



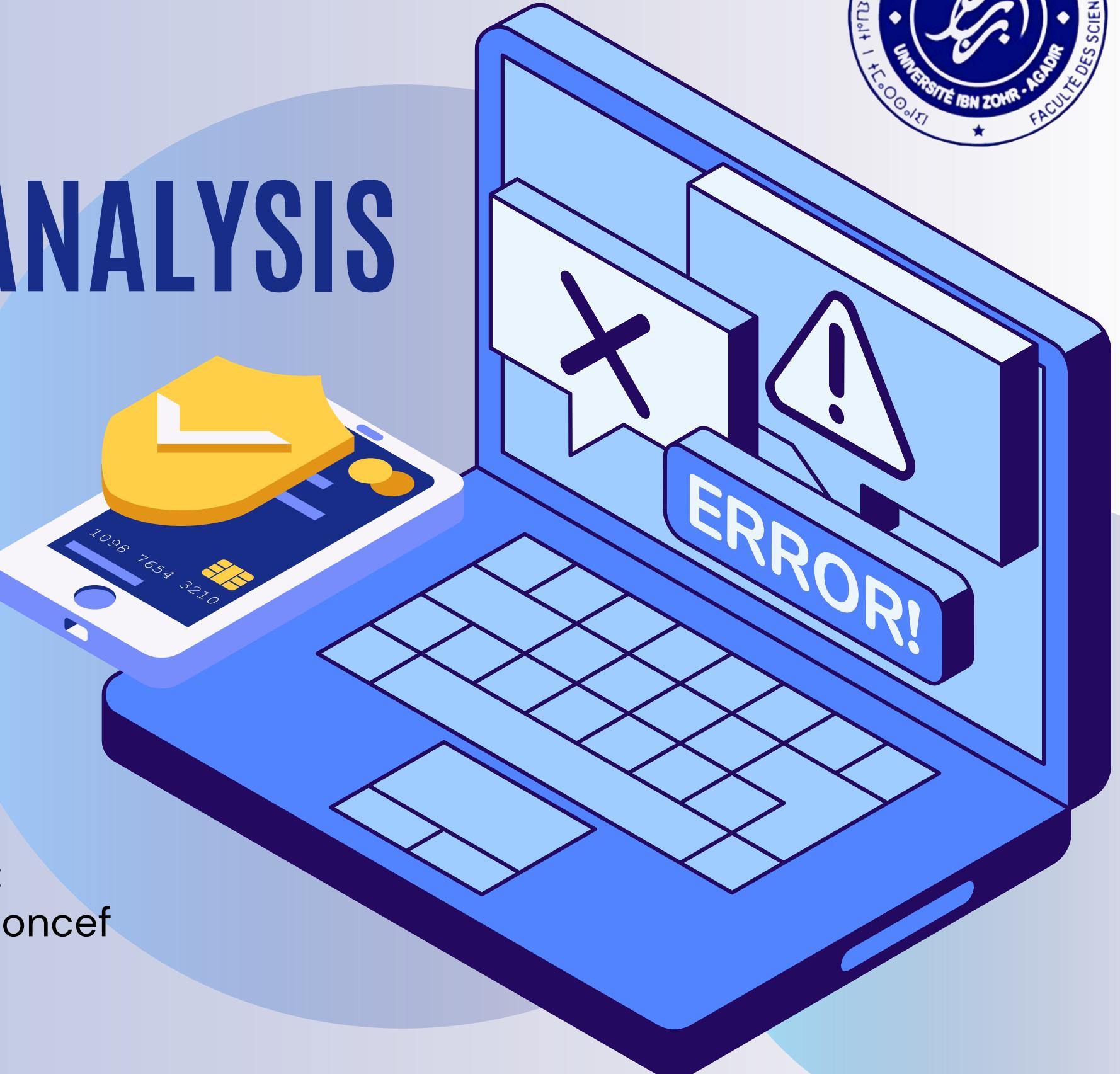
# SMART DEVICE TRAFFIC ANALYSIS

DETECTING UNENCRYPTED MQTT  
COMMUNICATION & DATA LEAKAGE IN  
IOT NETWORKS

**Prepared by:**

Khaoula EL HARRAZ  
Maryem EL-BOUCHTI  
Khawla EL HASSNAOUI  
Oussama GOUSSA

