Technology Trends

Internet of Things

Enterprise Architecture, Chief Technology Officer Branch

Version 0.1
Date 2019-5-8

Shared Services Canada
Services partagés Canada

Canada

Table of Contents

Business Brief [1]

The Internet of Things (IoT) market has grown tremendously over the past two decades. In 2018, total global spending on smart devices and services is expected to reach $3.7 trillion alone. The general prediction is that there will be 200 billion connected objects by 2020 (26 connected things per human being on earth). This is a great leap forward from the mere 2 billion IoT objects in 2006, and 15 billion in 2015.[2]

The term, Internet of Things (IoT), was allegedly first coined during a presentation entitled "Internet of Things" to Proctor & Gamble in 1999. However, the first IoT device, a Coke machine, already existed in the 1980s as a university project. Today, IoT is fast becoming a tangible technology that can be applied to collect information on just about anything that IT wants to measure and/or control.

There are a variety of ways in which IoT is defined. In general, IoT refers to physical devices (also known as "connected" or "smart" devices) that connect to each other via the Internet.[3] The ability to send and/or receive information makes objects or devices "smart". These smart devices are a mixed network of industrial and everyday web-enabled objects that can be remotely controlled and monitored, and work via a variety of software, cameras, and sensors.[4] The IoT is the two-way connection between the physical and the digital, where a certain extent of control can be exerted.

The IoT evolved from machine-to-machine (M2M) communication. The M2M data is commonly used as a way to determine the health and status of things – inanimate or living. Taking M2M communication to the next level, IoT is a "sensor network" that can be composed of billions of smart devices that connect people, systems, and other applications to collect and share data.

The IoT's systems and platforms enable physical objects and infrastructure to interact with monitoring, analytic and control systems over digital Internet-style networks.[5] Many IT administrators use IoT systems for anything in their physical environment that they want to collect information about. The IoT describes a world where almost anything can be connected and can communicate in an intelligent fashion. With IoT, the physical world is becoming an aggregated information system where everyday physical objects

[1] Further information will be added to this document based on additional research and consultation during the fiscal year 2019-20.
[2] Intel. (2019). "A Guide to the Internet of Things Infographic". Intel Corporation. Infographic. Retrieved 18-Jan-2019 from: https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html
[3] GCpedia. (January 7, 2018). "Internet of Things". GCpedia. Government of Canada Enterprise Security Architecture (ESA) Program. Government of Canada. Retreived 14-Jan-2019 from: http://www.gcpedia.gc.ca/wiki/Internet_of_Things
[4] Canadian Centre for Cyber Security. (2019). "Glossary". Government of Canada. Retrieved 15-Jan-2019 from: https://cyber.gc.ca/en/glossary
[5] Forrester. (2018). "Forrester Glossary". Forrester Research Inc. Retrieved 14-Jan-2019 from: https://www.forrester.com/staticassets/glossary.html#heading-i

are connected to the internet and are able to identify themselves to other devices. This is significant because an object that can represent itself digitally becomes something greater than the object by itself. The object no longer relates just to its user, but is now connected to the surrounding environment, objects, and to database data. When many objects act in unison, they are said to have "ambient intelligence"[6].

There are many types of IoT smart devices, and more emerge every day. The IoT technology in the home can consist of entertainment systems, including televisions, gaming systems, speakers, and headphones, as well as heating/cooling systems such as the thermostat, ceiling fan, carbon monoxide detector, smoke alarm, and lights. Home security IoT systems include alarms, smart locks, garage door openers, baby monitors, cameras, and home assistants. Home IoT appliances can include refrigerators, coffee makers, the oven, and the vacuum cleaner. External IoT objects can include connected smart cars, buses, trains, and airplanes. They also include wearables like fitness trackers and smartwatches, and healthcare devices like heart and blood pressure monitors. Even pets can be connected via IoT with a tracking collar. By combining these connected devices with automated systems and Artificial Intelligence (AI), it is possible to gather new information, analyse it in real-time, and create an immediate action to help with a particular task, improve processes, or gain new insights.

