

|  |
| --- |
| Internet of Things (IoT) |
| * History of IoT * How IoT works * Benefits of IoT * IoT security and privacy issues * Solutions of IoT Security Issues * Internet of Things Real Life Example * How to build custom IoT hardware with Arduino * Real-Time Applications of Arduino Uno Board |
| Microprocessors and its Applications    Submitted to : Ms. Samia Masood  Authored by : Summiya Zulfiqar Enrolment No : EP-1851048 |

# Internet of Things (IoT)

|  |
| --- |
| **The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (**[**UIDs**](https://internetofthingsagenda.techtarget.com/definition/unique-identifier-UID)**) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.**  **A**[**thing**](https://internetofthingsagenda.techtarget.com/definition/thing-in-the-Internet-of-Things)**in the internet of things can be a person with a heart monitor implant, a farm animal with a**[**biochip transponder**](https://internetofthingsagenda.techtarget.com/definition/injectable-ID-chip-biochip-transponder)**, an automobile that has built-in**[**sensors**](https://whatis.techtarget.com/definition/sensor)**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 is able to transfer data over a network.**  **Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, better understand customers to deliver enhanced customer service, improve decision-making and increase the value of the business.** |

### History of IoT

Kevin Ashton, co-founder of the Auto-ID Center at MIT, first mentioned the internet of things in a presentation he made to Procter & Gamble (P&G) in 1999. Wanting to bring radio frequency ID (RFID) to the attention of P&G's senior management, Ashton called his presentation "Internet of Things" to incorporate the cool new trend of 1999: the internet. MIT professor Neil Gershenfeld's book, When Things Start to Think, also appearing in 1999, didn't use the exact term but provided a clear vision of where IoT was headed.

IoT has evolved from the convergence of wireless technologies, microelectromechanical systems ([MEMS](https://internetofthingsagenda.techtarget.com/definition/micro-electromechanical-systems-MEMS)), [micro services](https://searchmicroservices.techtarget.com/definition/microservices) and the internet. The convergence has helped tear down the silos between operational technologies (OT) and information technology (IT), enabling unstructured machine-generated data to be analyzed for insights to drive improvements.

Although Ashton's was the first mention of the internet of things, the idea of connected devices has been around since the 1970s, under the monikers *embedded internet* and [pervasive computing](https://internetofthingsagenda.techtarget.com/definition/pervasive-computing-ubiquitous-computing).

The first internet appliance, for example, was a Coke machine at Carnegie Mellon University in the early 1980s. Using the web, programmers could check the status of the machine and determine whether there would be a cold drink awaiting them, should they decide to make the trip to the machine.

IoT evolved from machine-to-machine ([M2M](https://internetofthingsagenda.techtarget.com/definition/machine-to-machine-M2M)) communication, i.e., machines connecting to each other via a network without human interaction. M2M refers to connecting a device to the cloud, managing it and collecting data.

Taking M2M to the next level, IoT is a sensor network of billions of smart devices that connect people, systems and other applications to collect and share data. As its foundation, M2M offers the connectivity that enables IoT.

The internet of things is also a natural extension of [SCADA](https://whatis.techtarget.com/definition/SCADA-supervisory-control-and-data-acquisition) (supervisory control and data acquisition), a category of software application program for process control, the gathering of data in real time from remote locations to control equipment and conditions. SCADA systems include hardware and software components. The hardware gathers and feeds data into a computer that has SCADA software installed, where it is then processed and presented it in a timely manner. The evolution of SCADA is such that late-generation SCADA systems developed into first-generation IoT systems.

The concept of the IoT ecosystem, however, didn't really come into its own until the middle of 2010 when, in part, the government of China said it would make IoT a strategic priority in its five-year plan.

### How IoT works

An IoT ecosystem, also sometimes referred to as the Internet of Everything (IoE), consists of web-enabled mart devices that use embedded processors, sensors and communication hardware to collect, send and act on data they acquire from their environments. [IoT devices](https://internetofthingsagenda.techtarget.com/definition/IoT-device) share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices -- for instance, to set them up, give them instructions or access the data.

