. Developers have the options of a dual core board and a Raspberry Pi board. Developers need only provide an IP address, Ethernet connection, power supply, and light programming to set data collection.

The kit automatically establishes the necessary connection, registers with the central Predix system, and begins transmitting environmental data from sensors. Users subscribe to hardware/software output, and GE Digital owns and manages the hardware and software for the user.

This kit replaces the awkward and involved assemblies of simulations and testing environments. In other simulations, developers typically use a large set of software (one for each device), and specific configurations for each connection. They also program the monitoring of each device, which can sometimes take hours. The kit reduces much of the time spent performing these tasks from hours to only minutes.

Eclipse IoT is an ecosystem of entities (industry and academia) working together to create a foundation for IoT based exclusively on open source technologies. Their focus remains in the areas of producing open source implementations of IoT standard technology; creating open source frameworks and services for utilization in IoT solutions; and developing tools for IoT developers.

Smarthome Project

SmartHome is one of Eclipse IoT's major services. It aims to create a framework for building smart home solutions, and its focus remains heterogeneous environments, meaning assorted protocols and standards integration.

SmartHome provides uniform device and information access to facilitate interaction between devices. It consists of OSGi bundles capable of deployment in an OSGi runtime, with OSGi services defined as extension points.

OSGi bundles are Java class groups and other resources, which also include detailed manifest files. The manifest contains information on file contents, services needed to enhance class behavior, and the nature of the aggregate as a component. Review an example of a manifest below −

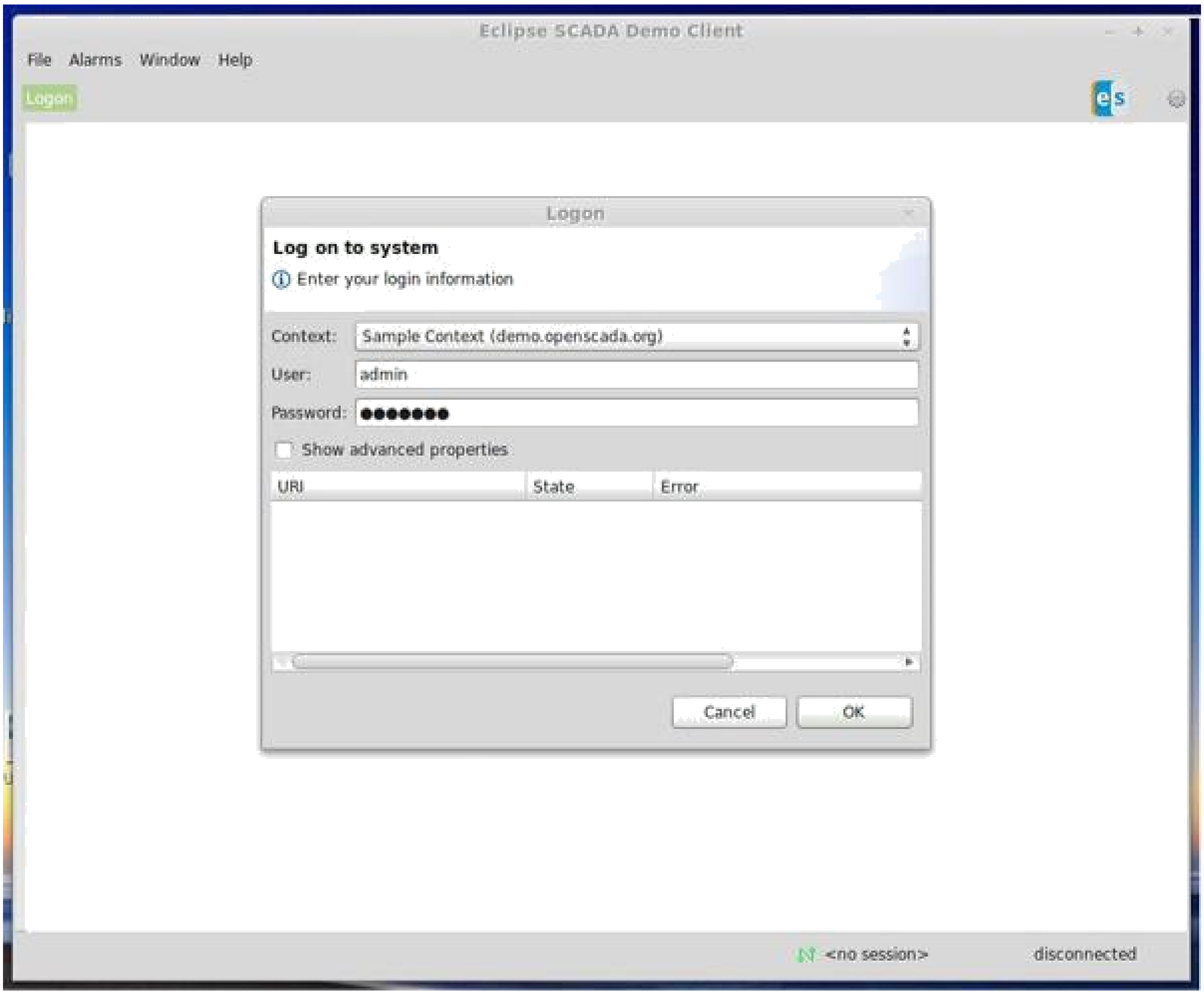
```
Bundle-Name : Hi Everyone                    // Bundle Name

Bundle-SymbolicName : xyz.xyz.hievery1          // Header specifying an identifier
Bundle-Description : A Hi Everyone bundle       // Functionality description
Bundle-ManifestVersion : 2                      // OSGi specification
Bundle-Version : 1.0.0                          // Version number of bundle
Bundle-Activator : xyz.xyz.Activator            // Class invoked on bundle activation
Export-Package : xyz.xyz.helloworld;version = "1.0.0" // Java packages available
externally

Import-Package : org.osgi.framework;version = "1.3.0" // Java packages needed from
// external source
```

Eclipse SCADA

Eclipse SCADA, another major Eclipse IoT service, delivers a means of connecting various industrial instruments to a shared communication system. It also post-processes data and sends data visualizations to operators. It uses a SCADA system with a communication service, monitoring system, archive, and data visualization.



It aims to be a complete, state-of-the-art open source SCADA system for developing custom solutions. Its supported technologies and tools include shell applications, JDBC, Modbus TCP and RTU, Simatic S7 PLC, OPC, and SNMP.

Contiki is an operating system for IoT that specifically targets small IoT devices with limited memory, power, bandwidth, and processing power. It uses a minimalist design while still packing the common tools of modern operating systems. It provides functionality for management of programs, processes, resources, memory, and communication.

Contiki

It owes its popularity to being very lightweight (by modern standards), mature, and flexible.

Many academics, organization researchers, and professionals consider it a go-to OS.

Contiki only requires a few kilobytes to run, and within a space of under 30KB, it fits its entire operating system − a web browser, web server, calculator, shell, telnet client and daemon, email client, vnc viewer, and ftp. It borrows from operating systems and development strategies from decades ago, which easily exploited equally small space.

Contiki Communication

Contiki supports standard protocols and recent enabling protocols for IoT −

•**uIP (for IPv4)** − This TCP/IP implementation supports 8-bit and 16-bit microcontrollers.

•**uIPv6 (for IPv6) −** This is a fully compliant IPv6 extension to uIP.

•**Rime** − This alternative stack provides a solution when IPv4 or IPv6 prove prohibitive. It offers a set of primitives for low-power systems.

•**6LoWPAN −** This stands for IPv6 over low-power wireless personal area networks. It provides compression technology to support the low data rate wireless needed by devices with limited resources.
•**RPL −** This distance vector IPv6 protocol for LLNs (low-power and lossy networks) allows the best possible path to be found in a complex network of devices with varied capability.

•**CoAP −** This protocol supports communication for simple devices, typically devices requiring heavy remote supervision.

Dynamic Module Loading

Dynamic module loading and linking at run-time supports environments in which application behavior changes after deployment. Contiki's module loader loads, relocates, and links ELF files.

The Cooja Network Simulator

Cooja, the Contiki network simulator, spawns an actual compiled and working Contiki system controlled by Cooja.

Using Cooja proves simple. Simply create a new mote type by selecting the **Motes** menu and **Add Motes → Create New Mote Type**. In the dialog that appears, you choose a name for the mote, select its firmware, and test its compilation.

Every connected device creates opportunities for attackers. These vulnerabilities are broad, even for a single small device. The risks posed include data transfer, device access, malfunctioning devices, and always-on/always-connected devices.

The main challenges in security remain the security limitations associated with producing lowcost devices, and the growing number of devices which creates more opportunities for attacks.

Security Spectrum

The definition of a secured device spans from the most simple measures to sophisticated designs. Security should be thought of as a spectrum of vulnerability which changes over time as threats evolve.

Security must be assessed based on user needs and implementation. Users must recognize the impact of security measures because poorly designed security creates more problems than it solves.

Example − A German report revealed hackers compromised the security system of a steel mill. They disrupted the control systems, which prevented a blast furnace from being shut down properly, resulting in massive damage. Therefore, users must understand the impact of an attack before deciding on appropriate protection.

Challenges

Beyond costs and the ubiquity of devices, other security issues plague IoT −

- **Unpredictable Behavior** − The sheer volume of deployed devices and their long list of enabling technologies means their behavior in the field can be unpredictable. A specific system may be well designed and within administration control, but there are no guarantees about how it will interact with others.

•**Device Similarity −** IoT devices are fairly uniform. They utilize the same connection technology and components. If one system or device suffers from a vulnerability, many more have the same issue.

