CS-6580 Distributed Systems

# Final Project – *Internet of Things*

**Team Members**

Gayathiri Shriram (**MS5754**)

Madhushri Kanathoor Subrahmanya Bhat (**DM9677**)

# Executive Summary

The Internet of Things is an emerging topic of technical, social, and economic significance. Consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and other everyday objects are being combined with Internet connectivity and powerful data analytic capabilities that promise to transform the way we work and live. Projections for the impact of IoT on the Internet and economy are impressive, with some anticipating as many as 100 billion connected IoT devices and a global economic impact of more than $11 trillion by 2025.

At the same time the Internet of Things raises significant challenges that could stand in the way of realizing its potential benefits. Concerns about hacking of Internet-connected devices, surveillance concerns, and privacy fears have captured every ones attention. Technical challenges remain and new policy, legal and development challenges are emerging. The Internet of Things engages a broad set of ideas that are complex and intertwined from different perspectives.

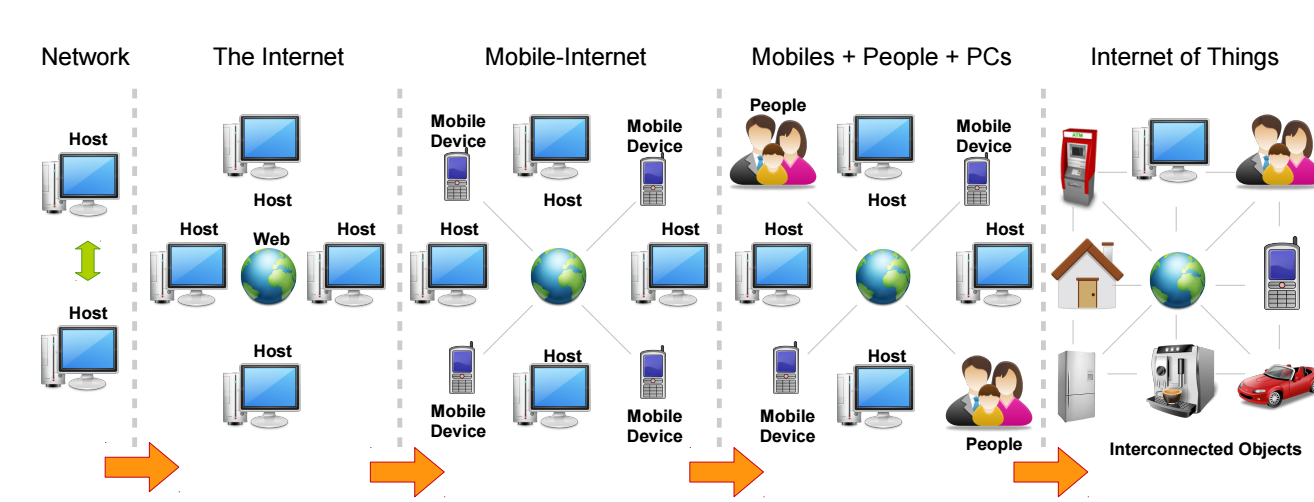
This document is designed to capture below aspects of Internet of Things:

* IoT definitions and the importance of this technology
* Application domains that drive IoT
* General IoT architecture and implementation
* Architecture and scalability implementation issue and possible solutions
* Context-awareness (developing analytical applications) and possible solutions.
* IoT project development idea – Home Automation System

The Internet of Things is all about convergence and integration of the latest advancements in the research areas of software and hardware with industrial technologies invented many decades ago. Research carried out in the context-aware computing domain aims to create a pleasant user experience at the workplace, in public areas as well as in the home environment by simplifying human interactions with everyday services and making them less intrusive.

**Internet of Things** (**IoT**) is the network of physical objects like devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data. The goal is to connect things into a network using various information sensor equipments including RFID (Radio Frequency Identification) equipments and the information system can indentify, locate, track, supervise, and trigger the relative events. IOT is the third tide of world information industry after computer, Internet and mobile telecommunication networks.

The data these devices report can be collected and analyzed in order to reveal insights and suggest actions that will produce cost savings, increase efficiency or improve products and services. The IoT is growing rapidly, with an estimated 25 billion connected objects throughout the world by 2020, and added value from the IoT of US$1.9 trillion by the same year.



**Architecture**

M2M communication is the communications infrastructure of the Internet of Things. It refers to communications technologies, which enable embedded computing devices to share data with each other via wireless or wired connections without the need for human interaction or triggering the communication

**Internet Of Things Key Elements:**

**Sensing:** The first step in IoT workflow is gathering information at a point of activity. This can be information captured by an appliance, a wearable device, a wall mounted control or any number of commonly found devices. The sensing can be biometric, biological, environmental, visual or audible. This forms the lowest layer made up of smart objects integrated with sensors. The sensors enable the interconnection of the physical and digital worlds allowing real-time information to be collected and processed. Smart objects can be embedded with both an RFID tag and a sensor to measure data. The sensor may capture fluctuations in the surrounding temperature, changes in quantity, or other types of information.

