Module 3:

# Principles of Secure Architecture on IoT

Dr. Maria Valero

KENNESAW STATE
UNIVERSITY

Agenda

- Physical Computing Architecture
- Physical small computers for IoT
- Arduino
- Beagle Bone Black
- Raspberry Pi
- IoT Security Framework
- IoT Platform Security Tools

Physical Computing Architecture

- Building interactive physical systems by the of software and hardware that can sense and respond to the analog world.
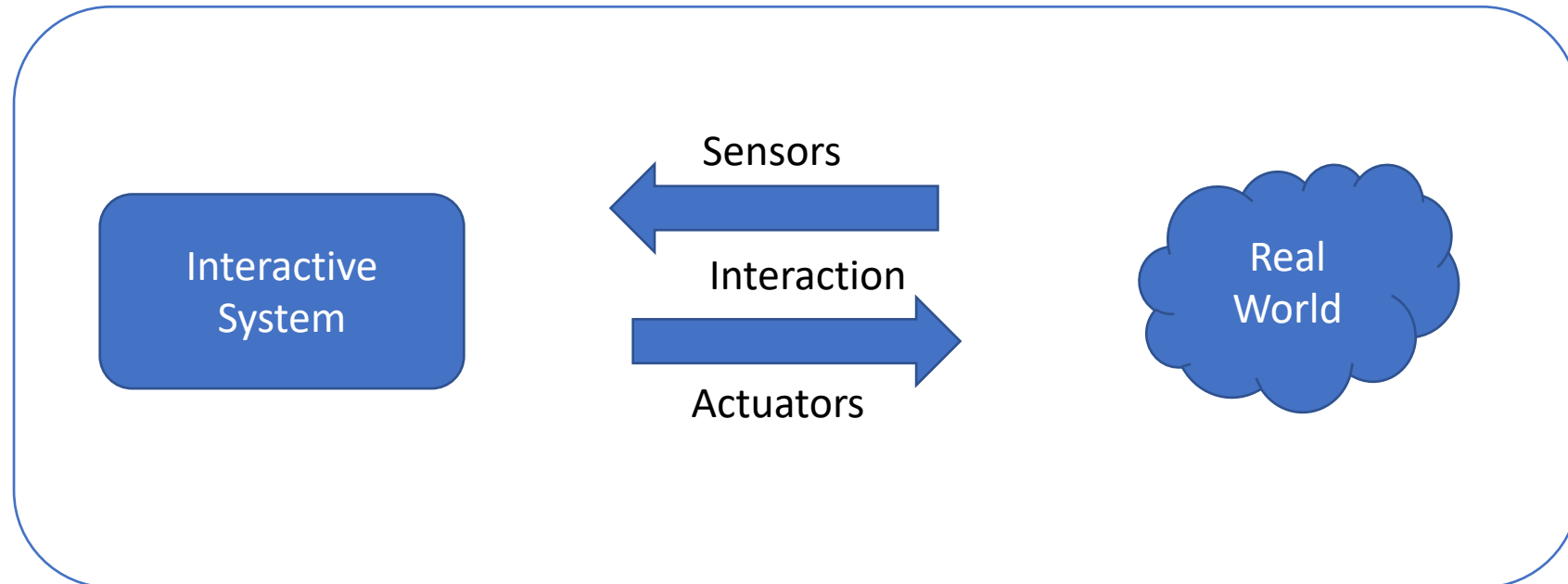
Physical Small Computers for IoT

- 8-bit SoC (System on Chip) Controllers
  - Arduino
  - No Operating System

- System based on Atheros or ARM processors
  - Arduino Yun

- 32/64 bit computing platform
  - Raspberry Pi
  - BeagleBone

Arduino

- Arduino is an open-source hardware and software company, project, and user community that designs and manufactures single-board microcontrollers and microcontroller kits for building digital devices.
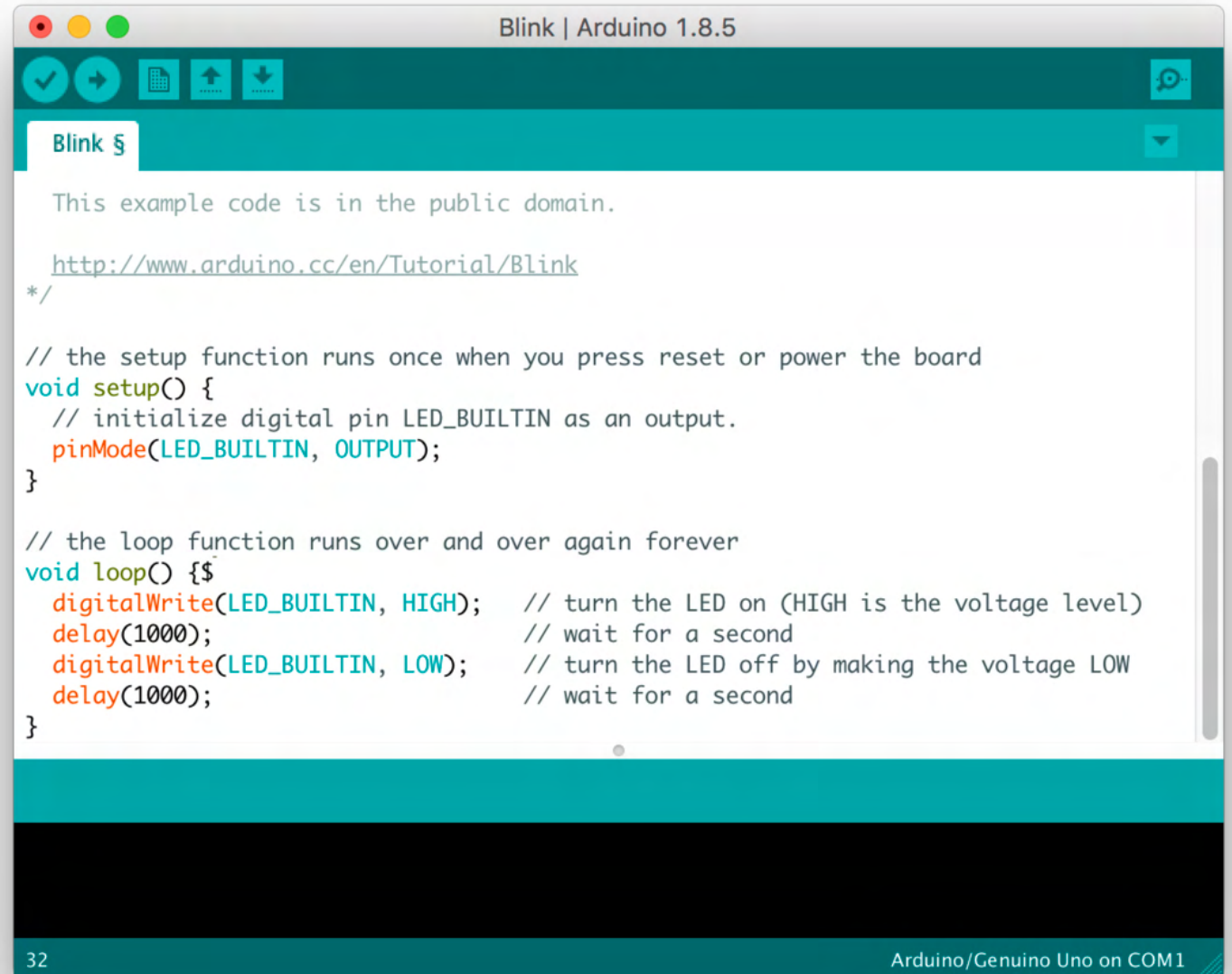
Arduino (Interfaces)

Reset Switch

USB Connector

USB Interface Chip

Crystal Oscillator

Voltage Regulator

Power Port

Digital Pins

TX RX LEDs

Microcontroller

Analog Input Pins

Arduino IDE

- The Arduino Integrated Development Environment is a cross-platform application that is written in functions from C and C++. It is used to write and upload programs to Arduino compatible boards, but also, with the help of third-party cores, other vendor development boards

Arduino Shields

- Shields are boards that can be plugged on top of the Arduino PCB extending its capabilities. The different shields follow the same philosophy as the original toolkit: they are easy to mount, and cheap to produce.

