Living in a Connected World

We have defined a network as an organization of computers which allow network applications to communicate. The concept of a network is greatly enhanced with the development of the Internet. The latter has allowed the sharing of resources and information at a world-wide level. This sharing has had a profound effect on each of our lives. From the road we use to drive to work with synchronized traffic lights for maximize traffic flow, to development of new communities through social media. Clearly, the Internet has made the world seen smaller and simplified our lives. This extension of the Internet into all facets of technology has coined a new term "The Internet of Things" (IoT)[1]. Robert Belda explains:

> People may not realize it but the Internet of Things is already gaining traction and slowly influencing how people live in this connected world. Right now, its perceived advantages may far outweigh its feared drawbacks. Some analysts even called the up-and-coming technological paradigm shift as bigger than the Industrial Revolution.

While the Internet has created many benefits, it has also brought its own set of problems, which negatively affect our lives. Let's investigate the positive and negative effects of the Internet.

Electronic Communication

Before the Internet, communication with people, who lived far away, was limited to the telephone or postal mail. Now, we can send and receive messages through electronic mail instantly and without the need of a postage stamp. Today, most Canadians do their banking online. instead of driving to the bank and waiting in line to be served. Similarly, rather than driving to a mall and waiting in long lines to make a purchase, Canadians are shopping with a few clicks of the mouse any time day or night. Electronic communication has made it easier to work, bank and shop from home, simplifying and providing greater flexibility, but there has been a corresponding decline in personal security and privacy.

Electronic communication has proven an effective vehicle for cybercriminals to distribute spam and malware. Malware hiding in email attachments, can install spyware or ransomware. Cybercriminals can distribute malware through drive by downloads. This technique is very popular with high volume online shopping websites. The high volume makes the web site attractive to criminals to infect in order to distribute malware to visitors who click on an infected link. Or, cybercriminals can create fake websites that offer goods at unbelievable prices to attract individuals, or deceive individuals by posing as a legitimate site, such as a bank or PayPal. When users click on the spoofed web site or link they are redirected to a site controlled by the criminal to steal personal information. You might think you're

[1] Kevin Ashton is the person widely credited for coining the phrase in 1999 while working for Procter & Gamble. Since then, the phrase caught on and was used in a variety of articles, which appeared in scientific and academic journals

making a legitimate purchase, but the cybercriminal has just taken your personal information; the information will be used to commit identity theft or sold for profit on the black market.

To protect yourself always do the following:

- Install and keep up to date antivirus and anti-phishing software on your personal PC. Cybercriminals can take advantage of vulnerabilities in outdated software and use it to infect your PC with malware that can steal your banking credentials, so be sure to have adequate PC security software and keep your operating system, Web browsers, and other applications up-to-date.
- Don't open any email attachment unless you checked the source, even if the email is sent from one of your contacts. Call by phone or email the source to ensure that they sent you an email with an attachment. If not delete it.
- Never comparison shop using a search engine. This method will always bring criminal web sites to your browser. Go to the official web site and do your own comparison.
- Never buy goods from an unknown retailer, regardless of how good the deal seems. Think before you click. Remember the adage, "If it seems too good to be true, it probably isn't true" and you are being scamming by a criminal. Did you get an email indicating there was unusual activity with your account and that you should click on this link to verify? Or, did you receive an email confirmation of a flight you did not make? In either instance, do not panic. If you're unsure whether the email is legitimate or not, the best way to find out is to log into your online account directly to check on the claim. As always, never open email attachments from a sender you do not know. In addition, make sure your PC has an antivirus and a good two-way firewall.

IoT

The Internet of Things pertains to the concept of devices connected to the Internet where data gathered by such devices are reported to users. People can then act on the said data or the devices themselves are empowered to act on it. The ease of data transmission, reception and implementation are all meant to improve people's quality of life.

Internet is medium which connects all people and we can call it as "Internet of People" . IoT or Internet of things connects all things. The things can be sensors, actuators, home appliances, mobile devices, or anything that can communicate via internet

Components of IoT

Sensors

Sensor are low powered devices that have a capability to monitor some physical or environmental phenomena and collect that information for further processing. Sensor nodes have limited battery power, but now there are some sensors available that can recharge themselves. They consume very little battery power for their operation, so even if they cannot recharge the battery, they still can live on batteries for a long time.