##### **Communication:** IoT devices require a means for transmitting the information sensed at the device level to a Cloud-based service for subsequent processing. This is where the value inherent in IoT is created. This requires either Wi-Fi (wireless LAN based communications) or WAN (wide area network… i.e. cellular) communications. Depending on the need short-range communication, other capabilities may also be needed. These could include Bluetooth, ZigBee, near field or a range of other short-range communication methods. For positioning, GPS is often required as well. Current networks, often tied with very different protocols, have been used to support machine-to-machine (M2M) networks and their applications.

**Cloud Based capture and Consolidation:** Gathered data is transmitted to a cloud based service where the information coming in from the IoT device is aggregated with other cloud based data to provide useful information for the end user. The data being consolidated can be information from other Internet sources as well as from others subscribing with similar IoT devices. There will be some data processing required to provide useful information that is not necessarily obvious in the raw data.

**Delivery of Information**: The last step is delivery of useful information to the end user. That may be a consumer, a commercial or an industrial user. It may also be another device in the M2M workflow. The goal in a consumer use case is to provide the information in as simple and transparent a method as possible across multiple device platforms – tablets, smart phones, desktop – across multiple operating systems – iOS, Android, Windows, etc.

Context Awareness Overview:

Context can be defined as any information that can be used to characterize the situation of an entity. An entity is a person, place, piece of software, software service or object that is considered relevant to the interaction between a user and an application, including the user and applications.

Context-awareness can be defined as the ability of a system to provide relevant information or services to users using context information where relevance depends on the user’s task

## Context Awareness and Developing Analytical Applications

Developing analytical applications for the IoT is a complex process that needs diverse knowledge of domains, sensors, algorithms, programming, and deployment infrastructure.

In the diverse IoT world, we can no longer afford to build vertical applications from scratch—a platform-based development approach promoting software re-use via APIs and services is a must. Going further, one of the fundamental game-changers for successful IoT adoption will be the democratization of knowledge derived from IoT data. To make this happen, we need a crowd sourced application development and consumption ecosystem.

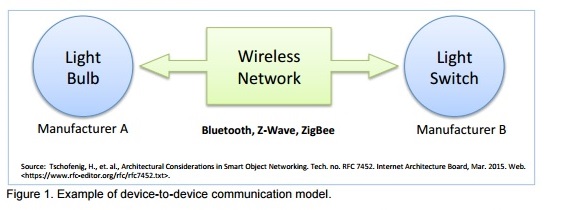
Tutorial Q/A which readers usually like to know step-by-step (3-4 pages)

**Internet of Things Communications Models**

The four basic communication models demonstrate the underlying design strategies used to allow IoT devices to communicate.

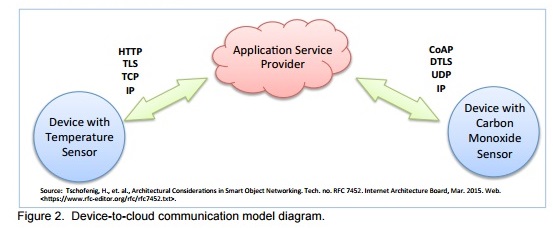
March 2015, the Internet Architecture Board (IAB) released a guiding architectural document for networking of smart objects, which outlines a framework of four common communication models used by IoT devices.

**Device-to-Device Communications**



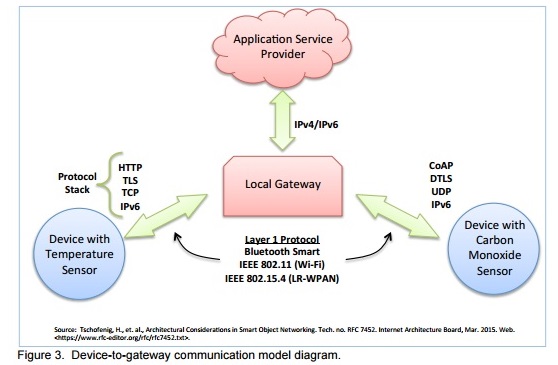
This represents two or more devices that directly connect and communicate between one another, rather than through an intermediary application server using many types of networks. Devices use protocols like Bluetooth, 40 Z-Wave,41 or ZigBee42 to establish direct device-to-device communications. This model is commonly used in applications like home automation systems, which typically use small data packets of information to communicate between devices with relatively low data rate requirements.

