IoT: a Machine to Cloud

Vaidehi Muley#1, Varsha Kesavan\*2, Vaibhavi Patil#3

*Roll no.s-301530,301521,301537*

Department of Electronics and Telecommunication

*Fr. Concacio Rodrigues College of Engineeering, Mumbai University*

*Sector-9A,Vashi,Navi Mumbai,India*

vaidehimuley5@gmail.com

varz.kesavan@gmail.com

vaibhaviapatil997@gmail.com

***Abstract* - Every year IoT brings new things to biotechnology, manufacturing, home living and every aspect of our daily lives. We’ve seen it disrupt traditional industries, transform our cities and contribute to the autonomous transport of the future. IoT has begun to become part of the popular parlance. In the coming years, IoT will look completely different than it does today. IoT is a greenfield market. New players, with new business models, approaches, and solutions, can appear out of nowhere and overtake incumbents. Organizations creating products may have to develop variants to support multiple standards or ecosystems and be prepared to update products during their life span as the standards evolve and new standards and related APIs emerge the Internet of Things (IoT) has become a vital instrument to interconnect devices Consumer-facing industries will be changed by IoT. We’re moving into sober analysis of the capabilities of IoT. The IoT is comprised of smart machines interacting and communicating with other machines, objects, environments and infrastructures. As a result, huge volumes of data are being generated, and that data is being processed into useful actions that can “command and control” things to make our lives much easier and safer—and to reduce our impact on the environment. The creativity of this new era is boundless, with amazing potential to improve our lives. The following thesis is an extensive reference to the possibilities, utility, applications and the evolution of the Internet of Things.**

**C-RAN (Cloud-RAN), sometimes referred to as Centralized-RAN, is a proposed architecture for future cellular network. Simply speaking, C-RAN is a centralized, cloud computing-based architecture for radio access networks that supports 2G, 3G, 4G and future wireless communication standards. Its name comes from the four 'C's in the main characteristics of C-RAN system, "Clean, Centralized processing,** **Collaborative radio, and a real-time Cloud Radio Access Network"**

**Keywords— greenfield market, command and control.**

1. INTRODUCTION

IoT is a network of devices, buildings, vehicles and other physical objects embedded with sensors that transmit data between a company and the consumer. The purpose of all this communication between the two is to provide consumers smarter products and services, a better customer experience, and for businesses a competitive edge and ability to build revenue. By the year 2020, the Internet of Things is predicted to consist of close to 50 billion objects.

In the beginning, a British technology pioneer by the name of Kevin Ashton invented the term Internet of Things. The term was used to describe exactly what it means today; a system of connected ubiquitous devices communicating data over the Internet.

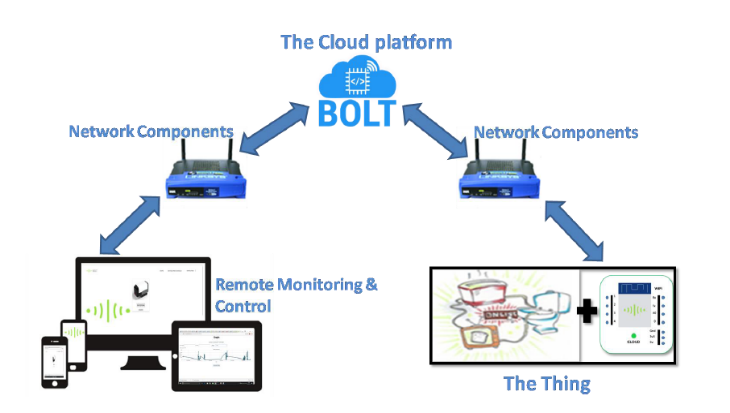


Fig. 1 Block diagram of the process1.

*A. Evolution*

Rather than being a foundational technology itself, the IoT has evolved on the back of various other innovations, including wireless communication, real time analytics, machine learning, sensors and embedded systems. These have been combined to transform ‘things’ - whether that’s physical objects, devices, vehicles or buildings - into a connected part of the internet, enabling them to be controlled or sensed remotely. Doing so brings the power of computing to the physical world, removing the need for human intervention and introducing much greater automation to everything we do.