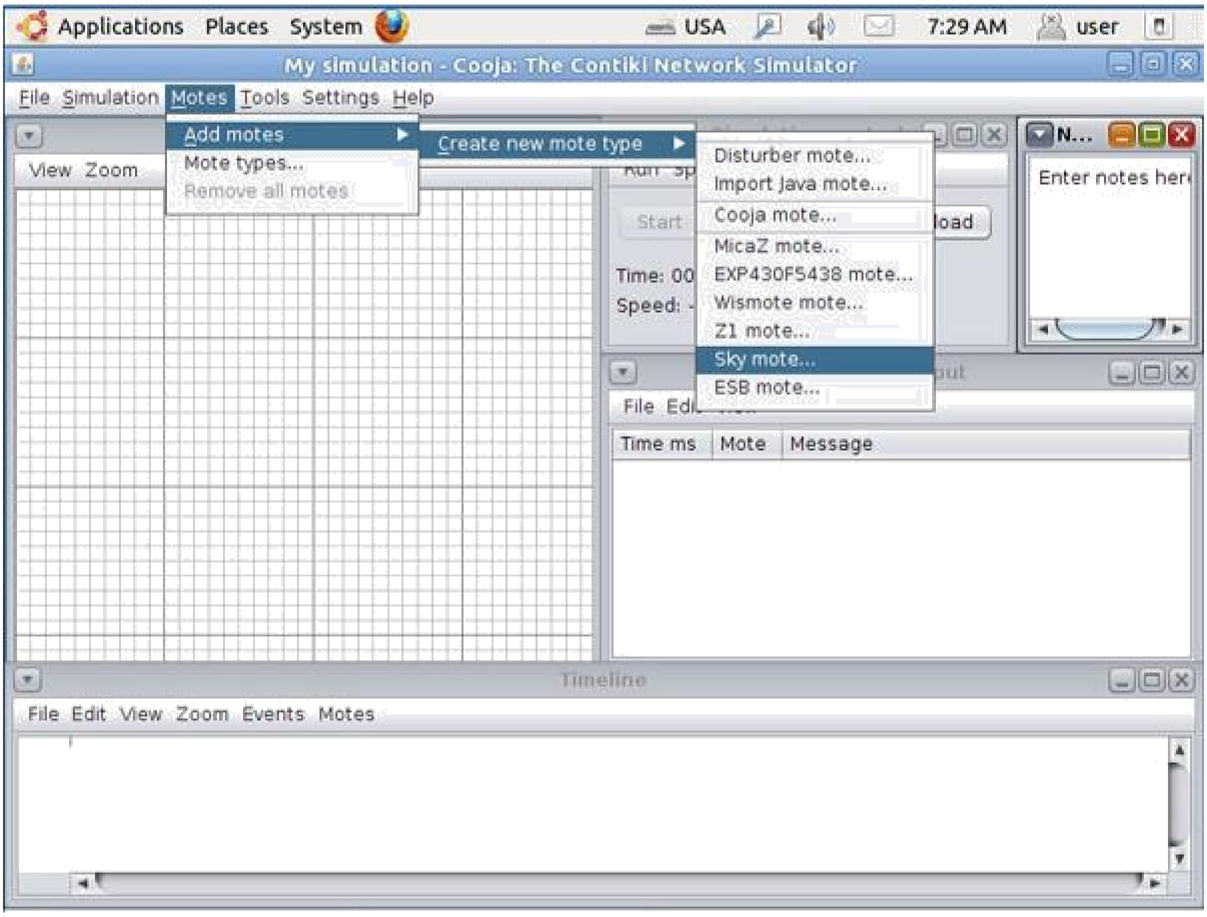
•**Problematic Deployment −** One of the main goals of IoT remains to place advanced networks and analytics where they previously could not go. Unfortunately, this creates the problem of physically securing the devices in these strange or easily accessed places.

•**Long Device Life and Expired Support −** One of the benefits of IoT devices is longevity, however, that long life also means they may outlive their device support. Compare this to traditional systems which typically have support and upgrades long after many have stopped using them. Orphaned devices and abandonware lack the same security hardening of other systems due to the evolution of technology over time.

•**No Upgrade Support −** Many IoT devices, like many mobile and small devices, are not designed to allow upgrades or any modifications. Others offer inconvenient upgrades, which many owners ignore, or fail to notice.

•**Poor or No Transparency −** Many IoT devices fail to provide transparency with regard to their functionality. Users cannot observe or access their processes, and are left to assume how devices behave. They have no control over unwanted functions or data collection; furthermore, when a manufacturer updates the device, it may bring more unwanted functions.

•**No Alerts −** Another goal of IoT remains to provide its incredible functionality without being obtrusive. This introduces the problem of user awareness. Users do not monitor the devices or know when something goes wrong. Security breaches can persist over long periods without detection.



After creation, add motes by clicking **Create**. A new mote type will appear to which you can attach nodes. The final step requires saving your simulation file for future use.

The security flaws of IoT and its ability to perform certain tasks open the door to any associated liability. The three main areas of concern are device malfunction, attacks, and data theft. These issues can result in a wide variety of damages.

Device Malfunction

IoT introduces a deeper level of automation which can have control over critical systems, and systems impacting life and property. When these systems fail or malfunction, they can cause substantial damage; for example, if an IoT furnace control system experiences a glitch, it may fail in an unoccupied home and cause frozen pipes and water damage. This forces organizations to create measures against it.

This smart thermostat allows attackers to gain remote access, and breach the rest of the network.

Cyber Attacks

IoT devices expose an entire network and anything directly impacted to the risk of attacks. Though those connections deliver powerful integration and productivity, they also create the perfect opportunity for mayhem like a hacked stove or fire safety sprinkler system. The best measures against this address the most vulnerable points, and provide custom protections such as monitoring and access privileges.

Some of the most effective measures against attacks prove simple −

•**Built-in Security** − Individuals and organizations should seek hardened devices, meaning those with security integrated in the hardware and firmware.

•**Encryption** − This must be implemented by the manufacturer and through user systems.
•**Risk Analysis** − Organizations and individuals must analyze possible threats in designing their systems or choosing them.

•**Authorization –** Devices, whenever possible, must be subject to privilege policies and access methods.

Bitdefender BOX secures all connected devices in the home.

Data Theft

Data, IoT's strength and weakness, proves irresistible to many. These individuals have a number of reasons for their interest − the value of personal data to marketing/advertising, identity theft, framing individuals for crimes, stalking, and a bizarre sense of satisfaction. Measures used to fight attacks are also effective in managing this threat.

The Predix developer kit

The kit also includes software components for designing an IoT application that partners with Predix services. GE plans to release other versions of the kit for different applications.

History[edit]

The concept of a network of smart devices was discussed as early as 1982, with a modified Coke vending machine at Carnegie Mellon University becoming the first Internet-connected appliance,[6] able to report its inventory and whether newly loaded drinks were cold or not.[7] Mark Weiser's 1991 paper on ubiquitous computing, "The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of the IoT. [8][9] In 1994, Reza Raji described the concept in *IEEE Spectrum* as "[moving] small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories". [10] Between 1993 and 1997, several companies proposed solutions like Microsoft's at Work or Novell's NEST. The field gained momentum when Bill Joy envisioned device-to-device communication as a part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999.[11]

The term "Internet of things" was likely coined by Kevin Ashton of Procter & Gamble, later MIT 's Auto -ID Center, in 1999,[12] though he prefers the phrase "Internet *for* things".[13] At that point, he viewed Radio-frequency identification (RFID) as essential to the Internet of things,[14] which would allow computers to manage all individual things. [15] [16][17]

A research article mentioning the Internet of Things was submitted to the conference for Nordic Researchers in Norway, in June 2002,[18] which was preceded by an article published in Finnish in January 2002.[19] The implementation described there was developed by Kary Främling and his team at Helsinki University of Technology and more closely matches the modern one, i.e. an information system infrastructure for implementing smart, connected objects.[20]

Defining the Internet of things as "simply the point in time when more 'things or objects' were connected to the Internet than people", Cisco Systems estimated that the IoT was "born" between 2008 and 2009, with the things/people ratio growing from 0.08 in 2003 to 1.84 in 2010.[21]

Applications[edit]

A Nest learning thermostat reporting on energy usage and local weather.

A Ring doorbell connected to the Internet

An August Home smart lock connected to the Internet

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

Consumer applications[edit]

A growing portion of IoT devices are created for consumer use, including connected vehicles, home automation, wearable technology (as part of Internet of Wearable Things (IoWT)[25]), connected health, and appliances with remote monitoring capabilities.[26]

Smart home[edit]

IoT devices are a part of the larger concept of home automation, which can include lighting, heating and air conditioning, media and security systems. [27] [28] Long-term benefits could include energy savings by automatically ensuring lights and electronics are turned off.

A smart home or automated home could be based on a platform or hubs that control smart devices and appliances.[29] For instance, using Apple's HomeKit, manufacturers can have their home products and accessories controlled by an application in iOS devices such as the iPhone and the Apple Watch.[30][31] This could be a dedicated app or iOS native applications such as Siri.[32] This can be demonstrated in the case of Lenovo's Smart Home Essentials, which is a line of smart home devices that are controlled through Apple's Home app or Siri without the need for a Wi-Fi bridge.[32] There are also dedicated smart home hubs that are offered as standalone platforms to connect different smart home products and these include the Amazon Echo , Google Home , Apple's HomePod, and Samsung's SmartThings Hub.[33] In addition to the commercial systems, there are many non-proprietary, open source ecosystems; including Home Assistant, OpenHAB and Domoticz.[34] [35]

Elder care[edit]

One key application of a smart home is to provide assistance for those with disabilities and elderly individuals. These home systems use assistive technology to accommodate an owner's specific disabilities.[36] Voice control can assist users with sight and mobility limitations while alert systems can be connected directly to cochlear implants worn by hearing-impaired users.[37] They can also be equipped with additional safety features. These features can include sensors that monitor for medical emergencies such as falls or seizures.[38] Smart home technology applied in this way can provide users with more freedom and a higher quality of life.[36]

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

Commercial application[edit]

Medical and healthcare[edit]

The **Internet of Medical Things** (also called the **internet of health things**) is an application of the IoT for medical and health related purposes, data collection and analysis for research, and monitoring. [39] [40] [41] [42][43] This 'Smart Healthcare',[44] as it is also called, led to the creation of a digitized healthcare system, connecting available medical resources and healthcare services.[45]

IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids.[46] Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses.[39] A 2015 Goldman Sachs report indicated that healthcare IoT devices "can save the United States more than $300 billion in annual healthcare expenditures by increasing revenue and decreasing cost." [47][48] Moreover, the use of mobile devices to support medical follow-up led to the creation of 'm-health', used "to analyze, capture, transmit and store health statistics from multiple resources, including sensors and other biomedical acquisition systems".[49]

Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people regain lost mobility via therapy as well.[50] These sensors create a network of intelligent sensors that are able to collect, process, transfer, and analyse valuable information in different environments, such as connecting in-home monitoring devices to hospital-based systems.[44] Other consumer devices to encourage healthy living, such as connected scales or wearable heart monitors, are also a possibility with the IoT. [51] End-to-end health monitoring IoT platforms are also available for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements.[52]

Advances in plastic and fabric electronics fabrication methods have enabled ultra-low cost, use-and -throw IoMT sensors. These sensors, along with the required RFID electronics, can be fabricated on paper or e-textiles for wirelessly powered disposable sensing devices.[53] Applications have been established for point-of-care medical diagnostics, where portability and low system-complexity is essential.[54]

As of 2018 [update] IoMT was not only being applied in the clinical laboratory industry,[41] but also in the healthcare and health insurance industries. IoMT in the healthcare industry is now permitting doctors, patients, and others involved (i.e. guardians of patients, nurses, families, etc.) to be part of a system, where patient records are saved in a database, allowing doctors and the rest of the medical staff to have access to the patient's information.[45] Moreover, IoT-based systems are patient-centered, which involves being flexible to the patient's medical conditions.[45] IoMT in the insurance industry provides access to better and new types of dynamic information. This includes sensor-based solutions such as biosensors, wearables, connected health devices, and mobile apps to track customer behaviour. This can lead to more accurate underwriting and new pricing models.[55]

The application of the IOT in healthcare plays a fundamental role in managing chronic diseases and in disease prevention and control. Remote monitoring is made possible through the connection of powerful wireless solutions. The connectivity enables health practitioners to capture patient's data and applying complex algorithms in health data analysis.[56]

Transportation[edit]

Digital variable speed-limit sign.

