Data storage, sharing & security.

ESME – INGE1 INTERNATIONAL TRACK

zakaria@elbazi.co

During this semester:

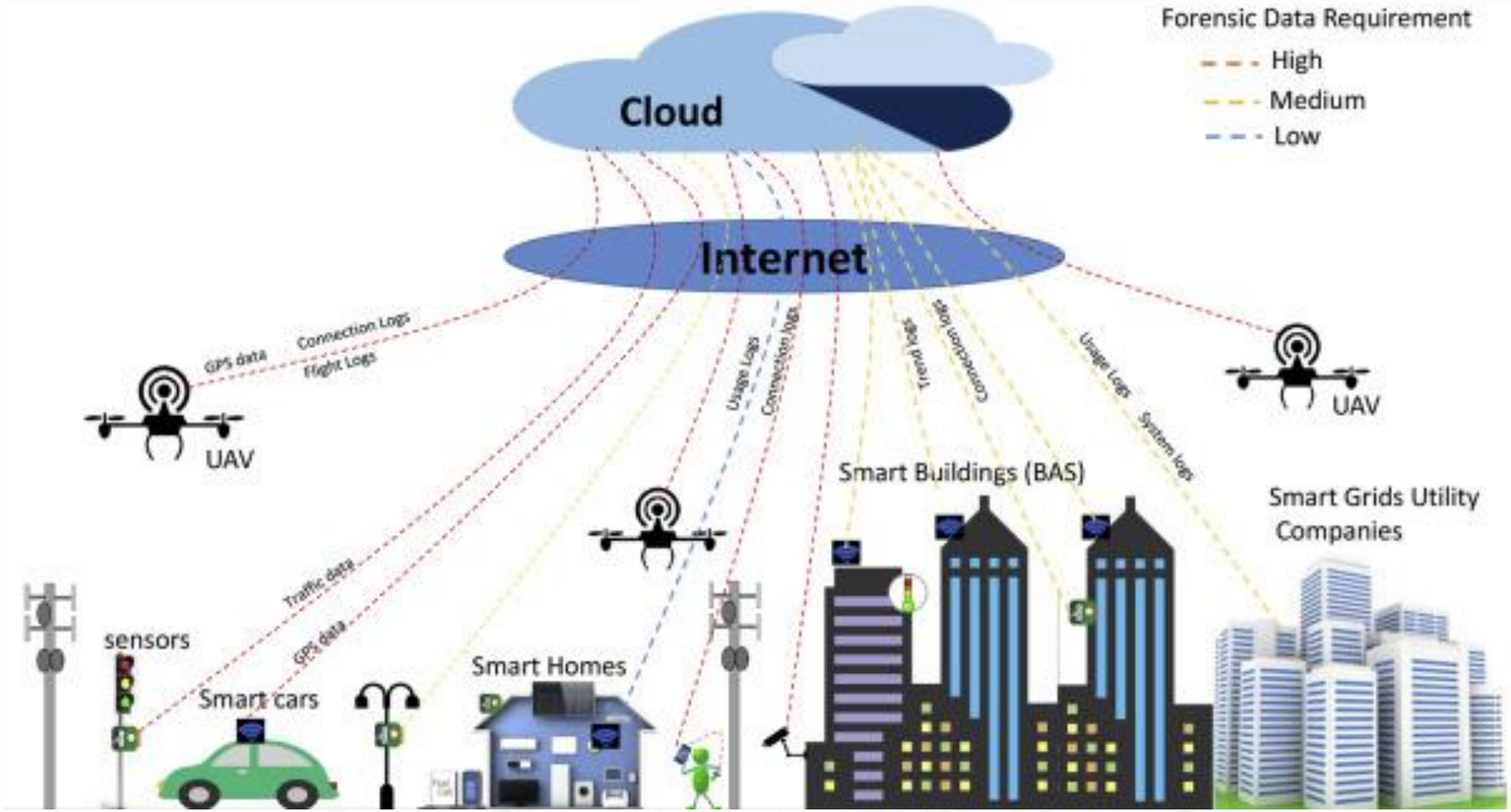
- Data collection and processing (IoT, mobile and web apps, etc.)
- Cyberattacks risks and challenges (Data breaches, etc).
- IoT & smart city monitoring (extending your existing projects).
- Data protection & privacy.
- Cyber security roles and career paths.

About your instructor:

- Zakaria EL BAZI (cybersecurity and data science engineer @exceleratesystems_france).
- I teach sometimes (ISEG, Kedge, ESME).

Smart cities:

Smart cities:



- How many captors do we need ?
- With what frequency the data must be retrieved from these devices ?
- How much data we will store ?

Smart cities:

Deploying sensors and captors

- Cameras
- Captors
- etc.