Local processing and storage devices

Each sensing node is equipped with low power processor and a limited amount of memory. The sensed data is briefly stored in the sensing node before transmitting it to data collecting device. Some analog to digital data conversion and data aggregation operations are performed by the small power processor.

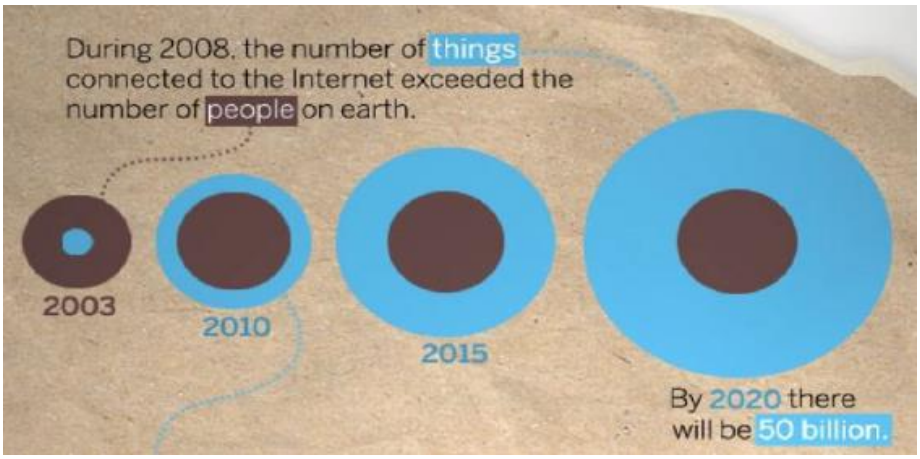
Network and Internet

The hardware is needed which connects sensor nodes to the internet for the transmission of sensed and processed data to the cloud to be stored. The protocols that are used for this communication are: HTTP, XMPP which functions as a chat, CoAP, MQTT (less secure and designed for machine to machine communication)

Cloud

The last phase of operation is done at the cloud. At this level, the received data is processed according to nature of data as well as the type of application for which it has been collected.

IoT Growth



Estimated number of IoT devices by the end of 2020 is between 30 to 50 billion, much more than the human population on the earth.

IoT Applications

Some of the application IoT are: Smart home, smart grid, smart cities, smart refrigerator, under water habitat monitoring, monitoring of plants, habitat monitoring, smart cars, smart industries etc.

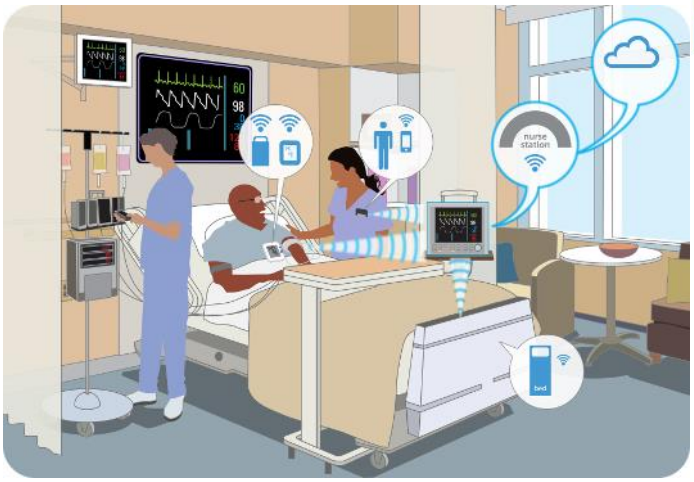


Figure 1: Smart Health (BAN-Body area networks- Remote patient monitoring

Figure 2: Smart Refrigerator

Figure 3: E-helath-> Smart watch Fitness tracker

Figure 4: Smart Washer

Smart Home

The IoT is a revolution that promises to change people's lives, from inside the home to right across society The Internet creates convenience in sharing and receiving information between devices.

Figure 4: Controlling Home via Phone or Tablet

Right now, many smart devices like laptops, smart phones and tablets communicate with each other using Wi-Fi internet technology. The next step is IoT devices and sensors, which communicate with each other and automatically perform a designated task or function without user intervention. Household devices such as refrigerators, washing machines, microwave ovens, thermostat, door locks, among others, will all be part of a household local area network. Each device is equipped with a computer chips, software and access to the Internet making the "smart home" a reality. There is no doubt this it will happen; the lower cost computing today will be a boom for these smart devices. In fact, Steve Furber, who was the principal designer of the ARM processor, believes IoT will be the next big growth area for ARM.

