A STUDY ON IOT FUNCTIONS, TECHNOLOGIES AND APPLICATIONS

N. Manonmani

ABSTRACT

The Internet of Things (IoT) is an interconnected network of things, connecting all physical world objects to the computers through the internet. Every object that is connected in the IoT is assigned an IP address to communicate without human intervention. Data are collected from their surrounding environments using embedded sensors and send the data through network and stored for analysis or decision making. This paper focuses on the functions of IoT, technologies used and some of the applications of IOT. This will help to understand the growing trends in IOT and its scope in future.

I. INTRODUCTION

The physical world objects are sensed and can be remotely controlled across the network using IoT technology and these objects can be integrated with computer based systems.

Things on IoT refer to wide variety of devices such as automobiles with built-in sensors, biochip transponders on farm animals and so on.

Today computers and internet creates huge volume of information. The huge volume of data available on the internet and will grow exponentially when the IOT technology is implemented. Data collected from IoT devices needs to be stored where the cloud storage supports extensively. Security plays a vital role in cloud storage.

Every object connected to the internet need an IP address to communicate. The currently used IP4 standard does not provide address space for all objects. The IPv6's huge increase in address space can assign an IP address to everything on the earth surface and plays an important role in the development of the Internet of Things.

The IoT can be used in different sectors like business, education, research, industries, supply chain management, agriculture, smart homes and so on.

II. LITERATURE SURVEY :

[1] In this paper the author discusses about various communication models used in IoT. The Device to Device Communications establish direct device-to-device communication. It uses different types of networks protocols like Bluetooth, Z-wave or Zig Bee. In Device to Cloud Communications model, the IoT device is connected directly to an Internet cloud service for data exchange and control message traffic. In Device to Gateway Model the IoT device is connected to application-layer gateway. It acts as an intermediary between the device and the cloud

Assistant Professor, Department of CS, CA & IT, Karpagam Academy of Higher Education, Coimbatore.

service, it also provides security and protocol translation. And in Back End Data Sharing Model, the back-end data-sharing model enables users to export and analyze smart object data from a cloud.

[2] This paper addresses the security issues and challenges of Internet of Things and discusses about the introduction on Internet of Things, its elements and components such as Radio Frequency Identification, Wireless Sensor Network and Near Field Communication. In the context of security, the loopholes in the technology lead to the generation of malicious data, by compromising the devices. To handle the upcoming challenges new ideas are to be regulated periodically and a flexible mechanism to deal with the security threats is needed.

[3] In this paper the author discusses the functionality review of IoT solution available in different sectors like Smart Environment, Smart Homes, Smart Enterprise, Smart City and Smart Wearable. And also focuses on some of the technologies that are driving the IoT, that includes Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN).

FUNCTIONS OF IOT:

- Embedded Systems are interconnected through wireless connectivity and smart sensors
- They are small microcontroller based computers that require less human interface.
- Sensors are networked using networking protocols via the internet using WiFi or Ethernet to collect data.
- The collected data is sent over the network to the main hub or computer.
- This main computer collects and analyzes the data, and performs decision making based on the results of the analysis.

FUNCTIONAL ELEMENTS OF IOT:

The functional elements of IoT include:[5]

1. Connectivity
2. Data Collection
3. Processors and Power
4. Storage

1. Connectivity

A number of protocols are available for networking distributed embedded systems:

• WiFi :

It consumes more power.

Used for high data rate, and high amounts of data.

Useful for streaming applications such as security cameras.

• Bluetooth :

Useful for low power, short distance networks.

2. Data Collection

• Sensors & Actuators

The sensors that are the eyes and ears of IoT transforms energy into electrical data. The work of Actuators is to transform electrical data into energy.

• Wearables

IoT sensors and devices that are worn or embedded into clothing or accessories are called wearables.

