Internet of Things
An Indian Outlook

CONTEMPORARY CONCERNS STUDY

By

Taniya Patra | 1511365
Mohammad Sarosh | 1511335

Under the Guidance of
Prof. Rahul De

Year-2016

Contents

Introduction

IoT or Internet of Things is a phrase coined to define a system of interrelated physical devices embedded with sensors and network connectivity that enable them to collect, process and exchange data. In 2013 the Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as "*the infrastructure of the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies*" (ITU, 2015).

While machine-to-machine (M2M) communication already existed, IoT goes beyond it by offering advanced connectivity covering a variety of domains, protocols and applications. “Things” in IoT can refer to a wide variety of devices like heart monitoring implants, weather monitoring sensors, biochip transponders, home appliances connected to the internet, automobiles with sensors or any other object with an IP address assigned to it and the ability to transfer data over a network. The convergence of wireless technologies, micro-electromechanical systems and the internet has broken down the wall between operational technology and information technology allowing unstructured data generated by machines to be transmitted over a network and then analysed (Rouse, 2015). The presence of the IPv6 addressing scheme has allowed a manifold increase in the number of devices that can be connected to the internet and this has in turn facilitated the full-scale adoption of IoT. According to Gartner IoT will consist of 20 billion objects by 2020 which will amount to about 3 devices per person on earth, thus highlighting the sheer scale (Gartner, 2015).

Practical Applications

Practically every industry that requires devices to collect data and transmit over a network along with remote controlling can benefit by adopting IoT. These IoT devices also work on limited power and memory resources and therefore can be deployed anywhere. The range of adoption could vary from something as large as smart cities for urban planning to biochip transponders in implants.

Environmental monitoring is a fast growing adopter of IoT. Natural disaster tracking systems for earthquakes or tsunami early warning systems are being built on IoT where devices are spread across large geographical areas and can also be mobile (Ersue, Romascanu, Schoenwaelder, & Sehgal, 2014).These devices sense certain physical parameters or weather changes and give real time data to a hub that can analyse it. Similar devices are being used to assist environmental protection by monitoring air, water and soil quality; to detect the presence of wildfires and monitor the migration patterns of wildlife.

Managing big infrastructure projects where manual monitoring and surveillance is next to impossible also benefits from IoT. Bridges, railway tracks, wind farms, oil rigs and other such heavy infrastructural projects employ a number of IoT devices that can monitor events or changes in structural parameters thus preventing safety risks, schedule maintenance and repair activities from a central location and control critical infrastructural components. IoT greatly reduces the amount of human effort required in maintenance of these projects.

Industrial manufacturing has become such a big adopter of IoT that a term called Industrial Internet of Things (IIOT) has now been coined to refer to the industrial subset of IoT. The IoT devices enable rapid manufacturing, dynamic response to demand fluctuations, and real time optimisation of supply chain networks and manufacturing production (Ersue, Romascanu, Schoenwaelder, & Sehgal, 2014). IIOT could have such a big impact on the manufacturing industry that it is said that it could lead to the fourth Industrial Revolution and $12 trillion of global GDP by 2030 (Accenture, 2015).

Energy management has been the need of the hour for a lot of companies and IoT offers excellent solutions for it. Integrating IoT devices into all power consuming devices so that it can communicate with the energy supply company gives immense potential to optimise electricity usage and prevent theft. When implemented in home devices, it gives consumers the ability to remotely manage all the devices from a cloud based app and also monitor their usage. At the level of urban planning, IoT can be used to implement Smart Grids.

IoT is currently also being used heavily in medical and healthcare systems. Critical medical systems where sensing data on a real time basis is important can be integrated with IoT to allow centralisation of data collection and notification. IoT also opens the door to remote health monitoring where devices like blood

pressure and heart rate monitors can transmit data from the patient to a doctor remotely.

Homes are getting increasingly integrated with technology and IoT devices can be used to monitor and control electrical, mechanical and electronic systems in building complexes. We will use a certain water level management IoT device (waterSenz (TM)) as the focus of our discussion later on.

Consumer applications that include the fast growing industry of wearable devices form the final industry that has taken to IoT. Smart cars, smart entertainment systems, smart home appliances are just some of the applications that are available to the end customer.