**Device-to-Cloud Communications**



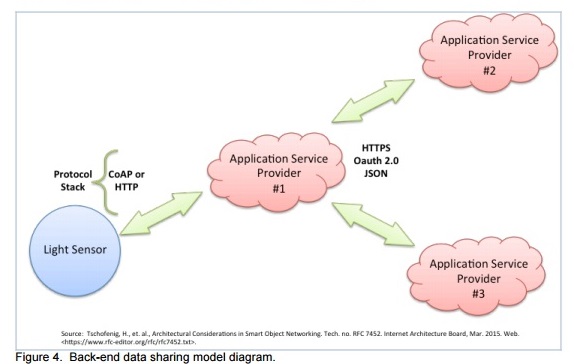
The IoT device connects directly to an Internet cloud service like an application service provider to exchange data and control message traffic. This uses traditional wired Ethernet or Wi-Fi connections to establish a connection between the device and network, which ultimately connects to the cloud service. Some popular consumer IoT devices like the Nest Labs Learning Thermostat44 and the Samsung Smart TV employ this communication model

**Device-to-Gateway Model**



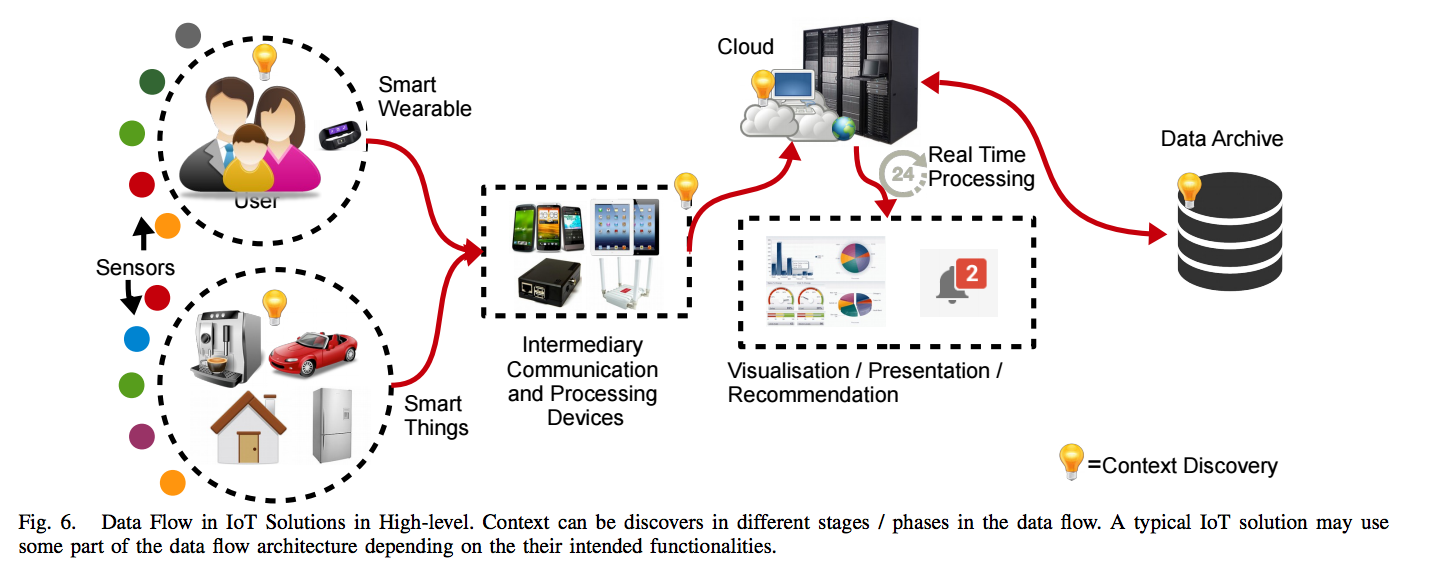
There is application software operating on a local gateway device, which acts as an intermediary between the device and the cloud service and provides security and other functionality such as data or protocol translation. In many cases, the local gateway device is a Smartphone running an app to communicate with a device and relay data to a cloud service. This is often the model employed with popular consumer items like personal fitness trackers. These devices do not have the native ability to connect directly to a cloud service, so they frequently rely on Smartphone app software to serve as an intermediary gateway to connect the fitness device to the cloud.

**Back-End Data-Sharing Model**



The back-end data-sharing model refers to a communication architecture that enables users to export and analyze smart object data from a cloud service in combination with data from other sources.

**Strategies Used By IoT Products to offer Context Aware Functionality:**



The Figure visualizes how data is being collected transferred, processed; context discovered and annotated in typical IoT solutions. It is important to note that not all solutions may use the exact same data flow. Each solution may use part of the architecture in their solution.

**Context Aware Tagging Section**

Context-aware tagging, which is also called context augmentation and annotation represent the idea of sensing the environment and collecting primary context information. We also believe that secondary context generation is also a part of context-aware tagging feature. Primary context is any information retrieved without using existing context and without performing any kind of sensor data fusion operations.

**Context Selection and Presentation Section:**

There are number of commonly used strategies, by most of the IoT solutions in the marketplace, to present context to the users. Most of the IoT products use some kind of visualization techniques to present context information the users. We call this visual presentation.

Study experiences: including what is most significant or difficult (1-2 pages)

Internet of Things is the next big thing. The Internet of Things revolves around increased machine-to-machine communication; it’s built on cloud computing and networks of data-gathering sensors; it’s mobile, virtual, and instantaneous connection; and it is said that it is going to make everything in our lives easy. However IoT has its own issues. Through our research we have listed few issues that IoT is currently facing and we have shared possible solutions.