Different sensors in the IoT node are used for collecting data. The value of the data being collected and the amount of data to be processed decides what type of the sensor is used. Many IoT systems have different type of environmental sensors to measure light, motion, position, pressure, temperature, humidity, etc. Optical sensors can detect the presence of light in different wavelengths, including infrared. In automated traffic management systems, Video camera sensors including CCD and CMOS light sensors are used. Some systems being monitored may already provide a signal and that can be fed to an analog to digital converter (ADC) or an analog front end. Smart Sensors are sensors that have some data processing on board.

3. Processors and Power

• Processors & Boards:

The intelligence behind IoT systems is provided by the processor by integrating into system-on-a-chip designs.

• Transceivers

This is a hardware that enables dual directional communication for collection of data and control message delivery. Examples include cellular, Ethernet, and Wi-Fi.

• Power Supplies

IoT power supplies vary based on their needs ranging from low power to high power requirements that use traditional, thin-film printed batteries to flexible photovoltaic panels.

An 8-bit microcontroller is useful for simple, low data low bandwidth nodes. The majority of IoT applications use either 16-bit or 32-bit microcontrollers. 16-bits are used for basic nodes of low to medium complexity where the data is not part of a realtime system. The advantage of 16 bits is that it can be the best compromise of low power and data throughput. However, the most common data bus for an IoT node is 32-bits where performance is essential and a high level of integration is required.

In the context of security, most 32-bit processors use encryption mechanism, like AES256. The data transmitted over the network is also encrypted, insuring that it is viewed only by authorized systems that receive the data.

4. Storage

For data storage some of the IoT nodes will use the internal memory available on the microcontroller. Some complex nodes may require additional Flash memory, either mounted on the circuit board or by a memory module inserted into an expansion slot. More sophisticated systems can have additional RAM on the board.

And last, there is The Cloud where the data can be uploaded, stored, and even processed then fed back to the IoT system.

II. Techonologies Used:

Various existing technologies are responsible to collect the data and the data flow between other devices in the network. Some of technologies used are discussed below:

Radio Frequency Identification (RFID)

In RFID system tags, or labels is attached to the objects to be identified. Two-way radio transmitter-receivers are used to send a signal to the tag and read its response. The readers generally transmit their observations to a computer system running RFID software or RFID middleware. [3].

There are two broad categories of RFID systems—passive and active RFID.

Passive RFID:

In Passive RFID systems tags there is **no internal power source,** an electromagnetic energy transmitted from RFID reader **powers the RFID tags**. Applications of Passive RFID tags include access control, supply chain management, file tracking, race timing, smart labels, and more. Passive RFID systems are economical and hence widely used in many industries.

Active RFID:

Active RFID systems tags uses **battery-power and** broadcast their own signal. Active RFID tags are used for real-time location tracking of objects. Compare to the passive tags Active tags are much more expensive and also read signals from a longer range.

Sensor

It is used to collect data from the environment and process the data to detect changes in the physical status of the things.

Wireless Sensor Networks (WSN)

A wireless sensor network (WSN) is a collection of distributed sensors that monitor physical or environmental conditions, such as temperature, sound, and pressure. Data from each sensor passes through the network node-to-node. [3]

Gateways & Routers

Technologies that enable legacy devices and other systems to connect to the IoT. They integrate technologies and protocols for networking.

IPV4 vs IPV6

Every object connected to the internet need an IP address to communicate. Every objects that are connected in the IoT are assigned an IP address to communicate without human intervention. IPv4's 32-bit address space of four billion is not even enough to give each person on earth a unique identifier. IPv6 has come just in time, providing (2^{128}) possible 128-bit addresses. This makes the address needs of the Internet of Things to be possible.

It helps IP-networked devices to communicate by providing secure and specific addresses to each of these devices. IPv6 eradicates the address depletion problem and future networks are based on IPv6.

III. Applications :

The IoT technology can be found in many industries today, including agriculture, healthcare, building management and transportation.

1. SMART AGRICULTURE:

In Agricultural industry the Internet of Things promises to transform farming and food production in the future.