Arduino Shields Examples

- Mini Weather Station
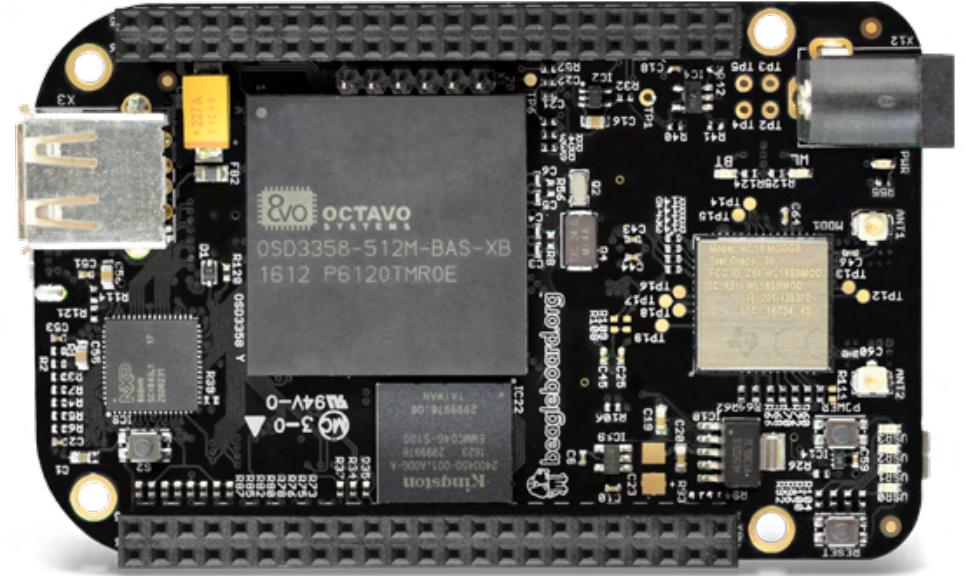 - Espressif Wemos D1 Mini
  - Seeed Grove - Barometer Sensor (BMP280)
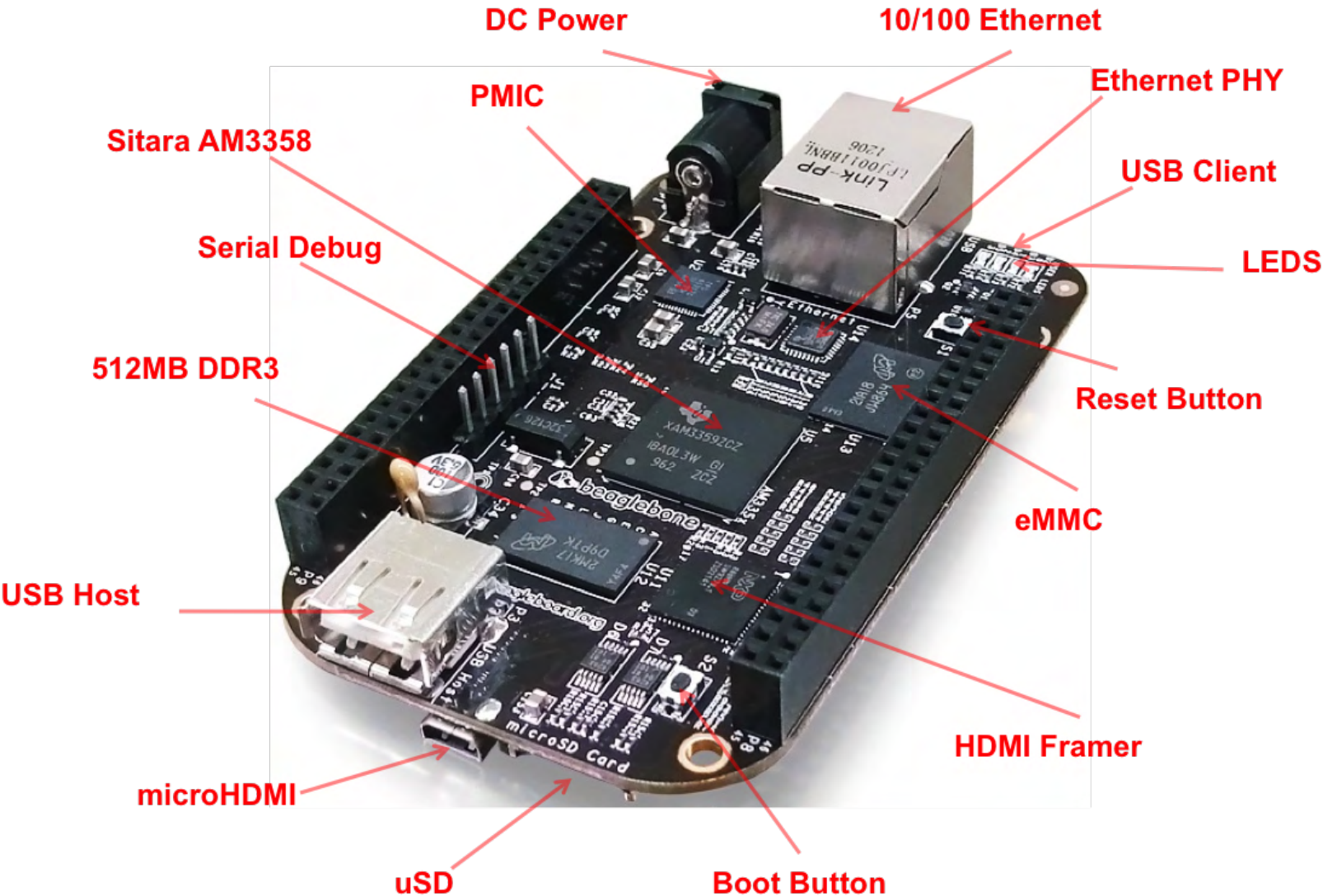 - DHT11 Temperature & Humidity Sensor (4 pins)
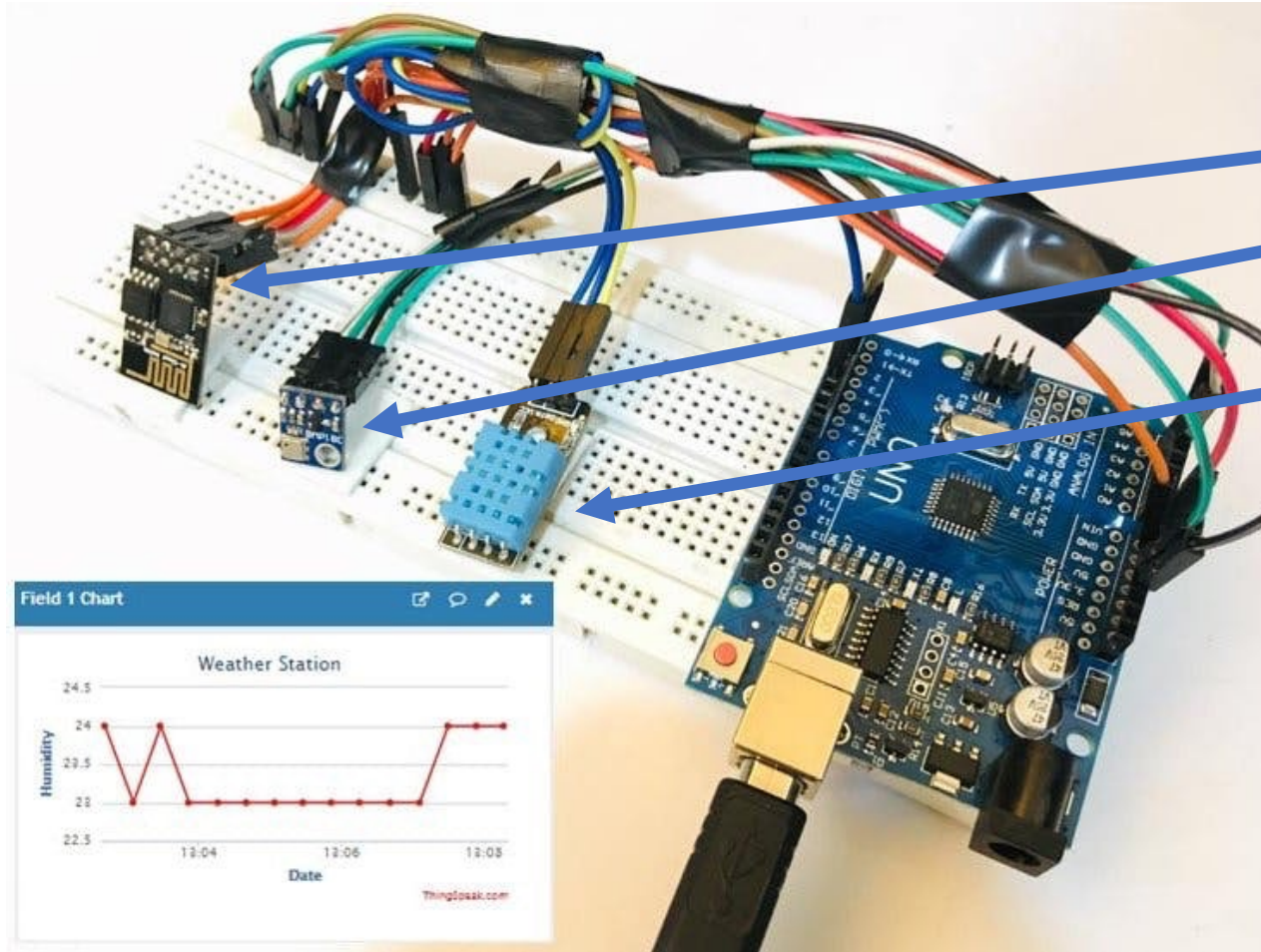
Beagle Bone Black