Challenges – Privacy & Control

Privacy of user's data seems to be the biggest concern with the explosion of IoT devices. With these devices being present in all facets of our life, and collecting data at all times, companies owning these devices have access to potentially private data of the users. Additionally, there are very few clear laws that control what companies can do with this data. In a world where data has become invaluable, companies are most likely to sell data to others who need it. For example, an IoT device that makes up a smart car could potentially keep records of every trip made by the car. This data could be of interest to companies who are looking to analyse traffic patterns. Therefore, while the IoT will enable our lives by making it "smarter", in exchange consumers will have to compromise on their privacy as privacy laws are being rewritten under their noses to suit the corporations (Wired, 2015).

However, a number of committees have been set up that are forming frameworks that can ensure that user privacy is retained even in the technologically immersive world of IoT. Some of the common privacy challenges discussed by these committees are

- User content acquisition: The device should never capture data without the consent of the user. On the web, this is possible through "terms and conditions" agreements that users agree to before using an application. How this will be done in the IoT world is a big question as consumers will

not have a dedicated interaction regarding privacy with the IoT device, nor will their technical limitations allow them to proactively do so (Perera, Ranjan, Wang, Khan, & Zomaya, 2015).

- Control, customization, and freedom of choice: Consumers should have full power to control the data that they have provided through IoT devices. They should also be able to shift their data from one service provider to another. However currently, the IoT setup hasn't reached either the level of standardisation or the level of competition in terms of number of players for this to happen (Perera, Ranjan, Wang, Khan, & Zomaya, 2015).
- Anonymity technology: While capturing of data is going to be inevitable in the IoT world, users should have the right to stay anonymous while providing it. Companies should come up with ways to anonymise the data being collected so it can't be traced back to a particular user. Technologies like Tor that hides user location could be used (Perera, Ranjan, Wang, Khan, & Zomaya, 2015).

Different IoT companies are finding different ways to tackle these challenges with their products. However, until formal privacy rules are created, the lines will always remain fuzzy. Privacy isn't the only issue at hand. Security of data from all sorts of attacks is a bigger issue in itself. The environmental damage that could be caused by billions of semiconductor devices is another issue.

The Indian context

IoT has a big role to play in the digital transformation of India. With increasing focus being given on digitizing the country by the government, the country has invited the interest of a number of IoT companies varying from big MNCs to small local startups. The government has already come out with an IoT policy that aims at creating an IoT ecosystem in the country and incentivising the players in it by creating a $15 billion industry by 2020 (Kolhi, 2016).

One of the key initiatives of the government is to create smart cities on a PPP model. Some of the key aspects of these smart cities include smart parking, telecare, intelligent transport system, smart grids, waste and water management, digital signage and women's safety (Sethu, 2015).

Various industries like manufacturing, automobile and IT are also readily adopting IoT to derive various benefits from it. One of the companies which is active in the IoT space in India is Cisco which is looking to create customised solutions to Indian companies and is also providing infrastructure (Sethu, 2015). A number of startups have also sprung up in Bangalore, Mumbai, Pune and Hyderabad that are coming up with disruptive solutions in the industry (Sethu, 2015). We will now take an example of an MNC and a startup to see what they've contributed to the Indian IoT space.

Cisco's solutions

Cisco is one of the biggest companies worldwide that is pushing the adoption of IoT and is investing big in this industry. Calling it the "Internet of Everything" (IOE), Cisco considers IoE to be a $19 trillion opportunity over the next decade in the private and public sector.

It has identified five key areas of value for the private sector which include better use of assets, increased employee productivity, elimination of process efficiencies, improving customer experience and tech innovations (Exhibit 1).

For the public sector, it has identified employee productivity, connected militarised defence, cost reductions, citizen experience and increased revenue as five key focus areas (Exhibit 2).

The Cisco Bangalore office consists of a team dedicated towards providing IoT solutions to its clients. It also performs R&D for solving common business and daily life issues using IoT technologies (Standard, 2015). Some of its recent solutions include helping Mahindra & Mahindra set up its first "connected factory" at Chakan, Maharashtra. It now boasts of automating all aspects of production – from shop floor to top floor. As a result, M&M have reduced their changeover time on the factory floor and improved quality as a result of discovering issues earlier. People are now connected with the equipment on the shop floor over WiFi and this has increased their output.

