The Internet of Things

Dr. Anurag Agarwal and Dr. Bhuvan Unhelkar

College of Business, University of South Florida (Sarasota-Manatee), Sarasota, FL, 34243. USA

agarwala@sar.usf.edu bunhelkar@sar.usf.edu

Introduction

The "Internet of Things", or the IoT, refers to an infrastructure of ubiquitous, context-aware devices communicating and interacting with each other over the Internet to accomplish some objective(s). The Internet of Things Global Standards Initiative (IoT-GSI) defines IoT as: *A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies*. Many existing technologies, such as the Internet platform, sensors and sensor networks, RFIDs, mobile computing, and the cloud which have evolved over the last few decades and are continuing to evolve, are now converging and integrating to create the IoT infrastructure. Traditionally, devices equipped with RFID and NFC chips, could only be used locally due to their limited near-field communication capabilities but with advances in telecommunications and the Internet technologies, the same devices can interact globally – ushering in the era of the IoT.

Devices interacting in the IoT infrastructure are referred to as IoT devices or smart objects. Each device is identified by a unique IP address. Some examples of IoT devices include self-driven vehicles, smart phones and smart watches. The number of active IoT devices in the world are estimated to reach over 50 billion by 2020 up from an estimated 25 billion in 2015. IoT devices can sense the context (i.e. their operating environment) through appropriate sensors, process the sensory data and become context aware and thereby build ambient intelligence and communicate with other IoT devices or humans. Theoretically, any device such as a refrigerator, a garage door opener, a thermostat or a drone, when equipped with sensing, processing and networking capability can act as an IoT device. IoT devices can be programmed to take certain corrective actions with the help of actuators based on the ambient intelligence gathered through sensors. They can also be programmed to learn from the environment in which they are operating and take certain actions. With the IoT, communication is possible between any two IoT-enabled “things”, at any place and at any time.

The Technology

The underlying IoT technologies can be broadly divided into hardware, software and architecture. In terms of hardware for the IoT, the critical elements include RFID (Radio Frequency Identification Devices), NFC (Near Field Communication), sensors and sensor networks and the Internet communication platform. The RFID technology is used to uniquely identify objects using RFID tags that include an Electronic Product Code or EPC. This RFID technology has been used for decades for purposes of tracking big ticket items such as vehicles and livestock. As the cost of RFID tagging has declined over the years, RFID tags are being used to tag even low-value items such as items at a grocery store or a retail outlet, for the purposes of tracking inventory or scanning objects for checkout or for monitoring inventory levels. The benefits of RFID, which were limited to close proximity, can be extended globally by replacing the EPC with a unique IP address and letting it communicate over the Internet.

The NFC technologies, which are rooted in RFID technologies, are a set of short-range wireless technologies, effective within 10 cm range typically. One NFC device is considered the active device (acting as the initiator) and the other is the passive (acting as the target). The, initiator device generates a radio frequency that powers the target device. NFC tags contain data which are usually read-only, but may also be writable. Another critical hardware component for IoT devices is sensors, used to sense and monitor the relevant aspects of the environment. Some examples of sensors include cameras, thermometers, barometers, motion detectors, distance sensors, speed sensors, heart rate sensors, blood pressure readers, transducers etc. When multiple sensors are used together, they form a sensor network. Sensor networks may also contain gateways that collect data from the sensors and pass it on to a server. The most critical hardware component for the IoT is the Internet communication network without which no communication is possible.

For all the hardware pieces to work together, new software must be written to support the devices and support the interoperability between numerous heterogeneous devices in the IoT. The software to power the IoT can be broadly classified as middleware and searching/browsing software. The IoT middleware sits between the IoT hardware and data and the applications that developers create to exploit the IoT to accomplish the intended objective. The IoT also relies on searching/browsing software for maximum effectiveness. The IoT browsers are different from the traditional web browsers because while the web search engines are designed to display and index relatively stable web content, the data in an IoT environment is very dynamic and massive as the data is most likely generated by a device in motion. IoT search engines need to be capable of searching high velocity, rapidly changing information generated by IoT-enabled objects.

