Internet of Things (IoT)

in the Federal Government

InquisIT

www.inquisitllc.com

Introduction

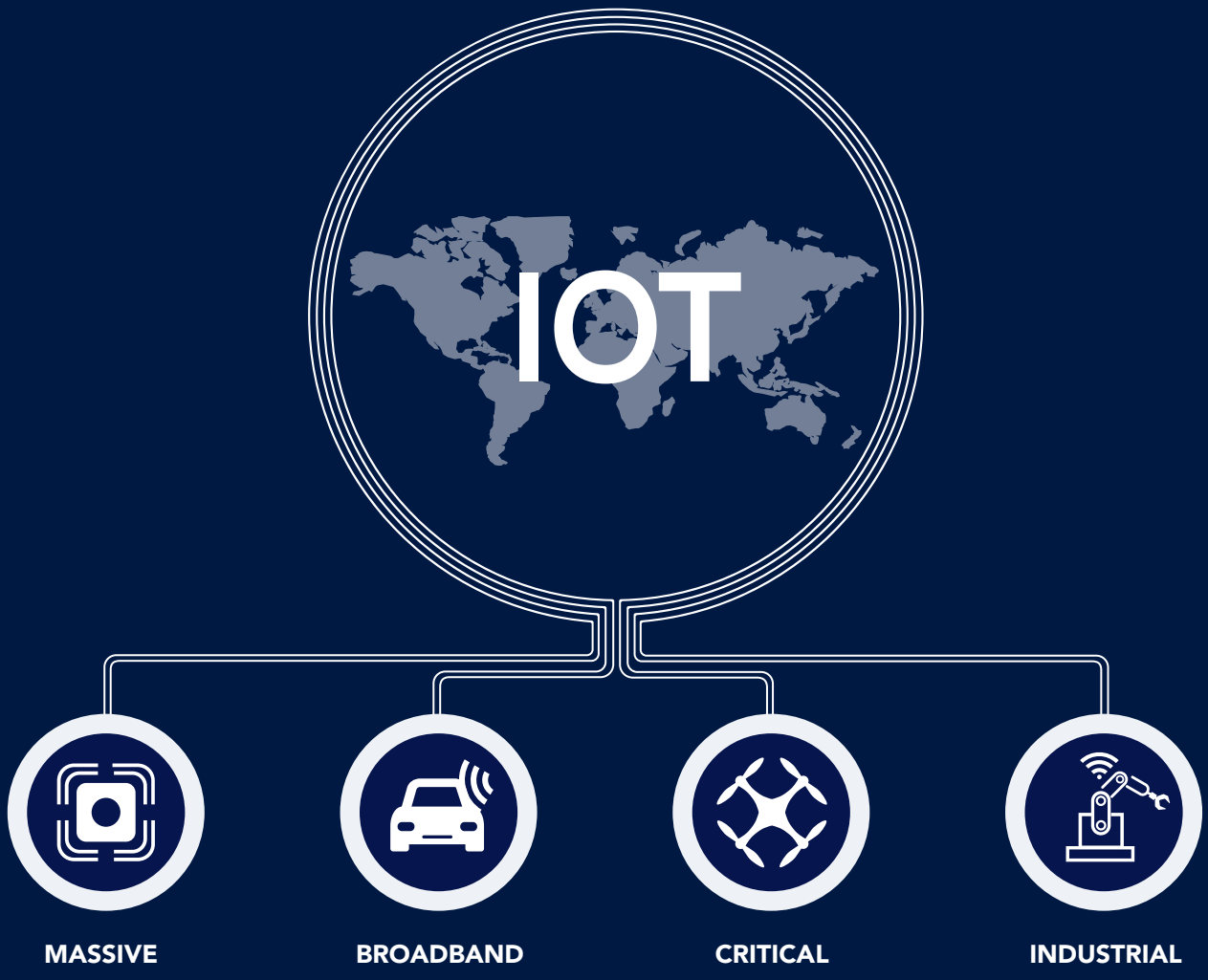
The Internet of Things (IoT) is one of the most impactful IT innovations of our time. As consumers, we already encounter the IoT in our daily lives with "smart" items such as TVs, watches, and phones. As we journey further in time, IoT will become a ubiquitous aspect of life at home and in the workplace.

