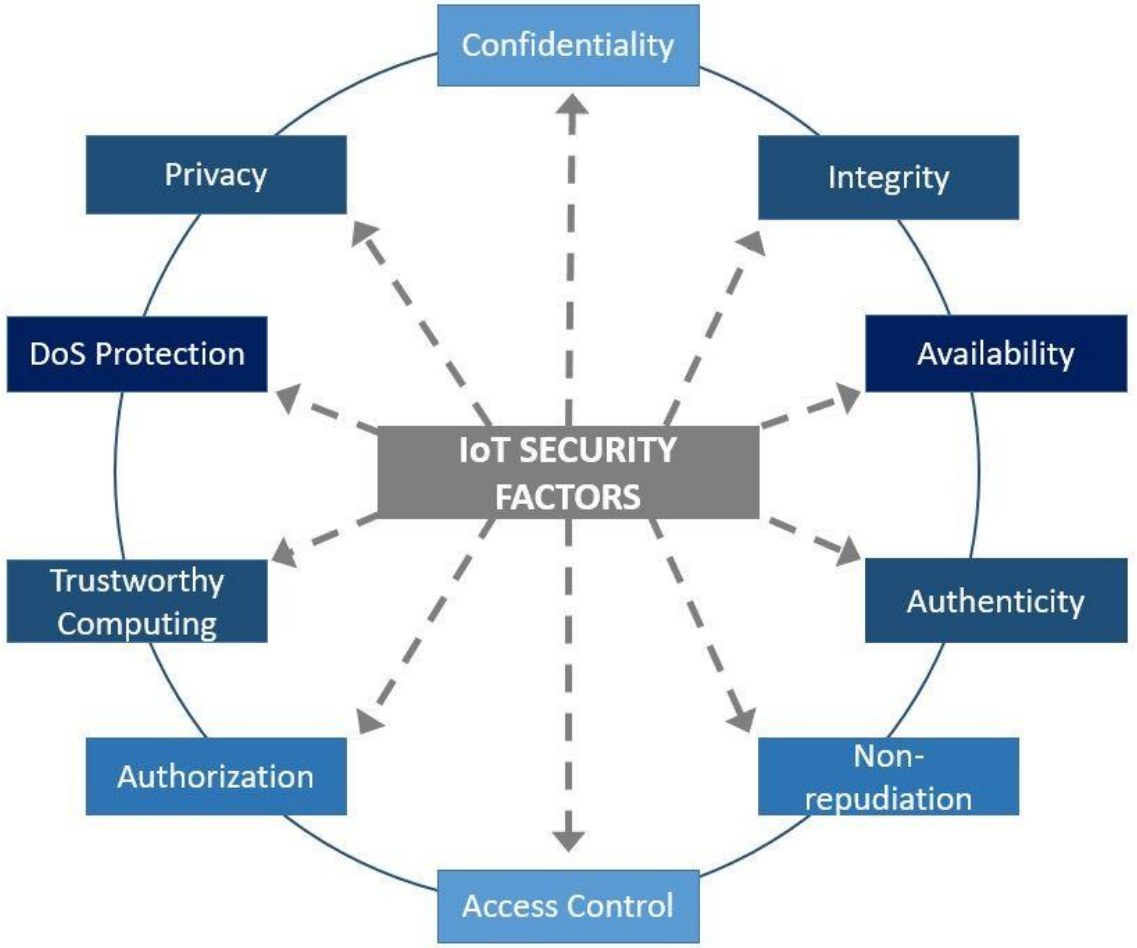
IOT SECURITY

DR. NINAD DILEEP MEHENDALE

"Securing the Internet of Things" refers to the process of implementing measures and strategies to protect IoT devices, networks, and data from potential threats, vulnerabilities, and unauthorized access.