**Architecture and Scalability implementation issue and possible solutions**

The Internet of Things domain will include an extremely wide range of technologies. Therefore, single reference architecture cannot be used as a blueprint for all possible concrete implementations. Even though reference model can be identified, there can be several reference architectures will co-exist in the Internet of Things.

Architecture in this context is defined as a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as data formats used in its operation.

For example, the RFID Tag based identification architecture may be different from a sensor-based architecture, which is more comparable to the current Internet. There will also be several types of communications models.

It is not clear that a single addressing model will be applicable to the entire IoT, nor necessarily a single addressing format. The wide range of resources and computing capabilities available to IoT devices may require many optimized address formats, which need to be unified by a common ID-to-Address translation service

**1.Privacy and Security**

One of the main concerns that the IOT has to address is privacy. Concerns over privacy and data protection as sensors and smart tags can track user movements, habits and ongoing preferences. Invisible and constant data exchange will take place unknown to the owners and originators of such data. IOT implementations would need to decide who controls the data and for how long.

**IoT may increase your attack surface**. Any device added to network is another potential entry-point for a hacker. A hacker could potentially compromise / seize control of one of the devices and could attempt to use it to access systems.

**Devices cannot always be stored in secure facilities.**  IoT device to monitor something outside the secure buildings. There should be a way to protect device from physical.

**IoT devices are autonomous – nobody is present to enter credentials.**IoT devices might be asked to execute commands on demand. Since they are designed to be autonomous and not require user interaction, the devices need to decide whether a

**Not many standards exist in IoT.**As an emerging technology, many devices and their packaged software use their own ports and protocols. How do you deal with all of these different approaches in your IoT implementation in a secure manner?

**Possible Solutions:**

**Use a pessimistic security strategy**. All devices and service accounts need to be configured to have the minimum amount of permissions possible to perform their tasks.

**Monitoring, logging, and operating system-level security.**Any actions that the device takes should be logged. Device up time, downtime, and overall health should be monitored. Device operating systems should be configured for secure boot, which will require all software to be signed and validated when starting up to ensure authenticity. Any software that cannot be validated should not be allowed to run, which will prevent malicious programs from running.

**Treating devices like external users.**All devices should be required to connect to your network just like any external user – with an authentication method that can prove that the device is who / what it claims that it is.

**Using accepted standards where possible, and add device-level security.** IoT devices need to have their own security layer to identify and reject suspicious or abnormal requests. Server-to-server firewalls will be required.

**Centralized architecture.** Centralized/decentralized architecture needs to be carefully evaluated and secured through standardized measures. Decentralized architectures are very often preferable from the security perspective due to denial of service attacks. Governance of centralized vs. decentralized architectures needs standardized ways for secure configuration and design of networks, as well as secure operational functioning.

**2. Network Management**

There is legitimate heterogeneity in the used networking technology and applications. This variation is necessary and useful, as for instance different applications and environments benefit from varying networking technology. The range and other characteristics of cellular, wireless local area networking, and RFID are very different from each other, for instance.

**3. Fair access to the infrastructure**

Access to the infrastructure will be important in order to develop and roll out new and innovative applications and services. It is important from a public policy point of view to ensure that IoT applications will benefit from a fair access to this infrastructure. The predictability of the development / deployment of such applications and the transparency in the service offering are key for the IoT success.

**4. Interoperability Challenge**

In order to ensure a minimum level of interoperability, it is necessary to define the interoperability requirements both from a communication and from a data perspective at one or more of these levels based on internationally agreed protocols. IOT domain is the emergence of a variety of solutions targeted at specific application domains. These application developments have limited interoperability between systems and technologies, and they do not adopt a common standardization and understanding of the IOT domain.

An example is in Greenfield applications such as home healthcare system developed for a single application and with only one scenario in mind. Future of IOT, system interfaces should be standardized, and solutions made interoperable at various levels (e.g., communication and service levels) and across various platforms in order to promote integration and scalability.

**5. Costs versus Usability**

IOT uses technology to connect physical objects to the Internet. For IOT adoption to grow, the cost of components that are needed to support capabilities such as sensing, tracking and control mechanisms need to be relatively inexpensive.

**6.Regulatory, Legal, and Rights Issues**

Data collected by IoT devices may not be constrained from being sent across jurisdictional boundaries. These devices use the Internet to communicate and the Internet spans jurisdictional boundaries at all levels. IoT devices can collect data about people in one jurisdiction and transmit that data to another jurisdiction for data storage or processing, often with few or no technical roadblocks. This can quickly become a legal problem.

**7. Scalability**

**Align network and device longevity.** When deploying an IoT system, consider the potential longevity of the network technology and compare it to the devices’ expected life spans. It is important to make sure to incorporate long-term support for devices based on technology projections.