One example is the Nest thermostat where it adjusts household temperature depending on usage patterns and billing rates. The Nest thermostat can be controlled using a mobile app. The company was recently bought by Google for $3.2 billion; Google plans to expand the product line to include smart smoke detector and other products as part of its "smart-home solutions". LG Electronics, the South Korean firm, is also now offering users the ability to control their appliances by way of text messages. The company has also been marketing an Internet enabled fridge. Utility companies have long advocated for better thermostats to help reduce energy costs. Smart thermostats can do this by adjusting the

temperature when it senses you have left the house. Additionally, it "learns" your heating and cooling preferences and adjusts them to your liking.

While a smart thermostat can aid in reducing your energy cost, the downside is that a hacker could exploit the hardware of the thermostat and use it to spy on home owners. Since smart thermostats have access to information such as when you're home or away, your postal code, and your WiFi credentials, a hacker who compromises the thermostat has access to all of this information.

This is not an idle problem. According to a recent study, 70% of IoT devices are vulnerable to cyber-attacks. This list includes thermostats, TVs, webcams, sprinkler control systems, home alarms, and door locks- just to name a few. The truth of the matter is that we are developing networked devices with insecure software; most vendors are producing retail products with security loopholes and vulnerabilities because security is not a priority.

To help network these devices together a new standard organization has emerged called the AllSeen Alliance, a nonprofit organization devoted to the adoption of the Internet of Things; the mission of the Alliance is to ensure interoperability of products made from different vendors, such as Cisco, Sharp and Panasonic. Gartner, an IT research company, estimates that by the year 2020, there will be 30 billion devices connected to the Internet of Things.

Advantages and Disadvantages of a Smart Home

The advantage highly networked smart devices is an enhanced quality of life. For example, health monitoring of out-patient clients is easy with connected RX bottles and medicine cabinets. Doctors supervising patients can remotely monitor their medicine intake, blood pressure, sugar levels and alert them when something goes wrong. This new type of medical monitoring is shown in the TV series Pure Genius with a medical command centre monitoring out patients from the BunkerHill Hospital.

Smart refrigerators, on the other hand, can suggest food supplies that are low on inventory and need immediate replenishment. When at work, it would be convenient to scan the barcodes of the fridge's contents and compare the result to a list of required items. The fridge would be able to tell you what to pick up on the way home. But, did you know that your local supermarket is also very interested in what is in your fridge and freezer? Based on historical purchasing, your local supermarket wants to send you a shopping list of things to buy, and coincidentally in store specials on those items. Is the latter, an intrusion of privacy, or a convenience? The answer has yet to be developed.

Utility companies have long wanted to use wireless power meters to remotely read household meters. This was accomplished in Ontario 3 years ago; utility companies want to create a "smart grid". One of the devices in your home utility companies want to control is your freezer. Energy can be saved by monitoring the internal temperature of the freezer and turning it off for periods of time when the everything is frozen and turning it back on when the temperature rise above a specified level. A smart home would also allow you to control the stove and other devices via the internet; the stove can be turned on and a nice meal, with music playing, is waiting for you when you get home. Lastly, TV companies want to monitor what you watch, so they can deliver highly targeted advertising to you in a mutually agreed manner.

Robots and Driver-Less Cars:

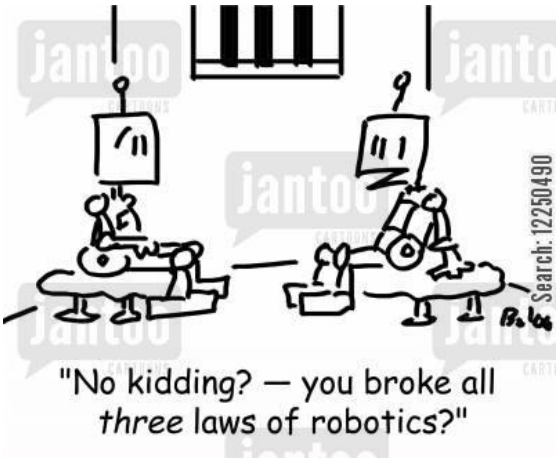
Figure 1: Uber Driverless Car

With the development of the smart home and RFID sensors strategically installed, robots to clean the house, set the table, serve meals, and provide security, will be common place by the end of the 2020's. Expand the concept of smart home to the neighbourhood and robotic driver-less cars can operate. This may sound like something out of "The Jetsons", but researchers believe we will soon be sharing our home and roadways with super-intelligent family robots. While some companies such as Uber and Tesla, have current drive-less models, fully automated driverless cars will not become common place until 2040.