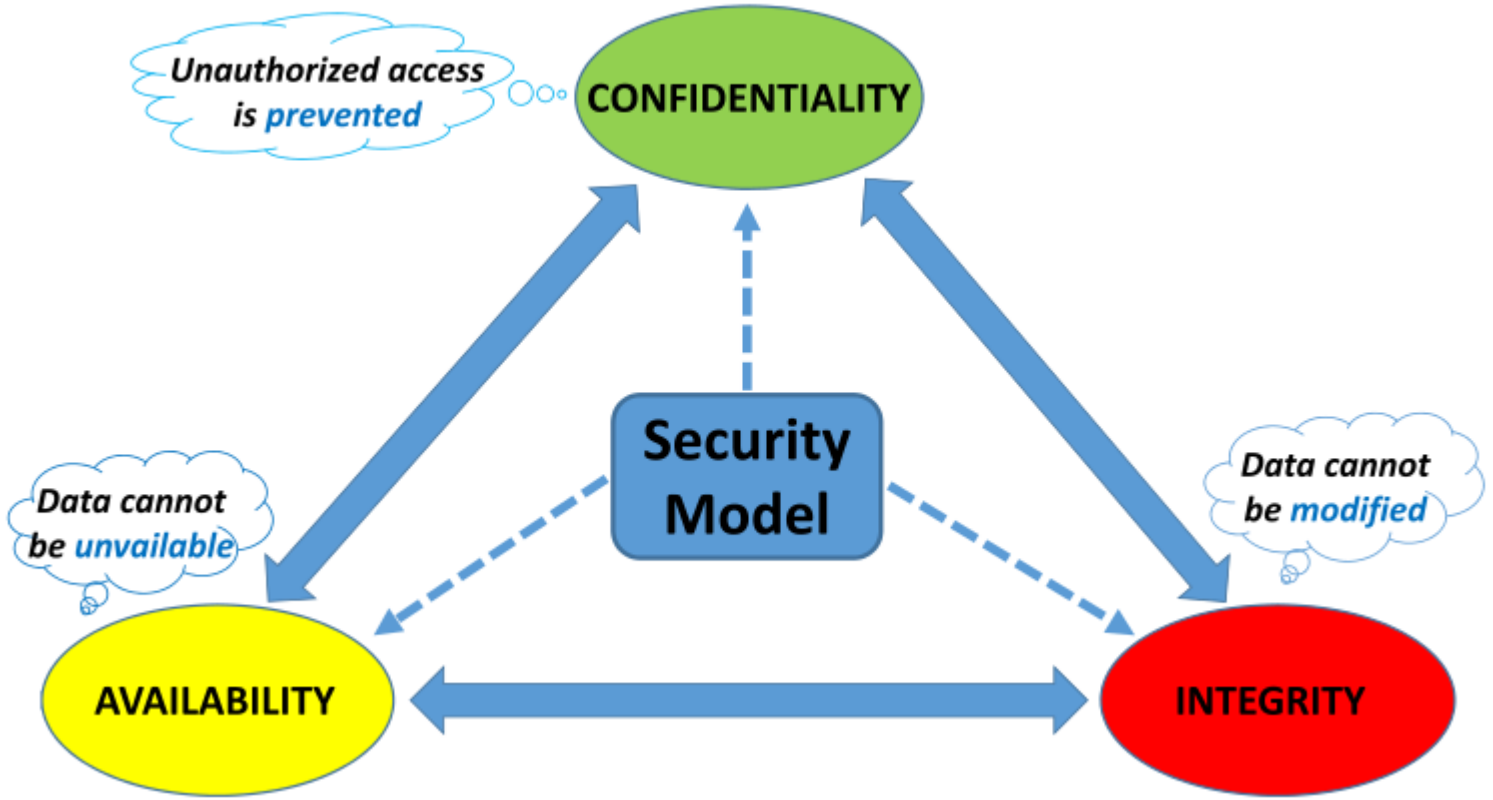
SECURITY REQUIREMENTS IN IOT ARCHITECTURE



CIA

CENTRAL INTELLIGENCE AGENCY

CIA MODEL


Unauthorized access is prevented
CONFIDENTIALITY
Security Model
Data cannot be unvailable
Data cannot be modified
AVAILABILITY
INTEGRITY

THE TARGET DATA BREACH:

- In 2013, hackers stole the credit card information of over 40 million customers from Target stores. The hackers were able to gain access to Target's network by exploiting vulnerabilities in the company's HVAC system.

THE STUXNET WORM:

- In 2010, a group of hackers created a worm called Stuxnet that targeted industrial control systems. The Stuxnet worm was able to infect the control systems of Iranian nuclear facilities, causing significant damage.

C O N F I D E N T I A L I T Y :

- The data that is collected and transmitted by IoT devices must be kept confidential. This means that unauthorized individuals should not be able to access the data.