TATA Motors has also been a client of Cisco and has got an IT platform that it believes will be crucial to its success. The company is located in 170 cities and has 6 plants for which Cisco has given it a stable communication network, solved its end to end routing needs and provided switching devices and video conferencing products to help teams collaborate. On top of this, the vehicles are proposed to be "connected cars" that will provide services including emergency

breakdown alerts and usage-based insurance programs. Owners of fleets of buses or trucks will also be given a portal to track current locations. There is special emphasis being given on providing this service to schools to let parents track school buses. Therefore, through IoT Cisco is able to make TATA Motor's more efficient in every part of the value chain – from sourcing to supply chain to manufacturing and also allows TATA Motors to give better service to customers through its IoT enabled products.

Gnarus Solut!ons

While Cisco is solving business problems of big clients, a lesser known startup based out of Bangalore is looking to disrupt the way water is managed by consumers in cities. The company named gnarus Solut!ons has developed a product named waterSenz (TM) which offers a digital assistance "for water availability monitoring, supply chain operations, periodic and preventive maintenance" for houses and buildings which have overhead water tanks (Solut!ons, 2016). The waterSenz (TM) sensor is a small device of the size which is fitted on top of the water tank or the underside of the lid and is not in direct contact with the water. Contact less sensors to check the water level in overhead tanks and sends the data via WiFi to the cloud every 10 to 15 minutes. The waterSenz (TM) application is installed in a user's mobile phone which receives information from the cloud.

The waterSenz (TM) mobile application is a multilingual platform which offers the user the service to check water availability, motor status, access to services and consumption analytics of his house or building. The User Interface of the application is shown in Exhibit 3. The features of the application are present in Exhibit 4, 5 and 6. It also allows the user to check the water level in the sump and overhead tank simultaneously. It lets the user remotely switch on the motor if the overhead tank needs to be filled or allows him to order for a tanker to refill the sump at an appropriate time. The motor turns off when the overhead tank is filled up, without overflow of water even when the motor is turned on manually. This helps in saving water as well as electricity which is used to pump water from the sump to the overhead tanks.

Previously, before the advent of waterSenz (TM), consumers had to order water tankers based on their estimates and had to pay for the ordered water even if the sump could not entirely hold it. The users of waterSenz (TM) technology are

now able to accurately identify water levels in the sump and therefore order for water exactly when it's needed. Thus this reduces water bill for the customers.

Consumption analytics show the users their hourly, daily and monthly water consumption patterns. This visible pattern of water usage makes users aware of their water usage. This has helped users save valuable water resource as they can now track, analyse, find out reasons and control the reasons of water overuse if any. This has further helped users to reduce their water and electricity bills too.

The application also offers out of the box notifications to the user's preferred service providers. The services providers include:

- Water Tanker supplier
- Sewage/Sludge Removal Tanker
- Calendared maintenance schedules for
    - tank/sump cleaners
    - motor pump service technicians
    - plumber
    - electrician (Solut!ons, 2016)

As the lifestyle of people are changing, this is a boon for working couples who are not at home always and can monitor water levels of their home from anywhere or schedule delivery of the water tankers at the appropriate time when they are at home. It also helps elderly couples living alone as they do not have to climb up the stairs which is physically challenging to them to check water levels of their overhead tanks. In housing complexes, the overhead tanks are placed high above, so it also helps to save the efforts of security guards of huge buildings to go up constantly to the top floors to the check the water level.

The basic application costs under INR 5,000 plus installation charges. There is also a monthly subscription fee. The Company says that they are liable if there are any issues in the sensor and replace or repair it free of cost (only the conveyance is charged to the user) till the time the users are paying the monthly subscription fees otherwise applicable price would be charged. At present, there have been 16 installations of waterSenz (TM) which include 11 installations in Bangalore and 5 installations outside Bangalore. They are currently in talks with two builders in Bangalore who are interested to use waterSenz (TM) in their buildings.

With their patent pending, they are not aware of any competition in India. They have not done any formal marketing till date and heavily rely on word of mouth marketing. The waterSenz (TM) technology besides being used in houses and buildings has huge market potential and can be used in industries, hospitals, hotels and restaurants for water management.

They are at a very nascent stage and hope to extend the waterSenz (TM) technology to many other applications like:

- In reorder level management where it can be used to send alerts for replacement of any fluids in the production lines.
- In Sewage Treatment Plant where an audio alarm can be put in for water overflows.
- In oil tankers or petrol pumps which still use dipstick method to find out the level of oil.