Gartner defines the IoT as "[…] the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment."[1] More simply, IoT devices are computers (typically very small), that are embedded into an object to perform a function (e.g., collect data, run software) and connect to a network (e.g., the internet). For example, an IoT device could be an assembly line sensor capable of detecting minute deficiencies and determining when equipment needs repair. It could also be GPS-guided agricultural equipment that plants and harvests crops, or even personal fitness trackers that transmit data directly to primary care providers[2].

Adoption of IoT devices within the federal government has been underway for more than a decade, with early use cases typically being asset tracking and surveillance. As advancements are made in telecommunications and micro computing, use cases for IoT devices have expanded greatly and will continue to do so until they are a ubiquitous presence in federal operations. Management of these new fleets of IoT devices will present a significant challenge for federal IT enterprises, as it will become critical to monitor, maintain, and secure hundreds, thousands, or even millions of devices.

IoT Categories

The IoT is divided into four sub-categories: Massive, Broadband, Critical, and Industrial[3]. These categories are defined by their processing and networking capabilities as well as the applications for which they are used. Less powerful IoT categories (Massive and Broadband) require comparatively lower bandwidth and higher latency, and are typically used for low complexity devices. More powerful IoT categories (Critical and Industrial) require higher bandwidth and lower latency, and are most commonly used for complex devices with highly sensitive tasks (e.g., managing a national traffic control system, controlling a factory robot in real-time).



Massive

Massive IoT comprises huge volumes of low-complexity devices that communicate infrequently. The most common Massive IoT use cases are sensors, meters, and trackers[4]. These devices have minimal bandwidth and latency requirements because the data they are transmitting is simple and not time-sensitive.

Broadband

Broadband IoT is applied to wide-area use cases that require higher bandwidth and lower latency than Massive IoT can support[5]. Common applications of Broadband IoT would be car dashboard tablets, advanced wearables, and smart appliances. Broadband IoT device capabilities vary greatly, as they may utilize 4G, 5G, or other similar technologies. By the end of 2026, 44% of cellular IoT connections will be Broadband IoT, and those will primarily be connected via 4G[6].

Critical

Critical IoT is intended for time-sensitive applications that require very low latency and very high reliability. The primary use cases for Critical IoT are real-time media (e.g., AR/VR, advanced cloud gaming), remote control (e.g., Autonomous Vehicles, Unmanned Aerial Vehicle), and mobility automation (e.g., control loops for vehicles and mobile robots)[7]. Critical IoT is powered by the most innovative capabilities of 5G and is enabling exciting new applications such as remote surgery, smart power grids, and intelligent transportation systems[8]. The first modules supporting Critical IoT began deployment this year.

Industrial

Industrial IoT (IIoT) is IoT used in automated industrial settings. These use cases span from simple devices like small sensors that periodically send health reports on factory components, to more complex devices like hydraulic machinery that is remote-controlled by a human operator. IIoT also enhances the use of Operational Technology (OT), which is technology used to automate building functions such as HVAC, lighting, and access control[9]. The recent introduction of 5G has made Critical IoT applications possible in industrial environments. IIoT powered by 5G technology will enable full industrial digitization and herald the next industrial revolution (Industry 4.0)[10].

Technologies Powering the IoT

Massive, Broadband, Critical, and Industrial IoT are each powered by a unique suite of telecommunication technologies. These technologies have different levels of bandwidth capacity, latency, reliability, battery life, and cost. More powerful technologies are often less battery- and cost-efficient and therefore do not suit every use case. The future of the IoT will require the implementation of each of these technologies to cover a wide variety of applications.