- Beagle Bone Black is a low-cost, community-supported development platform for developers and hobbyists. Boot Linux in under 10 seconds and get started on development in less than 5 minutes with just a single USB cable.
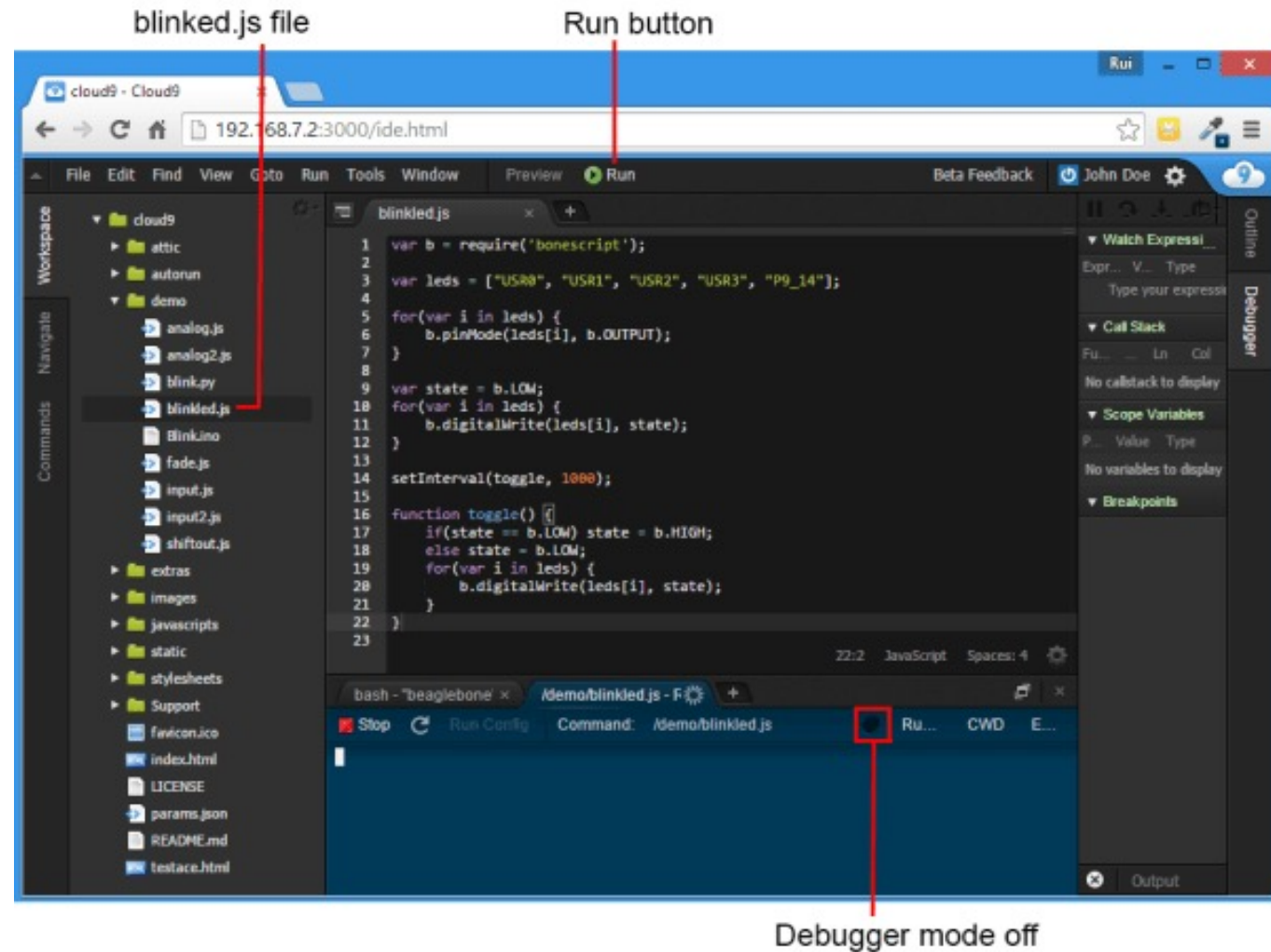
Beagle Bone Black (Interfaces)

Beagle Bone Black IDE

- The Cloud9 IDE is an open-source web-based programming platform that supports several programming languages.

- This software comes installed on the BeagleBone Black * by default.

