

# **CSC 116**

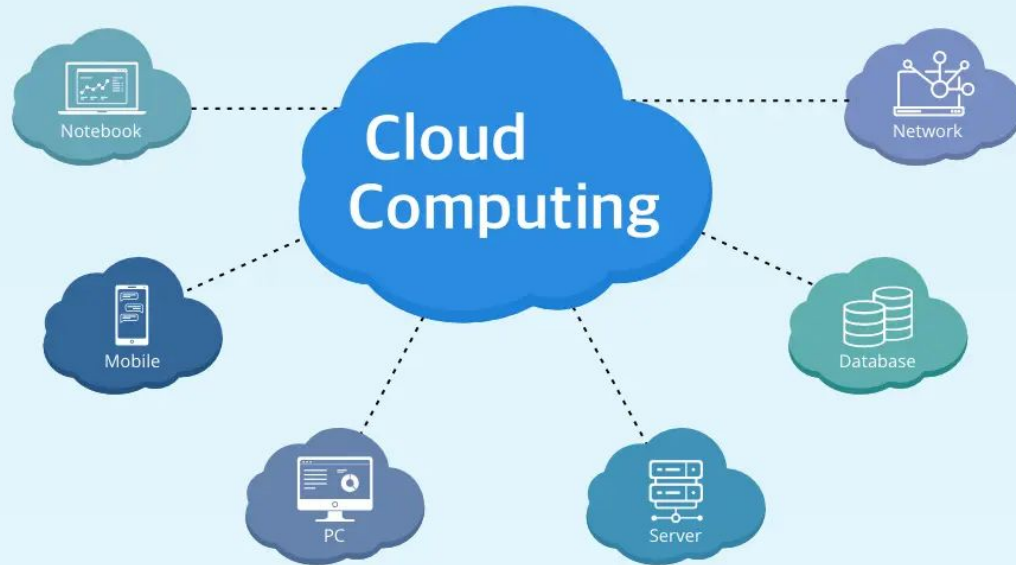
# **Homomorphic Encryption**

**Homomorphic Encryption** is a type of encryption that allows computations to be performed directly on encrypted data **without decrypting it**.

### **Why it's important:**

- Enables **privacy-preserving computation**.
- Useful in **cloud computing**, where a server can compute on encrypted data without learning the actual data.
- Vital for **secure data analysis, machine learning, finance, and healthcare** where sensitive data is involved.

# Cloud data is not secure

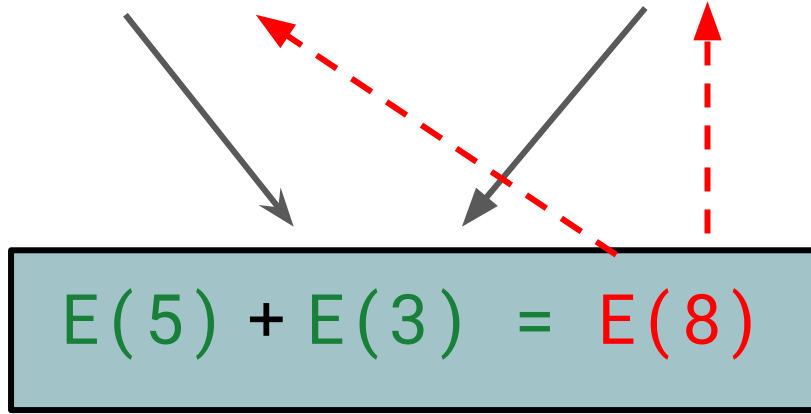


## Example:

Imagine you encrypt the numbers 5 and 3. A server can **add the encrypted values**, and when you decrypt the result, you get 8 — **without the server ever knowing what 5 or 3 were.**

Encrypt(5)

Encrypt(3)