To make the IoT function effectively, well-designed architectures are needed to represent, organize and structure the IoT. Architecture for IoT can be further classified as hardware/network architecture, software architecture and process architecture. Hardware/network architectures can be peer-to-peer or autonomic. Software architectures are necessary to provide access to and enable the sharing of services offered by IoT devices. Service oriented architectures (SOA) and representational state transfer (REST) model have been proposed for IoT because of their focus on services and flexibility.

Sourcing of data with IoT devices can include a wide variety – such as "crowd generated" machine sensor data, audio and video data and collaborative meta-data from one or more IoT devices. Finally, process architectures are necessary to structure and optimize business processes with IoT.

Applications

IoT is a rich technology for many practical applications at both individual and industry level. While many applications are already implemented in practice, many more are likely to emerge in the future as the possibilities are endless. Some areas of applications include smart infrastructure, smart homes, retail, healthcare, law enforcement, energy and mining, supply chains and logistics, manufacturing, military and social applications.

For example, IoT enabled smart infrastructure enables the vision of self-driven vehicles to become a reality. Self-driven vehicles use IoT driven GPS technology to navigate to their destinations. Through sensors, they are able to stop at traffic lights, change lanes, and navigate traffic with the help of context awareness and ambient intelligence. On a broader scale, IoT driven technologies can be employed to make cities more efficient. For example, in smart cities, IoT-enabled emergency vehicles and public transportation buses can interact with IoT-enabled traffic lights to allow them to their destinations faster and serving its citizens better. Taxi hailing services have been made possible through the IoT infrastructure.

Smart homes, equipped with sensors can optimize the use of electricity and gas and reduce waste. Smart homes can also allow remote access to control the thermostats, appliances and shades. Smart home technology, which is IoT based can also be used to monitor the residents, particularly elderly residents and call for response team or other help if necessary. Retail sector can capitalize on IoT applications such as “Fast Retail” checkout optimizers (integrated with RFID chips), shopper analytics, supply-chain visibility and optimizing service provider staff’s processes. Telecommunications and Information sector can use IoT enabled (video, mobile, social) applications that assist in operations optimization, equipping next-generation worker with current statuses, tower management through remote chips and tools, and even optimized service fleet management.

Healthcare is another domain where extended care, remote patient monitoring, staff mobility and security are key areas of application of IoT devices and applications. Good healthcare often depends on timely detection of a current or impending health issue and taking timely action to address the issue. Often, the patient living alone is unable to call the emergency number on account of disability due to a health condition. With appropriate sensing and actuating IoT devices, many health crises can be obviated by calling for help in a timely manner. For example, devices that can monitor heart rates, or falls or stroke symptoms or any other detectable medical condition can call for emergency care when necessary. In that sense, monitoring and decision making can be shifted from the humans to machines. Also, data from sensors can be continuously transmitted from the patient to the doctor’s office, or family members and other interested parties who can take appropriate actions in a timely manner. With advances in wearable sensors, such as smart watches and even sensors embedded in fabric, a much closer health monitoring is possible. Smart watches can send data to personal trainers who can recommend modifications to one’s life style to improve their health.

In supply chain management, RFID and sensor networks have long played a role in improving their effectiveness through continuous monitoring of flow of assets through the supply chain. The ubiquity and pervasiveness of the IoT will enable the use of these technologies across organizations and geographic boundaries. So, theoretically, it will be possible to locate any asset anywhere in the world, as long as it is tagged with a unique identifier and is IoT enabled. Traditionally, assets could only be located while they were at a warehouse or a store, and not during transit. With IoT, assets can even be tracked during transit. Theoretically, every piece of mail, can be IoT enabled and tracked without having to explicitly enter its current location. Inventory levels at retail shelves and warehouses can be monitored and manufacturers can get an idea of how fast certain items are moving through the supply chain. Manufacturers can plan their manufacturing activities more accurately, warehouses and retail can place their orders more timely and in appropriate quantities, resulting in less surplus or shortage throughout the supply chain.

IoT can also be used in preemptive and timely maintenance of equipment. The sensing technology has advanced enough that impending failures of equipment can be detected prior to actual failure. This information, when transmitted to the appropriate persons can allow preemptive maintenance and saving losses resulting from failed equipment.

