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

[for the *Handbook on Geographies of the Internet* for Edward Elgar publishers]

Introduction

The "Internet of Things", or IoT, refers to an infrastructure of ubiquitous, context-aware devices, or "things", capable of communicating over the Internet, interacting with each other through messages and sensors, to accomplish some objective(s). Objectives could be either personal, commercial, or industrial in nature. Traditionally, the Internet is thought of as a network of "computers" communicating with each other. The IoT is an extension of that idea, in which besides just computers, any network-enabled device can be connected; devices such as cars, phones, appliances, watches, security cameras and so on. The applications of IoT range from individual applications, such as remote health monitoring, navigating from point A to point B using a GPS system, to large industrial applications such as smart cities, smart farming, weather monitoring etc.

The Internet of Things consists of two fundamental concepts: the "Internet", signifying connectivity and communication, and "Things", representing a variety of objects or devices capable of communicating and interacting over the Internet. Advances in wireless communications and networking technologies, together with the shrinking size and cost of microcomputers, sensors, and actuators are driving the development of several IoT applications. Affordable miniaturized portable or wearable devices (pens, watches, buttons, and even clothing) are only adding to the popularity and permeation of IoT in our daily lives. This has enabled hitherto unimaginable

innovative potential of the Internet connectivity to be reflected in applications such as road navigation, health monitoring, contactless purchasing, crime monitoring, and even grocery shopping. This is so because the varied interconnected devices are themselves becoming smarter – collecting large amount of context-sensitive data automatically through their sensors without the intervention of their users. Once this data is transmitted over the internet, it can be used to undertake analytics for a group of people depending on their common areas of interest.

The Internet of Things is evolving rapidly – starting with the convergence of many technologies that have been developing over the last few decades, such as RFIDs, sensors, sensor networks, mobile computing, real-time analytics, machine learning, control systems, the Internet platform, broadband communication, cellular and wireless connectivity and the cloud. Traditionally, devices equipped with RFID and NFC chips, could only communicate locally due to their limited near-field communication capabilities. Advances in telecommunications and the Internet technologies have resulted in the ability of these very same devices to now connect globally and interact with each other on the cloud – 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. Theoretically, any device such as a refrigerator, an appliance, a car, a thermostat or a drone, when equipped with sensing, processing and networking capability can act as an IoT device. Some well-known 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.

For IoT devices to be useful, they have to be able to 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 towards

some objective. IoT devices can be programmed to take certain corrective actions with the help of actuators based on the ambient intelligence gathered through sensors. For example, a home security camera can be programmed to text the owner or call law enforcement if it senses an intruder. Or a smoke detector can be programmed to call the fire station automatically instead of simply setting off the alarm. They can also be programmed to learn from the environment in which they are operating and take appropriate actions.

This article starts by defining the IoT and outlining its origins and history. This discussion is followed by a brief outline of the technology of IoT and describing what constitutes the Industrial IoT (IIoT). The applications of IoT are outlined with specific focus on geospatial applications. Challenges in the use of IoT in practice are then highlighted followed by the conclusion and future directions.

Definition of IoT

Because of the broad nature of the IoT, there is no single universally accepted, all-encompassing definition of IoT. We provide here definitions from some well-known and reliable sources - 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. 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. Techopedia describes IoT as a world where just about anything can be connected and communicate in an intelligent fashion. It describes IoT as one big information system. Wikipedia defines IoT as the network of devices, vehicles, and home appliances that contain electronics, software, actuators, and connectivity which allows these things to connect, interact

and exchange data. Some other terms that are also used to describe the concept of IoT include ubiquitous computing, invisible computing and pervasive computing.

Origins and History:

The basic idea behind the IoT is rooted in the concepts of telemetry and telecommand. Telemetry is an automated communications process by which measurements and other data are collected at remote or inaccessible points and transmitted to receiving equipment for monitoring. An example of telemetry is a radiosonde, which is a helium balloon carrying sensors for atmospheric readings. Radiosodes measure atmospheric data such as temperature, pressure and humidity and transmit them to a weather station on the ground. Satellites are also essentially telemetry devices.

