# Understanding Internet of Things and Its Application to Deal with Medical Emergency

Shiv Kumar Goel
Deputy HOD, MCA Dept.
VESIT, Chembur, Mumbai

Harsha Varwani
MCA Dept.
VESIT, Chembur, Mumbai

Abhishek Jain
MCA Dept.
VESIT, Chembur, Mumbai

## ABSTRACT
Internet of Things (IoT) simply means connecting objects or things over the Internet. The paper discusses about the components of IoT, Application areas of IoT, and challenges related to it. It also discusses a novel approach to deal with medical emergencies.

## General Terms
Internet of Things, IoT, Healthcare, Smart Devices

## Keywords
Internet of Things, IoT, Medical Emergency, Smart Devices

## 1. DEFINITION
The Internet of Things (IoT) is a network of physical objects or "things" embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure.

The Internet of Things (IoT) refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems.

"A world where physical objects are seamlessly integrated into the information network, and where physical objects can become active participants in business processes. Services are available to interact with these 'smart objects' over the Internet, query, and change their state and any information associated with them."

There are many more definitions available. But what comes out clear from all these definitions are the following things that make up IoT- viz., An object or thing, Sensors, Network(LAN/WAN), Service Provider (Software/Cloud/Embedded Systems), End devices. Each of which is explained in detail in the coming paragraphs.

## 2. COMPONENTS OF IOT

### 2.1 Sensors
See figure 1. In the far left are Sensors that detect or measure a physical property and convert it into some kind of electronic representation. Sensors may be Passive or Active – with the difference being the amount of intelligence embedded in the sensor. A simple thermistor (a resistor whose resistance is greatly reduced by heating it) would be concerned passive because it simply varies its resistance and some other system must analyze the thermistor and interpret the temperature. If the thermistor were to be combined with a Microcontroller (MCU), the MCU could perform the translation from resistance to temperate and communicate the value over a serial protocol. In this configuration the sensor would be Active.

### 2.2 Device
A device is the "thing" when talking about IoT. Sensors terminate into devices. This means that the device provides the intelligence needed to work meaningfully with the data provided by the attached Sensors. This data from the sensor is translated, transformed and possibly combined with other data; this processing transforms the data from simple bits and bytes to useful information.

### 2.3 LAN/WLAN/PAN
From the Device to the cloud, network-type protocols are used to connect the pieces together. There are a number of protocols that can be chosen and that satisfy one's need. For e.g., for distance and speed (at the expense of power consumption), some variant of Wi-Fi (IEEE 802.11 a/b/g/n/ac) is appropriate. If a mesh-type network is needed because of the topology of the network, some variant of IEEE 802.15 (e.g., ZigBee) is the logical choice. It may be said that there is no single protocol that needs to be followed. One is free to follow any protocols or for that matter, a combination of protocols.

### 2.4 Device Gateway
Device Gateway is the aggregation device for an IoT deployment and typically has significant computing and networking capability. In some configurations, the Gateway may also connect directly to Sensors i.e. when the gateway is the device itself. The Gateway can also combine data from multiple devices and routes this data.

### 2.5 Router/Switch/Gateway
Its main purpose is to partition the network into two parts; the secure/trusted network, say Home network and the insecure/un-trusted network, like the Internet.

### 2.6 WAN
The WAN is typically, the Internet. It is a network fabric that allows all sorts of devices to communicate over the public network infrastructure (also known as the World Wide Web)

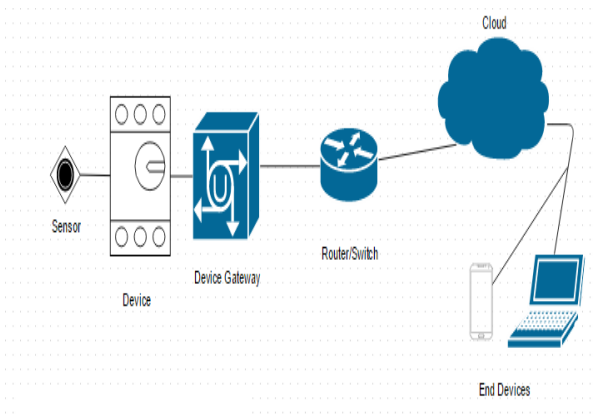


**Fig 1: Components of IoT**

## 2.7 Cloud

It is a term used to describe some processing or computing capacity which is hosted by a third party in case of a public cloud or same organization for private cloud. Processing can be performed by embedded systems or software systems present with cloud providers.

