International Research Journal of Computer Science (IRJCS)
Issue 09, Volume 4 (September 2017)
ISSN: 2393-9842
www.irjcs.com

ARTIFICIAL INTELLIGENCE MEET INTERNET OF THINGS

W. Malini Prema Kumari
Research Scholar,Periyar University,Salem,INDIA
malinipremakumari@gmail.com

Manuscript History
Number: **IRJCS/RS/Vol.04/Issue09/SISPCS10098**
Received: 08, September 2017
Final Correction: 13, September 2017
Final Accepted: 20, September 2017
Published: September 2017
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

Abstract-- The Internet of Things (IoT) is still in its infancy because of the limited capability of its embedded processor. In the meantime, research on artificial intelligence (AI) has made plenty of progress. The application of AI to IoT will significantly increase the capabilities of IoT, and this will benefit both economic and social development. The importance of Artificial Intelligence approaches to enable such Intelligent Communication Networks. Nowadays, sensor networks are becoming a reality, especially for remote monitoring of events in fields such as healthcare, military, forest integrity or prediction of seismic activity in volcanoes. Intelligent devices and sensors are also appearing, besides electronic home appliances and utilities, as gadgets to mobile phones or tablets. And some of these devices have capability to actuate on the world. The Internet of all these intelligent things connected and communicating. It addresses artificial intelligence techniques employed to create such intelligence, and network solutions to exploit the benefits brought by this capability.

Keywords— Internet of Things (IoT), Artificial Intelligence, Machine Learning

I. INTRODUCTION

IoT systems allow users to achieve deeper automation, analysis, and integration within a system. They improve the reach of these areas and their accuracy. IoT utilizes existing and emerging technology for sensing, networking, and robotics.IoT exploits recent advances in software, falling hardware prices, and modern attitudes towards technology. Its new and advanced elements bring major changes in the delivery of products, goods, and services; and the social, economic, and political impact of those changes.

IoT – Key Features

The most important features of IoT include artificial intelligence, connectivity, sensors, active engagement, and small device use. A brief review of these features is given below

- **AI** – IoT essentially makes virtually anything "smart", meaning it enhances every aspect of life with the power of data collection, artificial intelligence algorithms, and networks. This can mean something as simple as enhancing your refrigerator and cabinets to detect when milk and your favorite cereal run low, and to then place an order with your preferred grocer.
- **Connectivity** – New enabling technologies for networking, and specifically IoT networking, mean networks are no longer exclusively tied to major providers. Networks can exist on a much smaller and cheaper scale while still being practical. IoT creates these small networks between its system devices.

- **Sensors** – IoT loses its distinction without sensors. They act as defining instruments which transform IoT from a standard passive network of devices into an active system capable of real-world integration.
- **Active Engagement** – Much of today's interaction with connected technology happens through passive engagement. IoT introduces a new paradigm for active content, product, or service engagement.
- **Small Devices** – Devices, as predicted, have become smaller, cheaper, and more powerful over time. IoT exploits purpose-built small devices to deliver its precision, scalability, and versatility.

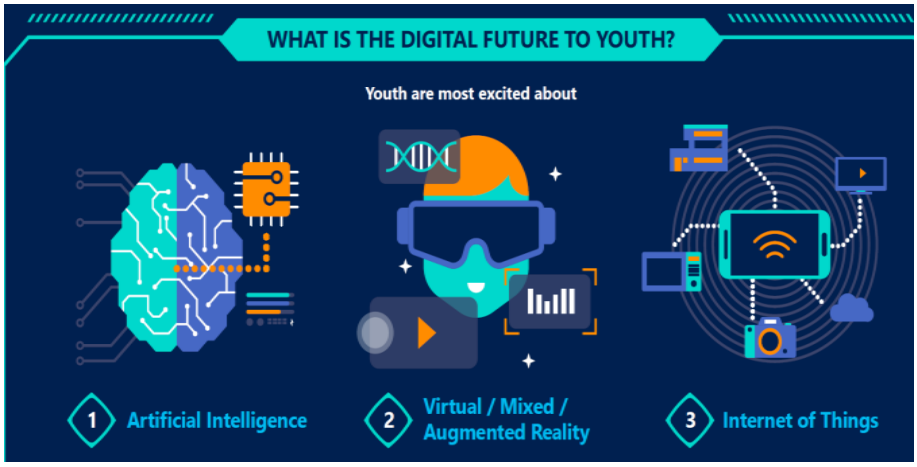

Figure: 1 depicts Internet of Things

II. TECHNOLOGIES INVOLVED

The actual implementation of IOT in the real world is done by combining various technologies available. This is possible with any one of the following:

A.RFID – Radio Frequency Identification

Radio-frequency identification (**RFID**) uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information. Passive tags collect energy from a nearby **RFID** reader's interrogating radio waves. This is a wireless device that uses electromagnetic fields. The objects are connected with the help of tags attached to them. An RFID is a small microchip attached to the object-new version of barcodes. This tag can be stuck onto the wrist, and it picks up all the RFID tags in the vicinity.

B. Near Field Communication

This is a set of thoughts and technologies with the help of which the smart phones and other objects that wants to communicate under IoT.

C. M2M - Machine to machine

M2M communication is often used for remote monitoring. In product restocking, for example, a vending machine can message the distributor when a particular item is running low. M2M communication is an important aspect of warehouse management, remote control, robotics, traffic control, logistic services, supply chain management, fleet management and telemedicine. It forms the basis for a concept known as the Internet of Things (IoT). Key components of an M2M system include sensors, RFID, a Wi-Fi or cellular communications link and autonomic computing software programme to help a network device interpret data and make decisions. The most well-known type of M2M communication is telemetry, which has been used since the early part of the last century to transmit operational data. Pioneers in telemetrics first used telephone lines and later, on radio waves to transmit performance measurements gathered from monitoring instruments in remote locations. The Internet and improved standards for wireless technology have expanded the role of telemetry from pure science, engineering and manufacturing to everyday use in products like home heating units, electricmeters and Internet-connected appliances. Products built with M2M communication capabilities are often marketed to end users as being "smart." In this technology, information between the machine is exchanged and work is executes without any manual help.

D Wireless Sensor Network (WSM)

It is a set of large number of sensors which monitor environmental conditions. A **wireless sensor network** (**WSN**) is a **wireless network** consisting of spatially distributed autonomous devices using **sensors** to monitor physical or environmental conditions. A **WSN** system incorporates a gateway that provides **wireless** connectivity back to the wired world and distributed nodes.

E. Addressing schemes (IPv6 addresses)

Addressing scheme is the basic tool by which IoT concept can be implemented by giving IP addresses to each object which we want to communicate. **IPv6** is the successor to the first **addressing** infrastructure of the Internet, Internet Protocol version 4 (IPv4). In contrast to IPv4, which defined an IP **address** as a 32-bit value, **IPv6 addresses** have a size of 128 bits. Therefore, **IPv6** has a vastly enlarged **address** space compared to IPv4.

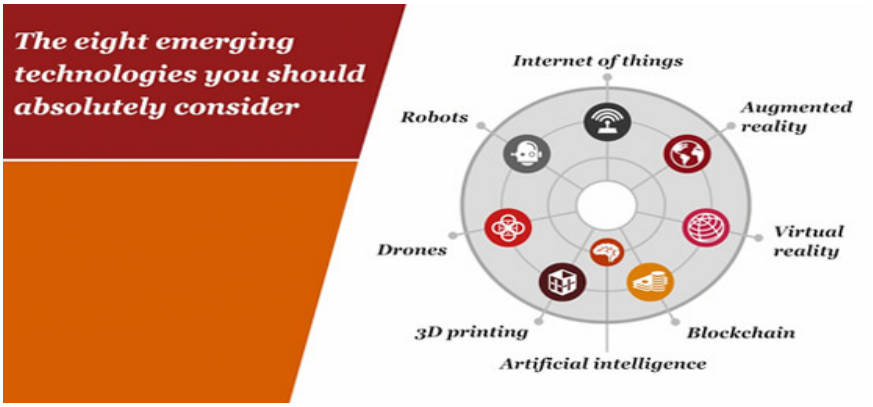

Figure 2: Varies Technology using Artificial Intelligence to IOT

The Internet of Things (IoT) has the potential to fall into the general pit of buzzword-vagueness. Artificial intelligence (AI) often falls into the same trap, particularly with the advent of new terms such as "machine learning," "deep learning," "genetic algorithms," and more. The purpose of this article is to flesh out the actual applications of combining AI and IoT being used in industry today, and to demonstrate important trends and future use cases for technologists who want get a lay-of-the-land of how artificial intelligence might help to facilitate and make sense of the myriad connected devices in the coming decade. This article has been written with the professional or executive in mind, rather than the researcher. Dozens of our interviews with emerging technology executives and researchers and hours of combining the insights of major market research firms (which I've compiled conveniently at the end of this article) seems to point to one overarching theme in the connection of artificial intelligence and the internet of things, namely:

Artificial intelligence will be functionally necessary to wield the vast number of connected "things" online, and will be even more important in making sense of an almost endless sea of data streamed in from these devices.