**Create a system for easy expansion.** System should be able to easily expand as more devices are added.

**Demand device durability.** Make sure the devices on the network can operate for many years and durable. With maintenance making up about 15 to 25 per cent of annual enterprise IT costs, investing in quality upfront will result in the lowest operational cost for the device as well as the network in the long term.

**Context Awareness and Developing Analytical Applications**

In the diverse IoT world, we can no longer afford to build vertical applications from scratch—a platform-based development approach promoting software re-use via APIs and services is a must. Going further, one of the fundamental game-changers for successful IoT adoption will be the democratization of knowledge derived from IoT data. To make this happen, we need a crowd sourced application development and consumption ecosystem. Developing analytical applications for the IoT is a complex process that needs diverse knowledge of domains, sensors, algorithms, programming, and deployment infrastructure.

**Possible Solutions:**

A viable way to address such complexity is through a **model-driven development (MDD) framework**. MDD is an approach that aims to model knowledge across different stakeholders (such as sensor providers, algorithm providers, domain experts, and infrastructure providers) by allowing separation of concerns for each stakeholder. It can assist an IoT application developer in easily creating an application based on data and goal descriptions. Domain-agnostic semantic data interoperation will also play a big role in such a framework.

The return on investment for major IoT deployments isn’t sufficiently motivating at this stage for most businesses. This is a primary reason why IoT applications have rarely moved beyond pilot deployments. There are deployment and cost issues when it comes to installing multitudes of sensing hardware across physical spaces. To make it more cost effective, enterprises are looking into **crowdsourcing sensing data** from mobile phones where appropriate. Mobile phones are already pervasive, and they come with rich sensors such as cameras, microphones, accelerometers, gyroscopes, magnetometers, GPS, and altimeters. Participatory and opportunistic sensing using mobile phones will play a key role in IoT deployment. A plethora of applications are possible using mobile phone sensors, prominent among them being road condition monitoring, driving behavior analysis, traffic monitoring, wellness/health monitoring, and so on. In the future, robots and unmanned aerial vehicles carrying sensors will also contribute to this pervasive, affordable sensing paradigm.

Using the intelligence of a vast interconnected organism, however, is nothing new: the venerable Oxford English Dictionary may in fact be the earliest example of crowdsourcing. From avoiding traffic jams, to analyzing pedestrian flow patterns, to finding the best public toilet in town, crowdsourcing apps are showing that many smartphones make for light work.

When information is gathered from or needs to be delivered to a remote entity, choices need to be made on where context will be stored. The following concerns are taken into account whether context information should be stored locally or remotely:

**Scope of relevance:** Certain information can be relevant only for computational artifacts that interact in particular with local services.

**Information sensitivity:** Tracking information retrieved from RFID tags could be of interest to multiple parties on the network and be made available on a remote server for further analysis.

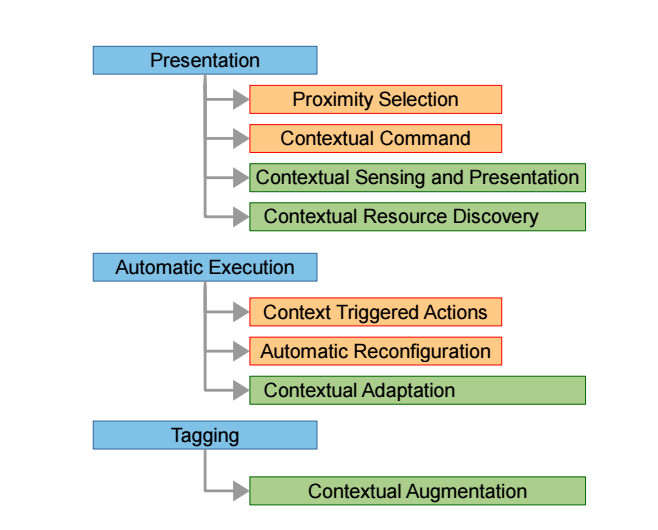
**Information correctness and period of relevance:** Static and profiled information is likely to remain valid for longer periods.

**Caching for information reachability:** If some sensor information can be obtained quite easily, then storing the information may not be worthwhile.

**Exploiting information history:** In some cases, an appliance might want to exploit the historic values of a certain context attribute in order to derive new information.

Detailed analysis, and evaluations including FURTHER development (3-4 pages)

**Elaboration of Context Awareness from IoT Perspective:**



**Presentation:** Context can be used to decide what information and services need to be presented to the user.

**Execution:** Automatic execution of services is also a critical feature in the IoT paradigm. Let us consider a smart home environment. When a user starts driving home from their office, the IoT application employed in the house should switch on the air condition system and switch on the coffee machine to be ready to use by the time the user steps into their house. These actions need to be taken automatically based on the context. Machine-to machine communication is a significant part of the IoT.

**Tagging:** In the IoT paradigm, there will be a large number of sensors attached to everyday objects. These objects will produce large volumes of sensor data that has to be collected, analyzed, fused and interpreted. Sensor data produced by a single sensor will not provide the necessary information that can be used to fully understand the situation. Therefore, sensor data collected through multiple sensors needs to be fused together. In order to accomplish the sensor data fusion task, context needs to be collected. Context needs to be tagged together with the sensor data to be processed and understood later. Context annotation plays a significant role in context aware computing research. The tagging operation also identified as annotation.