## 2.8 End Devices

End devices may be a smart phone/ desktop i.e. a UI device; or it can be an Electrical Appliance like Air Conditioner that would adjust according to information it receives.

# 3. IoT ARCHITECTURE

IoT architecture comprises of different collection of technologies supporting IoT. It specifies how different technologies, work at different layers to make up Internet of Things. Figure 2 shows layers of IoT architecture with their components and functionalities.


**Fig 2: IoT Architectural Layers**

## 3.1 Sensor Layer

Sensor Layer is the lowest layer, which has objects (things) integrated with sensors. It is used to interact between real and digital worlds to collect and process data. A sensor may be used to measure temperature, air quality, movement, heart rate, luminance, etc. A sensor can measure the physical property and may or may not convert it into signal that can be understood by an instrument. An IoT application must be designed keeping in mind this nature of sensors.

## 3.2 Gateways and Network

The tremendous amount of data that sensors produce is transported via a strong and high performance wired or wireless network infrastructure as a transport medium. A sensor may require connection with a sensor aggregator or device gateway. This can be achieved using LAN or Personal Area Network of say, Bluetooth. If the sensors do not require connectivity to sensor aggregators, they are connected directly to the backend servers/applications using Wide Area Network (WAN) such as GSM, GPRS and LTE.

## 3.3 Management Service Layer

The role of management service layer is to process and analyze data obtained from the previous layer. Analysis is done with the help of rules provided in the rule engine. These rules are predefined based upon the domain of application. These rule engines help in building decision logics and trigger processes to enable communication with the end user using IoT.

## 3.4 Application Layer

Applications and uses of IoT are gaining more light in the recent times due to availability of various open source sensor interfaces that connect to the devices and also because of introduction of IPv6 addresses. A few of the many applications are listed in the following section.

# 4. APPLICATIONS

## 4.1 Business

Traxx EKG is a wireless monitoring system that can help keep refrigeration equipment in good working order. A sensor (called a "mote") attaches to the outside of any freezer and keeps tabs on both temperature and power consumption. Each mote transmits data to a local hub over Wi-Fi or 3G, while a cloud server provides analytics and a dashboard for users to view the data. Freezers become less efficient as they age, drawing more power and providing less reliable temperature control. Traxx EKG's analytics can predict upcoming failures by detecting patterns of increased energy consumption, which is a sure sign that a freezer is in need of repairs. The platform can model the performance of each freezer in a facility to calculate the cost savings of preventative maintenance and allow facility managers to minimize downtime.

## 4.2 Household

Smart Homes: The concept of smart homes is widely gaining popularity with introduction of smart refrigerators that inform users about daily supplies that a user may need or whatever is available for the user in his fridge. Other such appliances that are connected or that use IoT are listed below-

- Heating & Cooling
- Security
- Safety: Fire, Smoke, & Carbon Monoxide Alarms
- Windows & Lighting
- Electrical / Power

## 4.3 City and Roads

CarVi is a windshield-mounted camera that uses machine vision software to improve driving behavior. Pair it with a smartphone in a dash-mounted holder and you've got an instant heads-up-display overlaid on the video feed. Between the camera and your phone's sensors, the CarVi app has everything it needs to provide real-time warnings about possible collisions, proper following distance, unsafe lane changes, and more. CarVi also collects data about your driving habits which you can visualize and study later. It is especially useful if you're trying to break habits like tailgating, hard braking, or jackrabbit starts.

## 4.4 Body and Health

HealthPatch contains a suite of sensors to monitor heart rate, respiration, temperature, steps taken, sleep cycle, stress levels, and whether the user has fallen or otherwise become incapacitated. Stuck to the chest, it's at most a quarter-inch thick and runs about three days on a watch battery. HealthPatch pairs over Bluetooth Low-Energy with a mobile device for WiFi connectivity, so patients and doctors can access real-time data (which is encrypted and compliant with HIPAA regulations on medical data privacy). The information is available through a cloud platform provided by a cardiac monitoring partner company, LifeWatch, based in Switzerland.