The connectivity, networking and communication protocols used with these web-enabled devices largely depend on the specific IoT applications deployed.

### Use Cases of IoT solutions

* Driverless cars

As mentioned earlier in this article, driverless cars seem to be the next best invention by car companies like Tesla, Volvo, Google and BMW. Although the cars are in the prototype stage and under continuous development, they are the most futuristic looking models.

These cars don’t have drivers but technology like sensors, cloud architecture, maps, gyroscopes and internet with massive data about traffic, roads, potholes, turns and speed breakers that are processed at a fast speed. All these sensors and tools are a part of IoT platform. This allows the car to drive through easily without any assistance from humans. However, we still are waiting on roads that are ready for driverless cars.

* Smart homes

A smart home is the best example of IoT use case. Imagine coming home to the right temperature, lighting and music after work and being able to do that all that with just one device. IoT application lets you control how your house functions at one tap from your smartphones.

It will let you record your favorite shows from anywhere or turn on and off any device such as microwave, coffee machine, etc. from your IoT mobile apps. Smart homes also have high security for the reason that monitoring each corner of the house becomes easy with IoT apps.

* Wearables

These are devices that have been in use a lot and most likely everyone owns at least one. Fitness tracking bands like Fit bit, Nike, Mio, Misfits, etc. and smart watches from Apple or watches that run on Android devices are some of the Wearables.

Wearables are devices that are connected to the internet to provide accurate data as per your needs. These devices also use sensors to detect and record data and gives you the right information after analysis and that is how IoT works in every case.

People have been able to track their health with these wearable devices. The IoT applications in healthcare is a huge advantage for people. Heart rate, food habits, medicine reminders, calories burnt count, etc. are some of the things at the back of which Wearables are becoming one of the most [emerging trends of Healthcare industry](https://appinventiv.com/blog/future-mhealth-goes-beyond-apps-wearables-enticing-healthcare-industry).

* Amazon Go

Amazon has come up with a fantastic solution for shopping in the future, *Amazon* *Go*. The purpose behind this IoT solution for retail shopping is to make shopping a much simpler process.

How IoT works in this is you just walk into an Amazon store and use your Amazon account QR code to enter. After that just pick anything and everything you need and just simply walk out. The IoT working model that connects each item at the store with the mobile app will automatically add up the billing amount as you walk out of the store. Isn’t it amazing?

* Smart Hotel rooms

This is new and many people may not be aware of this but big hotels like Hilton are trying to use IoT platforms to enhance the staying experience for the travelers. Hilton wants to replace the card-based keys with IoT mobile apps to unlock the room. This will not only ensure traveler’s safety but also make checking in and checking out much simpler.

The hotel rooms will have lights and temperature all controlled by the same IoT mobile app. You can set the perfect lighting at any time of the day or choose the right temperature as per your needs. This makes vacationing a whole new experience.

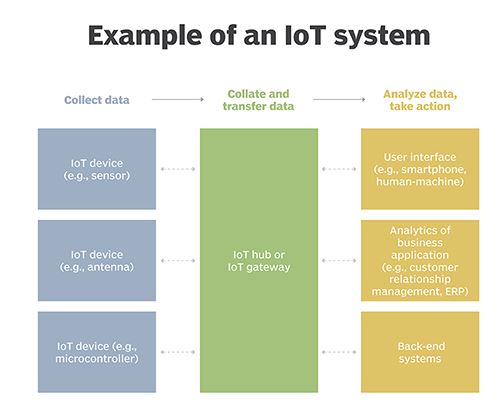
These were the most famous IoT use case, some of which are already in use and some are soon to be used. The IoT application developers are full of excitement seeing the rise in this technology. Needless to say how much this will affect the future lifestyle of humans.

The [IoT technology is going to become a massive trend](https://appinventiv.com/blog/8-statistics-prove-iot-will-become-massive-2018) in the coming years. Even the statistics show it, see for yourself here and know [how our lives are transforming with Applications of Internet of Things](https://appinventiv.com/blog/applications-internet-of-things-solutions-iot).

