COMPASS™
datacenters

IoT: The Present and the Future

The Internet of Things (IoT) is one of the world's fastest-growing technology segments. Over the next ten years, the IoT will become a pervasive presence. It has the potential to make **a substantial impact on every aspect of our lives**, whether it's in the home, our place of business, in airports and other transportation hubs, in hospitals, or in the cities and towns where we live.

The Internet of Things is a subset of technology, made up of numerous types of intelligent and connected devices. At a basic level, the Internet of Things consists of two elements:

- **The Internet** – The worldwide network of smaller networks that connects various devices with each other.
- **Things** – The millions of devices that are connected with and "talk" to other devices via these smaller networks.

However, if you ask 10 different people to define the Internet of Things, you'll get 10 different answers of what IoT technology means to them. **But their answers will all be based on the "Things" they use** – at home, in their jobs, etc. – and how they use them.

If you're an IT executive, it's time to start planning how your businesses, products, and services will incorporate and/or interact with IoT. Even if you've already made some initial deployments of IoT technology, or released some IoT-related products, **you may not have thoroughly examined the world of IoT**, and considered all the options you have, or will have, for utilizing, integrating, and/or profiting from IoT products and services.

This report will give you an overview of the current state, and future, of IoT technology – to set you up with **the insights you need to move forward, in fact to keep pace with, the explosive growth of IoT**.

14180 N. Dallas Parkway | Suite 610 | Dallas, Texas 75254 | 877.289.7577 | compassdatacenters.com

THE CURRENT STATE OF IoT

The statistics don't lie. The Internet of Things is growing at an incredible exponential rate. To quote just a few of the most relevant metrics:

- According to a frequently cited forecast by Gartner, Inc., **there will be 20 billion IoT devices in operation by the end of 2020**, up from 6.4 billion in 2016. Within the next decade, says Statistica, that number is projected to **rise to 50 billion**.
- Currently, in consumer vs. business IoT, the consumer sector is the larger of the two. In 2016, there were about 4 billion consumer-directed IoT devices (or 63%), and about 2.4 billion business-directed IoT devices (or 37%). Future growth in consumer vs. business IoT is expected to follow this percentage split. **Out of the predicted 20 billion IoT devices in operation by the end of 2020 (that's barely a year away), about 12.9 billion will be consumer related.**
- In 2016, spending on IoT devices amounted to $1.38 trillion, with approximately $0.53 trillion spent on consumer-directed devices, and about $0.85 trillion spent on business-directed devices. **In 2020, however, an estimated $2.93 trillion will be spent on IoT devices**, with consumer and business spending being about equal (approximately $1.43 trillion for each side).
- On the business side, a 2018 Vanson Bourne survey looked at 800 worldwide organizations with global annual revenues of $500M+. **One in four of these companies ranked IoT development as their most important initiative.**

It's important to have a realistic perspective on where things stand today with the IoT. If we look at where things are now, we find:

- Many enterprises are still in the early stages of IoT investment and deployment. Organizations are adopting IoT technologies and seeing initial ROIs from their investments, but **some problems still need to be overcome.** (The Vanson Bourne survey found that the most common problem for organizations is a **lack of IoT expertise and skills** among their employees.)
- **Today's IoT technologies are in their infancy, with many more IoT technologies still in the development stages.**
- Also, while many **technologies that support IoT are in place, some are currently too complex or expensive for widespread deployment**. Others, such as 5G networks, are in the "rollout and testing" phase, and it may be a few years before they can be used to bring IoT technologies to their full potential.

14180 N. Dallas Parkway | Suite 610 | Dallas, Texas 75254 | 877.289.7577 | compassdatacenters.com

THE "THINGS" OF IoT

The term "Internet of Things" refers to an entire range of IP-connected devices (sometimes called "Machine-To-Machine" or "M2M" devices). In general, a "connected device" is defined as anything that has a sensor attached to it and can transmit data to another device or person over a data network. Connected devices are the "Things" of the Internet of Things.