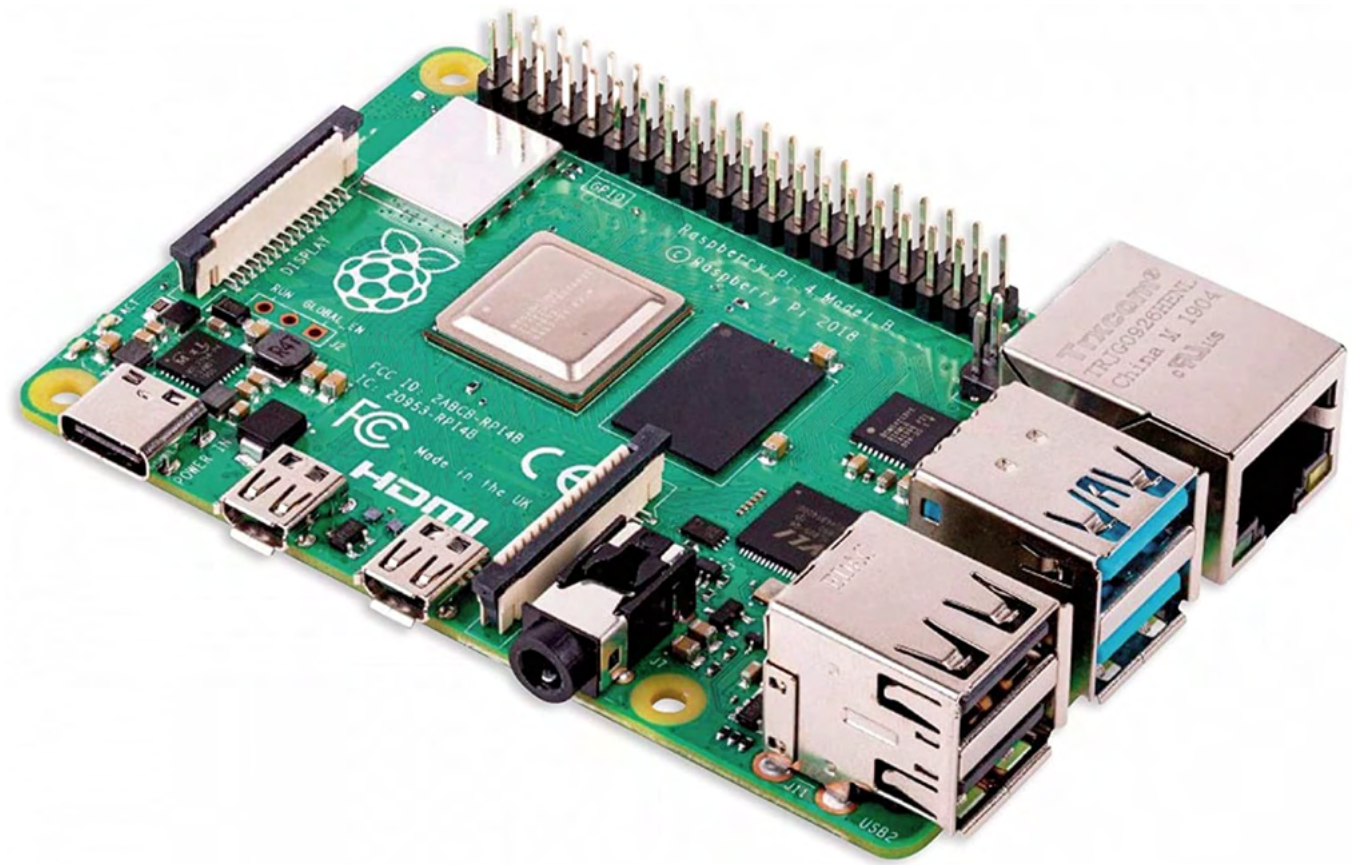blinked.js file   Run button

Debugger mode off

Beagle Bone Black Cluster

Raspberry Pi

- The Raspberry Pi is a low cost, **credit-card sized computer** that plugs into a computer monitor or TV and uses a standard keyboard and mouse. It is a capable little device that enables people to explore computing, and to learn how to program in languages like Scratch and Python.

Raspberry Pi (Interfaces)
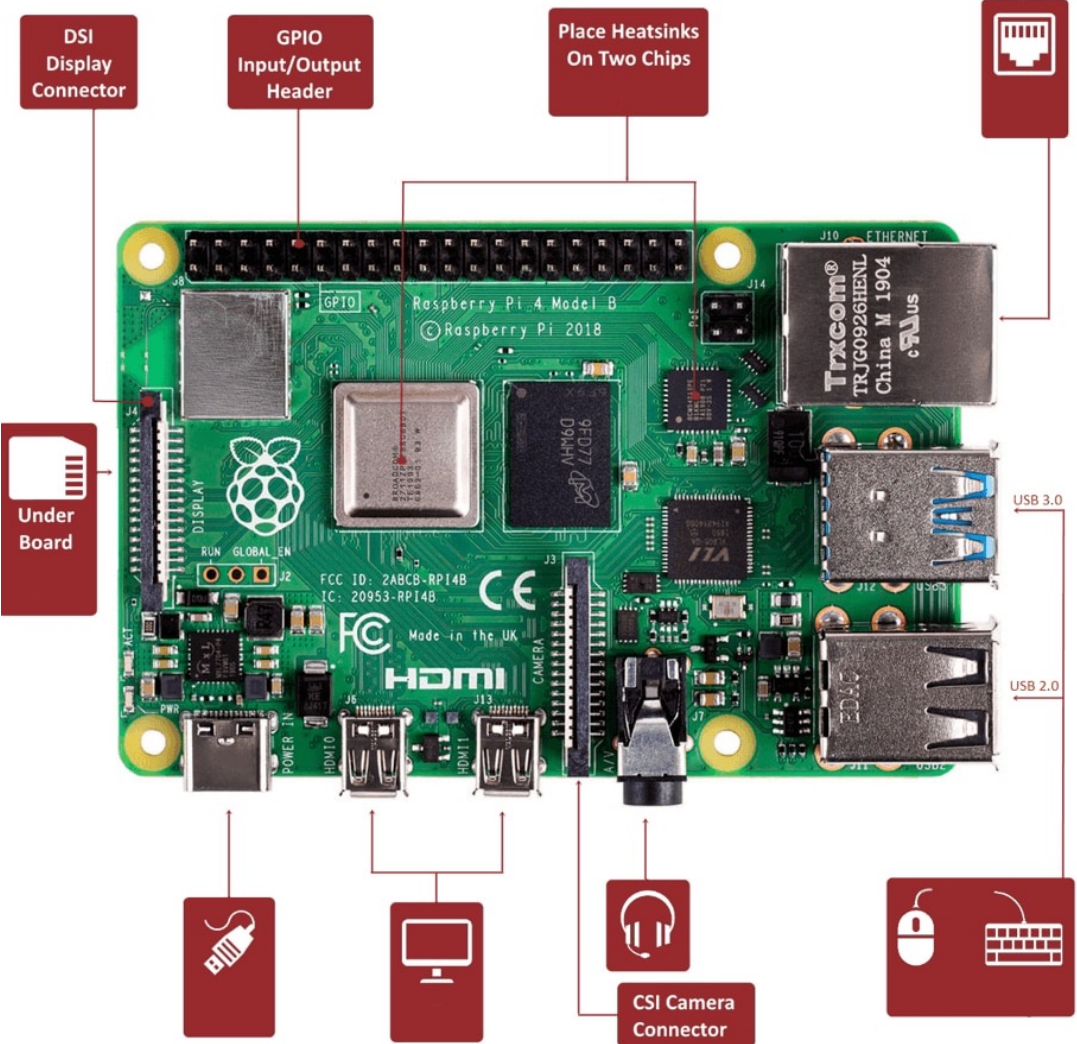
Raspberry Pi (Operating Systems)

- NOOBS
  - Recommended by some new users to the Pi and Linux
- Raspbian
  - Solid Debian based OS
- Ubuntu Mate
- Windows 10 IOT Core
  - Not really Windows, but gets their name in the list
- Kali
  - OS with security focus
- Others

Raspberry Pi (IDE)

- One of the most widely used programming languages on the Raspberry Pi is **none other than Python**
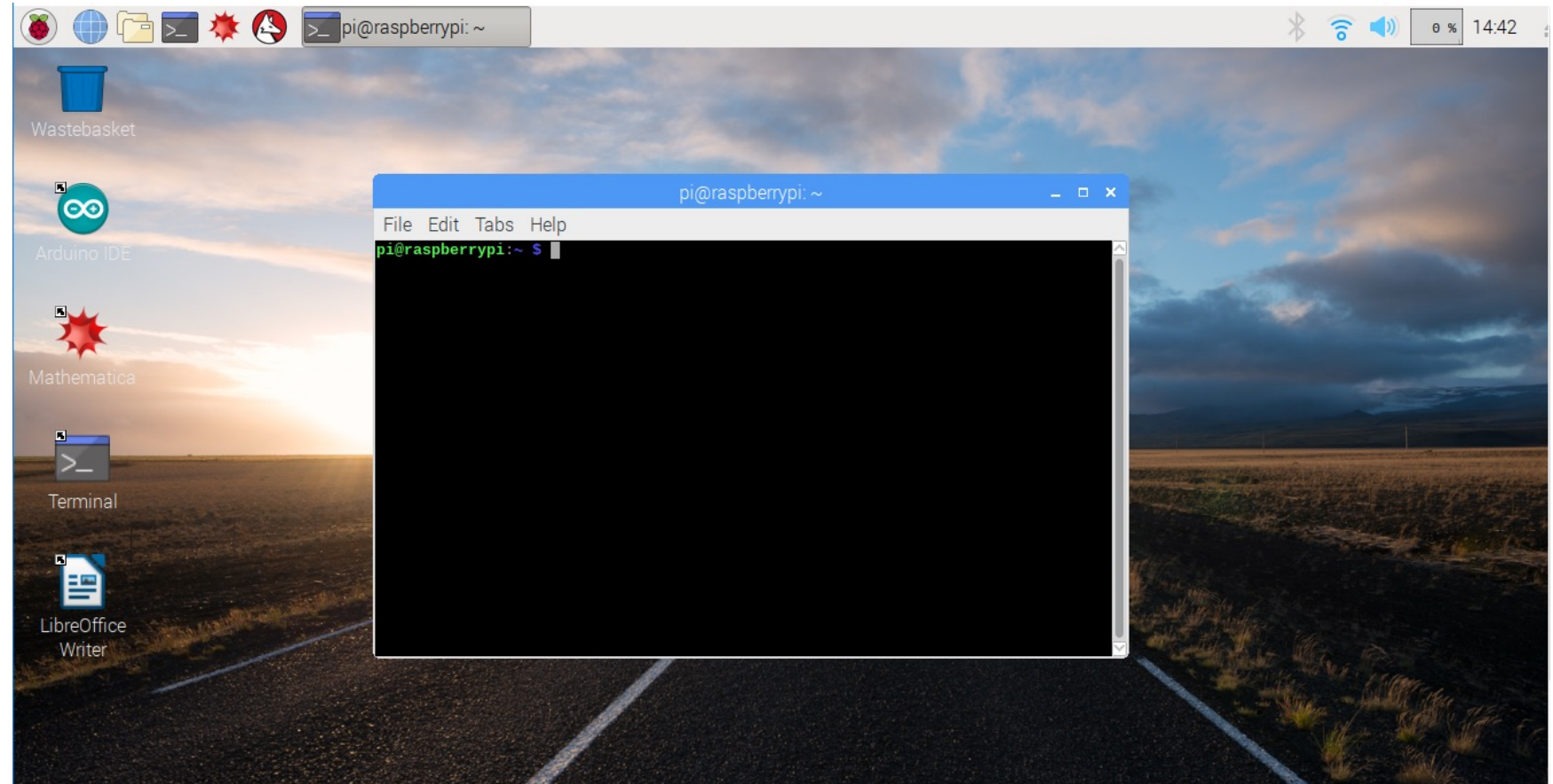
Raspberry Pi Cluster