LPWAN

Low-Power Wide Area Network (LPWAN) is a category of technologies that provide long-range wireless telecommunication between objects at a low data-transfer rate. "Low-power" describes the main goal of these technologies, which is to conserve the battery life of the device. Battery conservation is achieved through minimizing the frequency and size of data transfers, allowing LPWAN-powered devices to maintain a battery life of up to 10 years[11]. The other primary benefit of LPWAN is a communication range of up to 10km, which is a tremendous advantage over short-range technologies like Bluetooth and WiFi[12]. This is achieved with highly sensitive access-point receivers that can detect signals much fainter than traditional wireless technologies. The two primary LPWAN technologies are NB-IoT and LTE-M.

NB-IoT

Narrowband IoT (NB-IoT, officially classified as LTE Cat-NB) is used for extremely low complexity devices that require minimal communication. "Narrowband" refers to the small frequency band (200kHz) that NB-IoT operates in, limiting its data transfer rate to ~250 kilobits per second[13]. This is well suited to Massive IoT use cases that require vast quantities of cost efficient and battery efficient devices that transmit very little data.

LTE-M

Long Term Evolution Category M (LTE-M), is similar to NB-IoT in that they are both connected via 4G cellular service (better known as LTE). However, LTE-M uses wider frequency bands that enable higher data rates (1-4 megabits per second), lower latency, and more accurate GPS capabilities[14]. LTE-M supports common use cases within Broadband IoT, such as advanced wearables, connected vehicles, and alarm panels. Both NB-IoT and LTE-M coexist with 5G NR and are considered to be future-proof.

5G NR

5G New Radio (5G NR) is the transmission technology that enables 5G, the newest generation of wireless telecommunications standards. 5G NR is able to utilize high frequency signaling (<47gHz) which enables exceptional bandwidth and latency capabilities[15]. In addition, 5G features Ultra-Reliable Low-Latency Communication (URLLC), which is a suite of innovations that minimize transmission delays, provide interruption-free handovers between gateways, and accelerate the processing capabilities of IoT devices[16]. The enhanced capabilities of 5G NR support time-sensitive Critical IoT applications such as collaborative mobile robots, remote control with haptic feedback, and interactive VR cloud gaming[17].

SPE

Single Pair Ethernet (SPE) is an ethernet connection that can operate with just one pair of copper wires (ordinary ethernet connections require four pairs)[18] and plays an important role in IIoT. Industrial networking has historically used proprietary physical data transport technologies like HART and "CAN bus" which require a translator to communicate with ethernet networks connecting the factory floor to offices[19]. This is significant because the translation delays communications, hamstringing time-sensitive IIoT applications that require ultra-low latency (e.g., a factory worker remote-controlling a robot from their computer). SPE solves this problem by providing data transport that is viable for industrial applications and does not require translation. SPE also brings a major bandwidth upgrade, delivering 10 megabits per second (HART delivers 1200 bits per second[20] and CAN bus delivers 1 megabit per second[21]).

The IoT in the Federal Government

The federal government has been utilizing IoT devices for more than a decade. As early as 2011, the federal government was spending billions of dollars a year on IoT solutions[22]. That footprint is increasing over time as capabilities are expanding and new use cases are being developed, as illustrated in the examples on the next page.

Environmental Protection Agency

The EPA uses IoT devices to monitor significant ecological situations nationwide. For example, wirelessly networked sensors placed on water buoys allow the EPA to remotely measure chemical levels of important waterways and detect Harmful Algae Blooms (HAB) that, left unchecked, can shut down water supplies of entire regions[23]. The EPA also used IoT sensors during the 2018 eruption of Kilauea to monitor air quality and provide public health assessments[24].

Department of Transportation

The DoT is investing in many IoT solutions that make roads safer. One such solution is networked traffic signals that detect cars and pedestrians in real time[25]. This would dramatically mitigate risks to pedestrians, reduce wait times, and help anticipate traffic flows across an entire city or region.