One of the most useful ways to look at the current state of IoT is to look at who is *using* which connected devices. The connected devices of IoT fall into several categories that are divided between consumer and industrial applications:

Consumer-Facing IoT Devices

Even if many consumers aren't using (or haven't even heard of) the term "Internet of Things," they know what connected devices are. **They're buying and adopting them at astronomical rates, accepting them into their homes, and using them to automate their everyday lives.** The most common devices are:

- **"Personal assistant" devices**, such as Amazon Alexa, Apple Siri, Google Assistant, and Microsoft Cortana.
- **Wearable devices** such as Internet-connected Smart Watches.
- **Smart entertainment devices** such as smart speakers and home entertainment systems.
- **Smart appliances** such as refrigerators, dishwashers, and washing machines.
- **"Smart Home" devices** such as learning thermostats, lighting systems, video doorbells, and security systems.

The Internet of Things is slowly being integrated into retail, hospitality, and other consumer-facing services. Retailers like Amazon Go, Wal-Mart, and Kroger are introducing **"Smart Stores,"** where customers can automatically pay for items by using their smartphone to scan product barcodes. Also, hotel providers like Hilton are developing **"Smart Hotels,"** which will feature a range of connected devices. For example, hotel guests might use a smartphone app to access their room, in place of a key card.

14180 N. Dallas Parkway | Suite 610 | Dallas, Texas 75254 | 877.289.7577 | compassdatacenters.com

Industrial IoT

The **Industrial Internet of Things (IIoT)** refers to the connected devices that will operate in industrial settings. Many of the "things" of IIoT fall into two categories:

- **Operational Technology (OT) devices** (a.k.a. "smart machines") that automate physical devices (a.k.a. "dumb machines") such as valves and pumps, by turning them on, shutting them down, etc., as directed by a centralized operations system.
- **Sensors** that collect data about conditions and processes and return this data to a centralized IT server for analysis.

The major industry sectors that are currently adopting, developing, and using IIoT connected devices and applications are:

- **Agriculture** – Although still in the early stages, IIoT technology is being developed for use in large-scale crop production and livestock enterprises. Applications in development include everything from sensors designed to measure fertilizer, moisture, and temperature levels (known as precision farming) to **AI-driven robots that will assist in planting, irrigation, and crop harvesting.**
- **Energy** – All sectors of the energy industry (oil & gas, nuclear, solar, hydroelectric, wind) are integrating IIoT technologies. Energy distributors (e.g. power companies) seem to be leading the way in terms of adopting **smart metering sensors to measure distribution levels**. But energy explorers (e.g. oil drillers, solar operators) are lagging behind in integrating IIoT for **exploration, extraction & drilling, real-time process monitoring, predictive maintenance, automation, and tracking of energy production yields.**
- **Manufacturing** – Companies in numerous manufacturing sectors are investing in the development of "Smart Factories," where AI-powered robots and devices automate multiple tasks, and **IoT sensors measure everything from product yields to inventory levels**. (At this time, Schneider Electric has just opened America's first "Smart Factory" in Lexington, Kentucky, manufacturing electrical load centers and safety switches.)
- **Maritime** – Shipping and fishing companies are adopting IIoT solutions, mostly in an effort to keep up with international regulations. For example, many shipping companies are now using **IIoT sensors paired with satellite networks to monitor fuel consumption and emissions for cargo ships.** Fishing companies are using IIoT technology to document and certify that their catches are coming from sustainable sources.

14180 N. Dallas Parkway | Suite 610 | Dallas, Texas 75254 | 877.289.7577 | compassdatacenters.com

- **Mining** – Compared to other industries, the mining industry has been relatively slow to integrate IIoT solutions, but is now looking for ways to utilize IIoT devices to increase automation of mining activities, improve health and safety for workers, and improve environmental sustainability. One example: **Some mining companies are requiring workers to wear connected safety devices that can warn them of unsafe mine conditions, such as the presence of dangerous gases.**

Healthcare

Medical technology companies are now developing IoT devices that will collect and automatically transmit patient data to physicians, giving them insight into the patient's health and symptoms. At the same time, these devices will give the patients who use them more information and control over their own lives and treatments. **The range of connected medical devices includes everything from wearable sensors that monitor heart rate and blood pressure, to Glucose Monitoring Systems and Insulin Pens for diabetics, to connected inhalers for asthmatics, to "smart pills" with ingestible sensors that can be swallowed by patients to track the effects of a certain drug inside their body.**

NOTE: Medical IoT devices and IoT devices used in the transportation and shipping industries are sometimes classified together as "Commercial" IoT devices.