IoT can be very useful in law enforcement. Stolen cars, for example, can be traced with pin-point accuracy as each car will have an IP address and can be tracked remotely. Another practical IoT application in law enforcement is the Breath Alcohol Analyzer (BAA). This BAA is an IoT-based device used to monitor the breath-alcohol level of drivers. By periodic sampling of breaths while driving a vehicle, the driver and the law enforcement agencies can be alerted to the danger on the road. Additionally, smoothness of the drive itself can be evaluated using appropriate sensors, such as telematics device and vehicle’s curb camera.

In the domain of physical security and safety, the IoT-based surveillance of public places will enhance the overall physical security. The technology can also be used to detect counterfeit goods and spare parts used in airline or automotive industry.

There are a number of potential social applications. With each mobile phone acting as an IoT device that can transmit its location information, individuals can be informed when they are in proximity to friends, social events, or other activities of interest. Smart watches that collect data on fitness, can be shared with a community of friends for mutual encouragement. Further, IoT-enabled phones may connect directly to other mobile phones and share contact information when certain predefined friendship or dating profiles are matched.

Challenges

The IoT faces many challenges, both technical and social. Technical challenges include interoperability, standardization, and security challenges. Social challenges include privacy, legal/accountability and general challenges.

The IoT brings together a host of heterogeneous devices and technologies that interact with each other globally. Interoperability of these devices is at the core of the success of IoT. To achieve interoperability, standards must be agreed upon and be acceptable across organizations and various geographical regions. Companies and governments must come together to agree on standards allowing interoperability. Another huge challenge is maintaining security in the IoT. IoT devices communicate through wireless network and this communication needs to be made secure through encryption. Basic IoT devices may not be advanced enough to support robust encryption. The encryption technology needs to advance to be more efficient and less energy consuming. Besides encryption challenges, identity management is also a challenge. Ensuring that smart objects are who they say they are is critical to the success of IoT. The possibility of identity theft, which is a direct consequence of weak identify management, which can result from weak security, is a big challenge in IoT. When critical processes depend on machine-to-machine interaction, compromising a device's identity can potentially lead to very undesirable outcomes.

There are a number of social challenges as well. As devices become traceable through IoT, they increase the threat to personal privacy. Theoretically, one's location, at all times can be known to someone else in public, unless privacy is managed carefully. To protect privacy, it is critical to manage ownership of data collected from smart objects. The data owner must be assured that the data will not be used by any third party without their consent. For example, if health data through a smart watch can be tapped by a life insurance company, it can terminate the policy of those at a higher health risk. To tackle this challenge it is important to have data exchange protocols based on privacy policies. Whenever two objects interact with each other, they must check each other's privacy policies for communication before communicating.

The IoT is also a fertile ground for hackers. With so many devices sending signals around the world, preventing people from tapping onto this communication with malicious intent is going to be difficult. Finally, IoT will create new legal challenges. Establishing laws governing such a global resource as the IoT is difficult to outline and even more difficult to enforce. Governance cannot be dictated by a single group, but by a group of broad-based stakeholders. In addition, global accountability and enforcement will also be necessary.

Business Models

Just like the web enabled new business models, such as electronic commerce and just like mobile phones enabled new services such as taxi hailing services, mobile banking etc., the IoT has the potential of introducing new services that will capitalize on its pervasiveness and ambient intelligence. For example businesses will emerge that provide ubiquitous health monitoring and response for a service fee. Similarly, home monitoring services will go beyond just monitoring for break-ins and fires. All appliances, lighting etc. can be monitored and managed remotely through an app. Similarly, there will be business to business services for all types of monitoring and tracking and maintenance of assets.

Source: IoT-GSI. “Overview of the Internet of things.” http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 (accessed on 2/28/2017).

Source: Agarwal, A., Govindu, R, Ngo, F., Lodwig, S., "Solving the Jigsaw Puzzle: An Analytics Framework for Context Awareness in the Internet of Things," *The Cutter Journal*, 2016, 29(4) 6-11.

Source: Whitmore, A., Agarwal, A. and Xu, L., "The Internet of Things - A Survey of Topics and Trends," *Information Systems Frontiers*, 2015, 17(2) 261-274.