## Context Awareness Sensors:

**RFID:**

RFID is an emerging technology for embedding sensing capabilities in everyday objects and is gaining momentum as a popular means for automatic identification and tracking in supply chain management.

**IR Tags:**

IR tag readers and IR active tags that identify indoor locations and that recognize the user’s circumstances, such as sitting in a meeting room, sitting in the driver’s seat of a car, etc., microphone sensors that recognize the user’s voice, and GPS receivers that provide outdoor location information.

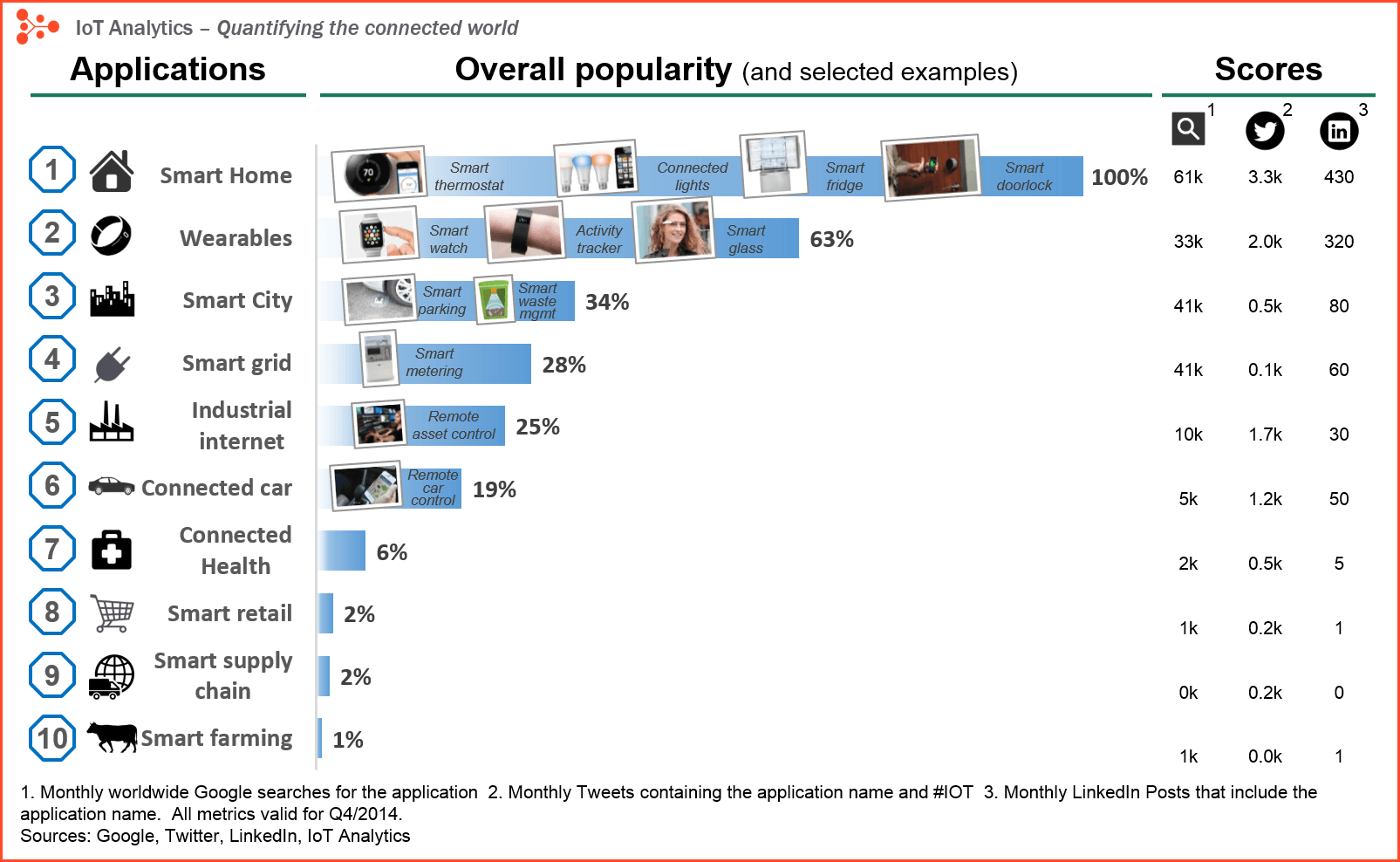
**Internet Connected Sensors:**

The Industrial Internet of Things (IIoT) is using contextual awareness to open new frontiers for improving processes. Industries such as chemical production are installing Internet-connected sensors to bring greater granularity to monitoring.