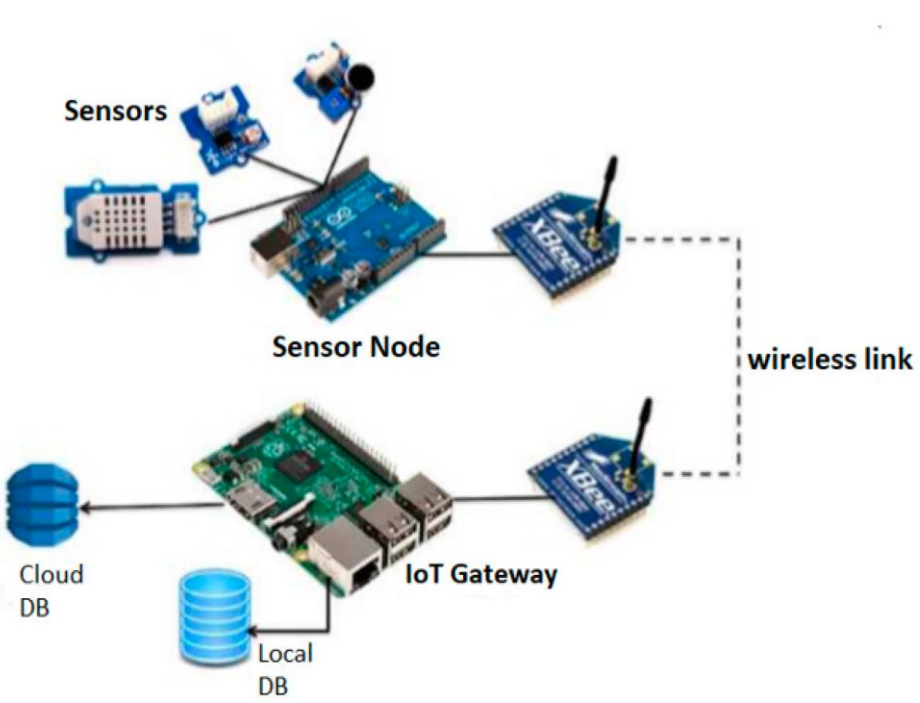
Get/collect the data.

- Get the data from the captors (frequency, **transfer** protocols).

Store & process the data

- Local storage
- External storage devices
- databases

Process the data and make use of it.



zakaria@elbazi.co

Smart cities:

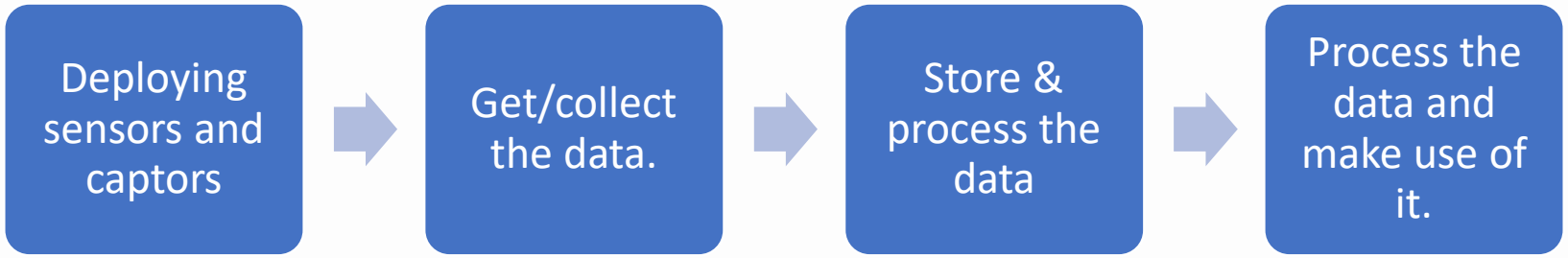
- Deploying IoT devices and making them accessible (connected to a network)
- Get the data from these devices and send it to IoT Gateway (raspberry pi for example) for processing & storage.
- External storage may be required, so the Gateway needs to send the data to an external storage/database.
- Make the data available for processing and exploitation (analysis, processing) and make it accessible for external applications.

Smart cities:

What about your projects ?

1. Connected ring Théo/P-J (Sport)
2. Automated ventilation system against COVID (Health)
3. Railed (crash detection system in roads)
4. God’s lights : guiding illumination in stores (Retail)

Points of failure:



- IoT devices may be exposed and publicly accessible.
- Data integrity
  - A sensor getting wrong measures for example.
  - Someone altering the data during the transfer.
- Data storage device or data base are publicly exposed and available.
  - Data integrity and availability risks.
- Applications are not enough secured (again data integrity issues).

ESME sudria

Points of failure:

- IoT devices may be exposed and publicly accessible. (shodan)
- Data integrity
  - A sensor getting wrong measures for example.
  - Someone altering the data during the transfer.
- Data storage device or data base are publicly exposed and available.
  - Data integrity and availability risks.
- Applications are not enough secured (again data integrity issues).

What should we do then ?

- Make sure everything is safe by :
  - Having access control systems (for IoT and storage devices).
  - Securing communications.
  - Continually monitoring the infrastructure to detect anomalies, unauthorized access ,etc.
  - Ensuring data privacy and protection (personal data, non personal data ,etc.)

Cyber security policy

What should we do then ?

- Build your projects again for the next session.
- Imagine how your project will scale/evolve :
  - Number of users
  - Amounts of data that will be collected
- We will add additional components for storage and visualization
- We will define a **security policy** to make sure everything is secured and safe.