Remote server

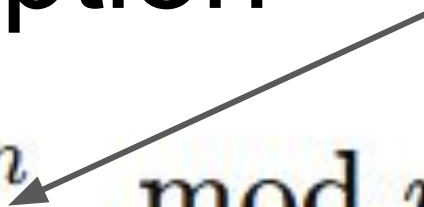
You have numbers  $x_1, x_2, \dots, x_n$  (e.g., pain scores). You want the **encrypted average**

$$\text{avg} = \frac{1}{n} \sum_{i=1}^n x_i$$

Homomorphic addition:  $\text{Enc}(a) + \text{Enc}(b) = \text{Enc}(a + b)$

# Paillier encryption

random  $r$

$$\text{Enc}(m) = g^m \cdot r^n \pmod{n^2}$$


$$p = 3, q = 5 \rightarrow n = pq = 15,$$

$$g = n + 1 = 16$$

$$r = 2$$

Encrypt  $A = 2$

1.  $g^2 \bmod 225 : 16^2 = 256 \Rightarrow 256 \bmod 225 = 31$

2.  $r^n \bmod 225 : 2^{15} = 32768 \Rightarrow 32768 \bmod 225 = 143$

3. Multiply and mod:  $31 \times 143 = 4433 \Rightarrow 4433 \bmod 225 = \mathbf{158}$

$\text{Enc}(2) = 158$

Encrypt  $B = 5$

1.  $g^5 \bmod 225 = \mathbf{76}$  (intermediate steps omitted)

2.  $r^n \bmod 225 = 143$

3.  $76 \times 143 = 10868 \Rightarrow 10868 \bmod 225 = \mathbf{68}$

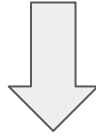
$\text{Enc}(5) = 68$

Multiplying ciphertexts (mod  $n^2$ ) equals adding the plaintexts.

$$\text{i.e., } \text{Enc}(A) \times \text{Enc}(B) \equiv \text{Enc}(A + B) \pmod{n^2}$$

$$\text{Enc}(2) \times \text{Enc}(5) \bmod 225 = 158 \times 68 = 10744 \Rightarrow \mathbf{10744 \bmod 225 = 169}$$

**Some HE only encrypt message for 0 and 1**



**200 into binary = 11001000**

# HE limitations:

Only numerical data.

Slow computation

Limited operations,  $+$   $-$   $*$   $/$ : Only good for Addition, Subtraction, Multiplication, Division.