- For a KSU Raspberry Pi Cluster
  - Visit IoT as Service Research Group
  - Atrium Building
  - J160A
  - Marietta Campus

  - For appointments email Dr. Valero

- Visit not required for this course
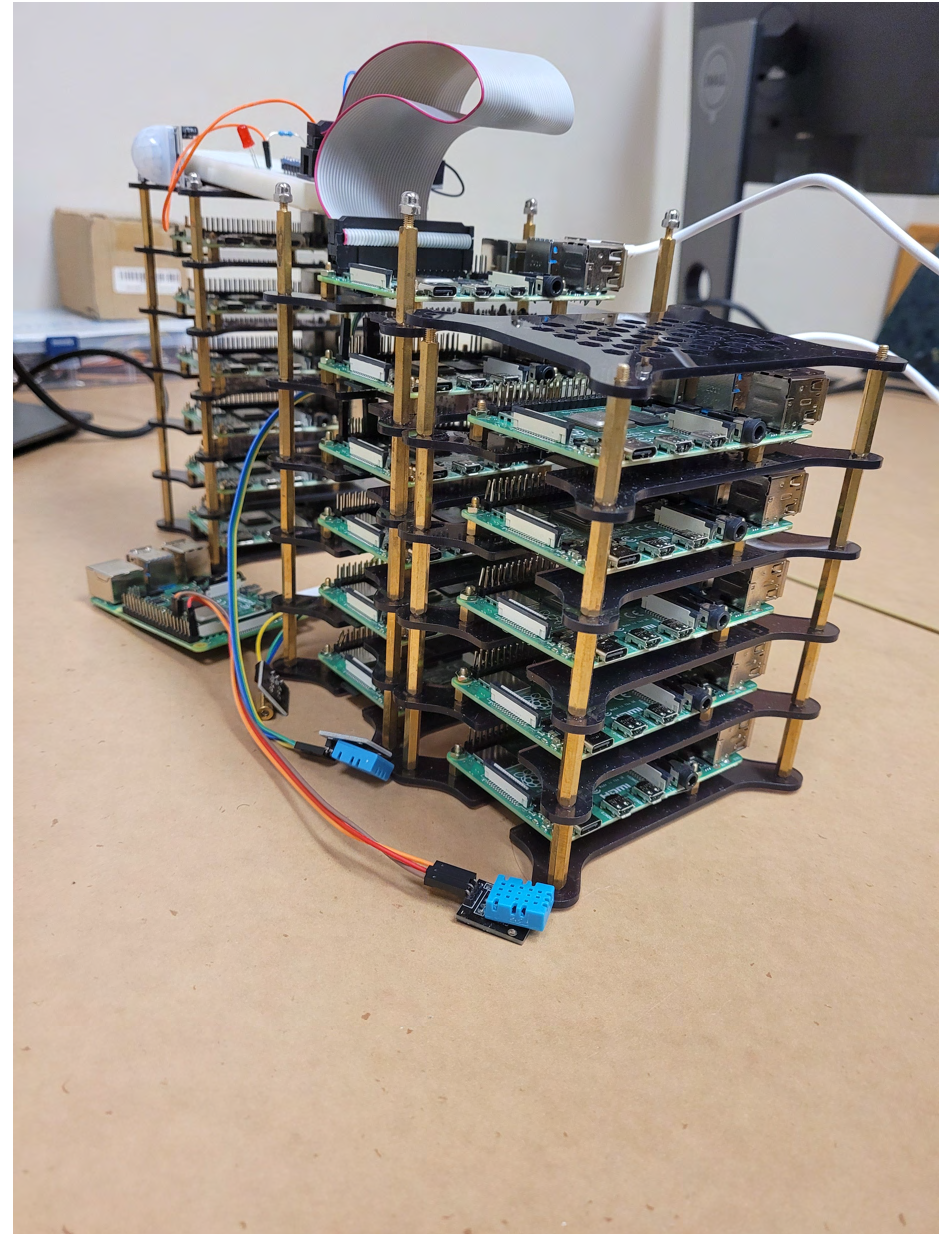
Raspberry PI Secure Architecture

- IoT (especially Raspberry PI) is perhaps the most complex and undeveloped area of network security

- Raspberry PI is the small computer that can gather data and perform some processing. However, in many scenarios, these devices are set unconstrained

- Unconstrained devices may or may not implement some security capabilities

- Raspberry PI in IoT Architecture usually communicate with a gateway that can provide some secure communication.