The IoT can assist in the integration of communications, control, and information processing across various transportation systems. Application of the IoT extends to all aspects of transportation systems (i.e. the vehicle,[57] the infrastructure, and the driver or user). Dynamic interaction between these components of a transport system enables inter- and intra-vehicular communication,[58] smart traffic control, smart parking, electronic toll collection systems , logistics and fleet management, vehicle control, safety, and road assistance. [46][59] In Logistics and Fleet Management, for example, an IoT platform can continuously monitor the location and conditions of cargo and assets via wireless sensors and send specific alerts when management exceptions occur (delays, damages, thefts, etc.). This can only be possible with the IoT and its seamless connectivity among devices. Sensors such as GPS, Humidity, and Temperature send data to the IoT platform and then the data is analyzed and then sent to the users. This way, users can track the real-time status of vehicles and can make appropriate decisions. If combined with Machine Learning, then it also helps in reducing traffic accidents by introducing drowsiness alerts to drivers and providing self-driven cars too.

V2X communications[edit]

Main article: V2X

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

Building and home automation[edit]

IoT devices can be used to monitor and control the mechanical, electrical and electronic systems used in various types of buildings (e.g., public and private, industrial, institutions, or residential)[46] in home automation and building automation systems. In this context, three main areas are being covered in literature:[60]

- The integration of the Internet with building energy management systems in order to create energy efficient and IOT-driven "smart buildings".[60]
- The possible means of real-time monitoring for reducing energy consumption[61] and monitoring occupant behaviors.[60]
- The integration of smart devices in the built environment and how they might to know how to be used in future applications.[60]

Industrial applications[edit]

Main article: Industrial Internet of Things

Manufacturing[edit]

The IoT can realize the seamless integration of various manufacturing devices equipped with sensing, identification, processing, communication, actuation, and networking capabilities. Based on such a highly integrated smart cyberphysical space, it opens the door to create whole new business and market opportunities for manufacturing.[62] Network control and management of manufacturing equipment, asset and situation management, or manufacturing process control bring the IoT within the realm of industrial applications and smart manufacturing as well.[63] The IoT intelligent systems enable rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply chain networks, by networking machinery, sensors and control systems together.[46]

Digital control systems to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IoT.[64] But it also extends itself to asset management via predictive maintenance, statistical evaluation, and measurements to maximize reliability.[65] Industrial management systems can also be integrated with smart grids, enabling real-time energy optimization.

Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by a large number of networked sensors.[46]

Industrial IoT (IIoT) in manufacturing could generate so much business value that it will eventually lead to the Fourth Industrial Revolution, also referred to as Industry 4.0. The potential for growth from implementing IIoT may generate $12 trillion of global GDP by 2030.[66]

Design architecture of cyber-physical systems-enabled manufacturing system[67] Industrial big data analytics will play a vital role in manufacturing asset predictive maintenance, although that is not the only capability of industrial big data. [68][69] Cyber-physical systems (CPS) is the core technology of industrial big data and it will be an interface between human and the cyber world. Cyber-physical systems can be designed by following the *5C* (connection, conversion, cyber, cognition, configuration) architecture, [67] and it will transform the collected data into actionable information, and eventually interfere with the physical assets to optimize processes.

An IoT-enabled intelligent system of such cases was proposed in 2001 and later demonstrated in 2014 by the National Science Foundation Industry/University Collaborative Research Center for Intelligent Maintenance Systems (IMS) at the University of Cincinnati on a bandsaw machine in IMTS 2014 in Chicago. [70] [71][72] Bandsaw machines are not necessarily expensive, but the bandsaw belt expenses are enormous since they degrade much faster. However, without sensing and intelligent analytics, it can be only determined by experience when the band saw belt will actually break. The developed prognostics system will be able to recognize and monitor the degradation of band saw belts even if the condition is changing, advising users when is the best time to replace the belt. This will significantly improve user experience and operator safety and ultimately save on costs.[72]

Agriculture[edit]

There are numerous IoT applications in farming[73] such as collecting data on temperature, rainfall, humidity, wind speed, pest infestation, and soil content. This data can be used to automate farming techniques, take informed decisions to improve quality and quantity, minimize risk and waste, and reduce effort required to manage crops. For example, farmers can now monitor soil temperature and moisture from afar, and even apply IoT-acquired data to precision fertilization programs.[74]

In August 2018, Toyota Tsusho began a partnership with Microsoft to create fish farming tools using the Microsoft Azure application suite for IoT technologies related to water management. Developed in part by researchers from Kindai University, the water pump mechanisms use artificial intelligence to count the number of fish on a conveyor belt, analyze the number of fish, and deduce the effectiveness of water flow from the data the fish provide. The specific computer programs used in the process fall under the Azure Machine Learning and the Azure IoT Hub platforms.[75]

Infrastructure applications[edit]

Monitoring and controlling operations of sustainable urban and rural infrastructures like bridges, railway tracks and on- and offshore wind-farms is a key application of the IoT.[64] The IoT infrastructure can be used for monitoring any events or changes in structural conditions that can compromise safety and increase risk. The IoT can benefit the construction industry by cost saving, time reduction, better quality workday, paperless workflow and increase in productivity. It can help in taking faster decisions and save money with Real-Time Data Analytics. It can also be used for scheduling repair and maintenance activities in an efficient manner, by coordinating tasks between different service providers and users of these facilities.[46] IoT devices can also be used to control critical infrastructure like bridges to provide access to ships. Usage of IoT devices for monitoring and operating infrastructure is likely to improve incident management and emergency response coordination, and quality of service, up-times and reduce costs of operation in all infrastructure related areas.[76] Even areas such as waste management can benefit[77] from automation and optimization that could be brought in by the IoT.[78]

Metropolitan scale deployments[edit]

There are several planned or ongoing large-scale deployments of the IoT, to enable better management of cities and systems. For example, Songdo, South Korea, the first of its kind fully equipped and wired smart city, is gradually being built, with approximately 70 percent of the business district completed as of June 2018[update]. Much of the city is planned to be wired and automated, with little or no human intervention.[79]

Another application is a currently undergoing project in Santander, Spain. For this deployment, two approaches have been adopted. This city of 180,000 inhabitants has already seen 18,000 downloads of its city smartphone app. The app is connected to 10,000 sensors that enable services like parking search, environmental monitoring, digital city agenda, and more. City context information is used in this deployment so as to benefit merchants through a spark deals mechanism based on city behavior that aims at maximizing the impact of each notification.[80]

Other examples of large-scale deployments underway include the Sino-Singapore Guangzhou Knowledge City;[81] work on improving air and water quality, reducing noise pollution, and increasing transportation efficiency in San Jose, California;[82] and smart traffic management in western Singapore.[83] Using its RPMA (Random Phase Multiple Access) technology, San Diego-based Ingenu has built a nationwide public network [84] for low-bandwidth data transmissions using the same unlicensed 2.4 gigahertz spectrum as Wi-Fi. Ingenu's “Machine Network” covers more than a third of the US population across 35 major cities including San Diego and Dallas.[85] French company, Sigfox, commenced building an Ultra Narrowband wireless data network in the San Francisco Bay Area in 2014, the first business to achieve such a deployment in the U.S. [86][87] It subsequently announced it would set up a total of 4000 base stations to cover a total of 30 cities in the U.S. by the end of 2016, making it the largest IoT network coverage provider in the country thus far. [88][89] Cisco also participates in smart cities projects. Cisco has started deploying technologies for Smart Wi-Fi, Smart Safety & Security, Smart Lighting, Smart Parking, Smart Transports, Smart Bus Stops, Smart Kiosks, Remote Expert for Government Services (REGS) and Smart Education in the five km area in the city of Vijaywada.[90]

Another example of a large deployment is the one completed by New York Waterways in New York City to connect all the city's vessels and be able to monitor them live 24/7. The network was designed and engineered by Fluidmesh Networks, a Chicago-based company developing wireless networks for critical applications. The NYWW network is currently providing coverage on the Hudson River, East River, and Upper New York Bay. With the wireless network in place, NY Waterway is able to take control of its fleet and passengers in a way that was not previously possible. New applications can include security, energy and fleet management, digital signage, public Wi-Fi, paperless ticketing and others.[91]

Energy management[edit]

Significant numbers of energy-consuming devices (e.g. switches, power outlets, bulbs, televisions, etc.) already integrate Internet connectivity, which can allow them to communicate with utilities to balance power generation and energy usage[92] and optimize energy consumption as a whole.[46] These devices allow for remote control by users, or central management via a cloud-based interface, and enable functions like scheduling (e.g., remotely powering on or off heating systems, controlling ovens, changing lighting conditions etc.).[46] The smart grid is a utility-side IoT application; systems gather and act on energy and power-related information to improve the efficiency of the production and distribution of electricity.[92] Using advanced metering infrastructure (AMI) Internet-connected devices, electric utilities not only collect data from end-users, but also manage distribution automation devices like transformers.[46]

Environmental monitoring[edit]

Environmental monitoring applications of the IoT typically use sensors to assist in environmental protection[93] by monitoring air or water quality,[94] atmospheric or soil conditions,[95] and can even include areas like monitoring the movements of wildlife and their habitats.[96] Development of resource-constrained devices connected to the Internet also means that other applications like earthquake or tsunami early-warning systems can also be used by emergency services to provide more effective aid. IoT devices in this application typically span a large geographic area and can also be mobile.[46] It has been argued that the standardization IoT brings to wireless sensing will revolutionize this area.[97]

Living Lab

Another example of integrating the IoT is Living Lab which integrates and combines research and innovation process, establishing within a public-private-people-partnership.[98] There are currently 320 Living Labs that use the IoT to collaborate and share knowledge between stakeholders to co-create innovative and technological products. For companies to implement and develop IoT services for smart cities, they need to have incentives. The governments play key roles in smart cities projects as changes in policies will help cities to implement the IoT which provides effectiveness, efficiency, and accuracy of the resources that are being used. For instance, the government provides tax incentives and cheap rent, improves public transports, and offers an environment where start-up companies, creative industries, and multinationals may co-create, share common infrastructure and labor markets, and take advantages of locally embedded technologies, production process, and transaction costs.[98] The relationship between the technology developers and governments who manage city's assets, is key to provide open access of resources to users in an efficient way.

Trends and characteristics[edit]

Technology roadmap: Internet of things.

The IoT's major significant trend in recent years is the explosive growth of devices connected and controlled by the Internet. [99] The wide range of applications for IoT technology mean that the specifics can be very different from one device to the next but there are basic characteristics shared by most.

