IOT

(Internet of Things)

L.Aswin
B.Sc., Computer Science
Madura College
Madurai, India
arronissac@gmail.com
www.aswin.esy.es

G.L.Nirmal
B.Sc., Computer Science
Madura College
Madurai, India
nirmalgl16@gmail.com
www.nirmalgl.blogspot.com

Abstract—

IoT (Internet of Things) is the network of physical objects-devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity-that enables these objects to collect and exchange data. The internet of things allows objects to be sensed and controlled remotely across existing network infrastructure

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -- or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network.

I. *INTRODUCTION*

Internet of Things (IoT) is an ecosystem of connected physical objects that are accessible through the internet. The 'thing' in IoT could be a person with a heart monitor or an automobile with built-in-sensors, i.e. objects that have been assigned an IP address and have the ability to collect and transfer data over a network without manual assistance or intervention. The embedded technology in the objects helps them to interact with internal states or the external environment, which in turn affects the decisions taken.

I. WHY IOT?

An article by Ashton published in the RFID Journal in 1999 said, "If we had computers that knew everything there was to know about things - using data they gathered without any help from us - we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory." This is precisely what IoT platforms does for us. It enables devices/objects to observe, identify and understand a situation or the surroundings without being dependent on human help.

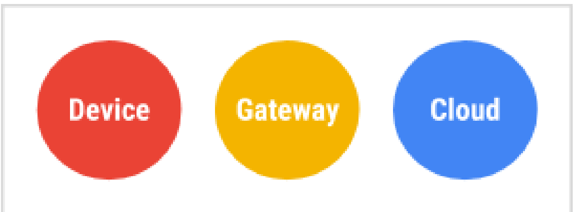
II. SCOPE OF IOT

Internet of Things can connect devices embedded in various systems to the internet. When devices/objects can represent themselves digitally, they can be controlled from anywhere.

The connectivity then helps us capture more data from more places, ensuring more ways of increasing efficiency and improving safety and IoT security.
IoT is transformational forces that can help companies improve performance through IoT analytics and **IoT Security** to deliver better results. Businesses in the utilities, oil & gas, insurance, manufacturing, transportation, infrastructure and retail sectors can reap the benefits of IoT by making more informed decisions, aided by the torrent of interactional and transactional data at their disposal.

III. COMPONENTS

Here we divide the system into three basic components, the device, gateway, and cloud:



- A ***device*** includes hardware and software that directly interacts with the world. Devices connect to a network to communicate with each other, or to centralized applications. Devices might be directly or indirectly connected to the Internet.
- A **gateway** enables devices that are not directly connected to the Internet to reach cloud services. Although the term *gateway* has a specific function in networking, it is also used to describe a class of device that processes data on behalf of a group or cluster of devices.
- The data from each device is sent to ***Cloud*** Platform, where it is processed and combined with data from other devices, and potentially with other business-transactional data.

A. Device

It's not always clear what constitutes a device. Many physical things are modular, which means it can be hard to decide whether the whole machine is the device, or each module is a discrete device. There's no single, right answer to this question. As you design your IoT project, you'll need to think about the various levels of abstraction in your design and make decisions about how to represent the physical things and their relationships to each other. The specific requirements of your application will help you understand whether something that generates information should be treated as a device, and therefore deserves its own ID, or is simply a channel or state detail of another device.

IoT hardware platforms use a number of common interfaces. Sensor and actuator modules can support one or more of these interfaces:

- **USB**. Universal Serial Bus is in common use for a wide array of plug-and-play capable devices.
- **GPIO**. General-purpose input/output pins are connected directly to the processor. As their name implies, these pins are provided by the manufacturer to enable custom usage scenarios that the manufacturer didn't design for. GPIO pins can be designed to carry digital or analog signals, and digital pins have only two states: HIGH or LOW.
- Digital GPIO can support Pulse Width Modulation (PWM). PWM lets you very quickly switch a power source on and off, with each "on" phase being a pulse of a particular duration, or *width*. The effect in the device can be a lower or higher power level. For example, you can use PWM to change the brightness of an LED; the wider the "on" pulses, the brighter the LED glows.
- Analog pins might have access to an on-board analog-to-digital conversion (ADC) circuit. An ADC periodically samples a continuous, analog waveform, such as an analog audio signal, giving each sample a digital value between zero and one, relative to the system voltage.
- When you read the value of a digital I/O pin in code, the value can must be either HIGH or LOW, where an analog input pin at any given moment could be any value in a range. The range depends on the resolution of the ADC. For example an 8-bit ADC can produce digital values from 0 to 255, while a 10-bit ADC can yield a wider range of values, from 0 to 1024. More values means higher resolution and thus a more faithful digital representation of any given analog signal.
- The ADC *sampling rate* determines the frequency range that an ADC can reproduce. A higher sampling