Technical Brief

Internet of Things refers to the ever-growing network of physical objects that feature digital Internet connectivity. The IoT technology works via web-enabled[7] smart devices that transmit information gathered from their surroundings using embedded sensors, software, and processors. The IoT extends Internet connectivity beyond traditional devices like desktops, laptops, smartphones and tablets to a more diverse range of devices, everyday objects and industrial devices that communicate via the Internet.

First, sensors or devices collect data from their environment. Data is then sent to the cloud connected through a variety of methods including: cellular, satellite, WiFi, Bluetooth, Low-Power Wide-Area Networks (LPWAN), an IoT gateway, other edge devices, or by connecting directly to the internet via Local Area Networks (LANs) or Wide Area Networks (WANs).[8] Some IoT devices have internal systems that are capable

[6] Ambient intelligence (also known as "ubiquitous computing") refers to electronic network technology that pervades physical environments to the extent that they become responsive and user interactive. Reference: Techopedia. (June 24, 2016). "The Awakening of Ambient Intelligence". Techopedia Inc. Retrieved 29-Jan-2019 from: https://www.techopedia.com/2/31587/it-business/it-marketing/the-awakening-of-ambient-intelligence

[7] In some cases, they are not per se web-enabled, but still provide interaction through similar protocols.

[8] Each option has tradeoffs between power consumption, range and bandwidth (here's a simple explanation). Choosing which connectivity option is best comes down to the specific IoT application, but they all accomplish the same task: getting data to the

of processing and analyzing data at their local level, such that data sent to the cloud is not simply raw data. In other words: data processing can occur closer to the point of contact, at the edge of the network. Edge computing and processing has become a major component in IoT. This saves data-driven decision-making time by allowing the IoT device to act upon its own analysis, rather then sending large data volumes to a data centre's analytic system and waiting for that system to signal an alert or make a decision. The connectivity, networking and communication protocols used with these web-enabled devices depend largely on the specific IoT applications deployed.

Once data gets to the cloud, analytic software processes it to enable decision making. This could be very simple, such as checking if a temperature reading is within an acceptable range, or very complex, such as using computer vision on IoT video to identify objects (such as prolonged unattended bags at airports). This information is made useful to the end-user in some way, usually in near real-time with an alert (email, text, notification, etc), although many IoT reactions can be performed automatically via predefined rules set by the user. As such, most of the work is done by the IoT devices without human intervention, although users can interact with the devices through initial set-up, establishing pre-defined instructions, or by accessing data.

The Operating Systems (OS) that run IoT devices are usually lightweight systems, which manage the device hardware and software resources. These OSs provide common services and APIs for IoT connectivity, management, security, computing, and analytics. This has the effect of boosting battery life depending on device and software efficiency. Additionally, IoT platforms connect to and manage multiple and diverse smart devices and infrastructure in order to integrate and control operational data into business and customer processes. These platforms are comprehensive Platform as a Service (PaaS) and are used for the rapid design, development, and deployment of the largest-scale big data, predictive analytics, AI, and IoT applications for any business value chain. These platforms may include Identity and Access Management (IAM) to manage the identity life cycle, governance, and authentication of IoT devices on the network. The IoT platforms monitor and manage the IoT devices, including the management of security patching and on-boarding of new IoT products. The IoT platforms are required in order to ensure patching is rigorously tested and deployed with a robust set of checks in place to confirm that IoT devices have been properly updated.

cloud. Reference: McClelland, Calum. (November 20, 2017). "IoT Explained — How Does an IoT System Actually Work?" A Medium Corporation. Medium.com. Retrieved 29-Jan-2019 from: https://medium.com/iotforall/iot-explained-how-does-an-iot-system-actually-work-e90e2c435fe7

Industry Use

The Fourth Industrial Revolution (Industry 4.0), is the fourth major industrial era since the Industrial Revolution began in the 18th century. It is characterized by technology that blurs the line between physical and digital (cyber-physical systems). The IoT, an important part of digital infrastructure, has emerged within Industry 4.0 as one of the fundamental technologies helping to create the "factory of the future". Industry 4.0 transforms the traditional production system into the new model called "Industrial Internet of Things" (IIoT). The IIoT involves accessing real-time data that allows manufacturing partners and their machines to share information accurately and quickly. The goal of Industry 4.0 is to achieve low-cost production efficiencies and create more reliable operations by leveraging IoT and automation. In this new IIoT paradigm, supply chain and material handling processes become integrated across the company, producing "lean manufacturing". In the oil and gas sector, oil companies spend substantial amounts on procuring and operating special-purpose oil drilling machinery. Smart sensors attached to oil rigs and the related equipment can continuously monitor and recommend preventative maintenance, enabling significant reductions in operating costs.