Challenges and the future

The major challenges in the Indian context are no different from the global ones. Data privacy still remains the number one area of concern. For example, waterSenz (TM) collects and stores water usage details of individual consumers for up to a month. While most users might not have problems with sharing data related to water consumption, other IoT products could be dealing with much more sensitive information. Moreover, the security issue still remains. Miscreants could tap into the network and make inferences on whether the residents are at home or if there is a guest in the house. Gnarus Solut!ons tackles the issue of privacy by letting the user know what data is being taken and ensuring that they provide full consent to sharing that data. They also store the data in an anonymised format so that user identity is not revealed. Other companies could take similar steps to mitigate the risks associated with data privacy.

In the case of Cisco, where it is dealing with providing B2B solutions, data privacy is not much of a concern since data is held by the client. However, in IoT products and services that reach the end user the concern remains. It is only hoped that big corporations like Cisco walk their talk on caring for customer privacy as they claim. The absence of strong laws in the Indian context to protect data privacy means that consumers should be doubly sure before signing up for such services.

On the implementation front, India still faces a few challenges. The integration of technology and language keeping in mind India's diversity, cyber security and last mile connectivity are some of the other key issues (Sethu, 2015). The infrastructural issue will be resolved slowly as the government is actively looking to improve connectivity throughout the country. The presence of private players in this realm has improved the situation.

Therefore, as seen by the applications of IoT, it is definitely here to stay. The value generated by it is immense and it has the ability to be a disruptor in every field. The market for IoT is huge as we see in the example of waterSenz (TM) it has the ability to reach every household. Once the infrastructure is taken care of, the full potential of IoT can be unleashed. In the midst of all this though, strong data privacy laws need to be formulated by the government to protect user data. But till these are formed, companies will have to hold themselves to high ethical standards.

Appendix

Five Key Areas of Value at Stake for the Private Sector

- $2.5 trillion: Better use of assets will improve execution and capital efficiency, reducing expenses and cost of goods sold.
- $2.5 trillion: Increased employee productivity will reduce person-hours and free your knowledge-workers to do more effective work.
- $2.7 trillion: Process inefficiencies will be eliminated through supply-chain improvements.
- $3.7 trillion: Improved customer experiences will build stronger relationships and bring more customers.
- $3 trillion: Tech innovations will increase return on R&D, reduce time to market, and create revenue from new business models.

Exhibit 1 (Cisco, 2014)

Five Key Areas of Value at Stake for the Public Sector

- Employee productivity ($1.8 trillion): IoE improves labor effectiveness for new and existing services.
- Connected militarized defense ($1.5 trillion): IoE generates a fourfold force-multiplier effect through improved situational awareness and connected command centers, vehicles, and supplies.
- Cost reductions ($740 billion): IoE improves labor efficiency and capital-expense utilization, while also reducing operational costs.
- Citizen experience ($412 billion): IoE shortens "search" times, improves the environment, and produces better health outcomes.
- Increased revenue ($125 billion): IoE improves the ability to match supply with demand while also enhancing monitoring and compliance.

Exhibit 2 (Cisco, 2014)