Transportation

Most consumer-owned cars today are "connected cars" with onboard Internet connections that enable the car to access and send data, download software and patches, provide Wi-Fi for passengers, and communicate with IoT devices. The most common IoT applications in consumer vehicles are safety and security (e.g. OnStar), GPS navigation systems, entertainment systems (e.g. BlueTooth), and diagnostics features.

Additionally, transportation-based businesses are rapidly incorporating IoT technologies:

- **Airlines** are heavily investing in IIoT for airplane operations (e.g. onboard fuel & engine monitoring), **navigational aids** (e.g. position tracking beacons and sensors), and **customer-based services** (e.g. in-flight transmitters that allow passengers to connect to outside networks using their smartphones, tablets, etc.).

- **Freight businesses** (plane, railroad, truck) have been using RFID tags for over a decade to track cargo as it moves across the world. They are now incorporating other IoT technologies to improve **operational efficiency, monitor fuel consumption and environmental impact, coordinate operations, and schedule deliveries.**
- Organizations with **large vehicle fleets** (ambulance, construction) are utilizing in-vehicle IIoT devices for fleet management, **including vehicle tracking, route planning, fuel and engine efficiency, preventive maintenance, and sending automated notifications to drivers about weather and traffic problems.**

No examination of IoT would be complete without mentioning **self-driving cars**. At this time, self-driving vehicle technology is still in the development stage. It may be a decade or more before driverless cars are perfected and made available for consumer purchase, and companies feel that driverless vehicles are safe enough to be used in their business.

Government

Local and state governments are rapidly adopting IoT devices in numerous areas.

- **"Smart Cities"** – Major cities have begun the process of integrating sensors and other connected devices into public sector infrastructure systems. For example**, Los Angeles now has over 145,000 connected streetlights and 4,500 connected intersections**.
- **Traffic & Public Transportation Management** – Cities such as Dallas, Texas, are deploying IoT devices to improve traffic flow and reduce congestion for motorists, and to add **automation and responsiveness**, provide data analysis, and **improve efficiency in public transit systems** such as bus services and light rail networks.
- **Utilities** – City and state governments are installing **connected sensors to monitor utility use**, functions and output, maintenance needs, and security on power grids, gas and water supply lines, and sewer systems.
- **Environmental** – Local governments are utilizing IoT sensors to **track and monitor air quality, pollution, temperature, humidity, and weather-related data such as snow levels.** As part of its "Internet of Trees" initiative, for example, Los Angeles is planting or replacing 200,000 trees, with installed sensors to monitor air quality and tree health.
- **Disaster Preparedness** – Cities and states are deploying IoT-based early warning systems. Los Angeles and San Francisco are installing **connected sensors to detect earthquakes**, while other city and state agencies are implementing IoT systems to give **advanced warnings for floods, tsunamis, and forest fires.**

The IoT Business Ecosystem

When high-tech experts talk about IoT ecosystems, they are usually talking about an **ecosystem of *technologies*.** The IoT ecosystem refers to the entire range of technologies that allows connected devices to operate and connect with each other, including networks, gateways, remotes, dashboards, analytics, data storage, and security.

However, there's another IoT ecosystem worth considering here, which might be called the **"IoT Business Ecosystem."** This refers to the range of companies in various high-tech sectors that are either creating specific IoT products or developing technologies that will support IoT purposes (as opposed to companies that are adopting and integrating IoT technologies for use in their products, services, or daily operations):

Device manufacturers – Global manufacturing corporations like GE, Schneider Electric, and Samsung have entire divisions dedicated to creating IoT devices. Even Google has an IoT division, Nest, which manufactures **connected sensors, thermostats, and security cameras.**

Hardware manufacturers – Companies like Dell and HPE are offering bundles that include a **full stack of hardware, software, security, and consulting** for IoT projects.

Hardware component manufacturers – These companies are manufacturing components that will be used to turn ordinary devices into connected devices. For example, chip manufacturers like Intel, Nvidia, and Qualcomm are creating processor **chips to connect consumer devices** such as cars, home appliances, and wearables.