There are numerous other industry applications of the IoT. Smart sensors in homes can carry out real-time pollution or pollen counts for asthma sufferers, consumers can be notified of lower operational costs via alerts on the optimum usage of dryer/washing machines, and control of heating/cooling and lighting can be optimized to suit the users needs. Wearable IoT devices, such as the Apple Watch or Samsung's Galaxy Watch, have sensors and software that collect and analyze user data, sending messages to other technologies about the user with the aim of making users' life easier. Smart devices can monitor various bodily activities and metrics to enhance safety and maintain health. Certain devices can track people's activity levels and help change their behaviours to improve well-being. Medical sensors, for example, can support overall health by monitoring blood sugar levels and dispensing insulin when necessary. New insights are gained as a result of analysis conducted on new and greater volumes of data that are collected via the IoT.

In healthcare, IoT offers many benefits, including the ability to monitor patient health more closely and to use the data that's generated for real-time and historical analysis. Hospitals often use IoT systems to complete tasks such as inventory management for both pharmaceuticals and medical instruments. In agriculture, IoT-based smart farming systems can help monitor, for instance, light, temperature, humidity and soil moisture of crop fields using connected sensors and IoT is instrumental in automating irrigation systems.

The IoT can also make public transportation more efficient and safer, as well as offer a more pleasant ride to commuters and provide cities with financial savings. Connected

trains display arrival and departure times so passengers can plan accordingly. Individuals can look at their smartphones to know the exact time to leave their houses to catch a train or the bus. In smart cities, the public transportation options are connected to buildings as well, so transport managers can provide more buses and trains after a sporting game or concert when there are more people in one area of the city. City managers can send public service announcements to connected individuals around the city who can then heed warnings or take action as necessary. New IoT features such as touchscreens in these locations can help riders find directions, check the weather and view real-time arrival and departure times.

Canadian Government Use

Internet of Things has the potential to transform the public sector by profoundly altering how government entities gather data and information by bringing together the major technical and business trends of mobility, automation, and data analytics. Although the Government of Canada (GC) has a large focus on introducing mobile applications to improve citizen interactions in obtaining GC data and services,[9] the broad adoption and use of IoT in the GC is still in its infancy. The Treasury Board of Canada Secretariat (TBS) is developing[10] an IoT guidance, overarching strategy, and policy direction. However, many departments, such as the Canada Border Services Agency (CBSA), have adopted IoT pilot programs without guidance in order to help solve their complex issues.

Although the CBSA is not the only GC department leveraging IoT, it provides a clear use case. The CBSA delivers integrated border services that support national security and public safety priorities and facilitate the free flow of legitimate trade and travel.[11] The IoT touches on many aspects of CBSA's operational technology that range from standard desktop computers with document readers attached to audio/video surveillance systems, RFID systems, non-intrusive imaging systems (e.g. X-Rays), non-intrusive detection systems (e.g. radiation/drug detectors), face recognition systems, and mobile/wearable devices. The CBSA uses IoT devices to sense, collect, analyse, and control situations, while also capturing vital information, providing deterministic automated responses, real-time alerts for officers, and data for trend analysis.

[9] Treasury Board of Canada Secretariat. (April 1, 2013). "Standard on Optimizing Websites and Applications for Mobile Devices". Treasury Board of Canada Secretariat. Government of Canada. Retrieved 22-Jan-2019 from: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27088

[10] Treasury Board of Canada Secretariat. (August 13, 2018). "Digital Policy: Ideas Stage - Report on What We Heard". Government of Canada. Retrieved 13-Feb-2019 from: https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/digital-policy-ideas-stage-what-we-heard-report.html

[11] Mungham, Tony. (April 19, 2018). "Integrating IoT to Bring Ideas to Life". IoT613 Conference 2018, Connected Transportation. Border Technology Development Team. Science and Engineering Directorate. Canada Border Services Agency (CBSA). Government of Canada.