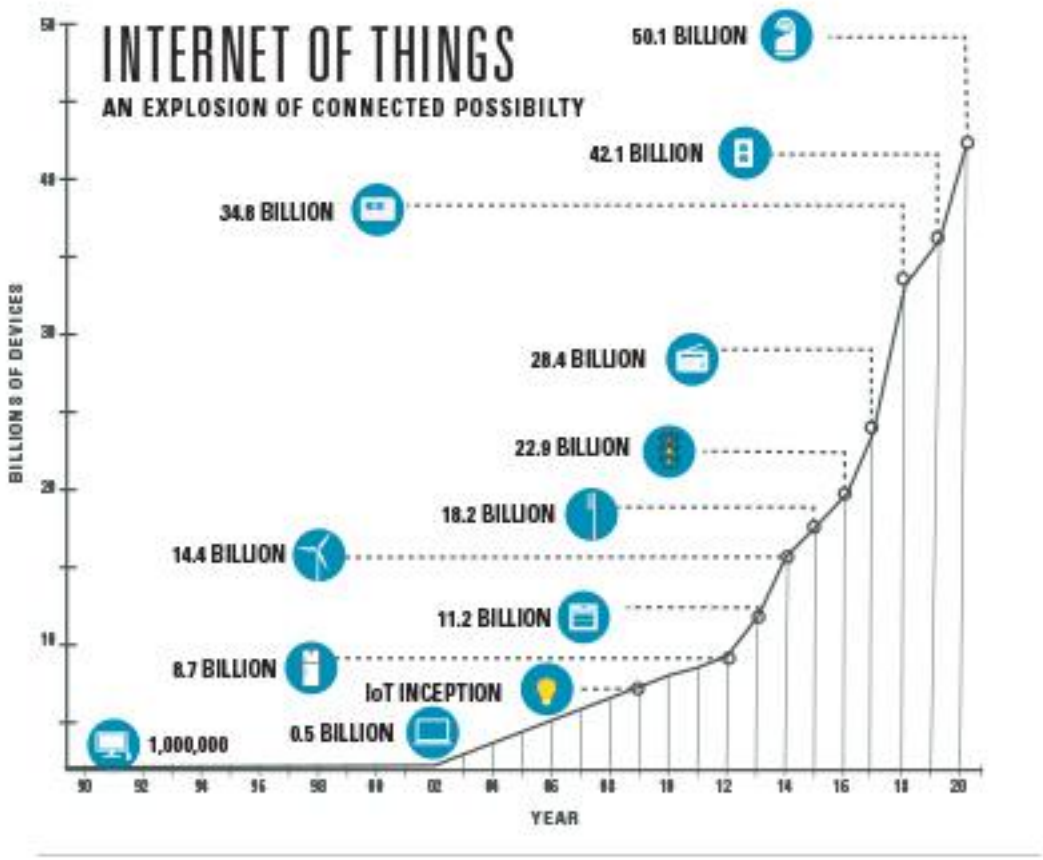
Telecommand is a command sent remotely to control a device. Both telemetry and telecommand become possible through machine-to-machine (M2M) interaction, where the machines are connected wirelessly. A garage opener or a TV remote are simple examples of telecommand devices that send command to a receiving device. Through telecommand, the receiving device is controlled remotely. As another example, through telecommand, NASA can control a rover sent to Mars; the rover in turn acts as a telemetry device for data about Mars.

M2M communication precedes the Internet. So some form of telemetry and telecommand has existed ever since M2M communication has existed, which dates back to the 60s and the 70s. As the sensor technology and wireless communication technology is advancing, telemetry and telecommand concepts are being applied to more and more devices. When communication happens through TCP-IP, we get the present day IoT.

The conceptual idea behind the IoT - of adding sensors and intelligence to basic objects, connected through the Internet has been under discussion since the 1980s. In 1989, a scientist by

the name of John Romkey created the first Internet 'device', a toaster that could be turned on and off over the Internet. The toaster was a device on TCP/IP network and could be controlled from another computer in the network. In 1998, Mark Weiser, the Chief Scientist at Xerox PARC, constructed a water fountain outside his office that mimicked the volume and price trends of the stock market. Basically, the fountain (the device), was in constant communication with the stock market computers. In 1999, the term "Internet of Things" was coined by Kevin Ashton, the then executive director of the Auto-ID Center. In 2000, LG announced its first plans for 'connected appliances' – the Internet Refrigerator.