### Components of IoT platforms

The working of IoT depends on four fundamental components on which it functions. Let’s look at them one at a time:

1. Sensors/Devices  
     
   a sensor picks up all the minute details from an environment. The environment can have many complexities. What makes IoT security so great is these sensors that pick up even the most sensitive changes. These sensors are built in the devices which collects all the data to be used later. For instance, our phone is a device with built in sensors like GPS, camera, etc.
2. Connectivity  
     
   Once the data is collected it is transferred to the cloud infrastructure (also known as IoT platforms). But to transfer the data, the devices will need a medium. That’s when connections like Bluetooth, Wi-Fi, WAN, cellular networks, etc. come into play. These mediums are all different and must be chosen wisely for best results.  
     
   The effectiveness IoT security highly depends on the speed and availability of these mediums.
3. Data processing  
     
   after reaching the cloud infrastructure the data has to be analyzed so that the right action can be taken. The analysis can be as simple as checking the temperature of the AC or a complex one such as a situation where an intruder comes in and the device has to identify it through cameras. The IoT application is made such that it can process all the data at a fast rate to take immediate actions.
4. User interface  
     
   the last step is when the user is notified about the action with the help of a notification or an alert sound sent to the IoT apps. This way the user will know that his command has been run through the systems.   
     
   However, this isn’t as easy as it seems. It all depends on how the IoT has been developed. It becomes crucial for [IoT app development companies](https://appinventiv.com/blog/leading-iot-app-development-company-best-choice-great-iot-apps) to develop a system that can also be manually adjusted. In a situation where the temperature of the fridge is not cold enough to freeze ice cubes, users should be able to do that manually without the system backfiring.



### Benefits of IoT

The internet of things offers a number of benefits to organizations, enabling them to:

* Monitor their overall business processes.
* Improve the customer experience.
* Enhance employee productivity.
* Integrate and adapt business models.
* Make better business decisions and Generate more revenue.
* Communication. IoT encourages the communication between devices, also famously known as Machine-to-Machine (M2M) communication.
* Automation and Control.
* Information.
* Automation of daily tasks leads to better monitoring of devices.
* Efficient and Saves Time and money.

IoT encourages companies to rethink the ways they approach their businesses, industries and markets and gives them the tools to improve their business strategies.

### IoT security and privacy issues

The internet of things connects billions of devices to the internet and involves the use of billions of data points, all of which need to be secured. Due to its expanded attack surface, [IoT security](https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security) and [IoT privacy](https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-privacy-IoT-privacy) are cited as major concerns.

One of the most notorious recent IoT attacks was Mirai, a botnet that infiltrated domain name server provider Dyn and took down many websites for an extended period of time in one of the biggest distributed denial-of-service (DDoS) attacks ever seen. Attackers gained access to the network by exploiting poorly secured IoT devices.

Because IoT devices are closely connected, all a hacker has to do is exploit one vulnerability to manipulate all the data, rendering it unusable. And manufacturers that don't update their devices regularly -- or at all -- leave them vulnerable to cybercriminals.

Additionally, connected devices often ask users to input their personal information, including names, ages, addresses, phone numbers and even social media accounts -- information that's invaluable to hackers.

However, hackers aren't the only threat to the internet of things; privacy is another major concern for IoT users. For instance, companies that make and distribute consumer IoT devices could use those devices to obtain and sell users' personal data.

Beyond leaking personal data, IoT poses a risk to critical infrastructure, including electricity, transportation and financial services.

### Solutions of IoT Security Issues

1. **Secure the IoT Network**

Protect and secure the network connecting IoT devices to the back-end systems on the internet by implementing traditional endpoint security features such as antivirus, anti-malware, firewalls, and intrusion prevention and detection systems.

1. **Authenticate the IoT Devices**

Allow the users to authenticate the IoT devices by introducing multiple user management features for a single IoT device and implementing robust authentication mechanisms such as two-factor authentication, digital certificates, and biometrics.