Economic and political pressures have increased the expectation for all GC departments to respond to operational challenges, without significantly increasing the existing workforce or operational footprint. Using the IoT, the focus of GC operations shifts toward higher efficiencies and facilitating services.

Implication for Shared Services Canada (SSC)

Value proposition

Deploying IoT devices and platforms offers a number of benefits to organizations such as: assisting in monitoring overall business processes; improving customer experience; saving time and money; enhancing cost-effectiveness; enhancing employee productivity; integrating and adapting business models; improving business decisions; and generating more revenue. The IoT can also assist in real-time and near-to-real-time visibility of the IT ecosystem and help in the pursuit of transforming traditional business to a data-driven business. The business impact of new data from IoT can help inform situational awareness, drive process improvements, and lead to overall better business decision making.

In most cases, organizations leverage the IoT to assist in boosting their existing processes as well as improving optimization, and business models. Organizations first use IoT to increase efficiency, reduce cost, or improve utilization rates. While this is beneficial, it largely keeps a business-as-usual culture. By contrast, leading organizations use IoT to fundamentally alter and enhance their business models based on the new data, analytics, and automation possibilities accrued from IoT. Here, the balance can shift from improving existing processes to transforming the business with entirely new models since almost all parts of the business processes become interconnected through the IoT. In today's integrated world, it is not enough to rely on business data from isolated business systems.

The IoT can assist in one of the GC's most complex areas – asset monitoring and control. Managing assets across the country where distances are vast and device numbers are huge, lessening the burden of asset tracking, monitoring, and managing would be a great benefit. The GC has a tremendous amount of materiel and assets which must be managed in a financially responsible way.[12] Assets and materiel must be managed by

[12] Total GC financial assets totalled $398.6 billion, and non-financial assets amounted to $87.5 billion at March 31, 2018. Reference: Department of Finance Canada. (October 19, 2018). "Annual Financial Report of the Government of Canada Fiscal Year 2017–2018". Department of Finance Canada. Government of Canada. Retrieved 25-Jan-2019 from: https://www.fin.gc.ca/afr-rfa/2018/report-rapport-eng.asp

departments in a manner that supports the cost-effective and efficient delivery of government programs.[13]

Challenges

There are many challenges SSC will face in the development and deployment of IoT devices and platforms. Most notable is the large amount of time, guidance, effort, resources, and funding required for establishing and maintaining a robust GC IoT program that also has a high level of interoperability. Additional planning will be needed for SSC's infrastructure to accommodate increased IoT data traffic and data processing.

Security is one of the biggest challenge facing IoT initiatives. The IoT connects billions of devices to the internet; these devices also represent billions of network end points, all of which need to be secured. Due to its expanded "attack surface", IoT security and IoT privacy are cited as major concerns. Hackers will target networks via IoT devices through their default usernames/passwords, which are usually admin/admin. Additionally, there is no single IoT industry standard for communication between IoT devices, although a number of competing groups have formed with the aim of designing the IoT standards of the future. The IoT standard-less situation resembles the early days of mobile operating-systems.[14] This lack of standards increases the complexity of managing network security. This poses significant risks to critical infrastructure, including electricity, transportation, and financial services as IoT devices are potential access points into these critical systems. Certification has emerged as a means to confirm IoT devices are secure, but there still remains no central standard.

In many cases, IoT devices lack the technical ability to apply security patches when vulnerabilities are discovered and as a result, exposed IoT devices can be used to carry out malicious activities.[15] In general, most IoT devices use proprietary software with weak encryption schemes and limited endpoint security to protect information. Many things connected to the internet also tend to send information about their use back to

[13] Treasury Board of Canada Secretariat. (November 1, 2006). "Policy on Management of Materiel". Treasury Board of Canda Secretariat. Government of Canada. Retrieved 25-Jan-2019 from: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12062