In 2005, UN's International Telecommunications Union (ITU) published its first report on IoT and had this to say – "A new dimension has been added to the world of information and communication technologies: from anytime, anyplace connectivity for anyone, we will now have connectivity for anything. Connections will multiply and create an entirely new dynamic network of networks – an Internet of Things. In 2008 the first European IoT Conference was held. A group of 50+ companies launched the IPSO Alliance to promote the use of Internet Protocol (IP) in networks of 'smart objects' and to enable the Internet of Things. In 2010, the number of Internet-connected devices (12.5 billion) surpassed the number of human beings (7 billion) on the planet. In 2011, IPV6 protocol was launched which allowed 2^{128} unique addresses, enough to provide an IPV6 address to every atom in every human on the earth. The IoT is considered the third wave in the development of Internet-based information systems. In the first wave (1990's), the Internet connected about 1 billion users. In the second wave (2000's), the Internet connected another 2 billion users. In the third wave (2010's) the IoT has the potential to connect as many as 50 billion 'objects' by 2020.



The Technology

The underlying IoT technologies can be broadly divided into hardware, software and communications architecture. In terms of hardware for the IoT, the critical elements include the Internet communication platform on which everything else resides, RFIDs (Radio Frequency Identification Devices), NFC (Near Field Communication) devices, sensors and local sensor networks. 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. Such RFID tagging facilitates tracking the inventories in a retail

outlet; it can also facilitate rapid scanning of checkout items. 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, typically effective within 10 cm range. 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 applications are required in order to support the devices and their corresponding interoperability. 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.

The biggest challenge in IoT is M2M communication that needs communication over long ranges with low power level usage. This issue is solved by a new wireless technology called as LoRa (Long Range). LoRa is long range, low power consumption technology that is used for building IoT networks worldwide. Public and private networks using this technology can provide coverage that is greater in range compared to that of existing cellular networks. LoRa technology uses LoRaWAN protocol which is developed by LoRa alliance. It uses unlicensed radio spectrum in ISM band 868 MHz-915 MHz for communication between sensors (nodes) and gateways connected to a network server.

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. This generation of data by machine sensors results in high volume data on a continuous, streaming basis. This propensity of IoT and machine sensors to significantly increase data workloads needs to be complimented by corresponding technologies for storage, retrieval and

processing (Unhelkar, 2018). As a result, process architectures become necessary to structure and optimize the usage of data according to needs of the corresponding business processes.

Thus, the potential of the devices is brought to fruition only when they are connected together through back-end cloud technologies. The value of an IoT device to its user is manifold when such a device is "alive." For example, GPS car navigation is of greater value if its back end collaborates with weather, traffic, and sporting events databases. The value of a pacemaker lies not only in its support to the heart, but also, potentially, its ability to alert relevant services in case of an emergency. And the wearer of a smart-watch (e.g. Fitbit) is encouraged to perform better through the encouragement of a group of friends all collaborating on a back-end cloud. It is thus imperative that IoT devices be innovatively integrated with the back-end cloud where data is stored, shared, and analyzed.

Industrial Internet of Things (IIoT)

The Industrial Internet of Things (IIoT) extends the technologies of IoT, referred to above, and applies them to industrial processes and digital transformations. A key requirement of IIoT is that the devices are able to operate with intelligence - based on feedback loops. Machine Learning (ML) algorithms are embedded in the devices as well as in the backdrop (typically on the Cloud) to enable the processes driving the devices to "Learn" from rapid as well as detailed data analytics. Such analytics – depending on their granularity – are able to provide immediate feedback to the IIoT devices to enable them to simulate intelligence and undertake decision with minimal or nil human intervention. Thus, IIoT is characterized by the following:

- Big Data: this characteristic of IIoT deals with the sensing, ingestion and storage of vast amounts of data, most of which is on the Cloud. By storing data on the Cloud,

it is possible to undertake Analytics on the Cloud across a range of devices, situations and times.

- Machine Learning: this characteristic of the IIoT framework enables detailed as well as rapid Analytics of the Big Data on the Cloud to produce insights. These insights generated by ML are continuously being updated to enable increasingly refined (intelligent) decision making.
- Automated Communication: this characteristic of the IIoT framework/ecosystem enables machine-to-machine communication in an automated manner to enable the IIoT devices to organize their activities, correct their actions and suggest improved actions – with minimal or nil human intervention.

The above characteristics of IIoT differentiate them from the typical Personal IoT devices – such as smart watches and cell phones. While PIoT also have the possibility of the above characteristics, they are not a mandatory requirements in personal usage. Furthermore, the individual user's processes are not necessarily based on the aforementioned characteristics – whereas, IIoT has these as mandatory characteristics.

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. We can classify the applications as consumer oriented, commercial, industrial and infrastructure.