The basic idea is 'Move from Internet of People ? Internet of Things':

Internet appears everywhere in the world. It is primarily connection between people.Internet of Things is a plan to connect things also using the same medium.

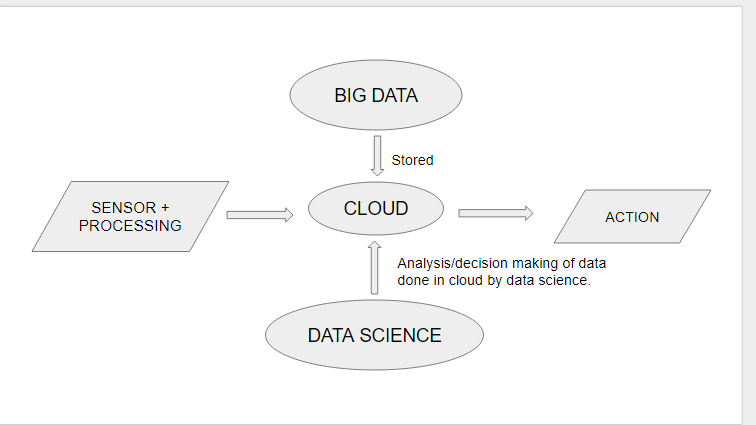


Fig.3 Flowchart of the process2.

*B.Big data:*

Big data is a term for data sets that are so large or complex that traditional data processing application software is inadequate to deal with them. Big data challenges include capturing data, data storage, data analysis, search, sharing, transfer, visualization, querying, updating and information privacy.

*C.Cloud:*

IoT Cloud is a platform that is designed to store and process Internet of Things (IoT) data. The platform is built to take in the massive volumes of data generated by devices, sensors, websites, applications, customers and partners and initate actions for real-time responses. For example, wind turbines could adjust their behavior based on current weather data; airline passengers whose connecting flights are delayed or cancelled could be rebooked before the planes they are on have landed.

*D.Data science:*

Data science, also known as data-driven science, is an interdisciplinary field about scientific methods, processes, and systems to extract knowledge or insights from data in various forms, either structured or unstructured, similar to data mining.

Data science is a "concept to unify statistics, data analysis and their related methods" in order to "understand and analyze actual phenomena" with data. It employs techniques and theories drawn from many fields within the broad areas of mathematics, statistics, information science, and computer science, in particular from the subdomains of machine learning, classification, cluster analysis, data mining, databases, and visualization.

II. APPLICATION

The potential benefits of the IoT are huge, not least the enormous time and cost savings to industry, business and individuals. The supply chain example is a really good one, where IoT allows organisations to track where their stock is at any given time, optimising efficiency, reducing losses and maximising sales.

It’s also praised for its ability to reduce waste and energy, by allowing us to better control our use of resources based on our actual needs.

NEST thermostat: it controls the central heating based on when person is at home, away, or even in bed. No more leaving the heating on when one's on holiday.

Another great example is a solution by Altiux, which aims to better control street lighting based on a city’s requirements. If it succeeds, the energy savings and environmental benefits will be enormous.

*A.Intelligent home*:

In recent years, there has been a huge growth in the world of intelligent devices for home automation. Such gadgets are designed in order to ease the interaction between people and daily home duties. Although individually they are simple to work with, each appliance has its own configuration interface which adds overhead to the general user experience. This paper presents a solution for connecting more devices into a signal entity which can be easily accessed at any time. The implementation integrates the functionalities of different home automation devices into a single application.

1. *Smart Egg Tray*:

'Egg Minder' wirelessly connects to your mobile device to track the number of eggs you have and tell you when they’re going bad. In-tray LED lights indicate the oldest egg, while push notifications alert you when you’re running low.

1. *Smart Washing Machine*:

'Smart Aqualtis' is the first Indesit Company washing machine designed to be integrated in 'Smart' ecosystems, covering a wide range of use cases.

1. *Smart Sleep System:*

Visualize your sleep cycles, understand what wakes you up and compare nights. From the palm of your hand you can control, your hand, you can control your wake ups and fall asleep programs.

1. *Smart Weather System:*

This includes sensors to measure temperature humidity and rain. These sensors provide live reporting to weather statistics. Thus, alerts are send to the users if the weather parameters cross a level.