**Supervised by:**  
Prof. BOUGHROUS Moncef





# INTRODUCTION

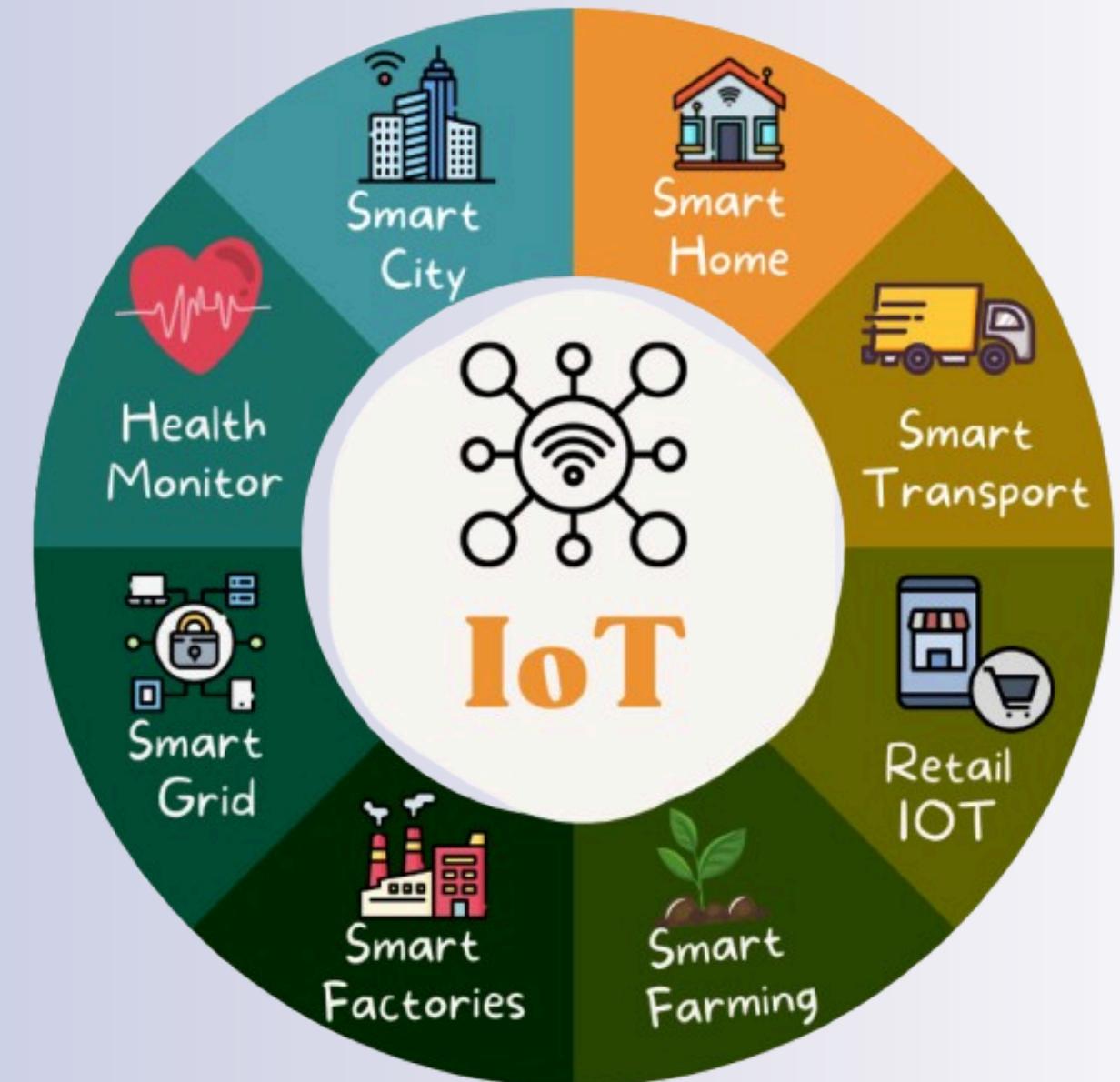
02/10

## IOT CONTEXT

IoT devices are everywhere today—smart homes, industrial sensors, health devices, and more.

Most of them use lightweight communication protocols, especially **MQTT**.