INTEGRITY:

- The data that is collected and transmitted by IoT devices must be kept accurate and complete. This means that the data should not be modified or tampered with in any way.

AVAILABILITY:

- The IoT devices and networks must be available when they are needed. This means that they should not be taken offline by malicious attacks or other disruptions.

AUTHENTICATION:

- The identity of the devices and users that interact with the IoT system must be authenticated. This means that they must be able to prove who they are before they are allowed to access the system.

AUTHORIZATION:

- The devices and users that are authenticated must be authorized to access the data and resources that they need. This means that they should only be able to access the data and resources that they are authorized to access.

AUTHENTICATION VS AUTHORIZATION

Authentication is about proving who you are, while authorization is about determining what you can do.

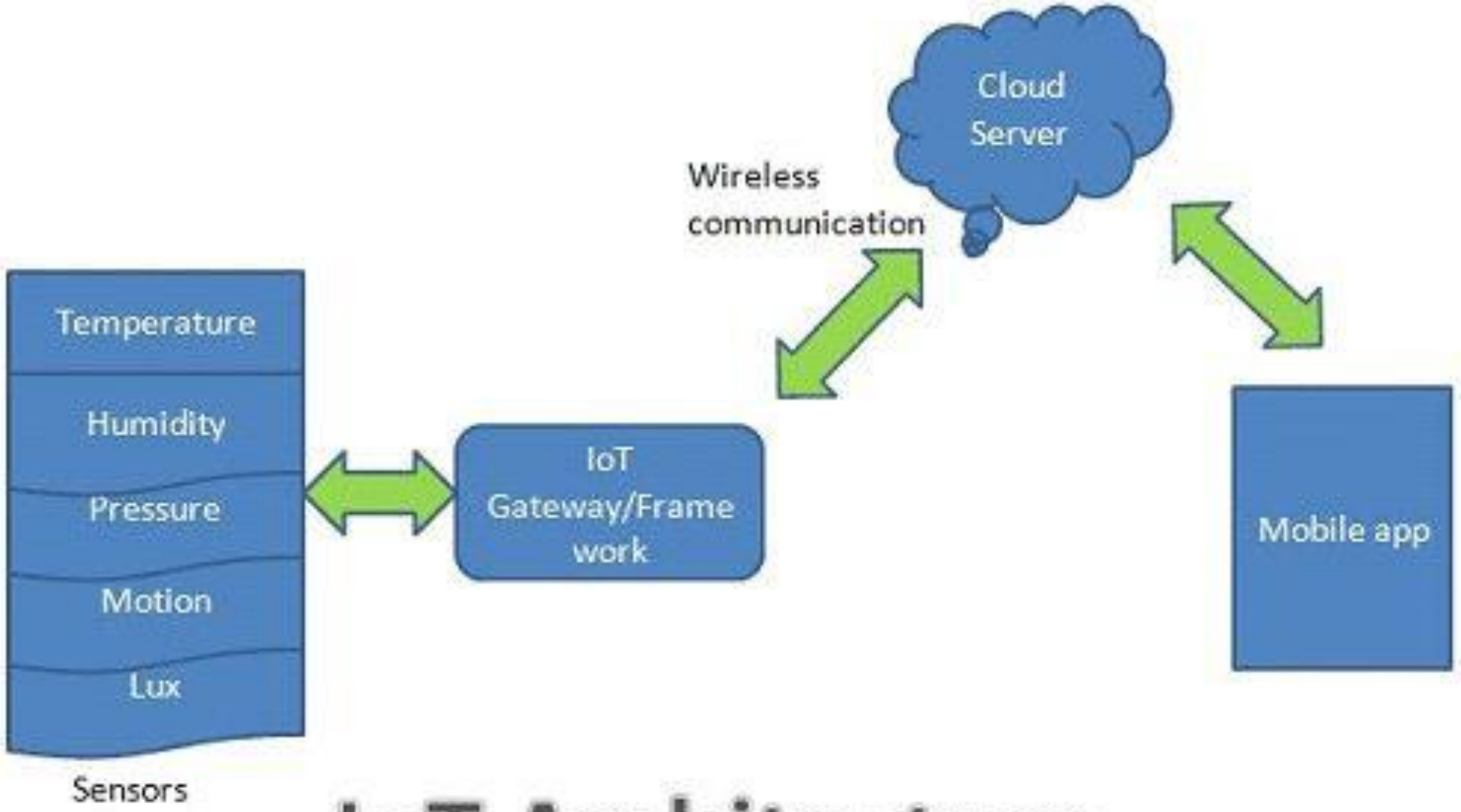
IOT ARCHITECTURE

- IoT architecture refers to the way that IoT devices, networks, and applications are interconnected and communicate with each other. There are many different IoT architectures, but they typically share some common features.