The IoT creates opportunities for more direct integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions. [100] [101] [102][103]

The number of IoT devices increased 31% year-over-year to 8.4 billion in the year 2017[104] and it is estimated that there will be 30 billion devices by 2020.[99] The global market value of IoT is projected to reach $7.1 trillion by 2020.[105]

Intelligence[edit]

Ambient intelligence and autonomous control are not part of the original concept of the Internet of things. Ambient intelligence and autonomous control do not necessarily require Internet structures, either. However, there is a shift in research (by companies such as Intel) to integrate the concepts of the IoT and autonomous control, with initial outcomes towards this direction considering objects as the driving force for autonomous IoT. [106] A promising approach in this context is deep reinforcement learning where most of IoT systems provide a dynamic and interactive environment.[107] Training an agent (i.e., IoT device) to behave smartly in such an environment cannot be addressed by conventional machine learning algorithms such as supervised learning. By reinforcement learning approach, a learning agent can sense the environment's state (e.g., sensing home temperature), perform actions (e.g., turn HVAC on or off) and learn through the maximizing accumulated rewards it receives in long term.

IoT intelligence can be offered at three levels: IoT devices, Edge/Fog nodes, and Cloud computing.[108] The need for intelligent control and decision at each level depends on the time sensitiveness of the IoT application. For example, an autonomous vehicle's camera needs to make real-time obstacle detection to avoid an accident. This fast decision making would not be possible through transferring data from the vehicle to cloud instances and return the predictions back to the vehicle. Instead, all the operation should be performed locally in the vehicle. Integrating advanced machine learning algorithms including deep learning into IoT devices is an active research area to make smart objects closer to reality. Moreover, it is possible to get the most value out of IoT deployments through analyzing IoT data, extracting hidden information, and predicting control decisions. A wide variety of machine learning techniques have been used in IoT domain ranging from traditional methods such as regression, support vector machine, and random forest to advanced ones such as convolutional neural networks, LSTM, and variational autoencoder.[109][108]

In the future, the Internet of Things may be a non-deterministic and open network in which auto-organized or intelligent entities (web services, SOA components) and virtual objects (avatars) will be interoperable and able to act independently (pursuing their own objectives or shared ones) depending on the context, circumstances or environments. Autonomous behavior through the collection and reasoning of context information as well as the object's ability to detect changes in the environment (faults affecting sensors) and introduce suitable mitigation measures constitutes a major research trend,[110] clearly needed to provide credibility to the IoT technology. Modern IoT products and solutions in the marketplace use a variety of different technologies to support such context-aware automation, but more sophisticated forms of intelligence are requested to permit sensor units and intelligent cyber-physical systems to be deployed in real environments.[111]

Architecture[edit]

> This section **needs attention from an expert in Technology**. The specific problem is: **The information is partially outdated, unclear, and uncited. Requires more details, but not so technical that others won't understand it..** WikiProject Technology may be able to help recruit an expert. *(July 2018)*

IoT system architecture, in its simplistic view, consists of three tiers: Tier 1: Devices, Tier 2: the Edge Gateway, and Tier 3: the Cloud.[112] Devices include networked things, such as the sensors and actuators found in IIoT equipment, particularly those that use protocols such as Modbus, Zigbee, or proprietary protocols, to connect to an Edge Gateway.[112]

The Edge Gateway consists of sensor data aggregation systems called Edge Gateways that provide functionality, such as pre-processing of the data, securing connectivity to cloud, using systems such as WebSockets, the event hub, and, even in some cases, edge analytics or fog computing.[112] The final tier includes the cloud application built for IIoT using the microservices architecture, which are usually polyglot and inherently secure in nature using HTTPS/OAuth. It includes various database systems that store sensor data, such as time series databases or asset stores using backend data storage systems (e.g. Cassandra, Postgres).[112] The cloud tier in most cloud-based IoT system features event queuing and messaging system that handles communication that transpires in all tiers. [113] Some experts classified the three-tiers in the IIoT system as edge, platform, and enterprise and these are connected by proximity network, access network, and service network, respectively.[114]

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

Network architecture[edit]

The Internet of things requires huge scalability in the network space to handle the surge of devices.[115] IETF 6LoWPAN would be used to connect devices to IP networks. With billions of devices[116] being added to the Internet space, IPv6 will play a major role in handling the network layer scalability. IETF's Constrained Application Protocol, ZeroMQ, and MQTT would provide lightweight data transport.

Fog computing is a viable alternative to prevent such large burst of data flow through Internet.[117] The edge devices' computation power to analyse and process data is extremely limited. Limited processing power is a key attribute of IoT devices as their purpose is to supply data about physical objects while remaining autonomous. Heavy processing requirements use more battery power harming IoT's ability to operate. Scalability is easy because IoT devices simply supply data through the internet to a server with sufficient processing power.[118]

Complexity[edit]

In semi -open or closed loops (i.e. value chains, whenever a global finality can be settled) the IoT will often be considered and studied as a complex system [119] due to the huge number of different links, interactions between autonomous actors, and its capacity to integrate new actors. At the overall stage (full open loop) it will likely be seen as a chaotic environment (since systems always have finality). As a practical approach, not all elements in the Internet of things run in a global, public space. Subsystems are often implemented to mitigate the risks of privacy, control and reliability. For example, domestic robotics (domotics) running inside a smart home might only share data within and be available via a local network.[120] Managing and controlling a high dynamic ad hoc IoT things/devices network is a tough task with the traditional networks architecture, Software Defined Networking (SDN) provides the agile dynamic solution that can cope with the special requirements of the diversity of innovative IoT applications.[121]

Size considerations[edit]

The Internet of things would encode 50 to 100 trillion objects, and be able to follow the movement of those objects. Human beings in surveyed urban environments are each surrounded by 1000 to 5000 trackable objects.[122] In 2015 there were already 83 million smart devices in people's homes. This number is expected to grow to 193 million devices by 2020.[28]

The figure of online capable devices grew 31% from 2016 to 8.4 billion in 2017.[104]

Space considerations[edit]

In the Internet of things, the precise geographic location of a thing—and also the precise geographic dimensions of a thing—will be critical.[123] Therefore, facts about a thing, such as its location in time and space, have been less critical to track because the person processing the information can decide whether or not that information was important to the action being taken, and if so, add the missing information (or decide to not take the action). (Note that some things in the Internet of things will be sensors, and sensor location is usually important.[124]) The GeoWeb and Digital Earth are promising applications that become possible when things can become organized and connected by location. However, the challenges that remain include the constraints of variable spatial scales, the need to handle massive amounts of data, and an indexing for fast search and neighbor operations. In the Internet of things, if things are able to take actions on their own initiative, this human-centric mediation role is eliminated. Thus, the time-space context that we as humans take for granted must be given a central role in this information ecosystem. Just as standards play a key role in the Internet and the Web, geospatial standards will play a key role in the Internet of things. [125][126]

A solution to "basket of remotes"[edit]

Many IoT devices have a potential to take a piece of this market. Jean-Louis Gassée (Apple initial alumni team, and BeOS co-founder) has addressed this topic in an article on *Monday Note*,[127] where he predicts that the most likely problem will be what he calls the "basket of remotes" problem, where we'll have hundreds of applications to interface with hundreds of devices that don't share protocols for speaking with one another.[127] For improved user interaction, some technology leaders are joining forces to create standards for communication between devices to solve this problem. Others are turning to the concept of predictive interaction of devices, "where collected data is used to predict and trigger actions on the specific devices" while making them work together.[128]

Enabling technologies for IoT[edit]

There are many technologies that enable the IoT. Crucial to the field is the network used to communicate between devices of an IoT installation, a role that several wireless or wired technologies may fulfill: [129] [130][131]

Addressability[edit]

The original idea of the Auto-ID Center is based on RFID-tags and distinct identification through the Electronic Product Code. This has evolved into objects having an IP address or URI.[132] An alternative view, from the world of the Semantic Web [133] focuses instead on making all things (not just those electronic, smart, or RFID-enabled) addressable by the existing naming protocols, such as URI. The objects themselves do not converse, but they may now be referred to by other agents, such as powerful centralized servers acting for their human owners.[134] Integration with the Internet implies that devices will use an IP address as a distinct identifier. Due to the limited address space of

IPv4 (which allows for 4.3 billion different addresses), objects in the IoT will have to use the next generation of the Internet protocol (IPv6) to scale to the extremely large address space required.[135] [136][137] Internet-of-things devices additionally will benefit from the stateless address auto-configuration present in IPv6,[138] as it reduces the configuration overhead on the hosts,[136] and the IETF 6LoWPAN header compression. To a large extent, the future of the Internet of things will not be possible without the support of IPv6; and consequently, the global adoption of IPv6 in the coming years will be critical for the successful development of the IoT in the future.[137]

Short-range wireless[edit]

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

Medium-range wireless[edit]

- LTE-Advanced – High-speed communication specification for mobile networks. Provides enhancements to the LTE standard with extended coverage, higher throughput, and lower latency.

Long-range wireless[edit]

- Low-power wide-area networking (LPWAN) – Wireless networks designed to allow long-range communication at a low data rate, reducing power and cost for transmission. Available LPWAN technologies and protocols: LoRaWan, Sigfox, NB-IoT, Weightless, RPMA.
- Very small aperture terminal (VSAT) – Satellite communication technology using small dish antennas for narrowband and broadband data.

Wired[edit]

- Ethernet – General purpose networking standard using twisted pair and fiber optic links in conjunction with hubs or switches.

- Power-line communication (PLC) – Communication technology using electrical wiring to carry power and data. Specifications such as HomePlug or G.hn utilize PLC for networking IoT devices.

Standards and standards organizations[edit]

This section **needs expansion**. You can help by adding to it.