1. *Smart Garbage Cans:*

Using sonar waves and sensors BigBelly alerts when it needs to be emptied so smarter collection decisions can be made.

1. *Smart Gardening:*

Using Iot with environmental sensors like light, humidity, temperature and others recommends you which plants will thrive or the optimal time for planting among others.

III.CHALLENGES

The small size and limited processing power of many connected devices could inhibit encryption and other robust security measures.Moreover, some connected devices are low-cost and essentially disposable. If a vulnerability is discovered on that type of device, it may be difficult to update the software or apply a patch – or even to get news of a fix to consumers.We could end up with relatively modern 64-bit x86 CPU cores in IoT devices, but they won’t come cheap, they will still be substantially more complex and therefore will need more battery power.Cheap and disposable wearables won’t be powered by such chips, at least, not anytime soon. Consumers may end up with more powerful processors, in some smart products, like smart refrigerators or washing machines with touchscreens, but they are impractical for disposable devices with no displays and with limited battery capacity.

security breaches would also affect a bigger number of devices.

*A.Privacy Concerns*

In present scenario, the vast majority of devices are collecting information like name, address, date of birth or even health and credit card information. Even worse is the fact that many devices transmit this information across networks without encryption. If users misconfigure their home network, then they are only one step away from exposing this data through wireless networks. Cloud services, which many of these devices use, are also extremely vulnerable. However, it is likely that the majority of these devices actually need personal information to function.

*B.IT Security Is Overstretched Already:*

Cloud computing which is providing a lot of benefit to the enterprise is also being used by cyber criminals to host their malware, steal data and help them build large networks to crack encryption. The rise of the nation state as a cyber-threat is also a serious worry as they have unlimited budget, can have exceptional security skills and are capable of designing complex attacks such as Advanced Persistent Threats (APTs), which means that they are more of a risk than organised crime.

All of this comes at a time when budgets are getting repeatedly cut and regulators are looking to increase the controls on what can be done with data. The result is an IT Security function that for most organisations is in disarray and without the right tools and guidance will be incapable of dealing with what is facing it.

*C.Healthcare IoT security issues:*

In healthcare, the Internet of Things offers many benefits, ranging from being able to monitor patients more closely to using generated data for analytics.

But that increased flow of information also brings risks that health IT professionals need to address.Those risks include possible harm to the patient's safety and health, loss of PHI and unauthorized access to devices.One problem is devices entering hospitals through a variety of channels, with some of these avenues being unknown When this happens it can be difficult to figure out the lifecycle management of that device and identify the operating system.Another issue is standalone devices that have developed networks and connectivity glitches,with those connectivity issues comes transference and movement of data, and so data migration might occurring.

*D.Others:*

Earlier this month, researchers found critical vulnerabilities in a wide range of IoT baby monitors, which could be leveraged by hackers to carry out a number of nefarious activities, including monitoring live feeds, changing camera settings and authorizing other users to remotely view and control the monitor in another development, it was proven that Internet-connected cars can be compromised, as well, and hackers can carry out any number of malicious activities, including taking control of the entertainment system, unlocking the doors or even shutting down the car in motion.More connected devices mean more attack vectors and more possibilities for hackers to target us.Wearables also can become a source of threat to your privacy, as hackers can use the motion sensors embedded in smartwatches to steal information you’re typing, or they can gather health data from smartwatch apps or health tracker devices you might be using.

IV. CONCLUSION

Based on our studies on Internet Of Things (IOT), we can say that this sector is just in the first steps of development and have a lot of potential development. It is looks like a trend to have one of these products and that is very good for the future of the Internet Of Things. As we can read it in my report, the predictions of a lot of people are very good for this sector. Using this type of products allow a lot of gains, productions, time, and so on. The temptation is very huge for a lot of companies to turn them self into the utilization of those products.

V. REFERENCE

[1].www.digitalrisks.co.uk/blog/the-internet-of-things-a-connectedfutureen.wikipedia.org/wiki/Internet\_of\_things#Intelligence

[2].www.raymondjames.com/

[3].www.quirky.com/invent

[4].www.readwrite.com