IoT

The **Internet of things** (**IoT**) is the network of devices, vehicles, and home appliances that contain electronics, software, actuators, and connectivity which allows these things to connect, interact and exchange data.

It involves giving internet connectivity to a variety of things other than smartphones, laptops and desktops. Using this connectivity they can be controlled remotely and gives rise to a variety of functionalities.

Used to make everyday products ‘SMART’ - smart fridge

**Languages used -** C,Java, PYTHON - most used as python is best for embedded programming

**Uses -** Smart Home, Wearables, Connected cars, Industrial Internet - Sensors in industries, Smart cities - smart surveillance, automated transportation, smart energy management systems

**Implementation:**

Earlier used Electronic Product Code

Modern uses IP address and URI - Uniform Resource Identifier

**Wireless -**

**Short Range** - Bluetooth mesh networking, Light-Fidelity (Li-Fi), Near-field communication (NFC), QR and Barcodes, Radio-Frequency Identification (RFID), Transport Layer Security, WiFi, Zigbee(Low power consumption, low cost but low data rate)

**Medium Range** - LTE-Advanced

**Long Range** - Low-power wide-area networking (LPWAN), Very small aperture terminal (VSAT)

**Wired -**

**Ethernet -** uses twisted pair and fiber optics with hubs and switches

**Power-line communication (PLC) -** uses electrical wiring to carry power and data

**Government Regulations -**

* **Data security** – At the time of designing IoT companies should ensure that data collection, storage and processing would be secure at all times. Companies should adopt a "defence in depth" approach and encrypt data at each stage.
* **Data consent** – users should have a choice as to what data they share with IoT companies and the users must be informed if their data gets exposed.
* **Data minimization** – IoT companies should collect only the data they need and retain the collected information only for a limited time.

**Criticisms -**

**Platform Fragmentation -** multiple products are incompatible with each other. It leads to separate apps/remotes for each of the many products. - Too many Remotes/Apps

**Privacy, Autonomy and Control -** Possibility for hacking, etc

**Data Storage -** The sensors produce an immense amount of data that needs to be stored somewhere and also analysed. A solution is Wireless Sensor Network

**Security and Safety -** As most IoT are controlled by apps, if the apps are buggy, they might cause dangerous scenarios like ‘Unlock door when nobody is at home’.

**Arduino -**

Arduino is an open-source electronics platform based on easy-to-use hardware and software. Arduino boards are able to read inputs - light on a sensor, a finger on a button, or a Twitter message - and turn it into an output - activating a motor, turning on an LED, publishing something online. You can tell your board what to do by sending a set of instructions to the microcontroller on the board. To do so you use the Arduino programming language (based on Wiring), and the Arduino Software (IDE), based on Processing.

Arduino gets a input - Touch, IR sensor, etc and gives according output - LED glows, Beeper beeps, etc