(September 2016)

This is a list of technical standards for the IoT, most of which are open standards, and the standards organizations that aspire to successfully setting them. [139] [140]

Short name	Long name	Standards under development	Other notes
Auto-ID Labs	Auto Identification Center	Networked RFID (radiofrequency identification) and emerging sensing technologies	
EPCglobal	Electronic Product code Technology	Standards for adoption of EPC (Electronic Product Code) technology	
FDA	U.S. Food and Drug Administration	UDI (Unique Device Identification) [redacted] system for distinct identifiers for medical devices	
GS1	—	Standards for UIDs ("unique" identifiers) [redacted] and RFID of fast-moving consumer goods (consumer packaged goods), health care supplies, and other things	Parent organization comprises member organizations such as GS1 US
IEEE	Institute of Electrical and Electronics Engineers	Underlying communication technology standards such as IEEE 802.15.4	
IETF	Internet Engineering Task Force	Standards that comprise TCP/IP (the Internet protocol suite)	
		MTConnect is a manufacturing industry	

MTConnect Institute	—	standard for data exchange with machine tools and related industrial [redacted] equipment. It is important to the IIoT subset of the IoT.	
O-DF	Open Data Format	O-DF is a standard published by the Internet of Things Work Group of The Open Group in 2014, which specifies a generic information model structure that is meant to be applicable for describing any "Thing", as well as for publishing, updating and querying information when used together with O-MI (Open Messaging Interface).	
O-MI	Open Messaging Interface	O-MI is a standard published by the Internet of Things Work Group of The Open Group in 2014, which specifies a limited set of key operations needed in IoT systems, notably different kinds of subscription mechanisms based on the Observer pattern.	
OCF	Open Connectivity Foundation	Standards for simple devices using CoAP (Constrained Application Protocol)	OCF (Open Connectivity Foundation) supersedes OIC

Short name	Long name	Standards under development	Other notes
			(Open Interconnect Consortium)
OMA	Open Mobile Alliance	OMA DM and OMA LWM2M for IoT device management, as well as GotAPI, which provides a secure framework for IoT applications	
XSF	XMPP Standards Foundation	Protocol extensions of XMPP (Extensible Messaging and Presence Protocol), the open standard of instant messaging	

•

Politics and civic engagement[edit]

Some scholars and activists argue that the IoT can be used to create new models of civic engagement if device networks can be open to user control and inter-operable platforms. Philip N. Howard, a professor and author, writes that political life in both democracies and authoritarian regimes will be shaped by the way the IoT will be used for civic engagement. For that to happen, he argues that any connected device should be able to divulge a list of the "ultimate beneficiaries" of its sensor data and that individual citizens should be able to add new organizations to the beneficiary list. In addition, he argues that civil society groups need to start developing their IoT strategy for making use of data and engaging with the public.[141]

Government regulation on IoT[edit]

One of the key drivers of the IoT is data. The success of the idea of connecting devices to make them more efficient is dependent upon access to and storage & processing of data. For this purpose, companies working on the IoT collect data from multiple sources and store it in their cloud network for further processing. This leaves the door wide open for privacy and security dangers and single point vulnerability of multiple systems.[142] The other issues pertain to consumer choice and ownership of data[143] and how it is used. Though still in their infancy, regulations and governance regarding these issues of privacy, security, and data ownership continue to develop. [144] [145] [146] IoT regulation depends on the country. Some examples of legislation that is relevant to privacy and data collection are: the US Privacy Act of 1974, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980, and the EU Directive 95/46/EC of 1995.[147]

Current regulatory environment:

A report published by the Federal Trade Commission (FTC) in January 2015 made the following three recommendations:[148]

- Data security – At the time of designing IoT companies should ensure that data collection, storage and processing would be secure at all times. Companies should adopt a "defence in depth" approach and encrypt data at each stage.[149]

- Data consent – users should have a choice as to what data they share with IoT companies and the users must be informed if their data gets exposed.

- Data minimization – IoT companies should collect only the data they need and retain the collected information only for a limited time.

However, the FTC stopped at just making recommendations for now. According to an FTC analysis, the existing framework, consisting of the FTC Act, the Fair Credit Reporting Act, and the Children's Online Privacy Protection Act, along with developing consumer education and business guidance, participation in multi-stakeholder efforts and advocacy to other agencies at the federal, state and local level, is sufficient to protect consumer rights.[150]

A resolution passed by the Senate in March 2015, is already being considered by the Congress.[151] This resolution recognized the need for formulating a National Policy on IoT and the matter of privacy, security and spectrum. Furthermore, to provide an impetus to the IoT ecosystem, in March 2016, a bipartisan group of four Senators proposed a bill, The Developing Innovation and Growing the Internet of Things (DIGIT) Act, to direct the Federal Communications Commission to assess the need for more spectrum to connect IoT devices.

Several standards for the IoT industry are actually being established relating to automobiles because most concerns arising from use of connected cars apply to healthcare devices as well. In fact, the National Highway Traffic Safety Administration (NHTSA) is preparing cybersecurity guidelines and a database of best practices to make automotive computer systems more secure.[152]

A recent report from the World Bank examines the challenges and opportunities in government adoption of IoT.[153] These include –

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

Criticism and controversies[edit]

Platform fragmentation[edit]

The IoT suffers from platform fragmentation and lack of technical standards [154] [155] [156] [157] [158] [159][160][*excessive citations*] a situation where the variety of IoT devices, in terms of both hardware variations and differences in the software running on them, makes the task of developing applications that work consistently between different inconsistent technology ecosystems hard.[1] For example, wireless connectivity for IoT devices can be done using Bluetooth, Zigbee, Z-Wave, LoRa, NB-IoT, Cat M1 as well as completely custom proprietary radios, each with its own advantages and disadvantages, creating a separate ecosystem for IoT devices.[161] Customers may be hesitant to bet their IoT future on a proprietary software or hardware devices that uses proprietary protocols that may fade or become difficult to customize and interconnect.[2]

The IoT's amorphous computing nature is also a problem for security, since patches to bugs found in the core operating system often do not reach users of older and lower-price devices. [162] [163] [164] One set of researchers say that the failure of vendors to support older devices with patches and updates leaves more than 87% of active Android devices vulnerable. [165][166]

Privacy, autonomy, and control[edit]

Philip N. Howard, a professor and author, writes that the Internet of things offers immense potential for empowering citizens, making government transparent, and broadening information access. Howard cautions, however, that privacy threats are enormous, as is the potential for social control and political manipulation.[167]

Concerns about privacy have led many to consider the possibility that big data infrastructures such as the Internet of things and data mining are inherently incompatible with privacy.[168] Writer Adam Greenfield claims that these technologies are not only an invasion of public space but are also being used to perpetuate normative behavior, citing an instance of billboards with hidden cameras that tracked the demographics of passersby who stopped to read the advertisement.[169]

The Internet of Things Council compared the increased prevalence of digital surveillance due to the Internet of things to the conceptual panopticon described by Jeremy Bentham in the 18th Century.[170] The assertion was defended by the works of French philosophers Michel Foucault and Gilles Deleuze. In *Discipline and Punish: The Birth of the Prison* Foucault asserts that the panopticon was a central element of the discipline society developed during the Industrial Era .[171] Foucault also argued that the discipline systems established in factories and school reflected Bentham's vision of panopticism.[171] In his 1992 paper "Postscripts on the Societies of Control," Deleuze wrote that the discipline society had transitioned into a control society, with the computer replacing the panopticon as an instrument of discipline and control while still maintaining the qualities similar to that of panopticism.[172]

The privacy of households could be compromised by solely analyzing smart home network traffic patterns without dissecting the contents of encrypted application data, yet a synthetic packet injection scheme can be used to safely overcome such invasion of privacy.[173]

Peter-Paul Verbeek , a professor of philosophy of technology at the University of Twente, Netherlands, writes that technology already influences our moral decision making, which in turn affects human agency, privacy and autonomy. He cautions against viewing technology merely as a human tool and advocates instead to consider it as an active agent.[174]

Justin Brookman, of the Center for Democracy and Technology, expressed concern regarding the impact of the IoT on consumer privacy, saying that "There are some people in the commercial space who say, 'Oh, big data — well, let's collect everything, keep it around forever, we'll pay for somebody to think about security later.' The question is whether we want to have some sort of policy framework in place to limit that."[175]

Tim O'Reilly believes that the way companies sell the IoT devices on consumers are misplaced, disputing the notion that the IoT is about gaining efficiency from putting all kinds of devices online and postulating that the "IoT is really about human augmentation. The applications are profoundly different when you have sensors and data driving the decision-making."[176]

Editorials at WIRED have also expressed concern, one stating "What you're about to lose is your privacy. Actually, it's worse than that. You aren't just going to lose your privacy, you're going to have to watch the very concept of privacy be rewritten under your nose."[177]

The American Civil Liberties Union (ACLU) expressed concern regarding the ability of IoT to erode people's control over their own lives. The ACLU wrote that "There's simply no way to forecast how these immense powers – disproportionately accumulating in the hands of corporations seeking financial advantage and governments craving ever more control – will be used. Chances are big data and the Internet of things will make it harder for us to control our own lives, as we grow increasingly transparent to powerful corporations and government institutions that are becoming more opaque to us."[178]

In response to rising concerns about privacy and smart technology, in 2007 the British Government stated it would follow formal Privacy by Design principles when implementing their smart metering program. The program would lead to replacement of traditional power meters with smart power meters, which could track and manage energy usage more accurately.[179] However the British Computer Society is doubtful these principles were ever actually implemented.[180] In 2009 the Dutch Parliament rejected a similar smart metering program, basing their decision on privacy concerns. The Dutch program later revised and passed in 2011.[180]

Data storage[edit]

A challenge for producers of IoT applications is to clean, process and interpret the vast amount of data which is gathered by the sensors. There is a solution proposed for the analytics of the information referred to as Wireless Sensor Networks.[181] These networks share data among sensor nodes that are sent to a distributed system for the analytics of the sensory data.[182]

Another challenge is the storage of this bulk data. Depending on the application, there could be high data acquisition requirements, which in turn lead to high storage requirements. Currently the Internet is already responsible for 5% of the total energy generated,[181] and a "daunting challenge to power" IoT devices to collect and even store data still remains.[183]

Security[edit]

Concerns have been raised that the IoT is being developed rapidly without appropriate consideration of the profound security challenges involved[184] and the regulatory changes that might be necessary. [185][186] Most of the technical security concerns are similar to those of conventional servers, workstations and smartphones, but security challenges unique to the IoT continue to develop, including industrial security controls, hybrid systems, IoT-specific business processes, and end nodes.[187]

Security is the biggest concern in adopting Internet of things technology.[188] In particular, as the Internet of things spreads widely, cyber attacks are likely to become an increasingly physical (rather than simply virtual) threat.[189] The current IoT space comes with numerous security vulnerabilities. These vulnerabilities include weak authentication (IoT devices are being used with default credentials), unencrypted messages sent between devices, SQL injections and lack of verification or encryption of software updates.[190] This allows attackers to easily intercept data to collect PII (Personally Identifiable Information), steal user credentials at login, or inject malware into newly updated firmware.[190]

In a January 2014 article in *Forbes*, cyber-security columnist Joseph Steinberg listed many Internet-connected appliances that can already "spy on people in their own homes" including televisions, kitchen appliances,[191] cameras, and thermostats.[192] Computer-controlled devices in automobiles such as brakes, engine, locks, hood and trunk releases, horn, heat, and dashboard have been shown to be vulnerable to attackers who have access to the on-board network. In some cases, vehicle computer systems are Internet-connected, allowing them to be exploited remotely.[193] For example, a hacker can gain unauthorized access to IoT devices due to their set-up; that is, because these devices are connected, Internet-enabled, and lack the necessary protective measures.[194] By 2008 security researchers had shown the ability to remotely control pacemakers without authority. Later hackers demonstrated remote control of insulin pumps[195] and implantable cardioverter defibrillators.[196] Many of these IoT devices have severe operational limitations on their physical size and by extension the computational power available to them. These constraints often make them unable to directly use basic security measures such as implementing firewalls or using strong cryptosystems to encrypt their communications with other devices.[197]