Water supply management

In Agricultural industry the IoT, is used for water supply management used in crop irrigation. Because excess water or shortage of water will affect the crop productivity, so this technology smartly analyzes crop water requirements and uses water supply resources available to reduce waste.[9]

Precision agriculture

The dynamic real time data related to agriculture process like temperature, rainfall, soil quality and weather forecast data, when communicated to farmed beforehand will help the farmers to produce higher productivity and reduce the losses.[9]

Livestock management

The livestock health is monitored by using sensor equipments, eg., the ear tags fixed in the cattle will detect the respiratory diseases in the cattle.[9]

2. SMART HEALTHCARE:

Real Time Location Services

Real time location services are used to track the devices like medical apparatus by tagging it with sensors and can be located easily with IoT and also help in environmental monitoring. [6]

Remote Monitoring

The death of many people can be prevented when they get timely and prompt medical attention. When there is any change in the vital functions of a person, devices fitted with sensors analyze and notify the concerned healthcare providers. [6]

3. SMART HOMES

There are many fire accidents that occur at home due to the negligence of humans. Most importantly stoves in the kitchen should be handled with due care. IoT plays a significant role where the gas and smoke sensors can be used to switch off the stove when excess smoke or gas is released, preventing fire accidents in the kitchen thereby saving human lives. Similarly all the equipments like fan, lights, air conditioners, refrigerator etc., can be controlled remotely by using smart phones that uses IoT technology.

3. SMART BUILDINGS

The IoT sensors embedded in the building collects many of data like space utilization, energy usage, in a building by monitoring these factors and make necessary changes to save energy and space and also temperature monitoring is done through sensors embedded in window glasses.

The fig 1, shows its extensibility and implementation of IoT in various sectors.

Fig ure 1. IoT implementation in various Sectors

IV. Challenges :

As the IoT involves embedded technology there exists several vulnerability in both hardware and software that includes

- Sensors
- Networking protocols
- Application Softwares
- Data Storage
- Data Transmission
- Physical theft and tampering

SECURITY:

As the number of smart nodes increases, amount of upstream data generated by the nodes also increases those results in an exponential growth in data that will raise new concerns about data privacy, data sovereignty and security.

Security features can be embedded in the hardware and also software should provide encryption, identity protection and access control.

SCOPE:

The scope of IoT is extended to a wide range that is going to occupy in all industrial sectors, and is capable of building smart homes, smart buildings, smart cities, smart agriculture, healthcare, transportation, industries and so on. Further research can be focused on using this smart technology economically and also utilize its complete potential.

V. Conclusion

The current decade is dominated by a new wave of network called Internet of Things. All physical objects can be connected through internet and can be monitored and controlled without human intervention. This paper discusses various technologies used in IoT that includes RFID's, sensors, processors etc. Various application areas of IoT like Smart agriculture, Smart healthcare and Smart buildings are also discussed. Finally some of the challenges and security issues are considered. The IoT is going to be the next technological trend that is to occupy every place and every sector including business, education, research and so on.

VI. References

1. Anupama Kaushik, "*IOT-An Overview*", International Journal of Advanced Research in Computer and *Communication Engineering Vol. 5, Issue 3, March 2016.*

2. Dolly Das, Bobby Sharma, "*General Survey on Security Issues on Internet of Things*", *International Journal of Computer Applications (0975 – 8887) Volume 139 – No.2, April 201.*

3. Yogita Pundir, Nancy Sharma, Yaduvir Singh, "*Internet of Things (IoT) : Challenges and Future Directions*", *International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 3, March 2016.*

4. https://www.iotone.com/vendor/iwave-systems-technologies/v1268.

5. http://www.mouser.in/applications/internet-of-things/

6. https://www.cabotsolutions.com/2016/02/applications-iot-healthcare-industry/

7. https://www.cbinsights.com/research/surprising-iot-applications/

8. https://www.ipv6.com/applications/using-rfid-ipv6/

9. https://www.ibm.com/blogs/internet-of-things/iot-agricultural-application