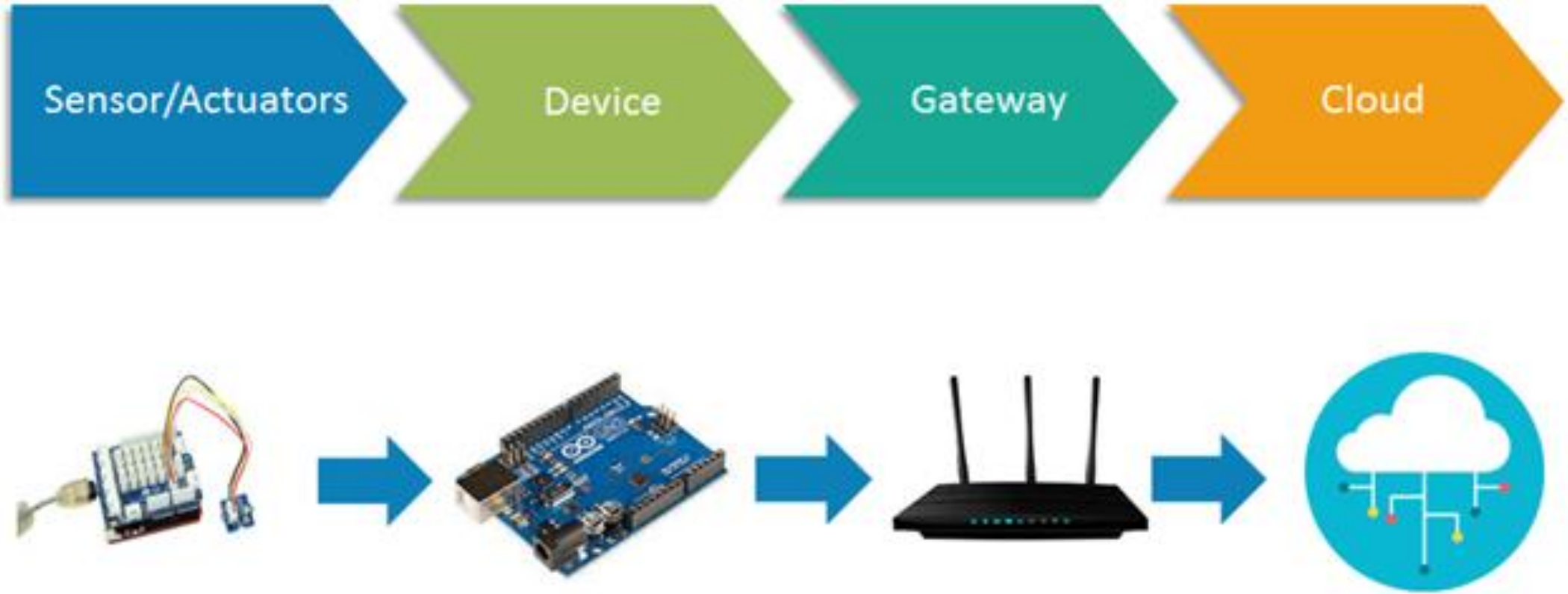
IOT ARCHITECTURE

One common feature of IoT architectures is the use of a three-tier architecture. This architecture consists of three layers:

- The perception layer: This layer is responsible for collecting data from the physical world. It typically consists of sensors and actuators that are connected to the internet.
- The network layer: This layer is responsible for transporting data between the perception layer and the application layer. It typically consists of routers, switches, and gateways that connect the IoT devices to the internet.
- The application layer: This layer is responsible for processing and interpreting the data collected by the perception layer. It typically consists of applications that run on servers or in the cloud.



IoT Architecture


Sensor/Actuators
Device
Gateway
Cloud

- #include <WiFi.h>
- #include <ThingSpeak.h>

- const char* ssid = "your_ssid";
- const char* password = "your_password";

- unsigned long channelID = 123456;
- const char* apiKey = "your_api_key";