The U.S. National Intelligence Council in an unclassified report maintains that it would be hard to deny "access to networks of sensors and remotely-controlled objects by enemies of the United States, criminals, and mischief makers... An open market for aggregated sensor data could serve the interests of commerce and security no less than it helps criminals and spies identify vulnerable targets. Thus, massively parallel sensor fusion may undermine social cohesion, if it proves to be fundamentally incompatible with Fourth-Amendment guarantees against unreasonable search."[198] In general, the intelligence community views the Internet of things as a rich source of data.[199]

In 2016, a distributed denial of service attack powered by Internet of things devices running the Mirai malware took down a DNS provider and major web sites.[200] The Mirai Botnet had infected roughly 65,000 IoT devices within the first 20 hours.[201] Eventually the infections increased to 200,000 to 300,000 infections.[201] Brazil, Columbia and Vietnam made up of 41.5% of the infections.[201] The Mirai Botnet had singled out specific IoT devices that consisted of DVRs, IP cameras, routers and printers.[201] Top vendors that contained the most infected devices were identified as Dahua, Huawei, ZTE, Cisco, ZyXEL and MikroTik.[201] In May 2017, Junade Ali, a Computer Scientist at Cloudflare noted that native DDoS vulnerabilities exist in IoT devices due to a poor implementation of the Publish–subscribe pattern. [202] [203] These sorts of attacks have caused security experts to view IoT as a real threat to Internet services.[204]

On 31 January 2019, the Washington Post wrote an article regarding the security and ethical challenges that can occur with IoT doorbells and cameras: "Last month, Ring got caught allowing its team in Ukraine to view and annotate certain user videos; the company says it only looks at publicly shared videos and those from Ring owners who provide consent. Just last week, a California family's Nest camera let a hacker take over and broadcast fake audio warnings about a missile attack, not to mention peer in on them, when they used a weak password"[205]

There have been a range of responses to concerns over security. The Internet of Things Security Foundation (IoTSF) was launched on 23 September 2015 with a mission to secure the Internet of things by promoting knowledge and best practice. Its founding board is made from technology providers and telecommunications companies. In addition, large IT companies are continuously developing innovative solutions to ensure the security for

IoT devices. In 2017, Mozilla launched Project Things, which allows to route IoT devices through a safe Web of Things gateway.[206] As per the estimates from KBV Research, [207] the overall IoT security market[208] would grow at 27.9% rate during 2016–2022 as a result of growing infrastructural concerns and diversified usage of Internet of things. [209]

[210]

Governmental regulation is argued by some to be necessary to secure IoT devices and the wider Internet – as market incentives to secure IoT devices is insufficient. [211] [185][186]

Safety[edit]

IoT systems are typically controlled by event-driven smart apps that take as input either sensed data, user inputs, or other external triggers (from the Internet) and command one or more actuators towards providing different forms of automation.[212] Examples of sensors include smoke detectors, motion sensors, and contact sensors. Examples of actuators include smart locks, smart power outlets, and door controls. Popular control platforms on which third-party developers can build smart apps that interact wirelessly with these sensors and actuators include Samsung's SmartThings,[213] Apple's HomeKit,[214] and Amazon's Alexa,[215] among others.

A problem specific to IoT systems is that buggy apps, unforeseen bad app interactions, or device/communication failures, can cause unsafe and dangerous physical states, e.g., "unlock the entrance door when no one is at home" or "turn off the heater when the temperature is below 0 degrees Celsius and people are sleeping at night".[212] Detecting flaws that lead to such states, requires a holistic view of installed apps, component devices, their configurations, and more importantly, how they interact. Recently, researchers from the University of California Riverside have proposed IotSan, a novel practical system that uses model checking as a building block to reveal "interaction-level" flaws by identifying events that can lead the system to unsafe states.[212] They have evaluated IotSan on the Samsung SmartThings platform. From 76 manually configured systems, IotSan detects 147 vulnerabilities (i.e., violations of safe physical states/properties).

Design[edit]

Given widespread recognition of the evolving nature of the design and management of the Internet of things, sustainable and secure deployment of IoT solutions must design for "anarchic scalability."[216] Application of the concept of anarchic scalability can be extended to physical systems (i.e. controlled real-world objects), by virtue of those systems being designed to account for uncertain management futures. This hard anarchic scalability thus provides a pathway forward to fully realize the potential of Internet-of-things solutions by selectively constraining physical systems to allow for all management regimes without risking physical failure.[216]

Brown University computer scientist Michael Littman has argued that successful execution of the Internet of things requires consideration of the interface's usability as well as the technology itself. These interfaces need to be not only more user-friendly but also better integrated: "If users need to learn different interfaces for their vacuums, their locks, their sprinklers, their lights, and their coffeemakers, it's tough to say that their lives have been made any easier."[217]

Environmental sustainability impact[edit]

A concern regarding Internet-of-things technologies pertains to the environmental impacts of the manufacture, use, and eventual disposal of all these semiconductor-rich devices. [218] Modern electronics are replete with a wide variety of heavy metals and rare-earth metals, as well as highly toxic synthetic chemicals. This makes them extremely difficult to properly recycle. Electronic components are often incinerated or placed in regular landfills. Furthermore, the human and environmental cost of mining the rare-earth metals that are integral to modern electronic components continues to grow. This leads to societal questions concerning the environmental impacts of IoT devices over its lifetime.[219]

Intentional obsolescence of devices[edit]

The Electronic Frontier Foundation has raised concerns that companies can use the technologies necessary to support connected devices to intentionally disable or "brick" their customers' devices via a remote software update or by disabling a service necessary to the operation of the device. In one example, home automation devices sold with the promise of a "Lifetime Subscription" were rendered useless after Nest Labs acquired Revolv and made the decision to shut down the central servers the Revolv devices had used to operate.[220] As Nest is a company owned by Alphabet (Google's parent company), the EFF argues this sets a "terrible precedent for a company with ambitions to sell self-driving cars, medical devices, and other high-end gadgets that may be essential to a person's livelihood or physical safety."[221]

Owners should be free to point their devices to a different server or collaborate on improved software. But such action violates the United States DMCA section 1201, which only has an exemption for "local use". This forces tinkerers who want to keep using their own equipment into a legal grey area. EFF thinks buyers should refuse electronics and software that prioritize the manufacturer's wishes above their own.[221]

Examples of post- sale manipulations include Google Nest Revolv, disabled privacy settings on Android, Sony disabling Linux on PlayStation 3, enforced EULA on Wii U.[221]

Confusing terminology[edit]

Kevin Lonergan at Information Age, a business-technology magazine, has referred to the terms surrounding the IoT as a "terminology zoo".[222] The lack of clear terminology is not "useful from a practical point of view" and a "source of confusion for the end user". [222] A company operating in the IoT space could be working in anything related to sensor technology, networking, embedded systems, or analytics.[222] According to Lonergan, the term IoT was coined before smart phones, tablets, and devices as we know them today existed, and there is a long list of terms with varying degrees of overlap and technological convergence: Internet of things, Internet of everything (IoE), Internet of Goods (Supply Chain), industrial Internet, pervasive computing, pervasive sensing, ubiquitous computing, cyber-physical systems (CPS), wireless sensor networks (WSN), smart objects, digital twin, cyberobjects or avatars,[119] cooperating objects, machine to machine (M2M), ambient intelligence (AmI), Operational technology (OT), and information technology (IT). [222] Regarding IIoT, an industrial sub-field of IoT, the Industrial Internet Consortium's Vocabulary Task Group has created a "common and reusable vocabulary of terms"[223] to ensure "consistent terminology" [223][224] across publications issued by the Industrial Internet Consortium. IoT One has created an IoT Terms Database including a New Term Alert[225] to be notified when a new term is published. As of March 2017[update], this database aggregates 711 IoT-related terms, while keeping material "transparent and comprehensive." [226][227]

IoT adoption barriers[edit]

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

Lack of interoperability and unclear value propositions[edit]

Despite a shared belief in the potential of the IoT, industry leaders and consumers are facing barriers to adopt IoT technology more widely. Mike Farley argued in Forbes that while IoT solutions appeal to early adopters, they either lack interoperability or a clear use case for end-users.[228] A study by Ericsson regarding the adoption of IoT among Danish companies suggests that many struggle "to pinpoint exactly where the value of IoT lies for them".[229]

Privacy and security concerns[edit]

According to a recent study by Noura Aleisa and Karen Renaud at the University of Glasgow, "the Internet of things' potential for major privacy invasion is a concern"[230] with much of research "disproportionally focused on the security concerns of IoT."[230] Among the "proposed solutions in terms of the techniques they deployed and the extent to which they satisfied core privacy principles",[230] only very few turned out to be fully satisfactory. Louis Basenese, investment director at Wall Street Daily, has criticized the industry's lack of attention to security issues:

> "Despite high-profile and alarming hacks, device manufacturers remain undeterred, focusing on profitability over security. Consumers need to have ultimate control over collected data, including the option to delete it if they choose...Without privacy assurances, wide-scale consumer adoption simply won't happen."[231]

In a post-Snowden world of global surveillance disclosures, consumers take a more active interest in protecting their privacy and demand IoT devices to be screened for potential security vulnerabilities and privacy violations before purchasing them. According to the 2016 Accenture Digital Consumer Survey, in which 28000 consumers in 28 countries were polled on their use of consumer technology, security "has moved from being a nagging problem to a top barrier as consumers are now choosing to abandon IoT devices and services over security concerns."[232] The survey revealed that "out of the consumers aware of hacker attacks and owning or planning to own IoT devices in the next five years, 18 percent decided to terminate the use of the services and related services until they get safety guarantees."[232] This suggests that consumers increasingly perceive privacy risks and security concerns to outweigh the value propositions of IoT devices and opt to postpone planned purchases or service subscriptions.[232]

Traditional governance structures[edit]

Town of Internet of Things in Hangzhou, China

A study issued by Ericsson regarding the adoption of Internet of things among Danish companies identified a "clash between IoT and companies' traditional governance structures, as IoT still presents both uncertainties and a lack of historical precedence." [229] Among the respondents interviewed, 60 percent stated that they "do not believe they have the organizational capabilities, and three of four do not believe they have the processes needed, to capture the IoT opportunity."[229] This has led to a need to understand organizational culture in order to facilitate organizational design processes and to test new innovation management practices. A lack of digital leadership in the age of digital transformation has also stifled innovation and IoT adoption to a degree that many companies, in the face of uncertainty, "were waiting for the market dynamics to play out",

[229] or further action in regards to IoT "was pending competitor moves, customer pull, or regulatory requirements."[229] Some of these companies risk being 'kodaked' – "Kodak was a market leader until digital disruption eclipsed film photography with digital photos"[233] – failing to "see the disruptive forces affecting their industry"[234] and "to truly embrace the new business models the disruptive change opens up."[234] Scott Anthony has written in Harvard Business Review that Kodak "created a digital camera, invested in

the technology, and even understood that photos would be shared online"[234] but ultimately failed to realize that "online photo sharing *was* the new business, not just a way to expand the printing business."[234]

The Internet of Things (IoT), sometimes referred to as the Internet of Objects, will change everything—including ourselves. This may seem like a bold statement, but consider the impact the Internet already has had on education, communication, business, science, government, and humanity. Clearly, the Internet is one of the most important and powerful creations in all of human history.