Cloud services – Amazon AWS, Microsoft Azure, Google Cloud, and IBM Watson offer IoT hosting platforms, each with its own set of **tools for IoT device management, connectivity, data collection, and analytics**.

Network providers – Companies like Cisco and Sierra Wireless are creating **gateways, embedded routers, and industrial switches** to provide connectivity between IoT devices, centralized data centers, and edge data centers.

Software Providers – **The range of companies offering IoT software includes everyone** from major players such as IBM, Oracle, and Microsoft who provide IoT services platforms, to "small shop" vendors who are focused on developing IoT solutions for specific business purposes (e.g. supply chain management, asset tracking) or specific markets (e.g. automotive, healthcare).

Service providers – The service providers of IoT are typically companies that provide a combination of home products and subscriptions. For example, a "smart home" products manufacturer may provide connected devices for the home – thermostats, lighting controls, door locks, etc. – coupled with monthly **subscription fees to monitor and support these devices**.

Wireless carriers – The four major U.S. wireless carriers – AT&T, Verizon, Sprint, and T-Mobile – have millions of IoT/M2M connections on their existing networks, and **are currently rolling out dedicated IoT networks** to handle enterprise needs.

The Future of IoT

IoT technology holds great potential to provide consumers and businesses with multiple benefits. But as exciting as its prospects are, **the reality is that numerous problems still need to be addressed if IoT is to reach its full potential**.

The Problems of IoT

Network Latency – Latency is the slow delivery of applications and data over a network. It is caused by several factors, including the distance that data transmissions must travel between servers and connected devices, the **number of network hops** involved, and the **density of network traffic**. Occasionally, latency can result in data loss during transference.

Many IoT devices will require real-time application processing and fail-safe transfer of data. For example, **self-driving cars will require split-second timing and data transfer** to communicate with smart traffic signals, and to avoid collisions with other vehicles and pedestrians. Network latency between IoT devices must be overcome if self-driving vehicles are ever going to operate correctly, to the point where they be accepted as safe by the general public.

Security – A major concern is how to keep IoT devices secure when they are connected to the open Internet. **Cybercriminals have already figured out how to use IoT** devices to launch Distributed Denial of Service (DDoS) attacks (e.g. the 2016 Mirai malware attack, which brought down the servers of Twitter, Netflix, and PayPal).

It should be noted that the lack of security in IoT is more of a cultural problem. Many companies are so focused on perfecting their IoT technologies and bringing them to market that installing security features is often an afterthought. **In the future, companies in the IoT business ecosystem will need to increase their focus on security, to protect IoT devices, systems, and users from outside cyberattacks.**

Privacy – A significant problem for IoT is **who gets access to what data, and how** will they be allowed to use it? This question is especially important due to the many connected devices now being adopted by consumers, which have the ability to collect user data and send it back to their home company. Also, **commercial and industrial users of IoT technology will need to consider what data they will collect, and what regulations they need to follow** (e.g. GDPR) to protect customer privacy and avoid legal and regulatory challenges.

Technology Standards – **At this time, there is a lack of standards for IoT devices and technology ecosystems**. Many IoT systems use a complex mix of protocols and technologies. There is also a lack of business processes for IoT devices, and limited best practices for IoT developers. Multiple IoT standards still need to be established, including:

- Programming and network standards for IoT devices.
- Authentication and authorization standards of IoT devices.
- Standardization of M2M protocols.
- Interfaces for interaction between IoT and security devices and applications.
- IoT life cycle management and maintenance standards.

The Technologies That Will Enable IoT

Several types of technologies will enable the successful deployment, integration, and performance of IoT, and will help to solve the problems described above. **These technologies will work in tandem** to operate connected devices, process and transmit applications, and collect, process, and analyze data.

The Impact of Data Centers

Two different types of data centers will be crucial to widespread deployment and adoption of IoT – traditional data centers and edge data centers.