Raspberry PI Example Architecture
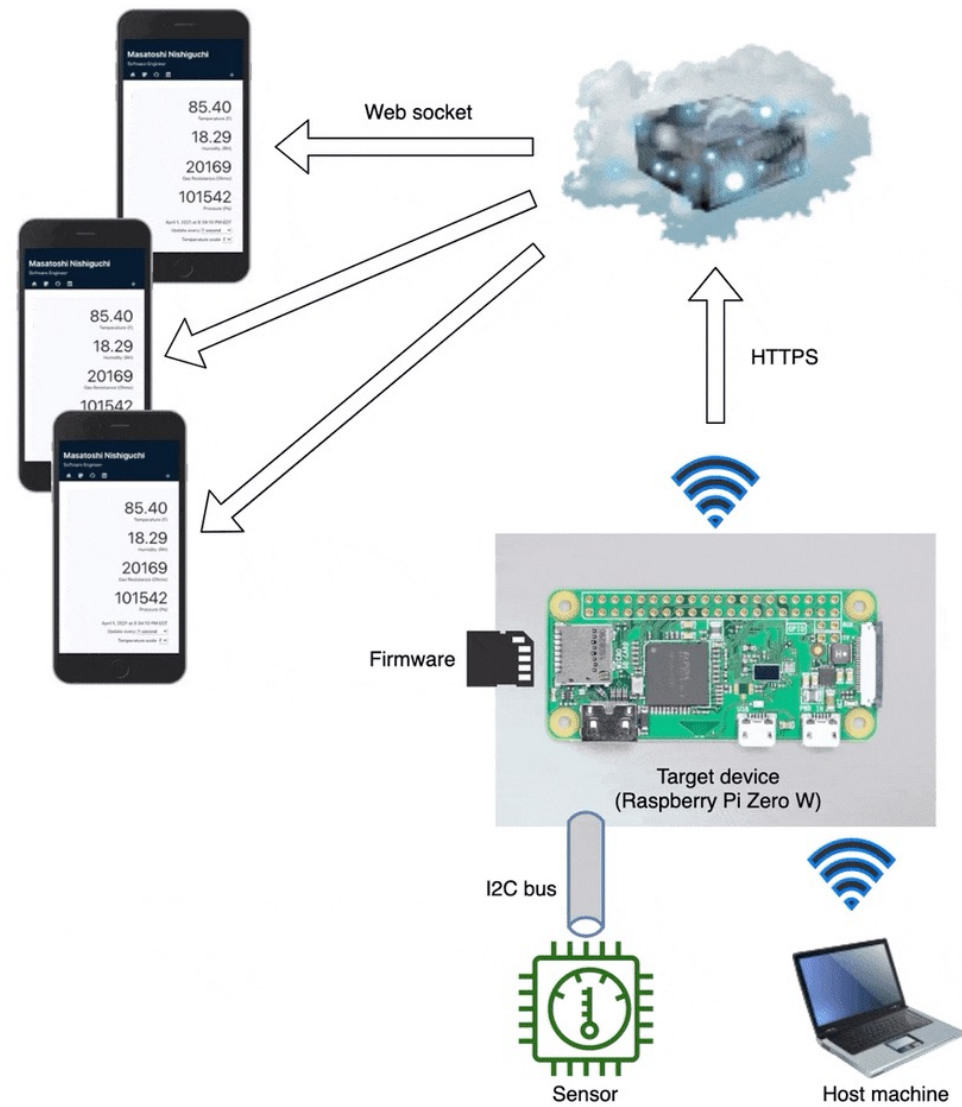
An IoT Security Framework
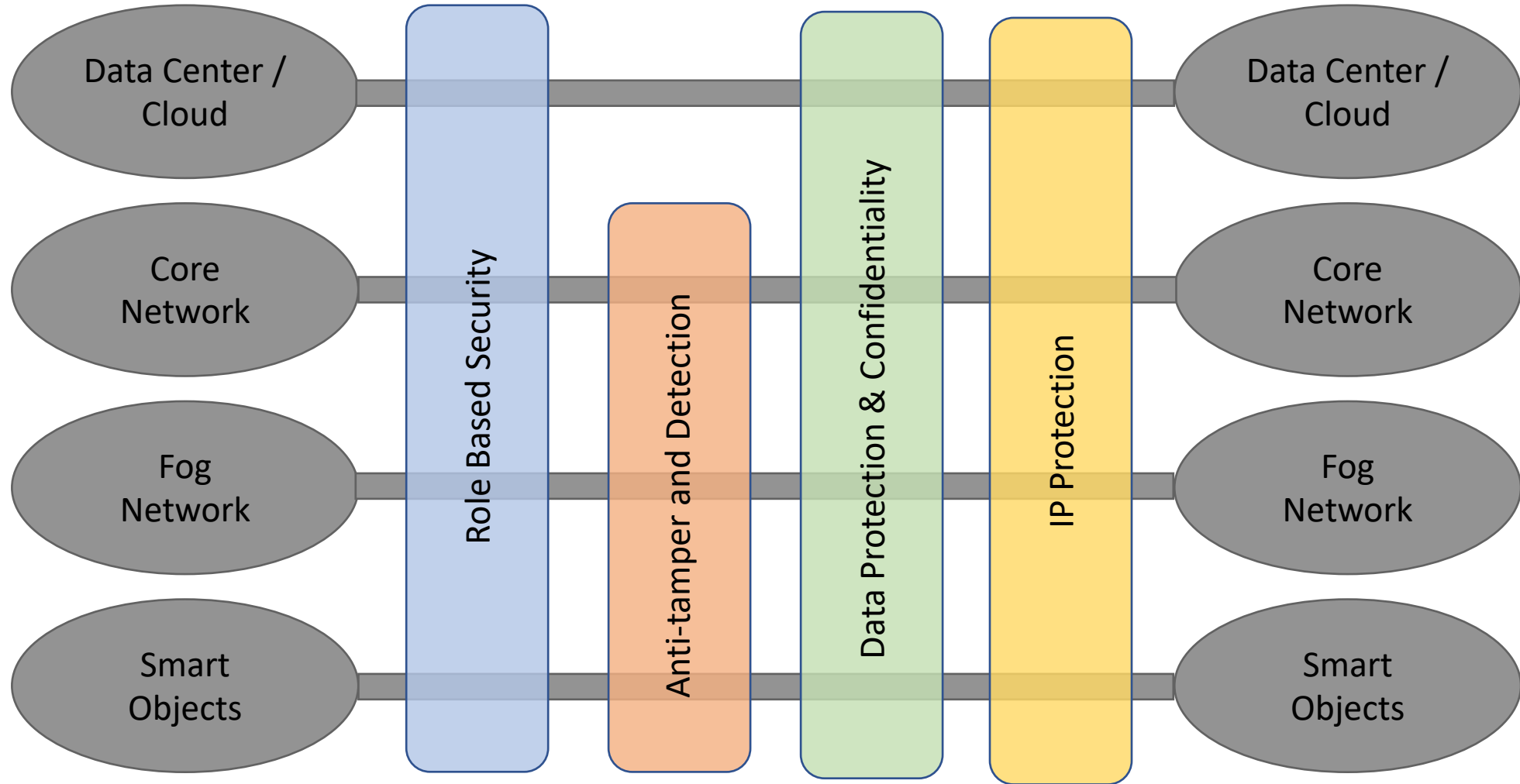
An IoT Security Framework (Smart Objects)
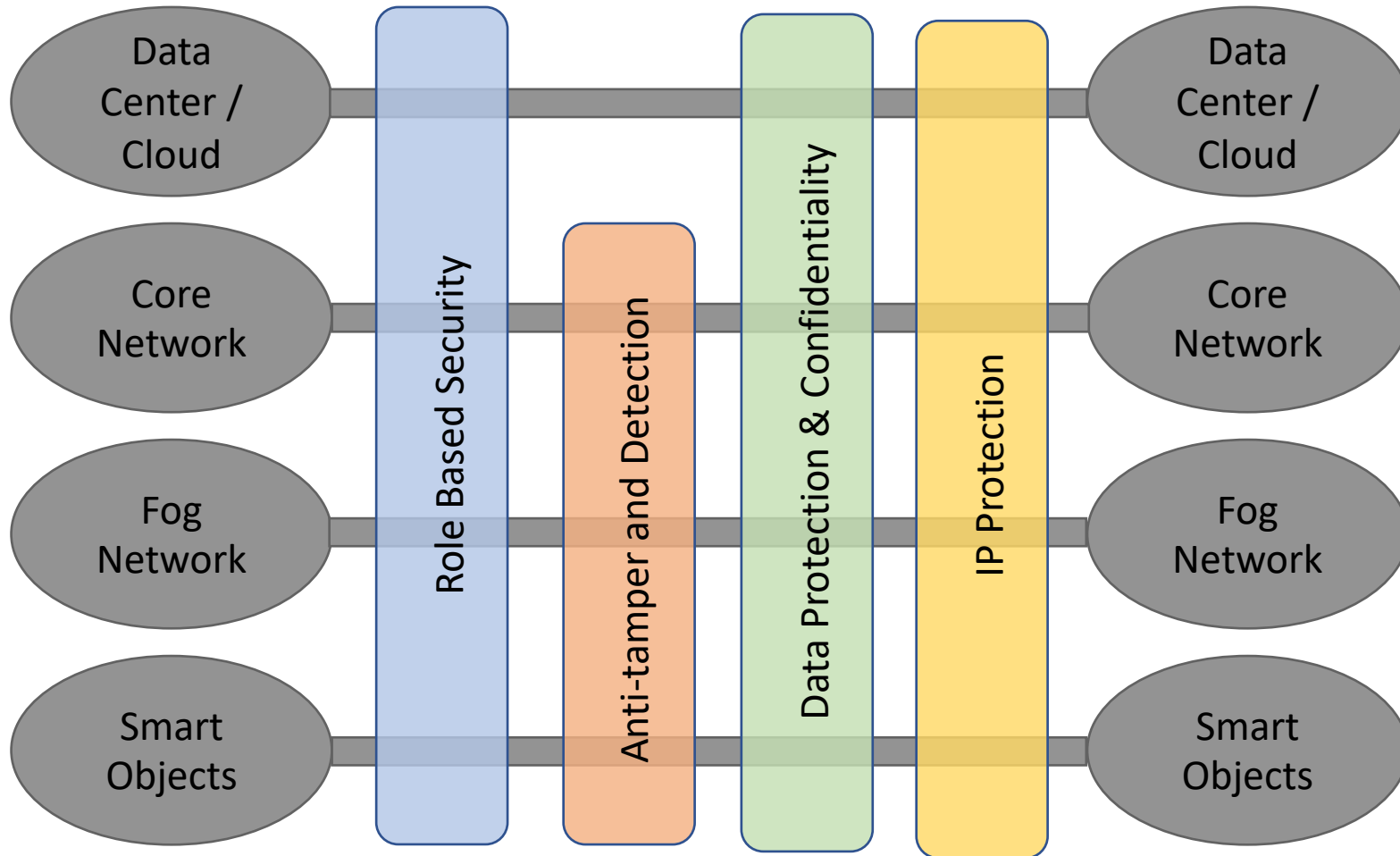
- Sensor and actuators
- The devices may not in a physically secure environment
- They need protection from unauthorized use, privacy and protection from eavesdropping