But **MQTT** is not secure by default. When used without encryption, all the data is transmitted in plaintext. This makes IoT systems easy targets for passive sniffing or data interception.



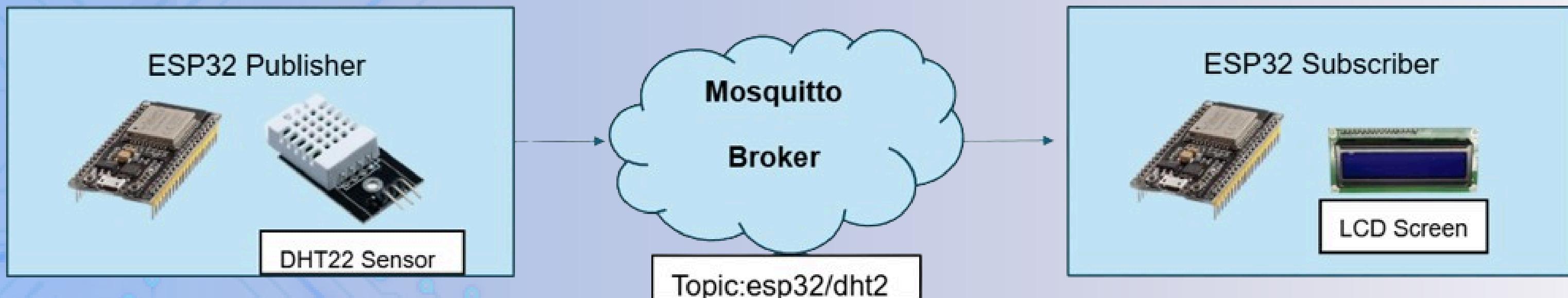
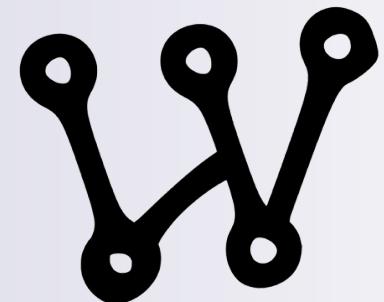