# 5. CHALLENGES OF IoT

## 5.1 Scalability

Internet of Things potentially has a larger overall scope than the conventional Internet of computers. But then again, things cooperate mainly within a local environment. Basic functionality such as communication and service discovery therefore need to function equally efficiently in both small scale and large-scale environments.

## 5.2 Interoperability

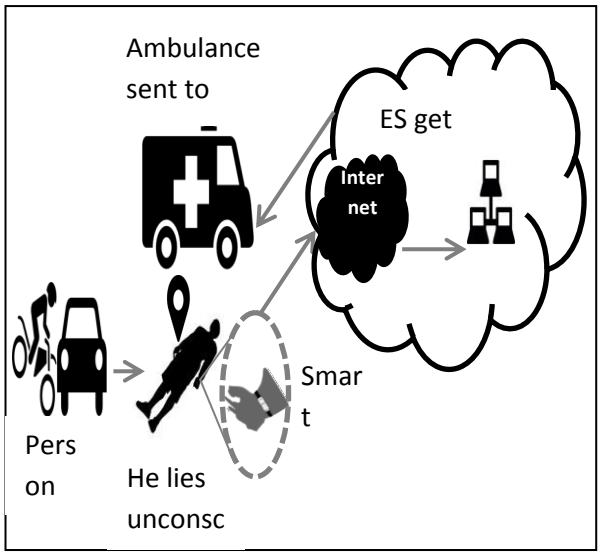


**Fig 4: Using IoT in Medical Emergencies**

Since the world of physical things is extremely diverse, in an Internet of Things each type of smart object is likely to have different information, processing and communication capabilities. Different smart objects would also be subjected to very different conditions such as the energy available and the communications bandwidth required. However, to facilitate communication and cooperation, common practices and standards are required. This is particularly important with regard to object addresses. These should comply with a standardized schema if at all possible, along the lines of the IP standard used in the conventional Internet domain.

## 5.3 Software Complexity

Although the software systems in smart objects will have to function with minimal resources, as in conventional embedded systems, a more extensive software infrastructure will be needed on the network and on background servers in order to manage the smart objects and provide services to support them.

## 5.4 Data Volumes

While some application scenarios will involve brief, infrequent communication, others, such as sensor networks, logistics and large-scale scenarios, will entail huge volumes of data on central network nodes or servers.

## 5.5 Security

Lack of security could enable intruders to access and misuse personal information collected and transmitted to or from the device. For e.g., Smart televisions or other such devices store sensitive financial account information, passwords, and other types of information, unauthorized persons could exploit vulnerabilities to facilitate identity theft or fraud. Unauthorized persons might exploit security vulnerabilities to create risks to physical safety in some cases. One participant described how he was able to hack remotely into two different connected insulin pumps and change their settings so that they no longer delivered medicine. Unauthorized access to Internet-connected cameras or baby monitors also raises potential physical safety concerns.

# 6. A NOVEL APPROACH TO DEAL WITH MEDICAL EMERGENCIES

Suppose a bike rider meets an accident on the road. Now, suppose this is a far-off highway with less frequency of passers-by. A situation like this can be dealt with Traditional approach or using IoT.

## 6.1 Traditional Approach

In this approach, the victim would lie unconscious, bleeding on the street until somebody notices him and calls an ambulance. The passer-by calls ambulance and tells him about the location of the victim and about his health condition to some extent.

Problems with this approach-

- It may be several minutes before somebody notices the victim, wasting precious minutes of his life.
- Ambulance relies on location information given by the caller. This may be misunderstood by the people at emergency call centre, who may send ambulance to some other location. See Figure 3.
- After all this, suppose the victim reaches nearest hospital. The hospital may not be prepared with doctors to handle such a situation.
- The hospital may even be not equipped to deal with victim's condition.

Such problems reduce life expectancy of roadvictims.

## 6.2 IOT Approach

A novel and easy to implement approach can be adopted using the Internet of Things.

