Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 12, December 2017, pg.65 – 69

Vision, Opportunities and Challenges in Internet of Things (IoT)

Prakash Tripathi

Prakashmca.tripathi91@gmail.com

Abstract— now a day's human is surrounded with various techniques that play an important role in human life. One of these is Internet of Things (IoT) where data collection is performed through various devices connected to each other that communicate one another and store those data in cloud. This cloud based data is used to analyze, extract and transmit data to required place. Internet of Things (IoT) not only play a role in home appliances, vehicular ad-hoc network (VANET), pollution control, healthcare but also women safety, agriculture, route navigation system, irrigation system, cloud computing and agri- business management. Thus Internet of Things (IoT) is a revolution in this era. Internet of Things acts as a bridge between real life and virtual world. Today most researchers are working in innovation in the area of IoT and developed embedded security system, cyber security system, network technology such as LTE, VOLTE, 5G and LIFI etc. In this paper we address the vision, challenges and opportunities of Internet of Thing (IoT). We used secondary data to devise the paper.

Keywords— RFID, Zigbee, WSN, WiFi, Cloud Computing.

I. INTRODUCTION

The Internet of things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, network connectivity which enable these objects to connect and exchange data. Each thing is uniquely identifiable through its embedded computing system but it is able to inter operate within the existing internet infrastructure. Experts estimate that the IoT will consist of about 30 billion objects by 2020. The term Internet of Things (IoT) was coined by "Kevin Ashton of Procter and Gamble, later MIT's Auto-ID Center, in 1999[1]. Internet of Things (IoT) is providing the means by which it is possible to collect and analyze data remotely without any human interaction therefore it indicates that it is possible to detect and prevent any future hazard. This technology facilitates connection of various devices to the Internet and thus automatically shares data among all the people who are using those devices. Some of the popular IoT devices; fitness band, smart watches, smart cars, solar backpack, and much more are gaining popularity among the new generation. The key technologies used in IoT include Wi-Fi, Radio Frequency Identification (RFID), Zigbee, Wireless Sensor Network, Bluetooth, NFC, and GPS, Computer, Cloud Computing.

II. VISION OF IOT

The vision of IoT is integration of various techniques and technical elements together. Its purpose is to create wireless identifiable objects that communicate with each other. Today a large number of IoT devices are created for consumers such as air purifiers, ovens, washers, dryers, robotic vacuums, refrigerators and health care components, wearable devices which use wifi and wireless sensor network for remote monitoring and sense the devices. The 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. Active tags have a local power source (such as a battery) and may operate hundreds of meters from the RFID reader. Unlike a barcodes, the tag need not be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method for Automatic Data Identification and Data Capture (AIDC).

III. WORKING OF RFID

A radio-frequency identification system uses tags, or labels attached to the objects to be identified. Two-way radio transmitter-receivers called interrogators or readers send a signal to the tag and read its response. RFID tags can be passive, active or battery-assisted passive. An active tag has an on-board battery and periodically transmits its ID signal. A battery-assisted passive (BAP) has a small battery on board and is activated when in the presence of an RFID reader. A passive tag is cheaper and smaller because it has no battery; instead, the tag uses the radio energy transmitted by the reader. However, to operate a passive tag, it must be illuminated with a power level roughly a thousand times stronger than for signal transmission. An RFID reader transmits an encoded radio signal to interrogate the tag. The RFID tag receives the message and then responds with its identification and other information. This may be only a unique tag serial number, or may be product-related information such as a stock number, lot or batch number, production date, or other specific information. Since tags have individual serial numbers, the RFID system design can discriminate among several tags that might be within the range of the RFID reader and read them simultaneously [1].

IV. FUNCTIONALITY OF WIRELESS SENSOR NETWORKS

Wireless Sensor Networks are similar to wireless ad-hoc network in the sense that they rely on wireless connectivity and spontaneous formation of networks so that sensor data can be transported wirelessly. WSNs are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location.

The WSN is built of nodes from a few to several hundred where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding [1].

V. OPPORTUNITIES OF IOT

The IoT will impact most of an organization's existing customers. IoT innovation will bring a new dimension to the existing business models across all sectors. Opportunities exist in many sectors, some of that are as follows [2]:

A. Smart Cities

Smart Cities aim to make public service infrastructures and business processes significantly smarter (i.e. more intelligent, more efficient, more sustainable) through tighter integration with Internet networking and computing capabilities. Sensors deployed throughout the city gather information about goods consumed, facilities used and other information pertaining to the life of the community. This information is given to the city council to take appropriate steps to improve the quality of life in the city.