1. **Use IoT Data Encryption**

To protect the privacy of users and prevent IoT data breaches, encrypt the data at rest and in-transit between IoT devices and back-end systems by using standard cryptographic algorithms and fully-encrypted key lifecycle management processes to boost the overall security of user data and privacy.

1. **Use IoT PKI Security Methods**

To ensure a secure connection between an IoT device & app, use IoT public key infrastructure security methods such as X.509 digital certiﬁcate, cryptographic key, and life-cycle capabilities including public/private key generation, distribution, management, and revocation.

1. **Use IoT Security Analytics**

Use IoT Security Analytics Solutions that are capable to detect IoT-specific attacks and intrusions, which can’t be identified by traditional network security solutions like ﬁrewalls.

1. **Use IoT API Security Methods**

Use IoT API Security methods not only to protect the integrity of the data movement between IoT devices, back-end systems, and applications using documented REST-based APIs, but also to ensure that only authorized devices, developers, and apps are communicating with APIs or detecting potential threats and attacks against speciﬁc APIs.

1. **Test the IoT Hardware**

Place a robust testing framework in place to ensure the security of IoT hardware.  This includes stringent testing of the IoT device’s range, capacity, and latency. The chip manufacturers of the IoT devices also need to reinforce the processors for more security and less power consumption without making them too expensive for the buyers or too impractical to be used in the current IoT devices given the fact that a majority of the IoT devices available today are cheap and disposable with a very limited battery power. Also, the IoT device manufacturers need to do a broad testing of all the third-party components and modules that they are using in their IoT devices to ensure their proper functioning with their IoT applications.

1. **Develop Secured IoT Apps**

Given the immaturity of the current IoT technology, the developers of the IoT applications must emphasize on the security aspect of their IoT applications by strictly implementing all the above-mentioned IoT security technologies. Before developing any IoT applications, the developers must also do a complete research on the security of their IoT applications and try their best to strike a perfect balance between the User Interface and Security of their IoT apps.

1. **Avoid Launching IoT Devices in a Rush**

To stay ahead in the competition, the manufacturers of the IoT devices are often in a rush to launch their products in the market at the lowest prices. And, while doing that, they don’t pay enough attention to provide security updates and patches. This poses a serious threat to the security of their IoT devices in the long run. To overcome this challenge, the manufacturers of the IoT devices should avoid launching their products without proper planning for the long-term support for the security of their IoT devices and applications.

1. **Beware of Latest IoT Security Threats & Breaches**

To ensure the security of the IoT devices and applications, the device makers and app developers must beware of the latest IoT security threats and breaches. Since the IoT is still an emerging technology, its security breaches are bound to happen. Hence, both IoT device manufacturers and the IoT app developers must be ready for the security breaches with a proper exit plan to secure maximum data in case of a security attack or data breach.  Last but not least, both IoT device makers and IoT app developers must also take an initiative to teach their employees and users about latest IoT threats, breaches, and security solutions.

### Internet of Things Real Life Example: Google Glass and Smart Farming

In distinguishing the best cases among the examples of Internet of Things, the key criterion is their successful application in real life. And here, the achievements of Google Glass and smart farming technologies deserve special attention.

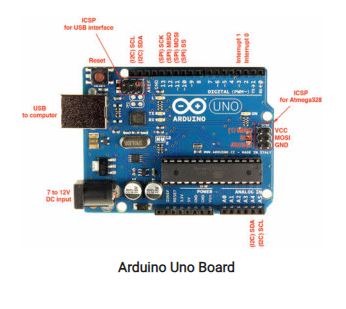


**Google Glass** is one of the most popular technologies that entered and changed the world. Being a headset with an optical-head display, it transformed the very understanding of the functionality limits of eyeglasses. In particular, Google Glass makes it possible to use voice for searching on the Internet, choosing pictures, and interacting with the digital world in different ways. Just like with a smartphone — but without the necessity to involve your hands. And the opportunities to use the innovation in real life are tremendous. For example, you can see your flight information right at the moment of entering the airport. Or scan the barcode to see the full information about the product. Or get directions to the best coffee shop in a new city — and behave like a local.