Implementation of IoT products is made easy using Processors provided by Intel or Applications with Intel Inside. The IoT solutions provided by Intel are cheap and easy to implement.This approach uses a smart watch like Android Wear or iWatch to send victim's data over the network to the cloud service provider (Here, Emergency Call Center).It works as described below and depicted in figure 4-

Consider the same scenario. A person gets hit and falls unconscious on the road. This time the victim has a smart watch on his wrist as shown in the figure. This smart watch has heart rate sensor, which is used to calculate a person's heart rate. Any significant change in person's heart rate is recorded and an automatic call is made to an emergency call center. Now, this call center has a network of computers that check the most nearby hospital equipped for the victim; and assign an ambulance to the victim. The ambulance is no way dependent on any person to provide location information as it gets the proper location from the GPS attached to victim's smart watch.After the ambulance has reached and picked up victim from the location, the scanning and diagnostic devices present in the ambulance can send real-time information on

victim's condition to the hospital. The paramedics in the ambulance can also perform preliminary tests and send reports to the hospital. See Figure 5. This system not only communicates with the hospital but also with the city's traffic monitoring system. Consider that there is traffic on the way to suggested, nearest hospital. The traffic monitoring system installed in cities inform about this traffic to the ambulance. Not only this, it may suggest a different way to reach the destined place in lesser time. The ambulance driver uses this information to reach hospital (same or other) with very less time wasted. See figure 6.

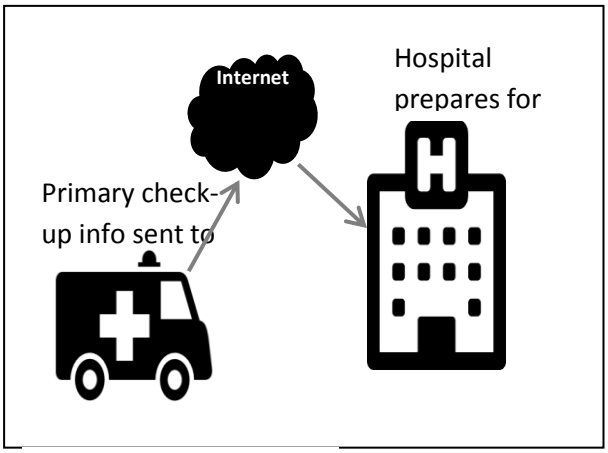


**Fig 5: Victim in transit**

### *6.2.1 Feasibility Study of this approach*

#### *6.2.1.1 Technical and Resource Feasibility*

This approach requires a smart watch; Android Wear and iWatch can be used. These watches have packaged heart-rate monitor, GPS and Internet Connectivity. All that is needed is an application built up on IoT architectural stack that achieves communication between these devices, processes information and sends this over to emergency call centers. Additionally, the ambulances require a GPS system to suggest routes, monitor traffic. It also requires internet connectivity. Availability of these components make this approach really feasible from technical point of view.

#### *6.2.1.2 Economic Feasibility*

This approach is quite feasible economically because the cost of technical components has reduced drastically over the years. Table 1 below shows cost of devices that may be needed.

| | |
|---|---|
| GPS Module | Approximately Rs.700 per module |
| Internet Connectivity for Hospitals and Ambulances | Approximately Rs. 5000 per month |
| Cloud Services | Microsoft Azure Hosting is $0.02 to $1.60 per hour. Storage prices range from $0.07/GB/month to $0.12/GB/month, depending on level of redundancy. |
| Smart Watch | Apple Smart Watch- Rs. 35000, Android Smart Watch- Rs. 15000 to Rs. 30000 |

**Table 1: Cost of Components**

Apart from these costs, another significant cost is that of Application Development. This can be negotiated.

### *6.2.2 Challenges/Shortcomings with this approach*

#### *6.2.2.1 Security*

Data about a person's location and his physical condition may be intercepted. Somebody may misuse a person's location information and may plan threatening activities for that person. Use of proper encryption techniques and SSL Certification may allow overcoming this challenge.