Now consider that IoT represents the next evolution of the Internet, taking a huge leap in its ability to gather, analyze, and distribute data that we can turn into information, knowledge, and, ultimately, wisdom. In this context, IoT becomes immensely important.
Already, IoT projects are under way that promise to close the gap between poor and rich, improve distribution of the world's resources to those who need them most, and help us understand our planet so we can be more proactive and less reactive. Even so, several barriers exist that threaten to slow IoT development, including the transition to IPv6, having a common set of standards, and developing energy sources for millions—even billions—of minute sensors.

However, as businesses, governments, standards bodies, and academia work together to solve these challenges, IoT will continue to progress. The goal of this paper, therefore, is to educate you in plain and simple terms so you can be well versed in IoT and understand its potential to change everything we know to be true today.

IoT Today

As with many new concepts, IoT's roots can be traced back to the Massachusetts Institute of Technology (MIT), from work at the Auto-ID Center. Founded in 1999, this group was working in the field of networked radio frequency identification (RFID) and emerging sensing technologies. The labs consisted of seven research universities located across four continents. These institutions were chosen by the Auto-ID Center to design the architecture for IoT.1

Before we talk about the current state of IoT, it is important to agree on a definition. According to the Cisco Internet Business Solutions Group (IBSG), IoT is simply the point in time when more “things or objects” were connected to the Internet than people.2

In 2003, there were approximately 6.3 billion people living on the planet and 500 million devices connected to the Internet.3 By dividing the number of connected devices by the world population, we find that there was less than one (0.08) device for every person. Based on Cisco IBSG’s definition, IoT didn’t yet exist in 2003 because the number of connected things was relatively small given that ubiquitous devices such as smartphones were just being introduced. For example, Steve Jobs, Apple’s CEO, didn’t unveil the iPhone until January 9, 2007 at the Macworld conference.4

Cisco Internet Business Solutions Group (IBSG)

White Paper

Explosive growth of smartphones and tablet PCs brought the number of devices connected to the Internet to 12.5 billion in 2010, while the world's human population increased to 6.8 billion, making the number of connected devices per person more than 1 (1.84 to be exact) for the first time in history.5
Methodology
In January 2009, a team of researchers in China studied Internet routing data in six-month intervals, from December 2001 to December 2006. Similar to the properties of Moore's Law, their findings showed that the Internet doubles in size every 5.32 years. Using this figure in combination with the number of devices connected to the Internet in 2003 (500 million, as determined by Forrester Research), and the world population according to the U.S. Census Bureau, Cisco IBSG estimated the number of connected devices per person.6

Refining these numbers further, Cisco IBSG estimates IoT was "born" sometime between 2008 and 2009 (see Figure 1). Today, IoT is well under way, as initiatives such as Cisco's Planetary Skin, smart grid, and intelligent vehicles continue to progress.7
Figure 1. The Internet of Things Was "Born" Between 2008 and 2009
Looking to the future, Cisco IBSG predicts there will be 25 billion devices connected to the Internet by 2015 and 50 billion by 2020. It is important to note that these estimates do not

take into account rapid advances in Internet or device technology; the numbers presented are based on what is known to be true today.

Additionally, the number of connected devices per person may seem low. This is because the calculation is based on the entire world population, much of which is not yet connected to the Internet. By reducing the population sample to people actually connected to the Internet, the number of connected devices per person rises dramatically. For example, we know that

Source: Cisco IBSG, April 2011

Cisco Internet Business Solutions Group (IBSG)

White Paper
approximately 2 billion people use the Internet today. 8 Using this figure, the number of connected devices per person jumps to 6.25 in 2010, instead of 1.84.

Of course, we know nothing remains static, especially when it comes to the Internet. Initiatives and advances, such as Cisco's Planetary Skin, HP's central nervous system for the earth (CeNSE), and smart dust, have the potential to add millions—even billions—of sensors to the Internet.9 As cows, water pipes, people, and even shoes, trees, and animals become connected to IoT, the world has the potential to become a better place.

“With a trillion sensors embedded in the environment—all connected by computing systems, software, and services—it will be possible to hear the heartbeat of the Earth, impacting human interaction with the globe as profoundly as the Internet has revolutionized communication.”

Peter Hartwell

Senior Researcher, HP Labs
IoT as a Network of Networks

Currently, IoT is made up of a loose collection of disparate, purpose-built networks. Today’s cars, for example, have multiple networks to control engine function, safety features, communications systems, and so on. Commercial and residential buildings also have various control systems for heating, venting, and air conditioning (HVAC); telephone service; security; and lighting. As IoT evolves, these networks, and many others, will be connected with added security, analytics, and management capabilities (see Figure 2). This will allow IoT to become even more powerful in what it can help people achieve.

Figure 2. IoT Can Be Viewed as a Network of Networks

Source: Cisco IBSG, April 2011

Interestingly, this situation mirrors what the technology industry experienced in the early days of networking. In the late 1980s and early 1990s, Cisco, for example, established itself by bringing disparate networks together with multi-protocol routing, eventually leading to IP as the common networking standard. With IoT, history is repeating itself, albeit on a much grander scale.

Why Is IoT Important?

Before we can begin to see the importance of IoT, it is first necessary to understand the differences between the Internet and the World Wide Web (or web)—terms that are often used interchangeably. The Internet is the physical layer or network made up of switches, routers, and other equipment. Its primary function is to transport information from one point to another quickly, reliably, and securely. The web, on the other hand, is an application layer that operates on top of the Internet. Its primary role is to provide an interface that makes the information flowing across the Internet usable.

Evolution of the Web Versus the Internet

The web has gone through several distinct evolutionary stages:

Stage 1. First was the research phase, when the web was called the Advanced Research Projects Agency Network (ARPANET). During this time, the web was primarily used by academia for research purposes.

Stage 2. The second phase of the web can be coined “brochureware.” Characterized by the domain name “gold rush,” this stage focused on the need for almost every company to share information on the Internet so that people could learn about products and services.

Stage 3. The third evolution moved the web from static data to transactional information, where products and services could be bought and sold, and services could be delivered. During this phase, companies like eBay and Amazon.com exploded on the scene. This phase also will be infamously remembered as the “dot-com” boom and bust.

Stage 4. The fourth stage, where we are now, is the “social” or “experience” web, where companies like Facebook, Twitter, and Groupon have become immensely popular and profitable (a notable distinction from the third stage of the web) by allowing people to communicate, connect, and share information (text, photos, and video) about themselves with friends, family, and colleagues.

IoT: First Evolution of the Internet

By comparison, the Internet has been on a steady path of development and improvement, but arguably hasn’t changed much. It essentially does the same thing that it was designed to do during the ARPANET era. For example, in the early days, there were several communication protocols, including AppleTalk, Token Ring, and IP. Today, the Internet is largely standardized on IP.

In this context, IoT becomes immensely important because it is the first real evolution of the Internet—a leap that will lead to revolutionary applications that have the potential to dramatically improve the way people live, learn, work, and entertain themselves. Already, IoT has made the Internet sensory (temperature, pressure, vibration, light, moisture, stress), allowing us to become more proactive and less reactive.

Cisco Internet Business Solutions Group (IBSG)
White Paper
In addition, the Internet is expanding into places that until now have been unreachable. Patients are ingesting Internet devices into their own bodies to help doctors diagnose and determine the causes of certain diseases.10 Extremely small sensors can be placed on plants, animals, and geologic features, and connected to the Internet.11 At the other end of the spectrum, the Internet is going into space through Cisco's Internet Routing in Space (IRIS) program.12

We Evolve Because We Communicate
Humans evolve because they communicate. Once fire was discovered and shared, for example, it didn't need to be rediscovered, only communicated. A more modern-day example is the discovery of the helix structure of DNA, molecules that carry genetic information from one generation to another. After the article was published in a scientific paper by James Watson and Francis Crick in April 1953, the disciplines of medicine and genetics were able to build on this information to take giant leaps forward.13

This principle of sharing information and building on discoveries can best be understood by examining how humans process data (see Figure 3). From bottom to top, the pyramid layers include data, information, knowledge, and wisdom. Data is the raw material that is processed into information. Individual data by itself is not very useful, but volumes of it can identify trends and patterns. This and other sources of information come together to form knowledge. In the simplest sense, knowledge is information of which someone is aware. Wisdom is then born from knowledge plus experience. While knowledge changes over time, wisdom is timeless, and it all begins with the acquisition of data.
Figure 3. Humans Turn Data into Wisdom

It is also important to note there is a direct correlation between the input (data) and output

(wisdom). The more data that is created, the more knowledge and wisdom people can obtain. IoT dramatically increases the amount of data available for us to process. This, coupled with the Internet's ability to communicate this data, will enable people to advance even further.

Source: Cisco IBSG, April 2011

White Paper
IoT: Critical for Human Progression

As the planet's population continues to increase, it becomes even more important for people to become stewards of the earth and its resources. In addition, people desire to live healthy, fulfilling, and comfortable lives for themselves, their families, and those they care about. By combining the ability of the next evolution of the Internet (IoT) to sense, collect, transmit, analyze, and distribute data on a massive scale with the way people process information, humanity will have the knowledge and wisdom it needs not only to survive, but to thrive in the coming months, years, decades, and centuries.
IoT Applications: What Cows, Water Pipes, and People Have in Common

When we crossed the threshold of connecting more objects than people to the Internet, a huge window of opportunity opened for the creation of applications in the areas of automation, sensing, and machine-to-machine communication. In fact, the possibilities are almost endless. The following examples highlight some of the ways IoT is changing people's lives for the better.
Holy Cow!

In the world of IoT, even cows will be connected. A special report in *The Economist* titled "Augmented Business" described how cows will be monitored (see Figure 4). Sparked, a Dutch start-up company, implants sensors in the ears of cattle. This allows farmers to monitor cows' health and track their movements, ensuring a healthier, more plentiful supply of meat for people to consume. On average, each cow generates about 200 megabytes of information a year.

Internet of Things: What It Is, How It Works, Examples and More

- **MONDAY, NOVEMBER 19, 2018**
- **MISCELLANEOUS**

This article was contributed by Jay M.

One of the most common buzzwords in the world of mobile app development right now is IoT, the Internet of Things.