Robots and driver-less cars will help the aging or visually impaired loved ones from giving up their independence. Time spent commuting could be time spent doing what you want to do. Deaths from traffic accidents—over 1.2 million worldwide every year—could be reduced dramatically, especially since 94% of accidents result from human error. As Elmo Telsa stated, in the future human driving may be outlawed because it is too dangerous. Robots and driver-less cars operate using sensors designed to detect objects such as walls, stairs, pedestrians and other vehicles. The sensors are combined with onboard cameras to help the robot interpret its surroundings. The software helps the robot understand its present location, and predicts what will happen next, so that the robot can make an intelligent decision to complete some function such as changing lanes on a street, or setting a table for dinner.

Current and Future Issues Smart systems are getting smarter, such as IBM's SuperComputer Watson. Clearly, machines, with the benefits of speed, perfect recall, objectivity, and repeatability, will greatly affect our lives and make many of the mundane day-to-day decisions. The social impact of this robotic revolution is not yet understood.[2] However, using robots raises profound questions which have little to do with the technology. For example, if a machine makes a decision, and causes and accident, who is responsible? Our current legal environment is based on some legal entity, like a person or corporation, to bear the liability, even if the machine does the work (that's why some jurisdictions, that have approved driverless cars, require a licensed person behind the wheel), but we are now starting to face a real dilemma. Smart machines are close to outsmarting humans – whether driving a car or determining a medical diagnosis – leaving the human overseer with the responsibility, but reduced capability. Over 70 years ago, science fiction author Isaac Asimov proposed the three laws of robotics. Maybe now would be a good time to review and consider the future of smart machines. Science fiction is fast becoming science fact!

[2] An excellent paper on the impact of driverless vehicles on Canadian social policy is "AutonomousVehicle Implementation Predictions:Implications for Transport Planning,1 September 2016, Todd Litman,Victoria Transport Policy Institute



1. *A robot may not injure a human being or, through inaction, allow a human being to come to harm.*

2. *A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.*

3. *A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.*[3]

Figure 2: Image taken from http://lowres.jantoo.com/books-literature-asimov-robots-sci_fi-crimes-science_fiction-12250490_low.jpg

For truly autonomous robots our legal system will need to change and give machines the responsibility for their own actions. If a human is injured or killed, because of a machine's wrongful decision, who pays restitution to the injured party? Is the machine sent to jail or deprived of power for a period of time?

The main stumbling block for IoT devices is the lack of connectivity standards. There are several proprietary networks, such as X10 and HomePNA. Wireless technologies also operate on a mix of spectrums, with the 2.4-2.5GHz band being used heavily by several non-compatible standards for data transfer and various remote controls.[4] As we saw in Week 2, overarching standards must be in place for connectivity and interoperability to occur. Presently, only products from the same vendor can be networked – similar to network operating systems in the early 80's. The new industry standard organization, AllSeen Alliance, was launched in December 2013, to improve interoperability. The AllSeen Alliance proposes to unite industry leaders with a shared vision, a common language and a collaborative path to advance the Internet of Everything. See youtube video https://www.youtube.com/user/AllSeenAlliance

[3] Issac Asimov's "Three Rules of Robotics", taken from Wikipedia, https://en.wikipedia.org/wiki/Three_Laws_of_Robotics
[4] Roberto I. Belda, "Internet of Things: Advantages May Far Outweigh Its Drawbacks ", January 26, 2014, at http://guardianlv.com/2014/01/internet-of-things-advantages-may-far-outweigh-its-drawbacks/

The AllSeen Alliance proposes devices be **AllJoyn** certified. The latter is an open source universal software framework and core set of system services that enable interoperability among connected products. It lets compatible devices and applications find each other, communicate and collaborate across the boundaries of product category, platform, brand, and connection type. Target devices include products in the Smart Home, but will later expand to Broadband Gateways and Driver-less cars. Presently, the communication layer (and thus hardware requirements) is limited to wi-fi.