An IoT Security Framework (Fog network)
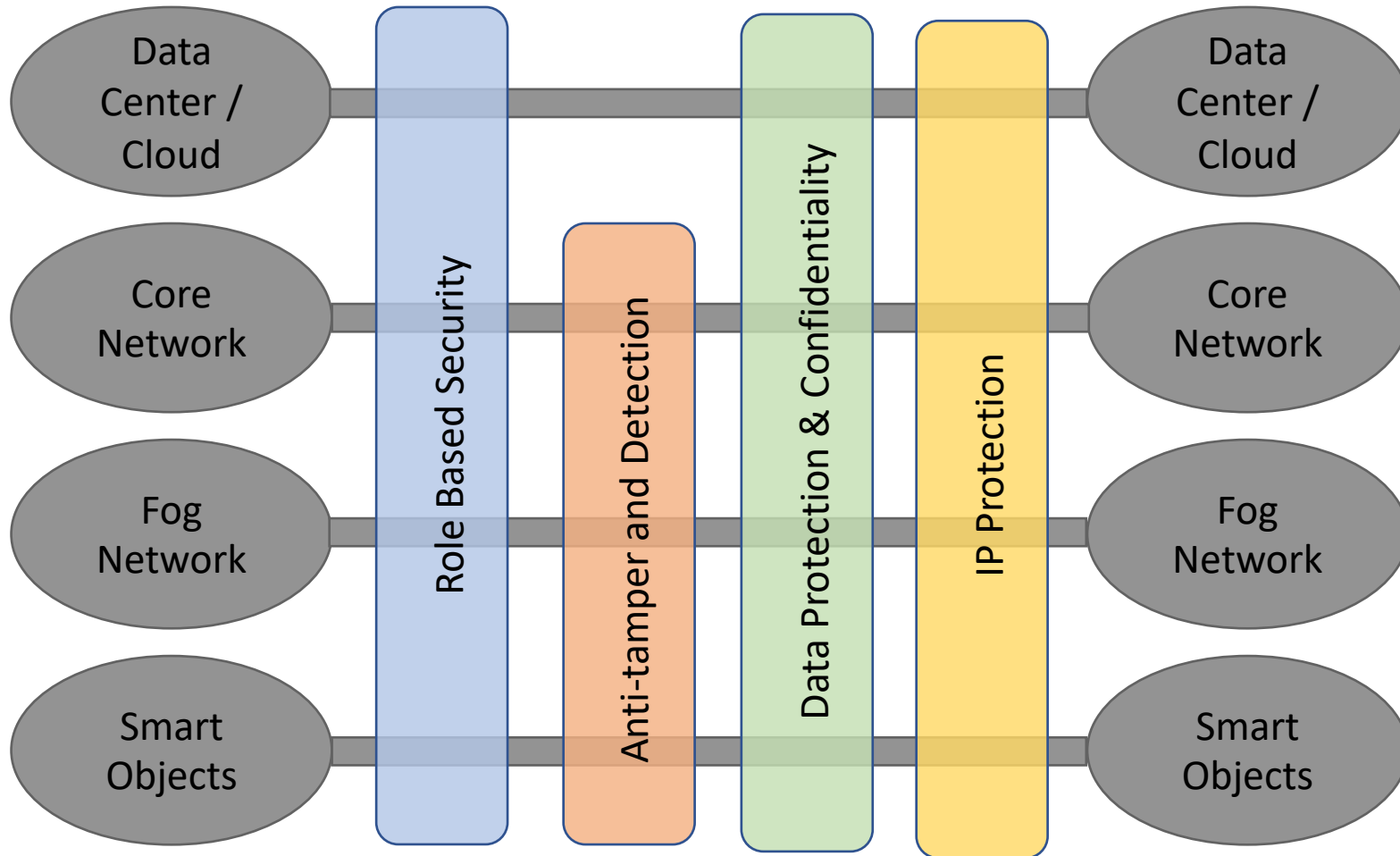
- It is concerned to wired and wireless interconnection of IoT devices

- A key issue is the variety of protocols used by various IoT devices and the need to develop uniform security policy

An IoT Security Framework (Core Network)

Data Center / Cloud

Core Network

Fog Network

Smart Objects

Role Based Security

Anti-tamper and Detection

Data Protection & Confidentiality

IP Protection

Data Center / Cloud

Core Network

Fog Network

Smart Objects
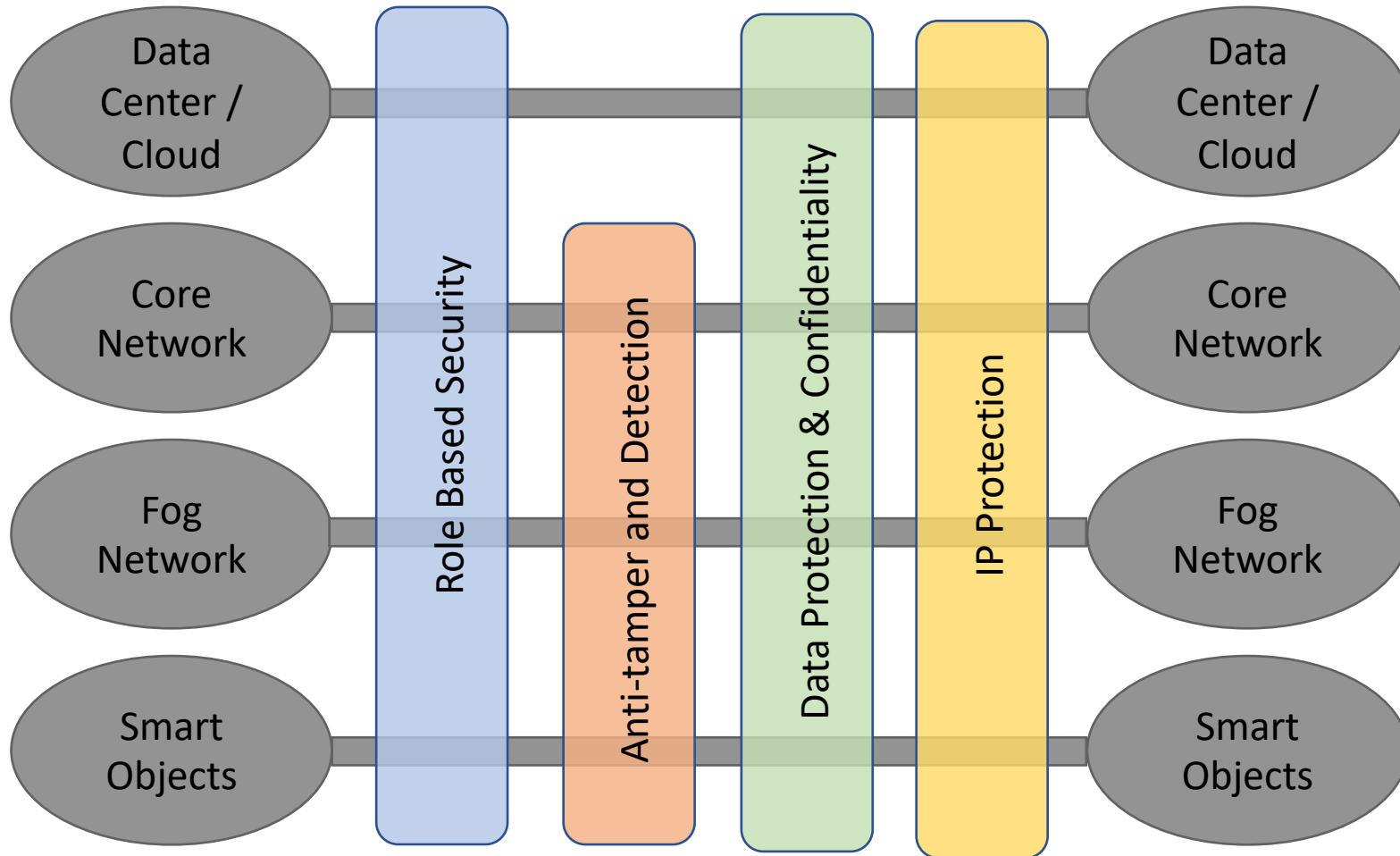
- Provides data paths between network center platforms and IoT devices
- The security issues here are those confronted in traditional core networks
- Security issues with endpoints used by IoT devices