**Position Sensors:**

Position sensors in IoT applications provide access to location.  A rotary-position sensor, for example, translates an angular mechanical position to an electrical signal and is used in applications where it is necessary to control a variable output such as frequency and speed

## The Internet of Things applications Progress



### Smart home

Smart Home ranking as highest Internet of Things application on all measured channels. The IoT Analytics company database for Smart Home includes 256 companies and startups. More companies are active in smart home than any other application in the field of IoT. The total amount of funding for Smart Home startups currently exceeds $2.5bn. This list includes prominent startup names such as Nest or Alert Me as well as a number of multinational corporations like Philips, Haier, or Belkin.

### Wearable's

There are plenty of wearable innovations like the Apple’s smart watch, Sony Smart B Trainer, the Myo gesture control, or LookSee bracelet. Of all the IoT startups, wearable’s maker Jawbone is probably the one with the biggest funding to date. It stands at more than half a billion dollars.

### Smart City

Smart city spans a wide variety of use cases, from traffic management to water distribution, to waste management, urban security and environmental monitoring. Its popularity is fueled by the fact that many Smart City solutions promise to alleviate real pains of people living in cities these days. IoT solutions in the area of Smart City solve traffic congestion problems, reduce noise and pollution and help make cities safer.

### Smart grids

Smart grids are a special one. A future smart grid promises to use information about the behaviors of electricity suppliers and consumers in an automated fashion to improve the efficiency, reliability, and economics of electricity.

### Industrial Internet

The industrial Internet is also one of the special Internet of Things applications. While many market researches such as Gartner or Cisco see the industrial Internet as the IoT concept with the highest overall potential, its popularity currently doesn’t reach the masses like smart home or wearable’s do.

## Project Summary:

**Home Automation System:**

Homes of the 21st century will become more and more self-controlled and automated due to the comfort it provides, especially when employed in a private home. A home automation system is a means that allow users to control electric appliances of varying kind. Many existing, well-established home automation systems are based on wired communication. This does not pose a problem until the system is planned well in advance and installed during the physical construction of the building. But for already existing buildings the implementation cost goes very high.



As everyday devices increasingly find their way online, we have seen a plethora of 'things' around the home becoming smarter - mainly owing to a new-found ability to connect to the internet - or a number of things you'd not usually find in the home making their way there owing to advances in technology making them cheaper and more accessible.

There are many applications available that provide this facility. We are proposing an application that can be built at a very low cost. We can build a simple raspberry pi home automation system that will allow you to control appliances in your home from anywhere in the world. And it will also allow you to view data from the PIR motion sensor via the Internet to detect intruders. This project will be using platforms like the Raspberry Pi, IBM’s IoTF (Internet of Things Foundation) and Blue mix packages.

**Hardware:**

1. Raspberry Pi 2 / B+.
2. USB wifi dongle.
3. USB keyboard and mouse.
4. HDMI monitor and cable.
5. Micro USB power adapter (smartphone charger).
6. PIR motion sensor.
7. Male-female and male-male jumpers.
8. Breadboard.
9. BC547 transistor.
10. 5V SPDT relay and 1n4001 diode.
11. LED and 220Ohm resistor.