III. COMBINING AI AND THE INTERNET OF THINGS, 3 USEFUL EXAMPLES

The example applications that I've outlined below are all in use today, and have been chosen as representative examples of a broader trajectory of applications. I aimed to avoid overly niche applications of IoT, (like the "connected pacifier" or the "tray that alerts you when you're out of eggs") or IoT applications that don't involve AI in any form. The following AI and IoT combinations are useful examples of how these two broad concepts collide.

It's important to note that many so-called "IoT" devices wouldn't make this list. By the criterion we're selecting for (connected devices that leverage artificial intelligence), a device isn't "smart" merely by virtue of being controllable via an iPhone app. Below are some useful examples:

1 – Automated vacuum cleaners, like that of the iRobot Roomba

iRobot set the standard with it's first commercially successful automated vacuum in 2002. Founded by MIT roboticist, the company has developed technology to help its puck-shaped vacuum robots to map and "remember" a home layout, adapt to different surfaces or new items, clean a room with the most efficient movement pattern, and dock itself to recharge its batteries. While the artificial intelligence applications in the Roomba aren't as celebrated as broad consumer AI advances such as Facebook's facial recognition or Apple's *Siri*, it is nonetheless the industry standard in it's class, and a clear example of artificial intelligence "embodied" in a robot.

2 – Smart thermostat solutions, like that of Nest Labs

Though the "smart home" hasn't exactly revolutionized life for most of us, some companies are ardently aiming to change that – and there are few better examples than Nest, the company acquired by Google for a reported $3.2 billion. As an IoT device, Nest's clean digital interface is (for many) a welcome change from the clunkier physical dial, and it's smartphone integration allow for temperature checking and controls from anywhere. This is "IoT" in principle, but many claims that Nest's look, feel, and interface made the device more inviting and simple to use (aided largely by the fact that Nest's founders were influential Apple employees, involved in the development of the iPod and iPad). In terms of artificial intelligence application, Nest's device "learns" the regular temperature preferences of it's users, and also adapts to the work schedule of it's users by turning down energy use.

3 – Self-driving vehicles, such as that of Tesla Motors

Cars are "things," and insomuch as we're interested in "things" that leverage powerful artificial intelligence, automotive technology is ahead of the curve (pun intended, I suppose). This isn't necessarily because autonomous vehicles will be the easiest IoT innovation to bring to life (with legal and ethical concerns, the jury is out on how long it'll take to have driverless highways anytime soon), but with nearly all major car manufacturers throwing billions of dollars at the problem, it certainly has momentum (pun intended, I suppose).

To use Tesla's technology as an example, we'll need to understand how Tesla's autonomous vehicle technology really works. An article in Fortune refers to Tesla CEO Elon Musk's response to the question of what makes Tesla's self-driving cards unique: "The whole Tesla fleet operates as a network. When one car learns something, they all learn it. That is beyond what other car companies are doing…" Interestingly enough, Google's self-driving approach isn't all that different, and employs machine learning (and many hundreds of thousands of road-miles of test data) to predict the behavior of cars and pedestrians in various circumstances.

POTENTIAL FUTURE USES FOR AI-POWERED IOT DEVICES

Today's IoT applications are useful in understanding trends, as they lay out areas in which "traction" is proven and directions where big-company and venture money is already moving. However, autos and vacuums account for the tip of proverbial iceberg of potential IoT+ AI applications:

1 – Security and access devices

In terms of purely IoT applications, companies like ACT (Access Control Technologies) are already furthering the use of key fob technologies for unlocking doors and uses of equipment. Even in organizations with well under a thousand employees, artificial intelligence could be used to determine regular access patterns of different employees or roles and tiers of employees – providing insight for future office layouts, and potentially detecting suspicious activity (using the same kind of technology that modern cyber security uses in detecting outliers).