rate results in a higher maximum frequency in the digital data. For example, an audio signal sampled at 44,100 Hz produces a digital audio file with a frequency response up to 22.5 kHz, ignoring typical filtering and other processing. The *bit precision* dictates the resolution of the amplitude of the signal.

- **I2C**. Inter-Integrated Circuit serial bus uses a protocol that enables multiple modules to be assigned a discrete address on the bus. I2C is sometimes pronounced "I two C", "I-I-C", or "I squared C".
- **SPI**. Serial Peripheral Interface Bus devices employ a master-slave architecture, with a single master and full-duplex communication. SPI specifies four logic signals:
  - SCLK: Serial Clock, which is output from the master
  - MOSI: Master Output Slave Input, which is output from the master
  - MISO: Master Input Slave Output, which is output from a slave
  - SS: Slave Select, which is an active-low signal output from master
- **UART**. Universal Asynchronous Receiver/Transmitter devices translate data between serial and parallel forms at the point where the data is acted on by the processor. UART is required when serial data must be laid out in memory in a parallel fashion.

B. Devices

A *gateway* manages traffic between networks that use different protocols. A gateway is responsible for protocol translation and other interoperability tasks. An IoT gateway device is sometimes employed to provide the connection and translation between devices and the cloud. Because some devices don't contain the network stack required for Internet connectivity, a gateway device acts as a proxy, receiving data from devices and packaging it for transmission over TCP/IP.

A gateway device might be used even when the participating devices are capable of communicating without one. In this scenario, the gateway adds value because it provides processing of the data across multiple devices before it is sent to the cloud. In that case, the direct inputs would be other devices, not individual sensors. The following tasks would likely be relegated to a gateway device:

- Condensing data to maximize the amount that can be sent to the cloud over a single link
- Storing data in a local database, and then forwarding it on when the connection to cloud is intermittent
- Providing a real-time clock, with a battery backup, used to provide a consistent timestamp for devices that can't manage timestamps well or keep them well synchronized
- Performing IPV6 to IPV4 translation
- Ingesting and uploading other flat-file-based data from the local network that is relevant and associated with the IoT data
- Acting as a local cache for firmware updates

C. Cloud

The state of a device generally can be modeled as a set of key:value pairs. Device applications can manage this state locally.
Some device state might be directly connected to the hardware. For example, when you check the state of a digital GPIO pin, it reads as HIGH or LOW, based on the physical reading of the voltage on the pin.
Other device state might exist at the application layer. For example, recording-audio might have a state condition of true or false, related to whether the application is sampling from the mic or writing to disk. At the hardware level, the mic itself might be left on.
From the software perspective, the application code running on the device maintains the source of truth. It is often valuable, even required, for other software, such as a mobile app or website, to read or modify that device's last known state. Given that IoT devices can spend some time in low-power sleep mode and might exist on particularly unreliable networks, it's often useful to mirror some of a device's state with the cloud. That way, state data can be made available even when the devices themselves are temporarily offline.
Firebase is one technology well suited for maintaining a local copy of the state. It lets you expose the mirrored view of the current device state through Firebase look-up keys. Firebase client libraries make it easier to give different observers and actors a consistent view of device state.

IV. CONCLUSION

In conclusion, the Internet of Things is closer to being implemented than the average person would think. Most of the necessary technological advances needed for it have already been made, and some manufacturers and agencies have already begun implementing a small-scale version of it. The main reasons why it has not truly been implemented is the impact it will have on the legal, ethical, security and social fields. Workers could potentially abuse it, hackers could potentially access it, corporations may not want to share their data, and individual people may not like the complete absence of privacy. For these reasons, the Internet of Things may very well be pushed back longer than it truly needs to be.

L.Aswin
B.Sc., Computer Science
Madura College
Madurai, India
arronissac@gmail.com
www.aswin.esy.es

G.L.Nirmal
B.Sc., Computer Science
Madura College
Madurai, India
nirmalgl16@gmail.com
www.nirmalgl.blogspot.com