In its turn, **smart farming** is the innovation changing the way plants are nurtured and grown right now. Among the tools that facilitate and improve the main processes in agriculture, drones, cloud platforms, various monitoring solutions, and enhanced analytics assist contemporary farmers significantly. Instead of relying on the old-fashioned predictions and various sources for data collection, smart farming means an ability to track climate change, weather condition, soil composition, and a crop’s state and growth progress instantly. As a special dimension within the innovation, the solutions for greenhouse automation enable full control and comprehensive care over the plants. In terms of proper lighting and irrigation especially. Finally, cattle monitoring and management capabilities include checking the health condition and the location of the animals.

# How to build custom IoT hardware with Arduino

Arduino is a single-board microcontroller meant to make the application more accessible which are interactive objects and its surroundings. The hardware features with an open-source hardware board designed around an 8-bit Atmel [AVR microcontroller](https://www.elprocus.com/types-of-avr-microcontroller-atmega32-and-atmega8/)or a 32-bit Atmel ARM. Current models consists a USB interface, 6 analog input pins and 14 digital I/O pins that allows the user to attach various extension boards.



The Arduino Uno board is a [microcontroller based](http://www.edgefx.in/microcontroller-based-projects-on-car-security-systems-using-gsm/) on the ATmega328. It has 14 digital input/output pins in which 6 can be used as PWM outputs, a 16 MHz ceramic resonator, an ICSP header, a USB connection, 6 analog inputs, a power jack and a reset button. This contains all the required support needed for microcontroller. In order to get started, they are simply connected to a computer with a USB cable or with an AC-to-DC adapter or battery. Arduino Uno Board varies from all other boards and they will not use the FTDI USB-to-serial driver chip in them. It is featured by the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter.

## **Features of the Arduino Uno Board:**

* It is an easy USB interface. This allows interface with USB as this is like a serial device.
* The chip on the board plugs straight into your USB port and supports on your computer as a virtual serial port. The benefit of this setup is that serial communication is an extremely easy protocol which is time-tested and USB makes connection with modern computers and makes it comfortable.
* It is [easy-to-find the microcontroller](https://www.elprocus.com/microcontrollers-types-and-applications/) brain which is the ATmega328 chip. It has more number of hardware features like timers, external and internal interrupts, PWM pins and multiple sleep modes.
* It is an open source design and there is an advantage of being open source is that it has a large community of people using and troubleshooting it. This makes it easy to help in debugging projects.
* It is a 16 MHz clock which is fast enough for most applications and does not speeds up the microcontroller.
* It is very convenient to manage power inside it and it had a feature of built-in voltage regulation. This can also be powered directly off a USB port without any external power. You can connect an external power source of up to 12v and this regulates it to both 5v and 3.3v.
* 13 digital pins and 6 analog pins. This sort of pins allows you to connect hardware to your Arduino Uno board externally. These pins are used as a key for extending the computing capability of the Arduino Uno into the real world. Simply plug your electronic devices and [sensors](https://www.watelectrical.com/6-different-types-of-temperature-sensors-with-their-specifications/) into the sockets that correspond to each of these pins and you are good to go.
* This has an ICSP connector for bypassing the USB port and interfacing the Arduino directly as a serial device. This port is necessary to re-boatload your chip if it corrupts and can no longer used to your computer.
* It has a 32 KB of flash memory for storing your code.
* An on-board LED is attached to digital pin 13 to make fast the debugging of code and to make the debug process easy.
* Finally, it has a button to reset the program on the chip.

Arduino was created in the year 2005 by two Italian engineers David Cuartielles and Massimo Banzi with the goal of keeping in mind about students to make them learn how to program the Arduino Uno microcontroller and improve their skills about electronics and use it in the real world.

Arduino Uno microcontroller can sense the environment by receiving input from a variety of sensors and can affect its surroundings by controlling lights, motors, and other actuators. The microcontroller is programmed using the Arduino programming language (based on Wiring) and the Arduino development environment (based on Processing).