**Software:**

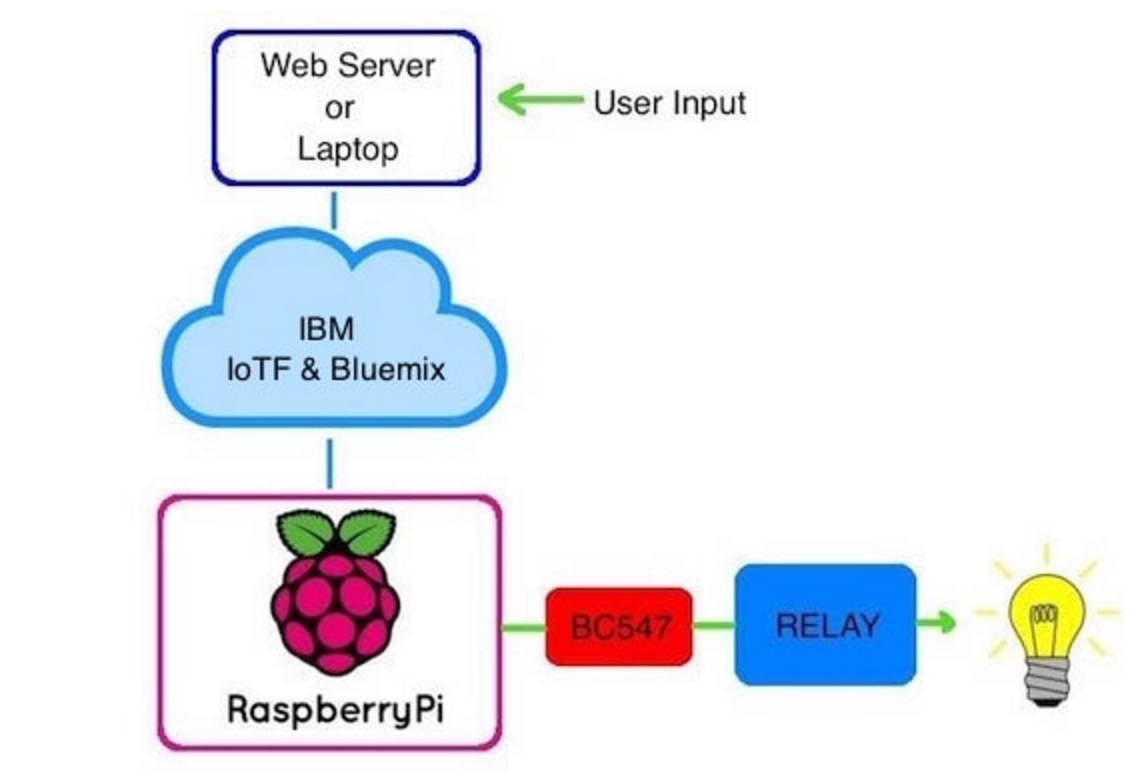
Raspbian OS

The Raspberry Pi home automation system uses client and server side python scripts. These can communicate with each other through IBM’s IoTF platform.

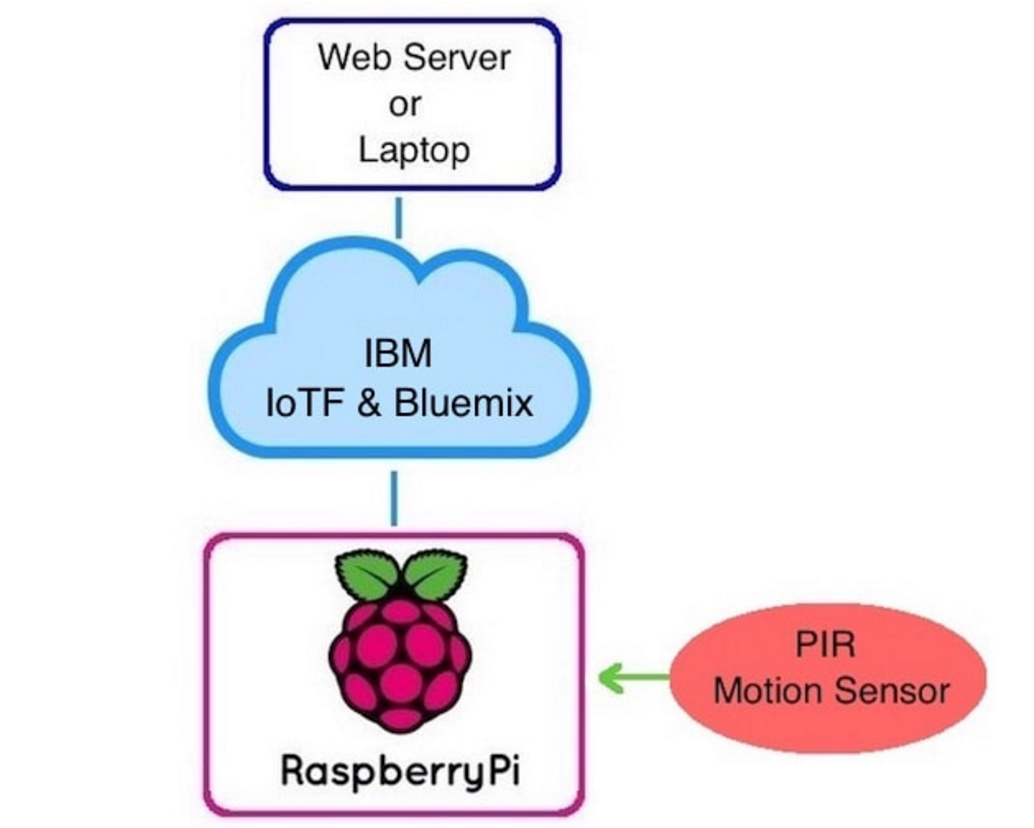
This whole Internet of Things project can be divided into two parts:

**1. Sending commands to the Raspberry Pi**

The server side script running on our laptop or on a web server takes input commands from the user and correspondingly sends it to the client (Raspberry Pi). Here, we will be using commands to turn a light ON/OFF. When we pass the command to turn ON a light through the server side script, the information is relayed to the Raspberry Pi and it’s GPIO pin turns ON a relay. The system also sends status updates to the server on whether the light is ON/OFF.



**2. Receiving data from the Raspberry Pi**  
In case of sending data from the PIR motion sensor connected to the Raspberry Pi, we run a script, which reads the sensor through a GPIO pin and broadcasts the data through the IoTF platform. This can then be viewed through the IoTF console or through a custom web application designed using the platform.



## Team Work Details:

Team Member: Gayathiri Shriram

Worked on context awareness, developing analytical applications and possible solutions. Also worked on the project summary.

We as a team found the research about Internet Of Things very interesting and challenging. We gained an insight on current developments and the impacts these developments are about to make to our daily life. Looking forward to the full-fledged sales of IoT products in the market.

On Personal front we learnt about time management and effective ways of representing the data.