[14] While there may be a role for federal agencies to play in setting out IoT guidelines for specific critical industries—such as ensuring interoperability of electronic health data—full government regulation of IoT standards may actually slow innovation rather than accelerating it. Reference: Mariani, Joe. (February 14, 2017). Guiding the IoT to Safety: The Internet of Things and the role of government as both user and regulator." Deloitte Insights. Deloitte Touche Tohmatsu Limited (DTTL). Retrieved 24-Jan-2019 from: https://www2.deloitte.com/insights/us/en/focus/internet-of-things/regulating-iot-technology-role-of-government.html

[15] Communications Security Establishment. (June, 2017). "Cyber Journal". Communications Security Establishment. Government of Canada. Cyber Journal – Edition 11 – June 2017. Retrieved 28-Jan-2019 from: https://www.cse-cst.gc.ca/en/node/2097/html/27699#a4

the manufacturer, which can be hacked by outside parties.[16] Likewise, if manufacturers don't update their devices regularly, or at all, they leave their products vulnerable to cybercriminals. In many cases, IoT devices lack the actual technical ability to apply security patches that are pushed by the manufacturer when vulnerabilities are discovered.[17] As with any emerging technology, mitigations and streamlined patch solutions are not always available.

Privacy is another major concern for IoT users, including GC employees who may be required to input personal information on IoT devices in order to use them for work purposes. Connected devices often ask users to input their personal information, including names, ages, addresses, phone numbers, and even social media accounts – valuable privacy information for hackers. Public Service organizations may also expose employees to privacy risks by asking them to use these IoT devices, thereby increasing their digital footprint beyond what the employee would normally have done. Lastly, even the companies that make and distribute consumer IoT devices could use those devices to obtain and sell users' personal data either legally through terms of use or illegally.

Implementing an IoT project with real-time analytics is a complex undertaking. For most organizations, the technological logistics to interconnect IoT devices and the increased levels of data traffic are unprecedented. Even consumers who have purchased one of the myriad smart home products – from lightbulbs, switches, to motion sensors – will attest to the fact that IoT is in its infancy, where products and devices do not always easily connect to or work with each other. In order for IoT to work in data centers and platforms from competing vendors, the devices need to be able to communicate with one another. Focusing on organizations, project managers who wish to use IoT tools may find that their IT departments simply cannot provide the ability to connect all the IoT devices or the back-end IT infrastructure needed to collect, store, and analyze the new streams of data.

Data privacy and integration is always more costly and more difficult to implement than organizations originally estimate.

Considerations

A strategic policy approach to IoT investments will need to be developed to ensure that the IoT opportunities are properly leveraged. The GC invests a significant portion of its annual budget on IT and supporting infrastructure. Without strategic IoT direction, the

[16] Canadian Centre for Cyber Security. (September 1, 2017). "How to #ConnectSmarter on the Internet of Things (IoT)". Canadian Centre for Cyber Security. Government of Canada. Retrieved 25-Jan-2019 from: https://www.getcybersafe.gc.ca/cnt/blg/pst-20170901-en.aspx

[17] GCpedia. (January 7, 2018). "Internet of Things". GCpedia. Government of Canada Enterprise Security Architecture (ESA) Program. Government of Canada. Retreived 14-Jan-2019 from: http://www.gcpedia.gc.ca/wiki/Internet_of_Things

fragmented approaches to IT investments, coupled with rapid developing technology and disjointed business practices, can undermine effective and efficient delivery of GC programs and services. [18]

A clear vision and mandate for how IoT will transform services and what the end-state IoT initiative is supposed to look like is a prominent consideration. In fact, most IoT considerations will need to be made on the non-technical side. Questions such as why a particular IoT solution is needed, what business requirements it will solve, how clients will use the IoT service from SSC, what the IoT service should look like from a client's perspective etc., should all be taken into account first. Often the organizational cost of deploying and integrating IoT is higher than expected with regard to funding, time, and resource expertise.

Considerable IoT needs and requirements come from the operational level of an organization. This includes managers and/or operators who require additional visibility on their operations or devices, for example asset handlers, transportation managers, database managers, project managers, etc. Usually, IoT projects are enacted for small focussed problems by these lower organizational personnel. Due to little to no upper management strategy and guidance, these projects often do not notify or even involve IT in the process. This often leads to quick but siloed implementations where old off-the-shelf IoT tech is used, which frequently fails or is not operational. Thinking strategically may not be part of lower operational personnel's job requirements. Many of these personnel are attempting to solve a small isolated problem they have without much thought for how an IoT solution could help the rest of the organization, making senior management strategic policy and direction so crucial to consider for IoT investments.