An IoT Security Framework (Data Center)
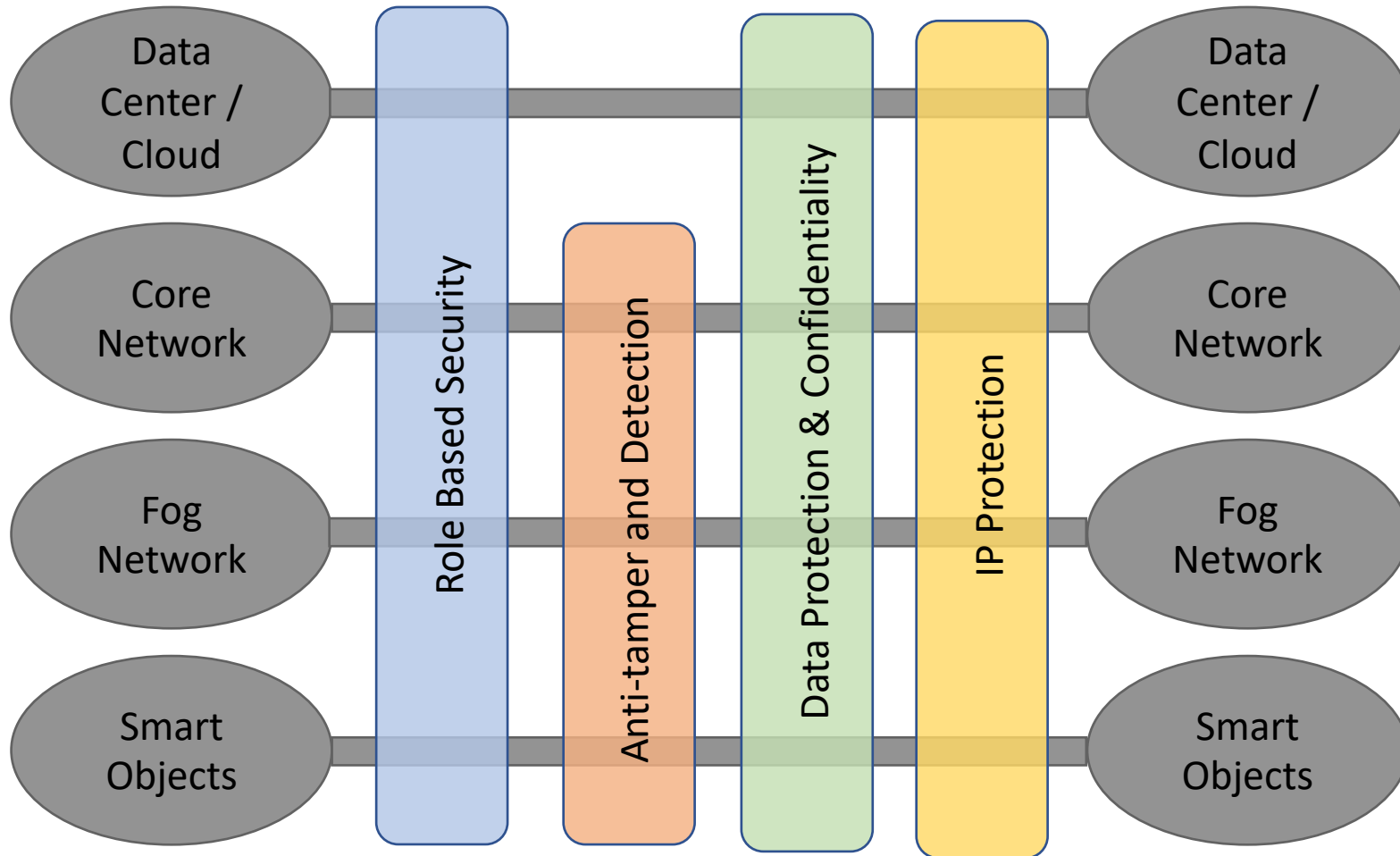
- Contains the application, data storage, and network platforms

- IoT does not introduce any new security issues at this level, other than the necessity of dealing with huge numbers of individual endpoints

IoT Platform Security Tools (1)

- Encryption
- Password Protection
- Hardware Security Modules
- Two-factor authentication
- Secure Elements
- Data erasure
- PKI Certifications
- Biometrics
- Hardware Crypto Processor
- Blockchain

- Devices need lightweight cryptography (LWC) to be implemented in RFID tags, sensors, contactless smart cards, healthcare devices

- Is less attractive due to:
  - Passwords don't work well on dumb devices
  - Passwords require human intervention

- Is a physical computing device that safeguard and manage digital keys for strong authentication and crypto processing

IoT Platform Security Tools (2)

- Encryption
- Password Protection
- Hardware Security Modules
- Two-factor authentication
- Secure Elements
- Data erasure
- PKI Certifications
- Biometrics
- Hardware Crypto Processor
- Blockchain

- (2FA) is a security process in which the user provides two authentication factors to verify identity.
- Useful to sensitive data

- Is tamper resistant hardware component embedded in IoT connected equipment and machines to deliver smart card level digital security and device lifecycle management

- Is a software-based method of overwriting the data that aims to completely destroy all electronic data residing on a hard disk or other digital media

IoT Platform Security Tools (3)

- Encryption
- Password Protection
- Hardware Security Modules
- Two-factor authentication
- Secure Elements
- Data erasure
- PKI Certifications
- Biometrics
- Hardware Crypto Processor
- Blockchain

- A Public Key Infrastructure (PKI) is a set of roles, polices and procedures needed to create, manage, use, store, revoke digital certificates and public-key encryption. Important in banking and e-commerce

- Is the process of comparing data from the person's characteristics to that person's biometrics "template". Example, google home and Alexa

- Is a dedicated computer on a chip or microprocessor for carrying out cryptography operations, embedded in a packing with multiple physical security measures, which gives it a degree of tamper resistance.

IoT Platform Security Tools (4)

- Encryption
- Password Protection
- Hardware Security Modules
- Two-factor authentication
- Secure Elements
- Data erasure
- PKI Certifications
- Biometrics
- Hardware Crypto Processor
- Blockchain

- Blockchain is a database that maintains a continuously growing set of data records.
- It is distributed in nature, meaning that there is no master computer holding the entire chain
- Rather, the participant nodes have a copy of the chain
- It's also ever-growing – data records are only added to the chain.
- A blockchain consists of two types of elements:
  - Transactions are the actions created by the participants in the system
  - Block records these transactions and make sure they are in the correct sequence and have not been tampered with. Blocks also record a time stamp when the transactions were added.

IoT Platform Security Tools (5)

- Encryption
- Password Protection
- Hardware Security Modules
- Two-factor authentication
- Secure Elements
- Data erasure
- PKI Certifications
- Biometrics
- Hardware Crypto Processor
- Blockchain

- By merging Blockchain with IoT it is easier to implement confidentiality and integrity
- This allows the connected devices to respond to fabrication and modification attacks and enhances the trust between parties in communication