Consumer applications include devices such as Apples's iWatch for personal fitness and health. Another application of IoT is smart homes that are equipped with sensors to 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 or disabled residents and call for response team or other help if necessary. Smart assistant devices such as Amazon Echo, Google Home, Apple's HomePod and Samsung's SmartThings Hub are also consumer oriented 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 reach their destinations faster and serving its citizens better. Taxi hailing services have been made possible through the IoT infrastructure.

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 made possible through the application of IoT devices and IoT

infrastructure. Good healthcare often depends on timely detection of a current or impending health issues and taking timely action to address the issues. 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 preempted 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

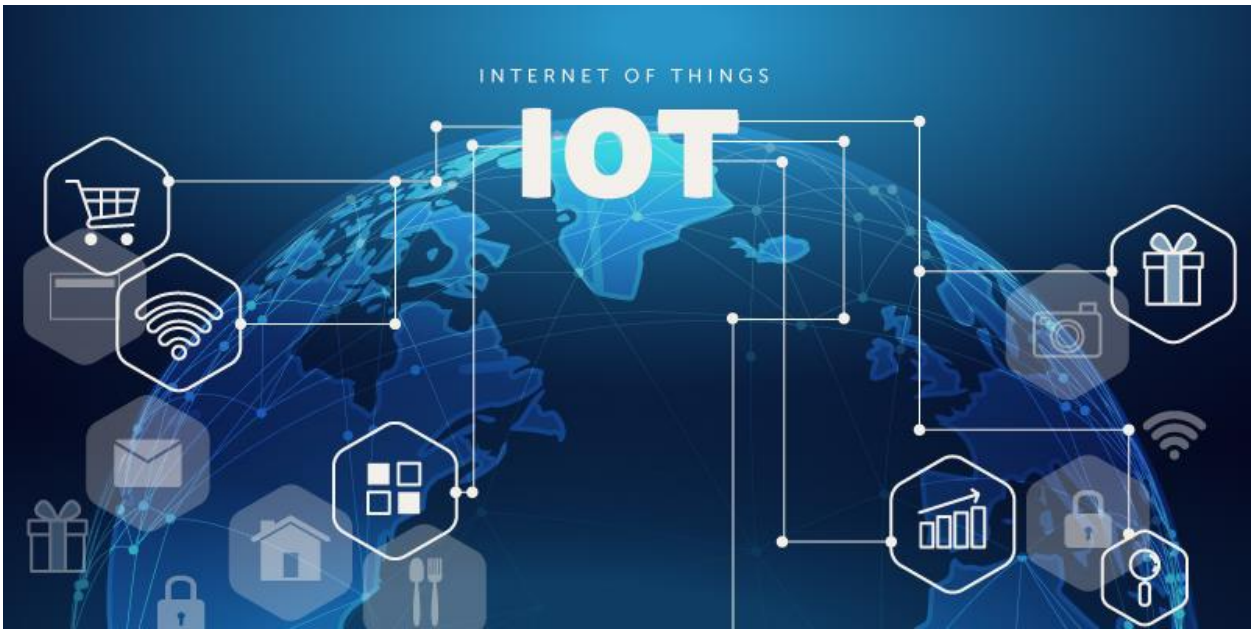
manufacturing activities more accurately, warehouses and retail can place their orders more timely and in appropriate quantities, resulting in less surplus or shortage throughout the supply chain.

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.



Spatial and Geographic implications:

When the IoT technologies are specifically focused on the three dimensional mapping of a point in space and then carry out its subsequent analysis, it is considered Spatial analytics. The data point in space is the IoT device itself or it could be an entity being located and moved by an IoT device. A large number of applications in day-to-day use are spatial in nature: for example, the 'Google maps' and 'Waze' applications are utilizing the position of a vehicle to which they are attached (usually through a smart phone) to analyze, in real time, the movement of the vehicle. The real-time nature of most of these applications also implies time management within these applications. Thus, all such applications incorporate time together with the geospatial locations. As a result, these spatial applications are specifically able to optimize the performance across a geographical space. Such applications are, therefore, specifically called geospatial applications.

Sensors on IoT devices enable location of the device followed by tracking its movement in time. These IoT devices can be put together in a group (temporary – such as when a group of vehicles are traveling on a road; or on a more permanent basis – such as a group of emergency vehicles belonging to a county of city). The data generated by these devices in real-time is a source

of substantial information which, when put together on the Cloud and analyzed, can reveal patterns that would not be possible to identify without the streaming data from these IoT devices.