Food & Drug Administration

The FDA is guiding manufacturers to use IoT devices in order to meet regulatory requirements. They are recommending the use of Process Analytic Technology (PAT), which provides continuous inline monitoring when transforming raw materials into end products[26]. PAT leverages IIoT networks to collect telemetry on factory floors and provide evidence of compliance to FDA regulations.

In a Government Accountability Office (GAO) survey last year, 62% of federal agencies reported that they are currently using IoT solutions[27]. A majority of agencies not currently using IoT solutions reported that they are planning to deploy IoT devices in the future, primarily in the areas of monitoring/remote-controlling, physical access control, and asset tracking. Also significant is that 75 percent of agencies reported that their use of IoT devices is reliant upon guidance from internal IT personnel. IoT device management is becoming a major component of federal IT enterprise services. To stay relevant, Federal IT service providers will need to adopt innovative solutions that bring value to agencies, keep networks secure, and centralize the management of massive fleets of IoT devices.

Cybersecurity for the IoT

IoT devices can possess vulnerabilities that expose agencies to significant cyber threats if left unaddressed. We cover three primary cybersecurity issues with IoT devices below.

Expanded Attack Surface Area

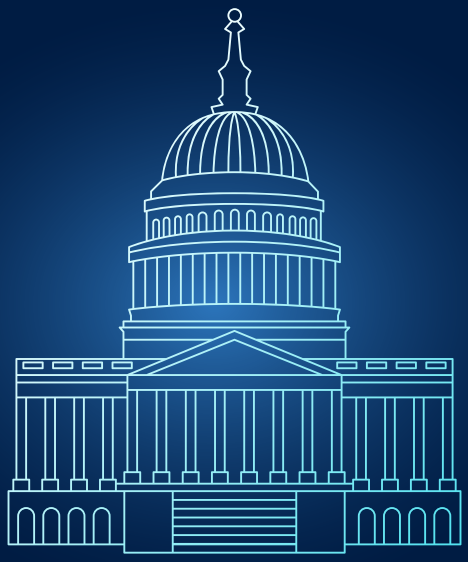
IoT devices introduce a vast quantity of new attack vectors for hackers to exploit. Instead of being limited to traditional entry points like desktop computers or servers, hackers can infiltrate networks via thermostats, refrigerators, or any other IoT-enabled objects. Agencies could see their IT inventories increase exponentially with the addition of IoT devices, and all of those new network-connected assets present opportunities for hackers to break into otherwise secure systems[28].

Lack of Security Functions

Due to their typically small size, IoT devices often lack the computational power required to safely encrypt data[29], provide transparency to asset owners[30], and harden security settings such as passwords and access control lists. IoT devices are especially vulnerable if they connect directly to the internet, which is often the case for devices connecting via commercial cellular service. An unsecured federal asset connected directly to the internet with high-bandwidth 5G is a potential homeland security disaster.

Device Management Challenges

Actively managing IoT devices with software updates, configuration changes, and data-flow monitoring is essential to maintaining cybersecurity. However, active management of IoT inventories is a major challenge due to the sheer number of devices deployed, the limited computational power of those devices, and the lack of management software available for IoT devices[31]. Deploying IoT devices without a management strategy will expose agencies to risk of high-severity attacks that are trivial for hackers to perform (e.g., legacy software exploits, brute force password discovery, DDOS attacks).



IoT Cybersecurity Improvement Act of 2020

To address IoT cybersecurity concerns, Congress unanimously passed H.R. 1668, the IoT Cybersecurity Improvement Act of 2020, which was signed into law last December. The law's purpose is to mitigate IoT cybersecurity risks by establishing rules for the procurement and implementation of IoT devices by federal agencies. The law requires the National Institute of Standards and Technology (NIST) to establish those guidelines, update those guidelines every five years, and publish additional guidelines for reporting and resolving IoT device security vulnerabilities[32].

The law also requires federal agencies and contractors to adhere to all NIST guidelines regarding IoT devices. These mandates will enable federal agencies to safely implement IoT solutions and benefit from the resulting technical revolution without compromising enterprise security.