Edge Data Centers

Edge data centers are distributed data centers that reside on the "edge" of a wide-area network. An edge data center houses IT servers and storage units that provide "edge computing," **or localized computing for connected devices**. Edge computing offers several advantages for IoT:

- By deploying computing resources in close proximity to IoT devices, edge computing cuts the distance that data transmissions have to travel over networks. This **reduces latency and enables real-time application processing**, which is especially important for IoT devices such as self-driving cars.
- Edge computing **improves the performance and reliability of IoT applications**, through localized computing, data storage, and data analytics.
- Edge computing **reduces the cost of data transmission and the risk of data loss by reducing the number of network hops** that IoT applications and data must make between servers and devices.

Examples of how edge data centers may be used in conjunction with IoT include locating them:

- Outside **manufacturing plants** to house the servers that operate robotic machines and collect data from sensors in the facility.
- Throughout **large-scale industrial farms** to support AI-driven farming robots and collect crop and weather data from local sensors.
- In urban areas to **operate smart traffic lights and streetlights**, while transmitting traffic data and commands to self-driving vehicles.

Traditional Data Centers

Traditional data centers will still have a critical role to play in the IoT technology ecosystem. First, the traditional data center will **serve as a host for the centralized IT cloud** (see below) that connects via a wide area network to edge data centers in remote locations.

Second, **we may see traditional data centers of a smaller size deployed in population centers, to host localized IT clouds that will support regional edge data centers** and optimize local IoT resources. For example, a small traditional data center might be opened in a mid-sized city to host a centralized IT cloud for local consumer services, such as "smart home" device services, Internet TV and streaming video, and smartphone-based online video games.

Other Technologies That Will Enable IoT

5G Networks – Major wireless carriers are currently rolling out 5th Generation (5G) networks, which promise greater speed for data transmissions and increased connectivity for edge deployments. The emergence of 5G networks promises to boost consumer demand for IoT products while also fueling further innovation of connected devices and related services.

Cloud and Fog Computing – As mentioned earlier, traditional data centers will continue to host centralized IT clouds, which will connect via wide area networks to edge data centers that provide local computing for IoT connected devices. Centralized IT clouds will be the "central hub" for distributed IoT devices, providing remote device lifecycle management and application enablement and updates. Edge computers will also send data collected from IoT devices back to the centralized IT core for analytics and storage.

Additionally, **edge data centers will host their own internal clouds**, a footprint of servers and storage units that provide aggregated computing resources for the IoT devices they operate. This is known as either "edge computing" or "fog computing." It's also likely that local groups of edge data centers will be connected with each other to form a pool of computing resources known as an "edge cloud."

AI and ML – Many IoT devices use a form of Artificial Intelligence (AI) called Machine Learning (ML). Connected devices are programmed in such a way that when they receive data, the machine can "learn" what the user's preferences are and adjust itself accordingly. For example, in a "smart home," an IoT thermostat may learn your preferred temperature range for different rooms, and adjust the temperature when you are in that room.

Big Data – Real-time processing and analytics is used to analyze data collected from IoT devices and sensors. In turn, some of this data will be used to improve AI and ML models that support operation of IoT devices and M2M communications.

CONCLUSION

Kevin Ashton, the man who coined the term "Internet of Things" back in 1999, recently offered the following advice for businesses who are looking for ways to benefit from IoT technology:

"A lot of CIOs and CEOs ask me, 'What do we do about the Internet of Things?' My answer is always, ***'Start gradually.'*** *I think the worst thing you can do is decide that the Internet of Things is a big deal, and therefore you're going to invest a hundred million dollars in it and hope that it becomes two hundred million dollars in a year."*

"It's really much better to ***look for a small problem that your customer has****, or an opportunity where they want you to deliver to them. Add a single network-connected sensor to a single product or a single, internal process. Get one specific piece of value out of that. When it's working, ask yourself two questions: What would happen if we added another, different sensor to this? Or, what else could we do with the data that our sensor is giving us now? Generally, the answers to those questions lead to more value."*

"And then you ***just ask the questions again****: What if we add another sensor? What if we do something else with this data? And over a period of several years, you go from two sensors to four, to 16, to hundreds. And you go from a few dollars to a few billion dollars of value. Just keep in mind that adjusting to the Internet of Things age is a gradual, continuous process, not some sudden revolution that delivers immediate benefits."*[1]

[1] Kevin Ashton, quoted in "What is the Future of IoT?" by Alison DeNisco Rayome, TechRepublic, July 20,2018. Edited for context.