Though we weren't able to find key fob / access key technologies integrating artificial intelligence or predictive analytics, we would suppose that as fob technology and adoption improve, this area may be rife with security insight (particularly for larger firms assessing data across many locations).

2 – Emotional analysis, facial recognition

Facial recognition has made some massive leaps and bounds in the last five years alone, and from surveillance to marketing, it seems safe to say that it's applications haven't been tapped. Companies like Kairos are honed in on marketing applications already, brandishing marquee clients like Nike and IMB on their homepage.

With a camera on nearly every computer and Smartphone made today, gleaning information from consumer reactions to products and marketing has probably never been easier. Facebook's auto-tagging is an example that most people will be familiar with – and other business models and uses are still to be fleshed out.

AI AND IOT, A USEFUL GLOSSARY OF TERMS

With a basic understand of use-cases, trends, and predictions at the intersection of AI and the internet of things, it'll help to understand the "lingo" (for your own further research, and in discussing these concepts to friends or colleagues). Bear in mind that "IoT" and "AI" are sometimes considered too broad to be nailed down as distinct "fields," but rather might be considered technology "concepts." We provide broad definitions (and related links) below:

Internet of things: Network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.

Artificial intelligence: An area of computer science that deals with giving machines the ability to seem like they have human intelligence (Merriam Webster) The famed John McCarthy (Stanford professors and argued to have originally dubbed the term "artificial intelligence") has articulated some of the difficulties of defining "artificial intelligence".

Machine learning: a method of data analysis that automates analytical model building. Using algorithms that iteratively learn from data, machine learning allows computers to find hidden insights without being explicitly programmed where to look (SAS)

Deep learning: a branch of machine learning based on a set of algorithms that attempt to model high-level abstractions in data by using multiple processing layers with complex structures, or otherwise composed of multiple non-linear transformations (Wikipedia)

Ambient intelligence: refers to electronic environments that are sensitive and responsive to the presence of people … In an ambient intelligence world, devices work in concert to support people in carrying out their everyday life activities, tasks and rituals in an easy, natural way using information and intelligence that is hidden in the network connecting these devices

Smart objects: an object that enhances the interaction with not only people but also with other Smart Objects. It can not only refer to interaction with physical world objects but also to interaction with virtual (computing environment) objects

IV. OPEN ISSUES

Major areas of concern include:

1. Security- This includes authentication of the entity which is being conveyed. In Iot, wireless devices are used to connect and thus authenticity must be provided.

2. Data Integity- All the data in IOT is conveyed through wireless media. There are chances of theft or hacking in the path.

3. Data Storage Complexity-Machine learning and IOT would make our lives more comfortable, but the main issue lies in storage of all the data. Integrity of the stored data must be maintained.

4. Expensive- The devices with which Iot works are very expensive. The initial cost for proper working of any idea would be high and not easily affordable.

V. CONCLUSION

IoT is a new emerging trend, the future of mobile technology and coupled with machine learning increases the usefulness of the Internet. It makes communication between smart-phones equipped with touch screens to unattached objects.

The first IoT devices are already in the market including NEST (a thermostat), LOCKITRON (remote control locks), Pay By Phone (parking system) This concept of IoT will be adopted by many, and the future shows lots of possibilities and discoveries in this area. IoT will change the lives of many, where the input and support of people is needed.

REFERENCES

1. Prajakta Pande and Anand R. Padwalkar," Internet of Things –A Future of Internet: A Survey", International Journal of Advance Research in Computer Science and Management Studies, ISSN:2321-7782
2. De-Li Yang Feng and Liu Yi-Duo Liang," A Survey of the Internet of Things", The 2010 International Conference on E-Business Intelligence`
3. Luigi Atzori ,Antonio Iera and Giacomo Morabito," The Internet of Things: A survey", _ 2010 Elsevier`
4. S.D.T. Kelly, N.K. Suryadevara, S.C. Mukhopadhyay, "Towards the Implementation of IoT for Environmental Condition Monitoring in Homes", IEEE, Vol. 13, pp. 3846-3853, 2013.
5. Chunguang Zhang, Guangping Zeng, Hongbo Wang, Xuyan Tu, "Analysis on Data Mining Model Objected to Internet of Things",