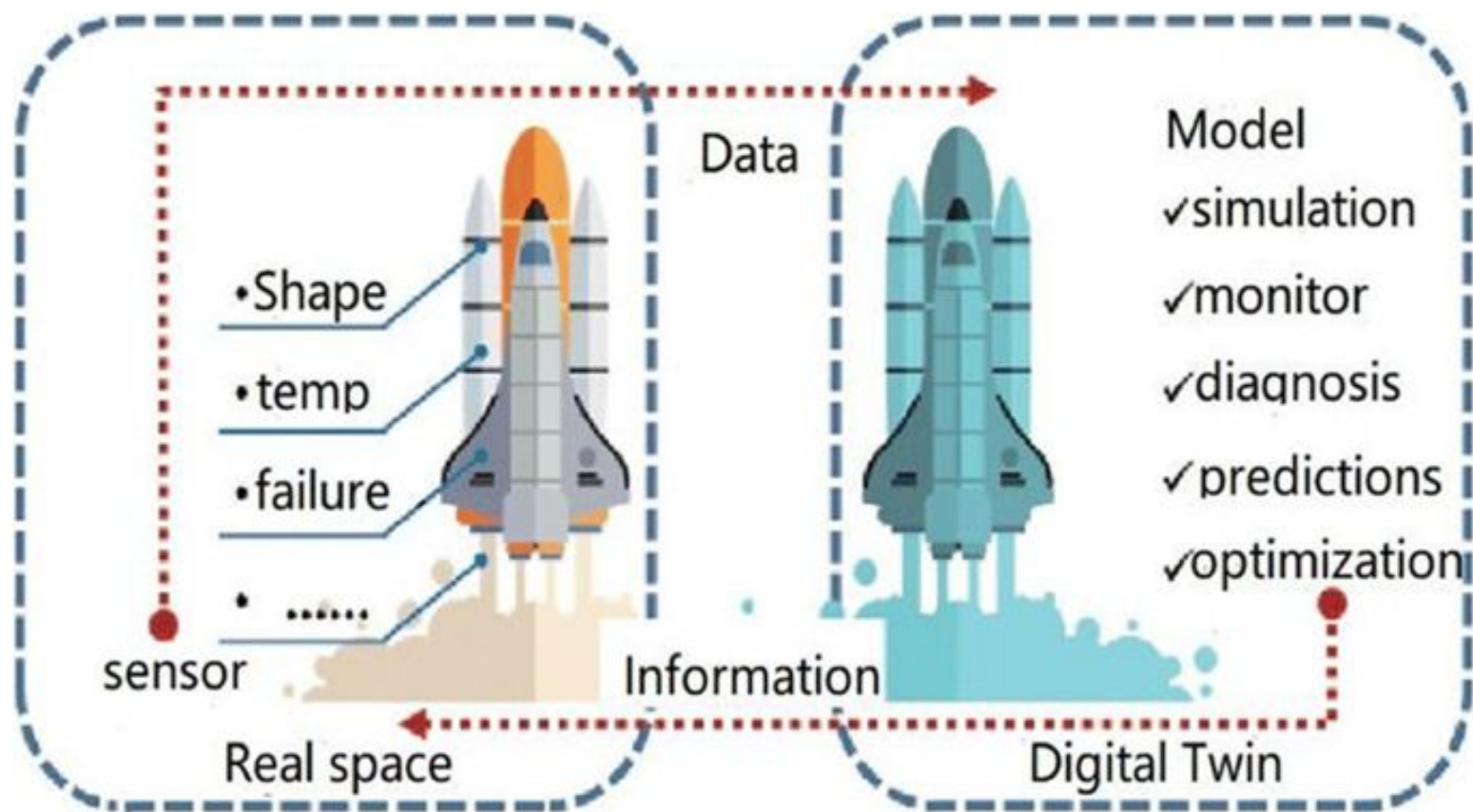


# Digital Twin

A digital twin is a virtual representation of a physical object or system that uses **real-time data** to accurately reflect its real-world counterpart's behavior, performance and conditions.

# Why does the world (and NASA) need digital twins?

*From its origin during NASA's Apollo missions, digital twins today drive everything from personalized medicine to autonomous operations in space by using data to simulate and forecast future behaviors based on what we already know.*



An aerial photograph of a city, likely Vancouver, with a digital twin overlay. The digital twin is a 3D model of the city's buildings and infrastructure, rendered in white, orange, and red. It is positioned over the real-world city, showing a comparison between the physical and digital environments. The text "DIGITAL TWIN: TRANSFORMING CITY PLANNING" is overlaid on the left side of the image.

# **DIGITAL TWIN:** TRANSFORMING CITY PLANNING

Missed the GTC D.C. keynote by Jensen Huang? Watch now to see how AI is powering a new

## Artificial Intelligence

Solutions ▾

Software ▾

Platforms ▾

Use Cases ▾

Develop world foundation models to advance physical AI.