Figure 3: AllSeen Alliance Logo

The other disadvantage is IoT devices need a lot of data and information about the environment in which they operate. This data can include personal schedules, shopping habits, medicine intake schedule and GPS location of the user at any given time. Each device only uses a small amount of bandwidth, but multiple this by an estimated 30 billion devices and the Internet bandwidth must greatly increase for IoT to become a reality. Wireless standards are increasing bandwidth regularly, with 802.11n access points from suppliers such as TP-Link and Netgear capable of running at 600 Mbps. New standards such as 802.11ad, are designed up to 7 Gbps. 4G mobile wireless using Long-Term Evolution (LTE) is already being introduced by telcos and cable companies across North America and Europe with speeds up to 300 Mbps. The expansion of LTE, higher bandwidth, and interoperability of products across multiple communication vendors, is required to make the IoT mainstream. However, the greatest problem is the lack of secure software in these products. Smart devices know a lot about you and your environment. This personal information, if accessed by criminals, will result in a severe loss of privacy and security.

- .

To protect yourself always do the following:

- If you chose to use IoT devices, always be conscious of the potential risks. Examine, the privacy policies and security features, before making a purchase decision, and weight the potential risks.
- Also, when new security patches or software updates are available, you should immediately update to the latest version.

And finally, don't be afraid to contact the company that manufacturers the device, should you have questions or concerns about the product

Platforms for IoT

IoT platform fills the gap that exists between sensing devices and the data network., to provide understanding of the data generated by the sensor nodes using backend application. There are many **IoT platforms** available now that provide option to deploy **IoT on the go.**

Amazon Web Services (AWS) IoT

This **IoT platform** will help developers to connect sensors for multiple applications ranging from automobiles to turbines to smart home light bulbs. Taking the scope of AWS IoT to the next level, the vendor has partnered with hardware manufacturers like Intel, Texas Instruments, Broadcom and Qualcomm to create starter kits compatible with their platform.

Microsoft Azure IoT

Features of Microsoft Azure IoT included in this platform are:

- Device shadowing
- A rules engine
- Identity registry
- Information monitoring

For processing the massive amount of information generated by sensors Azure IoT suite comes with Azure Stream Analytics to process massive amounts of information in real-time.

Google cloud

Regarded as the best IoT platforms. It can handle vast amount of data using Cloud IoT Core.

Some of the features of the Google Cloud platform are:-

- Accelerate your Business
- Speed up your devices
- Cut Cost with Cloud Service.
- Partner Ecosystem

ThingWorx IoT Platform

- Easy connectivity of devices to the platform
- Remove complexity from IoT application development
- Sharing platform among developers for rapid development
- Integrated machine learning for automating complex big data analytics
- Deploy cloud, embedded or on-premise IoT solutions on the go

IBM Watson provides:

- Device Management
- Secure Communications
- Real Time Data Exchange

- Data Storage
- Recently added data sensor and weather data service

Cisco IoT Cloud Connect

Cisco's IoT platform is for mobile operators offering:

- Voice and data connectivity
- SIM lifecycle management
- IP session control
- Customizable billing and reporting

Also partnered with National Farmers' Federation in Australia to provide internet of things in agriculture solutions.

Programming Languages for the IoT

Internet of Things (IoT) development projects are springing up at businesses all over the world. Choosing which language to use to write the project is as big a decision has which hardware platform to use. New languages and platforms are making it easier to engineer IoT projects than ever before. Once you've chosen the hardware platform, though, you still must develop the application software; here are some of the languages you should be familiar with.

Prior to the IoT, your choice of hardware platform dictated your choice of language. However, with the AllSeen Alliance open source project modern platforms can support multiple languages, increasing developer flexibility. How do you decide which programming language to use in a particular IoT project? Factors such as is the developer team familiar with the language or, whether it works within the environment used by other components of the project, or whether it produces code that is smaller, more efficient, or more rapidly written than that of other options.

Here are the top 7 languages that you should consider:

C and C++

C was first developed to program telephone switches and it is still a contender for IoT projects. It's available on nearly every advanced embedded system platform and requires little processing power. The language is ideal for programmers who write for the lowest layer of software, the one closest to the hardware. The language hides nothing from you, and that means you can fiddle with every part of the code to squeeze out the best performance from an underpowered device. Every bit can be flipped. Every value on the stack is available. C++ is an alternative if the IoT device requires more complex tasks, think thermostats and smart toasters rather than devices that detect moisture or heat. C++ adds data abstraction, classes, and objects. All of these features make C++ a popular choice for those who are writing embedded and IoT code with an interface. This programming language still is going strong after more than 30 years in the field.