From the simplest consumer-based applications like smart homes and wearables to complicated, industry-grade solutions like driverless forklifts, IoT is everywhere and gradually changing the way how consumers live, work and interact with their Internet-enabled devices.

According to a recent report from Statista, there will be almost 31 billion connected smartphones, wearables, smart watches, cars, and other devices by the end of 2020. Currently, this number is around 23 billion worldwide. This demonstrates how exponentially the IoT is growing.

While the concept of the IoT has been around for quite a long time, most of the people are still not familiar to it. If you're also one of them, this comprehensive guide is for you. Covering everything essential you need to know about the Internet of Things, this detailed guide is fabricated to help you learn what IoT actually is, how it works, its use cases and advantages, with appropriate real-life examples.

Let's get started!

What is the Internet of Things (IoT)?

The Internet of Things, or IoT, is essentially an ecosystem of physical devices, vehicles, appliances, and other things that have the ability to connect, collect and exchange data over a wired and wireless network, with little or no human-to-human or human-to-computer intervention. Allowing integration and data exchange between physical devices and the computer, this new wave of technology focuses on making human life more simplified and comfortable with the right mix of efficiency and productivity.

To be more specific, taking advantage of cutting-edge technologies like Machine Learning, Machine-to-Machine (M2M) Communication and Artificial Intelligence (AI), IoT aims at extending connectivity beyond standard Internet supported physical devices (smartphones, tablets, desktops, and laptops) to a wide spectrum of non-internet-enabled physical devices and everyday objects, such as coffee makers, washing machines, door locks, etc., so you can remotely monitor and control them with the help of a mobile or tablet device.

How Does IoT Work?

Since the mechanism of IoT devices is highly technical, so for many it's quite confusing how an IoT system actually works. Well, just like any other system has predefined steps and components to make it work, so the Internet of Things has its own. A complete IoT system is made up of four distinct components that work together to deliver the desired output. Let's look at each component and understand what it does.

1. Sensors/Devices

First of all, sensors or devices collect very minute data from the surrounding environment. The collected data could be as simple as a geographical location or as complex as health essentials of a patient.

To pick up the most sensitive changes in data, one can bundle multiple sensors together to be a part of a device that is capable of doing more than just sense things. For instance, the mobile phone is a device with several built-in sensors such as GPS, Camera, Accelerometer, without which the phone is not able to sense things.

Thus, be it a standalone sensor or a device having multiple sensors, the first step involves the collection of all the minute details from the surrounding environment.

2. Connectivity

Once the data is collected, it is sent to a cloud infrastructure aka an IoT platform with the help of a medium. That’s where several wireless and wired networking technologies, such as Bluetooth, Wi-Fi, Cellular Networks, LPWAN, Ethernet, etc come into handy. While each of these connectivity options represents a tradeoff between power consumption, connection range, and bandwidth, choosing the best one to transmit data to the cloud solely depends on the complexity level and specific requirements of an IoT application.

3. Data Processing

Once the data gets to the cloud infrastructure, it is stored, analyzed, and processed securely using a Big Data Analytics Engine for better decision making. This analysis can be as simple as checking whether or not the temperature reading on an AC or heater is within an acceptable range, or as complex as identifying intruders in your house with the help of surveillance cameras. The processed data is then used to perform immediate, intelligent actions that turn our ordinary physical devices into exceptionally smart devices.

4. User Interface

The last step involves notifying the end user about the action through an email, text, notification, or alert sound triggered on their IoT application. Depending on the complexity of the IoT system, the user can then either leave the automatically performed action intact, proactively check in on their IOT system, or manually perform an action to backfire or affect the system. For instance, if the user detects some changes in a particular room, he can remotely adjust that room temperature via an IoT app installed on his phone.

6 Benefits of IoT

While the ultimate goal of the Internet of Things is to automate human life to make it more insanely efficient and productive, there are countless benefits of IoT for both businesses and consumers. Mentioned below are just a few of them:

1. Access to High-quality Data

Everyone, especially marketers and entrepreneurs, loves data and with the invention of IoT devices, companies now have greater access to data related their customers and products than ever before. They can take advantage of these real-time operational insights to monitor consumer behavior, deliver better customer experiences and make smarter business decisions. Technically, the more information you have, the easier it is for you to take the right decision.

2. Better Tracking and Management

Whatever the industry is, IoT makes tracking and management a breeze for organizations. From keeping track of inventory item by item to monitoring road traffic and weather conditions to notifying the concerned authorities about any suspicious behavior, IoT revolutionizes the way how we currently track and manage our business assets. In fact, IoT is not just about the smart homes anymore, but it is now also about smart offices, smart warehouse, and smart anything else.

3. Efficient Resource Utilization

Be it home, office, hotel or car, IoT facilitates an efficient utilization of assets for improved productivity. Leveraging the power of machine-to-machine interaction, an IoT system collects real-time data with the help of sensors and actuators so you can further use it to improve process efficiency and minimize human intervention. As a basic example, if any of your Home Appliances notifies you about the task completion, you need not worrying about the inefficient consumption of the electricity.

4. Automation and Control

Automation is the need of the hour and IoT is renowned for the same. Since most of the IoT devices are connected with each other through a wireless infrastructure, they are able to operate on their own with little or no manual intervention. For instance, home appliances such as air conditioner, washing machines, ovens, and refrigerators can be automatically get operated and you can even monitor and control them remotely.

5. Comfort and Convenience

We live in a fast-paced world where busy people don't even care about small things like switching on/off lights and reading energy meters, and this is where the Internet of Things comes in. The interconnectivity of devices and aggregation of data provides you full control over your all devices that are connected with each other through the IoT system. Since you're able to control all your devices just through one centralized device like your phone, this leads to greater convenience and comfort.

6. Saves Time and Money

The concept of IoT revolves around getting more done in less time by automating tasks and requiring little to no human intervention. Allowing you to accomplish cumbersome tasks faster and with optimum utilization of energy, IoT not only saves your precious time but also your hard-earned money. For example, if your kitchen electronic appliance has the ability to turn off itself after the task is done, this saves your time and efforts required to manually switch off the appliance as well as extra expenditure caused by the unnecessary use of electricity.

6 Use Cases of Internet of Things (IoT)

If you look around, you'll find an ever-growing number of devices is getting smarter day after day and there is no industry that has remained untouched by the Internet of Things. Some real-world applications of IoT presently in use are:

1. **Smart Home**

Smart Home, which is also the most searched IoT associated feature on Google, is definitely the best example of IoT use case. With a focus on providing you optimum security and convenience, smart home systems and devices are designed to save your precious time and energy. You can control everything from lighting to temperature of your house with just a few taps on your smartphone. Isn't this really a cool thing?

2. Wearables

While wearables like Smart Watches and Fitness Tracking Bands have already flooded the market, many giant companies like Samsung and Intel are now investing heavily in building IoT-powered wearable devices. With the help of sensors and software installed, such devices can track and monitor crucial metrics like heart rate, blood pressure, sleeping and eating habits, caloric intake, etc, and share them with a third-party app or a healthcare service provider.

3. Smart Cities

Many countries like South Korea, Japan, Spain, and the UK are trying to colonize smart cities in order to provide their citizens with a better, safer and healthier living environment. Collecting the data from citizens, devices, and assets, a smart city promises to solve major problems of people living in a usual city, like water distribution, pollution, crime, traffic congestion, waste management, etc. To better understand how Smart Cities actually work, check out this amazing video.

4. Automotive and Transportation

With the Internet of Things, automotive companies like BMW, Ford, Tesla, and Volvo are looking forward to enhancing the in-car experience. Being equipped with technologies like sensors, maps, computer vision, sonar, and the Internet, these cars are driverless and can run with little or no human assistance. And, if combined with Machine Learning, the IoT also assists in various aspects of transportation systems like logistics and fleet management, smart traffic control and smart parking.

5. Medical and Healthcare

The Medical industry is also taking advantage of IoT-powered devices for remote health monitoring and emergency alerts. With the help of smart healthcare devices, the doctors can remotely monitor the health of patients outside of conventional clinical environments and give medicines on the basis of collected data. Likewise, in an emergency, doctors can keep themselves ready for the operation as they are already aware of the medical condition of the patient.

6. Industrial IoT

The Industrial Internet of Things (IIoT) is the industrial subset of the IoT which leverages this innovative technology to solve industrial concerns, automate processes and eliminate inefficiencies. While the term IIoT often denotes the use of IoT in manufacturing industries, other common applications of IIoT include futuristic farming, aerospace and defense, and energy management.

Internet of Things Examples

Amazon Go

Amazon Go is one of its kind retail store that facilitates customers shopping with no checkout required. All you need to sign in the Amazon Go app to enter the store, then shop as you normally would and leave the store. No lines, no checkout, just walk out! Can't believe it? Watch this interesting video.

Nest Learning Thermostat

Nest Learning Thermostat self-learning Wi-Fi-enabled smart thermostat that leverages Machine Learning to automatically optimize the heating and cooling of your home to conserve energy. You can also manually control your home's temperature with just a few taps on your smartphone or tablet.

Philips Hue

With Philips Hue, you can control your lights from your living room to the backyard. You can turn them off with a single tap and even change their hue to match your ambiance. Even, your lights even give you a warm welcome when you arrive home and switch off automatically as soon as you leave your home.

Hero Health

Hero Health is a smart medication dispenser that is widely used for home treatment and elderly care. This smart appliance not only allows your loved one to dispense doses at the push of a button but also sends alerts to your smartphone if they miss a dose.

Blossom

Blossom is a smart watering system that utilizes real-time weather data and forecasts for optimal water use in your yard and allows you to control your sprinklers from remotely from your Android or iOS device.

Internet of Things Platforms

Cloud IoT Core by Google: A fully managed service that allows you to securely connect and manage IoT devices, globally.

Microsoft Azure IoT Hub : An open-cloud platform that makes it easy for anyone to connect, monitor and manage billions of IoT devices.

AWS IoT Core: A managed cloud service from Amazon to provide a secure, bi-directional communication between the Internet of Things and the AWS Cloud.

IBM Watson IoT : The AI-powered IBM Watson IoT platform allows you to collect connected device data and perform real-time analytics on it to maximize the potential of your IoT devices.

MindSphere: Developed by Siemens, MindSphere is an open cloud platform that empowers you to unleash the full potential of data generated by the IoT devices with a leading-edge analytics.

Refferences

1. CSA 2009 – *„Security Guidance for Critical Areas of Focus in Cloud Computing V2.1”*
2. John Bird – *„Basic Engineering Mathematics” fifth edition*
3. Michael Batty – *„Essential Engineering Mathematics”*
4. J. D. Ullman, J. Lescovek, A. Rajaraman – *„Mining Massive DataSets”* third edition
5. Molina, Ullman, Widom – *„Database Systems”*
6. Tim Rougharden – *„Algorithm Design and Analisys”* lecture notes
7. Books and lecture notes from IICSE University PHD in Systems Engineering and Management

Thank you.