Download from GitHub ↗

Try Now

Front Camera

Overview

Models

Use Cases

Ecosystem

Next Steps

Resources

FAQs

<https://www.nvidia.com/en-us/ai/cosmos/>

### Overview

## What Is NVIDIA Cosmos?

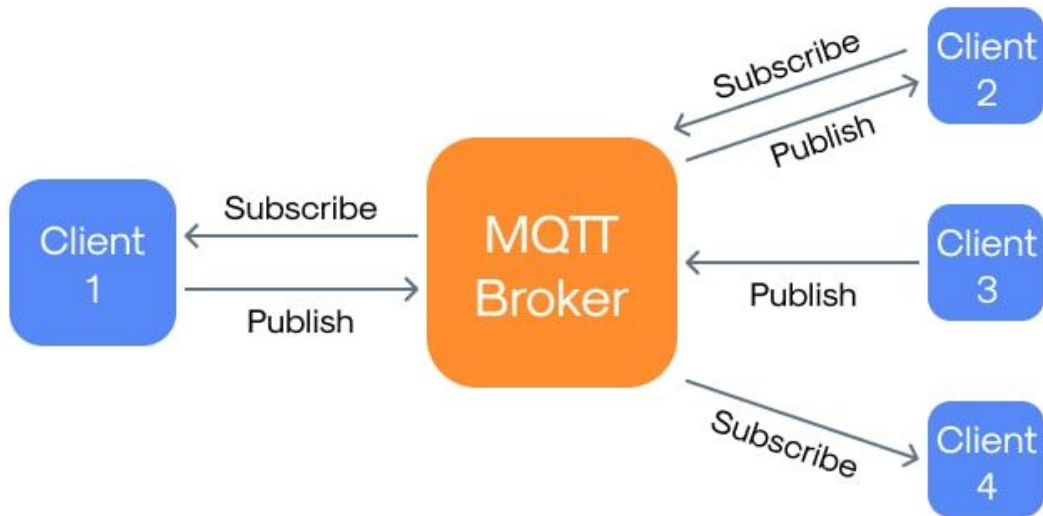
NVIDIA Cosmos™ is a platform purpose-built for physical AI, featuring state-of-the-art generative world foundation models (WFMs), guardrails, and an accelerated data processing and curation pipeline. Developers use Cosmos to accelerate the development of physical AI for autonomous vehicles (AVs), robots, and video analytics AI agents.