Java

C and C++ were designed from the ground up to allow very direct control of the hardware on which they would run. That's a good factor when you're trying to do very fine-grained monitoring and control of that hardware, and it means that the code written is very specific to the hardware. In programming parlance, the code is not terribly portable. The mentor of Java "write once, run anywhere makes it an ideal choice for an IoT project. Also, the Java compiler has very few hardware dependencies built into it. Developers can create and debug code on their desktop and then move it to any chip with a Java Virtual Machine. That means the code can run not just on places where JVMs are common (servers and smartphones), but also on the smallest machines. Today, most of the focus is on Java SE Embedded, which is much closer in capability to the Standard Edition. Developers can use the latest features of the Java 8 platform and then move their code to a smaller, embedded device. All of this makes Java great from an economic standpoint: An investment in Java code can be paid back across many different platforms. Java is also taught as one of the primary programming languages in hundreds of computer science and electrical engineering degree programs, so finding someone with Java skills is not terribly difficult.

Python

Python started as a scripting language to glue together real code, but it's increasingly used as the main language for many developers. It has become one of the "go-to" language in Web development, and its use has spread to the embedded control and IoT world. The syntax is clean and simple, which greatly improves readability. If the project requires taking data and putting it into any sort of database format, then draw upon the tables for control information, Python is a very real contender provided the device has the processing power for the application. For very small devices there is MicroPython and a software package for very small microcontrollers optimized to run Python on a small board that's only a few square inches. Python is very flexible in many ways. For example, it is an interpreted language that can either be submitted to a run-time compiler or run through one of several pre-compilers so that compact executable code may be distributed.

JavaScript

JavaScript is not an interpreted version of Java. It started as a scripting language, but has grown into a very full-featured language. The two languages were developed separately (JavaScript was developed by Netscape) and shares no syntax or semantics (however, there are libraries which allow Java and JavaScript to work together). JavaScript is heavily used for building Web-front-end applications. Forty-two percent of server based web applications use JavaScript. If you wanted to use the Apache server on a Raspberry Pi to gather data from a network of Arduino-based sensors, for example, JavaScript would be a good starting point for the effort. It's not for lightweight embedded controllers because its interpreted structure requires more processing power, but it works well with RaspberryPi.

Swift

Swift is an Apple programming language, replacing Objective C. The fact that many IoT devices will need to interface with iPhone or iPad makes Swift a good choice for an IoT project. There are other good

reasons to use this language, Apple wants to make its iOS devices the center of the smart home network of sensors, so it's been creating libraries and infrastructure that handle much of the work. These libraries are the foundation of its "HomeKit" platform, which provides support for integrating the data feeds from a network of compatible devices. This means that programming an IoT project will take less time with Swift because you can concentrate on the application and leave the details of integration overhead to HomeKit.

B#

Where many of the languages mentioned here are large system languages that have been scaled down to fit into an embedded platform, B# was designed from the ground-up as a very small, very efficient embedded control language. The embedded virtual machine (EVM) that allows B# to run on a variety of different platforms only takes 24k of memory -- much less than the overhead of other development languages. B# looks like C# (which will be familiar if you or your team is accustomed to working on Microsoft .NET projects), but it strips out many of the features not required for embedded projects and adds support for the real-time control functions that are critical when making things happen in the real world. If your project is going to live on embedded platforms that aren't as big and complex as a Raspberry Pi, then B# is a language that you will want to consider.

C#

C# is a good choice for an IoT project. Microsoft's strategy for IoT devices is to link them to the Azure cloud. Data collected from an almost limitless number of internet-connected sensors needs to be collated, analyzed and acted upon, and a public cloud is the logical route to do this. Presently, car companies such Corus, are using the cloud to provide mapping and integration to customers.

Microsoft has launched the Azure IoT Suite to aid developers in application development. The Suite acts as a bridge between customers' devices and the back-end application for storing, analyzing and acting on IoT data in real time. The Suite is scaled to handle billions of devices. The Suite supports multiple protocols and languages including C, Python, Java and JavaScript. Microsoft is positioning itself to use the cloud as an interface for end-to-end solutions of IoT devices from multiple vendors. This makes C# and Visual Studio a real contender for IoT projects.