Conclusion

The IoT is changing the world. In the 1990s, the internet began connecting all computers. By the end of that decade, cell phones began connecting all people. And now, IoT devices are connecting all objects. We will soon exist in a reality where nearly all electronic devices will be globally interconnected – constantly being measured, tracked, and controlled by central cloud-based processors.

We can expect to witness rampant growth of the IoT during the 2020s. Business Insider projects that there will be 41 billion IoT devices by 2027, with the global IoT solution market growing $2.4 trillion annually[33]. The explosion of the IoT will be enabled by falling manufacturing and connectivity costs[34] as well as innovations in cellular communications (5G and beyond) and Artificial Intelligence/ Machine Learning. Eventually, the IoT will be used ubiquitously to provide real-time insights into every asset, process, and system owned by an organization[35].

The integration of the IoT in the federal government is ongoing and accelerating. To facilitate that expansion, federal IT service providers must invest resources into becoming experts in IoT operations and maintenance best practices. The federal government's ability to implement IoT solutions intelligently and securely will be critical in maintaining US geopolitical influence in the coming decade.

InquisIT

InquisIT, LLC.
4301 N. Fairfax Drive, Suite 315
Arlington, VA 22203

Info@inquisitllc.com
www.inquisitllc.com

Endnotes

1 *Internet of Things,* Gartner, https://www.gartner.com/en/information-technology/glossary/internet-of-things

2 Meola, A., *The US government is pouring money into the Internet of Things,* 2016, Business Insider, https://www.businessinsider.com/the-us-government-is-pouring-money-into-the-internet-of-things-2016-5

3 *Cellular IoT Evolution for Industry Digitalization,* Ericsson, https://www.ericsson.com/en/reports-and-papers/white-papers/cellular-iot-evolution-for-industry-digitalization

4 *Ibid.*

5 Ibid.

6 Ibid.

7 Ibid.

8 *Cellular IoT Evolution for Industry Digitalization,* Ericsson, https://www.ericsson.com/en/reports-and-papers/white-papers/cellular-iot-evolution-for-industry-digitalization

9 *Single Pair Ethernet (SPE) is quite simply Ethernet transmission over a balanced pair of conductors. 10Mb/s SPE does some unique things that make it possible to bring Ethernet to the edge of OT networks, Ethernet Alliance*, 2019, https://etherne-talliance.org/wp-content/uploads/2020/08/EA_TechBrief-SPE-OT_final.pdf

10 *Cellular IoT Evolution for Industry Digitalization,* Ericsson, https://www.ericsson.com/en/reports-and-papers/white-papers/cellular-iot-evolution-for-industry-digitalization11 https://www.researchgate.net/publication/324531342_An_Analysis_of_the_Energy_Consumption_of_LPWA-based_IoT_Devices

12 *A Comprehensive Look at Low Power, Wide Area Networks,* LinkLabs, 2016, https://www.link-labs.com/hubfs/LPWAN%20Whitepaper-5.pdf?utm_campaign=00%20LPWAN%20Explained%20%5BWP%5D&utm_medium=email&_hsmi=86164977&_hsenc=p2ANqtz-__Rr6RVtOsPxCHSfE2JfGOiWKNVb3TH4hMoFlAELd7mV2fSzkHsQcmBZCEhJa4h_m6cvRayjM1PNz6mXus-EdQVYM1QrQ&utm_content=86164977&utm_source=hs_automation

13 *Know the difference between NB-IoT vs. Cat-M1 for your massive IoT deployment*, Ericsson, https://www.ericsson.com/en/blog/2019/2/difference-between-nb-iot-cat-m1

14 Ibid.

15 *What different 5G spectrum options mean for your business*, Ericsson, https://www.ericsson.com/en/blog/2020/6/what-different-5g-spectrum-options-mean-for-your-business

16 *Cellular IoT Evolution for Industry Digitalization,* Ericsson, https://www.ericsson.com/en/reports-and-papers/white-papers/cellular-iot-evolution-for-industry-digitalization