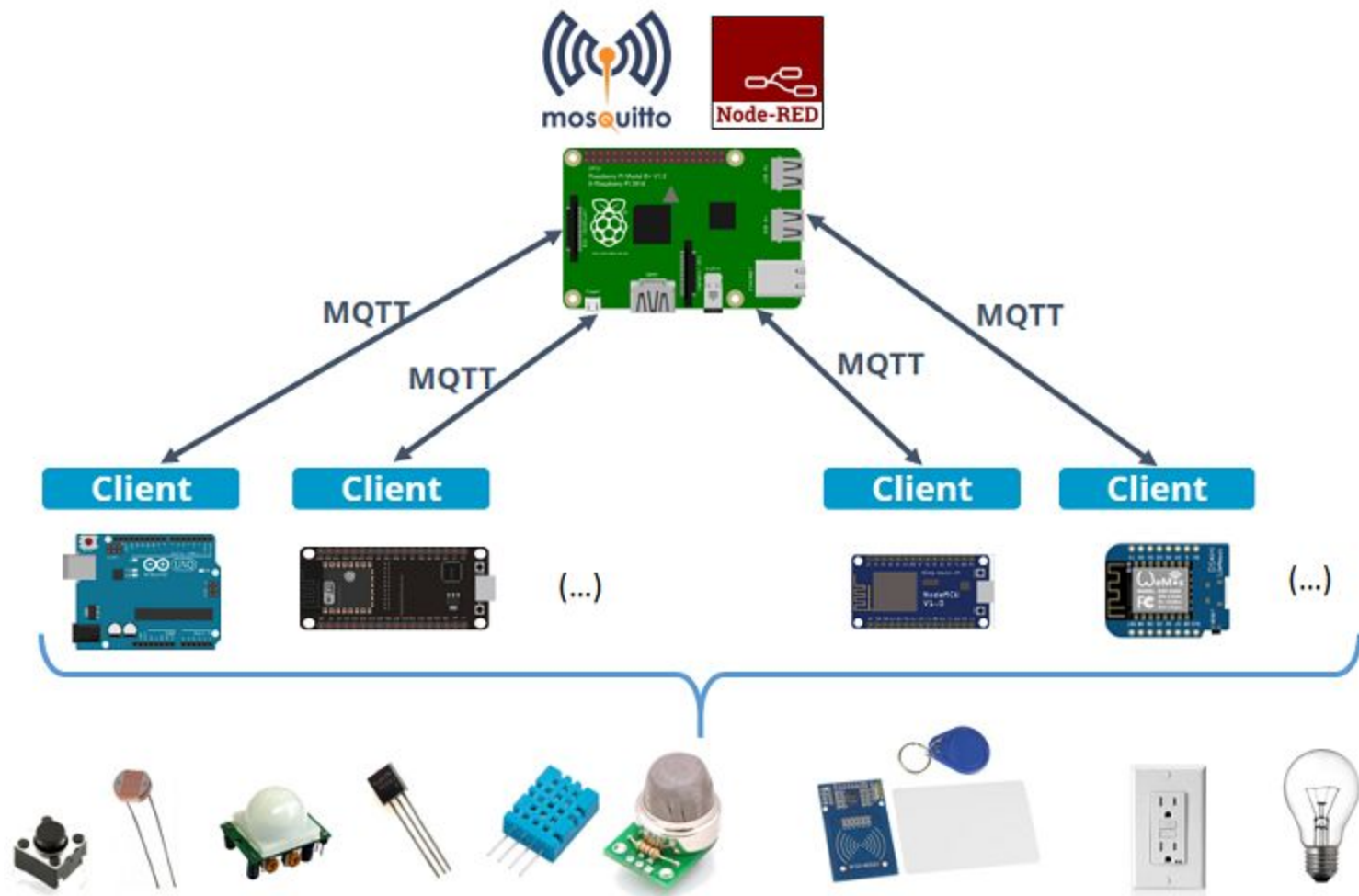


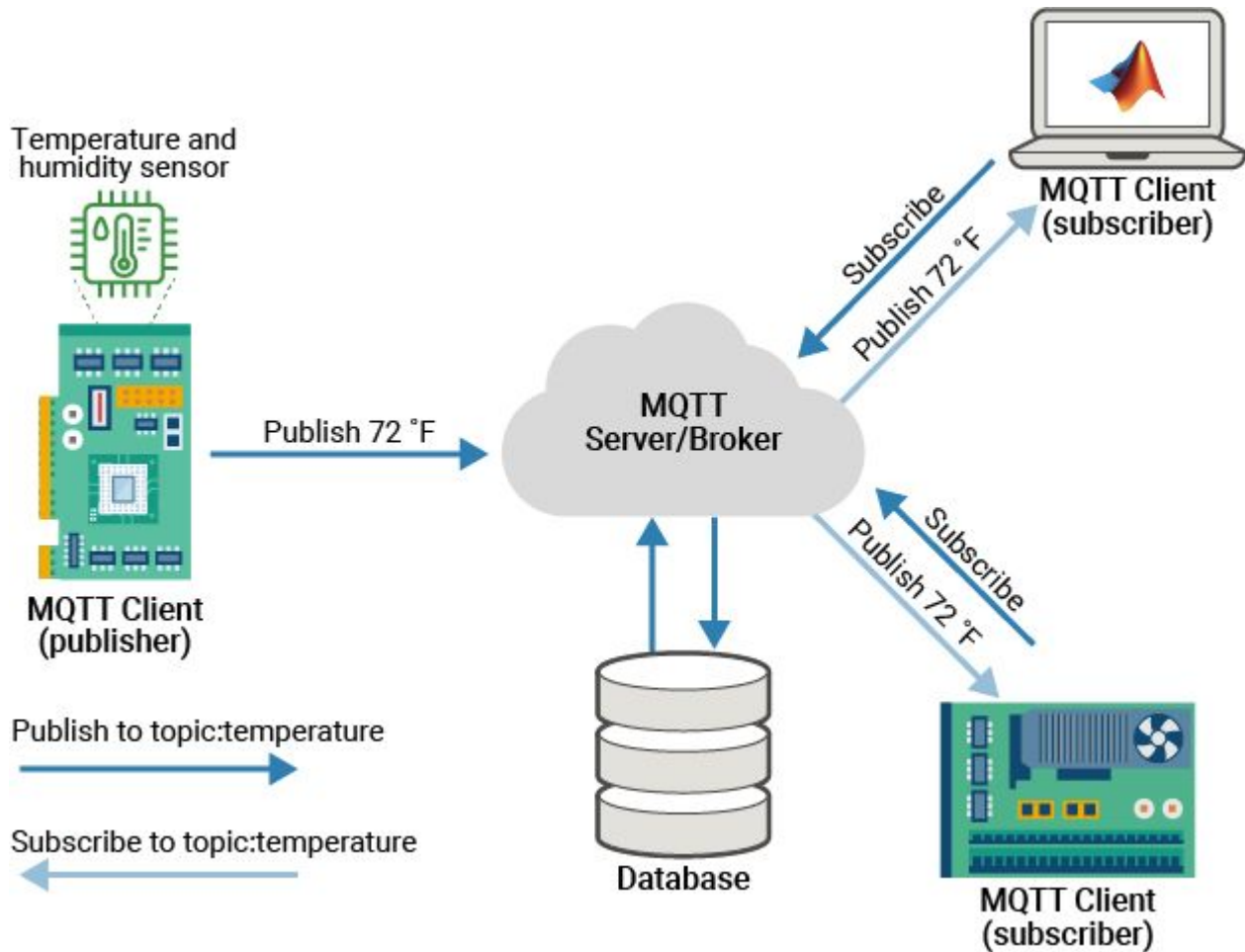
# MQTT for Publish-Subscribe



## MQTT Protocol



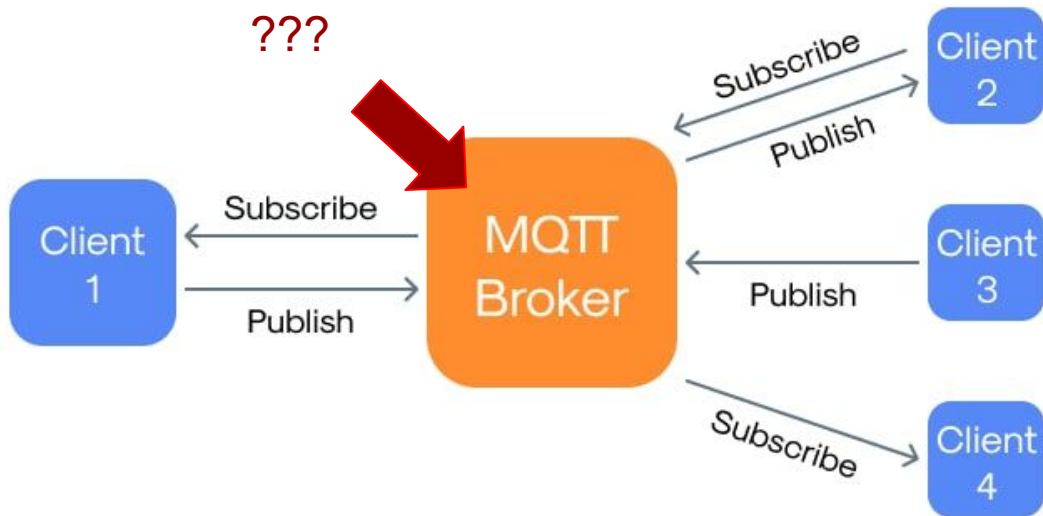


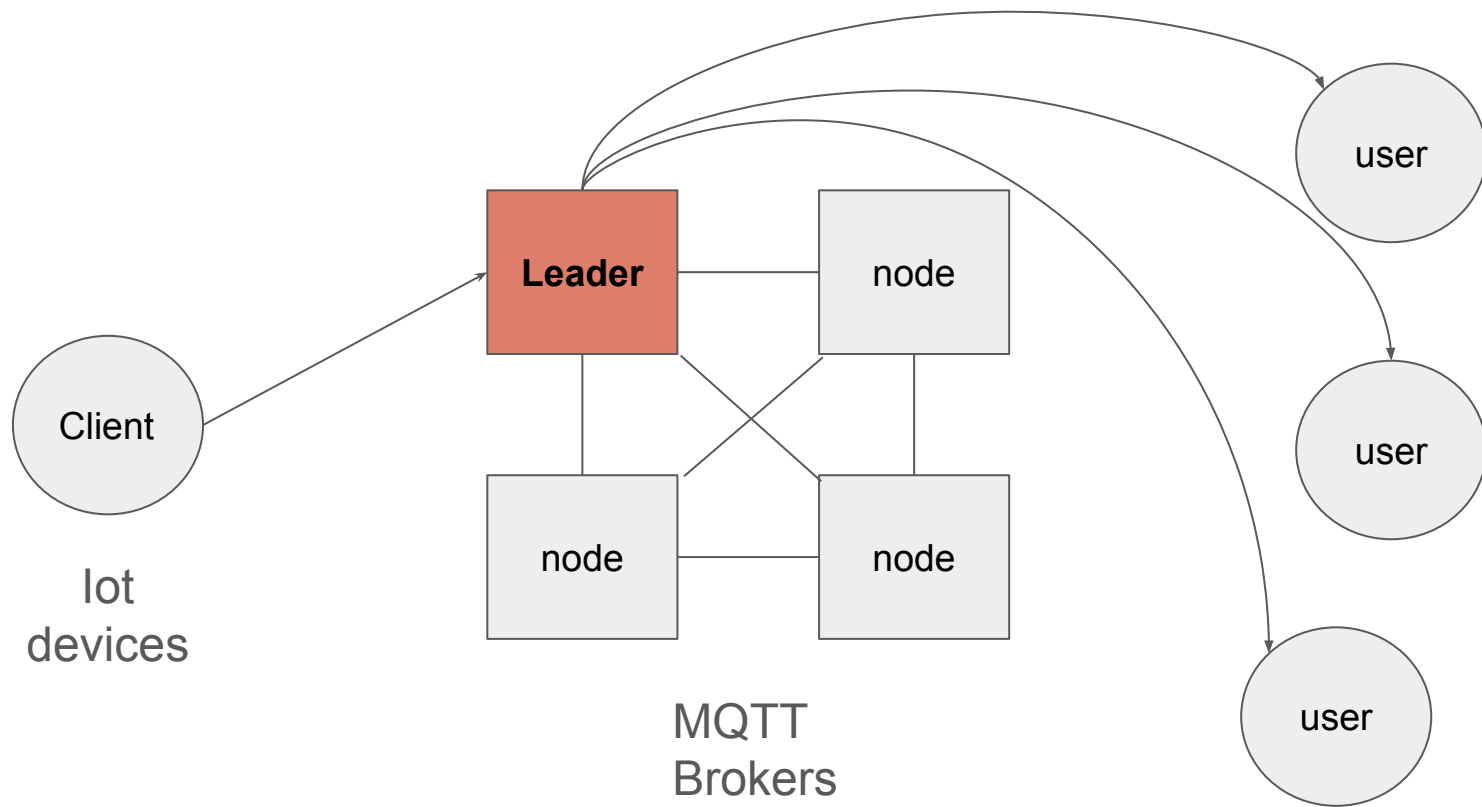


# MQTT for Publish-Subscribe



## MQTT Protocol







# **CSC 116**

## **Dark Web & Deep Web – What's Hidden Online?**

# Dark web

The dark web is a hidden part of the internet, not indexed by search engines, accessed through specialized software like Tor, and used for both **legitimate and illegal activities (trade by Bitcoins)**, including anonymous communication, bypassing censorship, and facilitating illegal transactions.

## SURFACE WEB VS. DEEP WEB VS. DARK WEB