B. Aviation Sector

In the aviation sector, the IoT can provide system status monitoring for aircrafts via sensors that measure various conditions, such as pressure, vibration, temperature, etc. This data then provides access to trends, maintenance planning and condition based maintenance. RFID tags could be used for aircraft parts helping to prevent counterfeiting. At least 28 accidents or incidents in the United States have been caused by counterfeits. There is important ongoing research about intelligent materials especially for aviation. These materials can detect and communicate with the maintenance team when the structure is damaged.

C. Automotive Industry

Some limited connecting capabilities have been seen appearing in high-end cars in the past years, for instance, real-time traffic information. Expanding these capabilities to make the car a truly connected object will allow it to contact the manufacturer to diagnose a malfunction in real-time, or even better, anticipate it; be informed of road hazards; negotiate charging prices with power stations7; and book maintenance operations. Vehicle-to-vehicle (V2V) communication will open the road to collaborative driving, addressing traffic issues from a global, rather than an individual standpoint, and will help find optimal solutions, relieving congestion and also averting collisions, leading to a decrease of road casualties. Google is developing self-piloted cars that are able to run 1,000 miles without human aid and about 14,000 miles with minimum human intervention.

D. Energy Sector

In the energy sector, the IoT will help manage and monitor energy consumption. Smart appliances will be able to operate optimally, conserving energy and at the same time satisfying the end user's need. Smart meters will send signals to customers to regulate their power consumption. This would result in lower power consumption and also lessen the burden on existing sources of energy. Sensors placed at strategic nodes in a gas pipeline would send signals to the control centre informing the controller about the pressure and volume of gas flowing through at the node at a given time.

E. Manufacturing

A lot of manufacturing companies are making use of RFID for tracking and tracing. Managing inventory is improved and easier. Tagging a device also helps to avoid counterfeiting. Sensors attached to products can give information about their health allowing the user to decide when that device should be recycled. The robots on the assembly line read the information on the bar code and then determine which parts are needed for that particular car. The parts are then sourced from the inventory. This allows Ford to use the same assembly line to manufacture different cars. Today, connected objects are still in their early

stages and there are still many challenges to be overcome before the benefits of connected objects can be fully realized.

F. Addressing and Tagging

The IoT should be able to tag or address about 50 to 100 trillion objects. To achieve this, the current IPv4 protocol will be insufficient. A key challenge is to agree on a common way of addressing and identifying objects. It is also important to have unique UIDs (user-ids), even for mass- produced objects (i.e. all objects coming out of a factory will have their own unique UID, not a common one). The relationship between objects, such as raw material (one UID) becoming refined material (another UID) or parts (each with their own UID) that are then assembled as a car (again a different UID) also needs to be considered to enable us to follow these relationships and thus maintain traceability.

VI. CHALLENGES OF IOT

Internet of Things is transforming and revolutionizing every aspect of our lives. Today the price and availability of the required hardware is the key challenge preventing companies and end users from having more 'connected objects'. Today the limitations on the hardware are:

A. Battery Life

Having connected objects can ease everyday life, but if one has to think of recharging all everyday objects, it will become too much work compared to the benefit.

B. Threat

The most widespread IoT fear also happens to be the most rampant. If there's a security loophole in a device that stores your credit card number or other personal information, hackers will try to exploit this vulnerability, often without encountering firewalls or other obstacles. Your safety could be compromised further by hackers who take over the entire system and hold your devices at ransom or even use your hardware to launch attacks against others without your knowledge. Understanding how your data is stored and accessed is something you must be aware of when considering an IoT device for your business.

C. Hardware Size

The new connected objects should not be much bigger than their non-connected counterparts.

D. Radio Connectivity

This element is of course crucial. If a user is using RFID, which is becoming quite cheap and may not require batteries, then they will have to install extra equipment to discuss with objects.

E. Surveillance

Any device with a microphone or camera can potentially be activated by a remote user with the right knowledge. That's why sites that seek out the IP address of webcams with unprotected ports stream millions of private video feeds to viewers willing to pay. Familiarize yourself with the terms and conditions of your device and the permissions its software may have to be sure no one can eavesdrop on you.

F. Company Security Policies

How does the manufacturer manage the security of their devices? Device security is the responsibility of the individual company, and since there aren't yet any laws protecting IoT security, most companies depend on self-regulation and self-reporting.

VII. CONCLUSIONS

The Internet of Things (IoT) uses the powerful combination of Wi-Fi and cloud technology to send information and perform actions through devices with Internet capabilities. This advance stems from the use of telemetry, decades-old machine-to-machine communication via wired sensors and transmitters. Most of the security concerns with IoT technology have to do with the engineering of the devices themselves. For this reason, knowledge and discretion are the most important safeguards to take when considering the switch to an interconnected network of smart devices.

REFERENCES

[1] www.wikipedia.com
[2] http://www.readwriteweb.com/archives/ibm_internet_of_things.php.