Additionally, strategic guidance will need to be considered regarding the analytic capabilities required for IoT deployments. Considerations for how much data traffic can be accommodated by the network and data centres, as well as what type of data and information should or should not be collected, will need attention.

Enterprises like SSC should be cognisant of not flooding their ability to conduct business with massive amounts of data without properly planning for its analysis, simply due to a fear-of-missing-out. An IoT device on its own does not understand what is happening around it, meaning that IoT devices and near-to-real-time analytics constitute a package that go hand in hand. Organizations will often deploy IoT for a specific purpose in silos but fail to handle the new influx of data or fail to connect these devices with other systems for aggregate analysis.

[18] Treasury Board of Canada Secretariat. December 3, 2018. "Directive on Management of Information Technology". Treasury Board of Canada Secretariat. Government of Canada. Retrieved 27-Dec-2018 from: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=15249

To add value, organizations should consider the Analytics of Things (AoT)[19] before creating sensors that stream enormous amounts of data to databases from the devices. This also means that decisions will need to be made on how much local processing the IoT device does, including what data to keep, what data to abbreviate or discard, what data to segment off and send immediately as an alert, and what data to simply log on local storage that can be later retrieved manually by personnel and transferred to databases for review. There are specific data transmission needs due to privacy retrictions or national security, where the data classification may not allow the information to be transferred over the network and instead require a physical pick-up for data transfer.

Additionally, there is a significant consideration to be made on whether real-time visibility and analytics is a business requirement or if near-to-real-time is adequate. In the vast number of business cases, real-time visibility is almost never needed for business operations. Near-to-real-time is sufficient for the vast majority of business processes, however, senior executives will need to consider the policy when deciding what processes will actually require real-time analytics.

Although security has been flagged as an issue, most of the IoT security issues can be resolved by banning the use of default device passwords of any device that comes onto the network. Banning default password and setting the IT requirements for any device that connects to the network will be a paramount project for SSC to consider in the future. In this way, the diverse nature of IoT services can be better managed based on the requirements set out by SSC. Shared Services will need to remain open to many different IoT solutions, however, it may want to consider how particular it will be concerning the low-level requirements of devices and software implemented on the network.

Shared Services will need to consider how to ensure it is an agile and flexible IT service provider as it pursues IoT deployments. This will be vital since the value, impact, and success of IoT initiatives can vary greatly from one organization to the next. Many enterprises have launched pilot projects to develop IoT-enabled products and services or have used the IoT to achieve operational improvements. Of these, less than 30 percent have taken their IoT programs beyond the pilot phase.[20] Even among companies with large-scale IoT efforts, a significant gap separates the top tier of performers from the bottom tier. The continued support and use of Open Standards, Open Source, and standard APIs may need to be considered as a means to maintain

[19] The concept of AoT is the analysis of the data collected from IoT devices. Reference: Pal, Kaushik. (August 11, 2016). "Analytics Of Things: Taking IoT to the Next Level". Techopedia Inc. Retrieved 22-Jan-2019 from: https://www.techopedia.com/2/31958/trends/big-data/analytics-of-things-taking-iot-to-the-next-level

[20] Chui, Michael, et al. (2019). "What separates leaders from laggards in the Internet of Things". McKinsey & Company. Digital McKinsey. Retrieved 22-Jan-2019 from: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/what-separates-leaders-from-laggards-in-the-internet-of-things

SSC as an agile and flexible organization. No single IoT platform will be able to meet all the diverse technical and business requirements of IoT devices and business processes. Using Open Source and Open Standards may be needed in order to accommodate diverse devices and software.

Lastly, SSC may wish to consider evaluating the current Service Catalogue in order to determine where IoT can be leveraged to improve efficiencies, reduce costs, and reduce administrative burdens of existing services as well as how a new IoT service could be delivered on a consistent basis. Any new procurements of devices or platforms should have high market value and can be on-boarded easily onto the GC network.