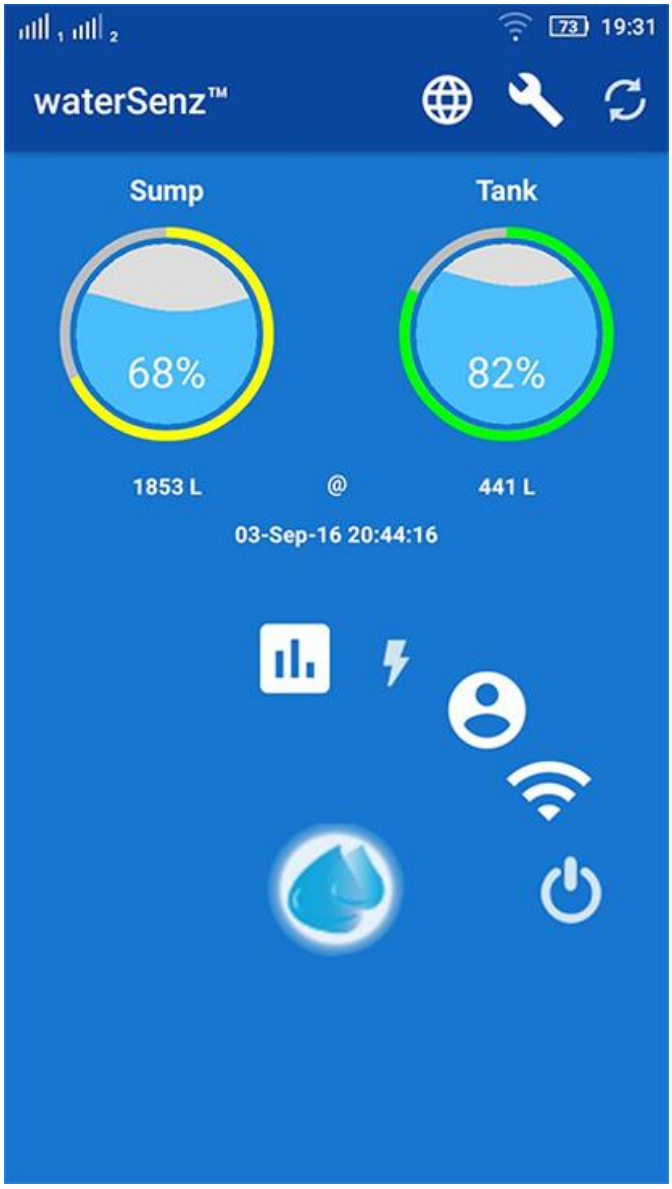

Exhibit 3: waterSenz (TM) Mobile UI

Exhibit 4: Multilingual Interface

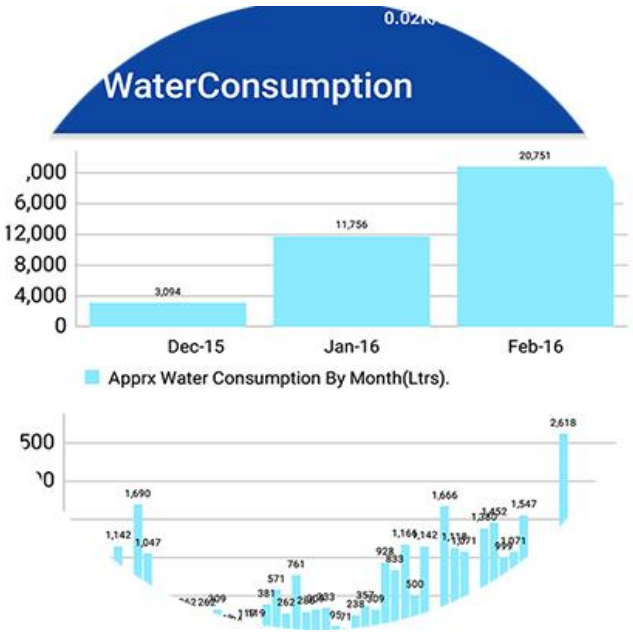

Exhibit 5: Consumption analytics

Exhibit 6: Services

References

Accenture. (2015). *Driving Unconventional Growth through the Industrial Internet of Things.*

Cisco. (2014). Retrieved from http://www.cisco.com/c/dam/en_us/services/portfolio/consulting-services/documents/consulting-services-capturing-ioe-value-aag.pdf

Ersue, M., Romascanu, D., Schoenwaelder, J., & Sehgal. (2014). *Management of Networks with Constrained Devices: Use Cases.*

Gartner. (2015). Retrieved from http://www.gartner.com/newsroom/id/3165317

ITU. (2015). Retrieved from http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

Kolhi, V. (2016). Retrieved from http://india.nlembassy.org/binaries/content/assets/postenweb/i/india/netherlands-embassy-in-new-delhi/import/iot-india.pdf

Perera, C., Ranjan, R., Wang, L., Khan, S., & Zomaya, A. (2015). *Privacy of Big Data in the Internet of Things Era.*

Rouse, M. (2015). Retrieved from http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

Sethu, K. (2015). Retrieved from http://www.iotleague.com/current-state-of-internet-of-things-iot-in-india/

Solut!ons, g. (2016). Retrieved from http://www.gnaruz.com/watersenz.html

Standard, B. (2015). Retrieved from http://www.business-standard.com/article/companies/cisco-rides-high-on-iot-115060600891_1.html

Wired. (2015). Retrieved from http://www.wired.com/insights/2015/02/say-goodbye-to-privacy/