#### *6.2.2.2 Shortcomings in application flow*

Many a times it is possible that even the smart device gets damaged during an accident How will the call be made in that scenario?In this case, the application can push a notification on person's mobile phone. If the person is able to acknowledge the receipt of notification, that would state that the person is fine and the device is damaged due to other reasons. This will avoid making emergency calls. However, if the notification is not acknowledged, a call can be made.Another issue is that if the person is working out/ in gym his/her heart rate tends to increase. The application may put up an emergency call. This needs to be avoided. A simple solution would be to activate this service only when the person needs it like while driving, etc

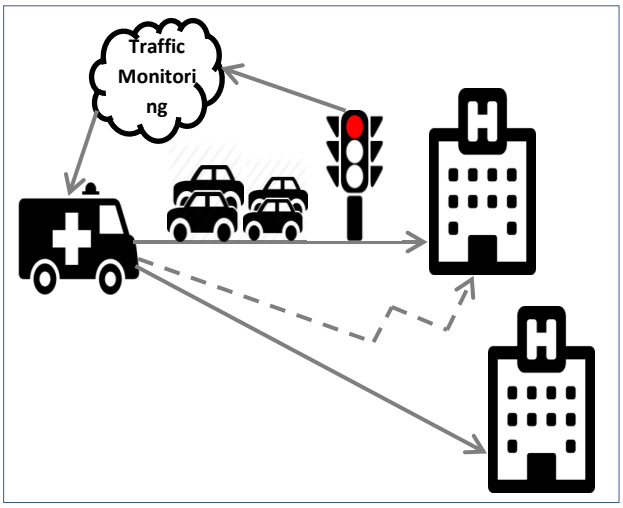


**Fig 6: Routes suggested by Traffic Monitoring System**

## 7. CONCLUSION

To conclude, one can say that use of Internet of Things in emergency situations, like the one mentioned above, can save critical minutes of a person's life and ultimately his life.

However, the application of IoT in the approach suggested above is not limited to the scope discussed here. It can be further enhanced in future to include the following –

A Doctor can remotely observe patients' vital signs with help of some sensing device that can be provided to patients during discharge for specific duration of time. This device can collect data and inform doctor about patients' condition and doctor can suggest future course of medical procedure. This can help hospitals to manage their resources like hospital beds more efficiently and help hospitals to cater to need of patients and also to increase their revenues.

In other case, rural areas face several challenges to establish full fledge hospitals but with the help of IoT and advances in the field of wireless communications, these technologies can be used to capture patient health data with help of sensors and then share it through wireless medium with medical

representatives who can make appropriate health recommendations.

In short, IoT will radically change the aspect of healthcare monitoring and treatment during medical emergency. By providing personalized and optimized services, it provides a timely and economical response to Medical emergency. Moreover, recent developments in sensor, internet, cloud, mobility and big data technologies have led to affordable medical devices and connected health programs, vastly increasing the potential of IoT in case of medical emergency.

## 8. REFERENCES

[1] "From the Internet of Computers to the Internet of Things"- by Friedemann Mattern and Christian Floerkemeier, Distributed Systems Group, Institute for Pervasive Computing, ETH Zurich {mattern,floerkem}@inf.ethz.ch

[2] Report of Workshop "The Internet of Things: Privacy and Security in a Connected World"- by FTC in November-13.

[3] December 18th, 2014 Cloud Architecture Internet of Everything. http://www.slideshare.net/machinepulse/iot-cloud-architecture?related=1

[4] The Internet of Things (IoT)[1] is the network of physicalorthings" embedded with electronics, software, s ensors http://en.wikipedia.org/wiki/Internet_of_Things

[5] The Internet of Things (IoT) refers to the ever-growing network of physical objects that feature an IP address for internet connectivity http://www.webopedia.com/TERM/I/internet_of_things.html

[6] The Internet of Things is upon us. A panel of security experts offers their insight into what they feel is right, http://www.techrepublic.com/article/why-experts-are-nervous-about-the-internet-of-things/

[7] Think of this post as an Internet of Things (IoT) 101 tutorial. We'll look at and define the various components which make up an IoT solution. http://www.bsquare.com/Bblog/Lists/Posts/Post.aspx?ID=48

[8] In the next century, planet earth will don an electronic skin. http://postscapes.com/internet-of-things-examples/