The potential applications of geospatial analytics are limitless and exist in almost all verticals:

- Traffic management in busy cities and express ways (such as Google maps and Waze mentioned above)
- Emergency vehicle management and movement (such as ambulances and police vehicles)
- Sports applications – training as well as execution of sports through precision in location-specific applications (such as timing a large group of runners in a marathon)
- Deliveries of goods and services (such as Amazon's drops and Pizza deliveries)
- Optimizing travels (such as Uber and Lyft).

Combining big data and machine learning provides opportunities to identify patterns and make sensible predictions in each of the above example applications.

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. Following are some of the risks and challenges in applying IoT and cloud in the business space:

- Security. The more devices connected to the network, the more vulnerable they are to being hacked. Thus the popularity and growth of IoT is confounding the industry users and the researchers in terms of security of devices. Additional challenges from a security standpoint arise due to the fact that many of these consumer IoT devices are not easily upgradable for their operating systems and

software versions. This lack of currency in the operations of these IoT devices leads to a major gap in security because the devices themselves are not upgraded corresponding to the threats faced by them. Furthermore, 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. 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

- Standardization and interoperability. There are too many competing standards, making IoT devices incompatible with each other. Google, Microsoft, Intel, Apple, and Samsung are all pushing their own versions, and there is no consensus in the industry on how to centralize around common standard(s). Without compatibility between devices from different manufacturers, the IoT domain finds it challenging to capitalize on the data collection, its analysis and provisioning of actionable insights. 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.

- Manageability. One analyst firm predicts that "the IoT market will grow from an installed base of 15.4 billion devices in 2015 to 30.7 billion devices in 2020 and 75.4 billion in 2025." How are these devices going to be managed? The 2.3 billion smartphones in use today — a number that will only grow — have spawned the global service provider industry (Verizon, AT&T, Vodafone, Bharti, China Mobile, etc.). The scaling of the smartphone coupled with smart devices is resulting in an industry that is extremely challenging to monitor, regulate, and standardize.
- Network optimization. The IoT is characterized by a large amount of control traffic (the device connecting to the network, authenticating itself, going to sleep when not active, paging periodically to announce its presence, etc.) and very little data traffic (a few bytes to a few Kbytes per data cycle). In contrast, current networks are meant to handle a small amount of control traffic and a large amount of data traffic. This is a challenge from networks and communications viewpoint as there is a need to align current networks with requirements that are opposite – emanating from the emerging IoT devices.
- Analytics. It is clear that for an IoT to be useful, it has to process of lot of data, data that is not stationary but streaming. IoT therefore requires real-time or streaming analytics algorithms. Many existing algorithms, such as Map Reduce

works on stationary data. Thus, there is a need for analytics to evolve in order to facilitate incorporation of streaming data from the IoT devices to be of immediate value to the users. The question as to what kind of big data analytics will be needed to harvest useful information from the massive flood of data that the IoT devices generate is an interesting challenge. For example, "a Boeing jet generates 10 terabytes of information per engine every 30 minutes of flight, according to Stephen Brobst, the CTO of Teradata. So for a single six-hour, cross-country flight from New York to Los Angeles on a twin-engine Boeing 737 — the plane used by many carriers on this route — the total amount of data generated would be a massive 240 terabytes of data." How and where to store this data and how to enable its sensible analytics are challenges that demand creative approaches to data sourcing, storage, analytics, and display.

- Social aspects. There are a number of social challenges as well. How will society evolve when we are being watched or monitored by IoT devices (e.g., Amazon Alexa) all the time? How will governments use this information to serve, spy on, or prosecute their citizens? Will there be a few mega-corporations controlling the IoT ecosystem, or will there be a more democratic setup of constructively competing smaller players?
- 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.

.

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.

Conclusions

This article provides a summary of the Internet of Things (IoT) from technology and applications viewpoint. The ability of the devices to connect over the Internet provide significant opportunities for automated data collection, analytics and provisioning of insights for the users – in making better business decisions as well as improving the quality of life of the individual users. Furthermore, this article discusses the various challenges that are presented by IoT – and an approach to handling those challenges in order to apply IoT in business.

References

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, Ed. B. Unhelkar, 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.

Source: Ashton, K. 2009, *The RFID Journal*, https://www.rfidjournal.com/articles/view?4986, accessed 26 Dec, 2018.

Source: Unhelkar, B., (2018), *Big Data Strategies for Agile Business*, CRC Press, (Taylor and Francis Group/an Auerbach Book), Boca Raton, FL, USA. ISBN: 978-1-498-72438-8