### Programming:

* The Arduino integrated development environment (IDE) is a cross-platform application written in Java, and is derived from the IDE for the Processing programming language and the Wiring projects
* The Arduino Uno board can be programmed with the Arduino software.
* Select “Arduino Uno from the Tools > Board menu (according to the microcontroller on your board).
* The ATmega328 on the Arduino Uno comes pre-burned with a boot loader that allows you to upload new code to it without the use of an external hardware programmer. It communicates using the original STK500 protocol.
* You can also bypass the [boot loader and program the microcontroller](http://www.edgefx.in/know-about-boot-loader-technique-for-programming-microcontroller/) through the ICSP (In-Circuit Serial Programming) header.
* The ATmega16U2 (or 8U2 in the rev1 and rev2 boards) firmware source code is available.

### The ATmega16U2/8U2 is loaded with a DFU boot loader, which can be activated by:

* On Rev1 boards: connecting the solder jumper on the back of the board (near the map of Italy) and then resetting the 8U2.
* On Rev2 or later boards: there is a resistor that pulling the 8U2/16U2 HWB line to ground, making it easier to put into DFU mode.

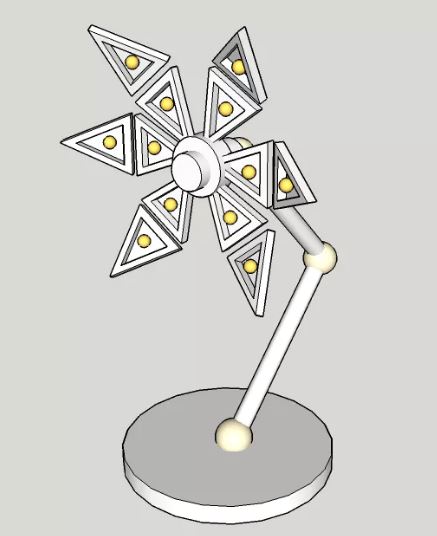
You can then use Atmel’s FLIP software (Windows) or the DFU programmer (Mac OS X and Linux) to load a new firmware. Or you can use the ISP header with an external programmer (overwriting the DFU boot loader).



Microcontroller                                ATmega328  
Operating Voltage                          5V  
Input Voltage (recommended)      7-12V  
Input Voltage (limits)                     6-20V  
Digital I/O Pins                               14 (of which 6 provide PWM output)  
Analog Input Pins                           6  
DC Current per I/O Pin                  40 Ma  
DC Current for 3.3V Pin                50 Ma  
Flash Memory                            32 KB (ATmega328) of which 0.5 KB used by boot loader  
SRAM                                              2 KB (ATmega328)  
EEPROM                                         1 KB (ATmega328)  
Clock Speed                                  16 MHz

# Real-Time Applications of Arduino Uno Board: Corolla Desk Light

**Corolla is a lamp that can be adjusted to focus its light on a reading/working spot or to spread light around for ambient lighting.**



LEDs are widely used these days to provide light in public places, workspaces or at home. Still, there are not many LED lamps which allow for users to adjust the light temperature (or color) or how/where this light is projected.

This project consists of a custom made lamp in the shape of a flower with six petals connected to a central hub. Each petal have two articulated parts and each half host a RGB LED.

Petals can change their angle relative to central hub and the tips of the petals can further change angle made with the root of the petal, this allowing the light produced by LEDs to be focused on an area or spread around.

The main roles of the Arduino 101 board are to control the motors or servos for petals position, to generate the PWM signals to control RGB LEDs and communicate with the user through Bluetooth with the help of a mobile app or another Bluetooth device.

With the help of the mobile app, user can control petals position, light color and intensity, create and store patterns for petals positions and LEDs working modes.

Commands can be given directly to lamp without a mobile app, with switches and potentiometers or by tapping the lamp base which hold Arduino board. These taps are detected with the help of Arduino's onboard accelerometer.

Being an Arduino powered device will have the possibility to be connected to a number of sensors like temperature sensor, PIR, RTC, humidity, etc. and display their status in a visual way or react to parameters given by these sensors.  