17 *Critical IoT connectivity: Ideal for time-critical communications*, Ericsson, 2020, https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/critical-iot-connectivity

18 *Single Pair Ethernet (SPE) is quite simply Ethernet transmission over a balanced pair of conductors. 10Mb/s SPE does some unique things that make it possible to bring Ethernet to the edge of OT networks, Ethernet Alliance*, 2019, https://etherne-talliance.org/wp-content/uploads/2020/08/EA_TechBrief-SPE-OT_final.pdf

19 Higginbotham, S., *Technology Profile: Time Sensitive Networking aims to bring Ethernet to Industrial IoT*, Stacey on IOT, 2017 https://staceyoniot.com/technology-profile-time-sensitive-networking-aims-to-bring-ethernet-to-industrial-iot/

20 Schosker, R., *General Characteristics of HART Communication,* Pepperl+Fuchs, 2014 https://blog.pepperl-fuchs.us/blog/bid/337937/General-Characteristics-of-HART-Communication

21 *CAN Physical Layers*, Kvaser, https://www.kvaser.com/about-can/the-can-protocol/can-physical-layers

22 Meola, A., *The US government is pouring money into the Internet of Things,* 2016, Business Insider, https://www.businessinsider.com/the-us-government-is-pouring-money-into-the-internet-of-things-2016-5

23 *AquaRealTime awarded $100,000 EPA grant*, AquaRealTime, 2020, https://www.algaetracker.com/post/aquarealtime-awarded-100-000-epa-grant

24 Lee, J., *Scientists Deploy an IoT Network to Battle Kilauea's Deadly Fumes*, Particle, 2018, https://blog.particle.io/scientists-deploy-an-iot-network-to-battle-kilaueas-deadly-fumes/
25 *DOT - How the Internet of Things (IoT) Can Bring U.S. Transportation and Infrastructure into the 21st Century,* US Department of Transportation, 2016, https://www.transportation.gov/government-affairs/testimony/dot-how-internet-things-iot-can-bring-us-transportation-and
26 *Industrial Networking Enabling IIoT Communication*, Industrial Internet Consortium, https://hub.iiconsortium.org/networking-enabling-iiot-comm
27 *Internet of Things Information on Use by Federal Agencies,* GAO*, 2020,* https://www.gao.gov/assets/gao-20-577.pdf
28 *NSTAC Report to the President on the Internet of Things*, NSTAC, 2014, https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf
29 *Key technology choices for optimal massive IoT devices*, Ericsson, 2019, https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/key-technology-choices-for-optimal-massive-iot-devices
30 Bedwell, P., *The U.S. Government is Creating Security Standards for IoT Devices*, Security Boulevard, 2020, https://securityboulevard.com/2020/12/the-u-s-government-is-creating-security-standards-for-iot-devices/
31 *Top 10 Internet of Things 2018*, OWASP, 2018, https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf
32 *H.R.1668 - IoT Cybersecurity Improvement Act of 2020*, Congress.gov, https://www.congress.gov/bill/116th-congress/house-bill/1668/text
33 *The Internet of Things Report, Insider Intelligence*, 2019, https://store.businessinsider.com/products/the-internet-of-things-report?IR=T&utm_source=businessinsider&utm_medium=content_marketing&utm_term=content_marketing_store_text_link_the-us-government-is-pouring-money-into-the-iot-2016-5&utm_content=report_store_content_marketing_text_link&utm_campaign=content_marketing_store_link&vertical=iot#!/The-Internet-of-Things-Report/p/59665942
34 *Gartner Says Government IoT Revenue for Endpoint Electronics and Communications to Total $15 Billion in 2020*, Gartner, 2020, https://www.gartner.com/en/newsroom/press-releases/2020-10-05-gartner-says-government-iot-revenue-for-endpoint-electronics-and-communications-to-total-15-billion-in-2020
35 McClelland, C., *What's the Future of IoT?,* IoT For All, 2019, https://www.iotforall.com/whats-the-future-of-iot