# INTRODUCTION

03/10

## PROBLEM STUDIED

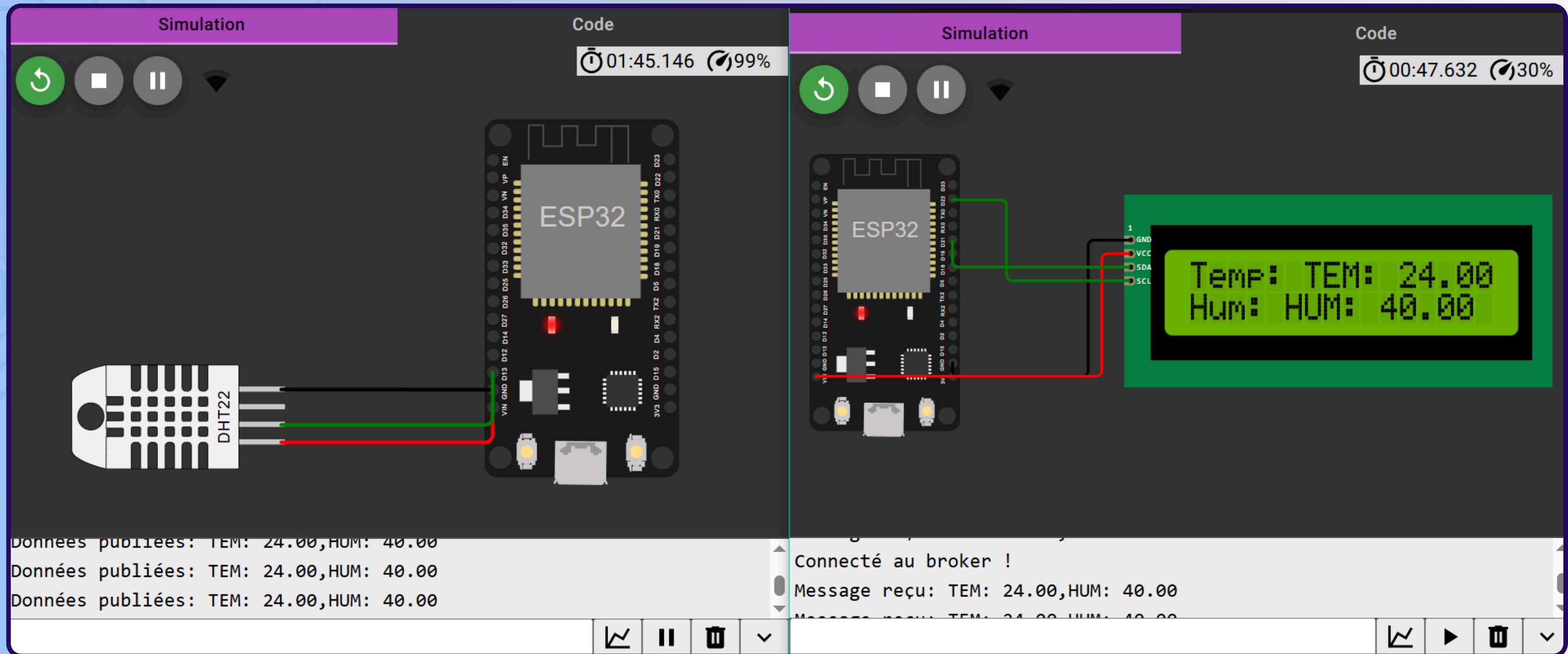
MQTT communication between two ESP32s (DHT22 → LCD)  
tested using Wokwi, Mosquitto, and Wireshark in both  
**unencrypted and TLS-encrypted modes**





# METHODOLOGY

04/10





# DEMONSTRATION

## UNENCRYPTED MQTT

05/10

Wireshark capture of unencrypted **MQTT** traffic. Both the **JSON** payload (temperature and humidity) and the topic are fully visible, showing that all data is transmitted in plaintext and easily readable by anyone on the network.

Topic Length: 11	
Topic: esp32/dht22	
Message: 54454d3a2033392e38302c48554d3a2034392e3030	
0000	08 01 00 00 42 13 37 55 aa 01 24 0a c4 00 01 10
0010	42 13 37 55 aa 01 e0 03 aa aa 03 00 00 00 08 00
0020	45 00 00 4c 00 3a 00 00 40 06 88 11 0a 0a 00 02
0030	36 24 b2 31 e5 a1 07 5b 70 07 f2 ac 34 dc f1 50
0040	50 18 16 70 bd d9 00 00 30 22 00 0b 65 73 70 33
0050	32 2f 64 68 74 32 32 54 45 4d 3a 20 33 39 2e 38
0060	30 2c 48 55 4d 3a 20 34 39 2e 30 30



# SECURITY RISKS OF UNENCRYPTED MQTT

06/10

01

## Confidentiality

Data is sent in plaintext, so anyone on the network can read sensor values and topics.

02

## Integrity (Message Injection)

Since topics are visible and there's no authentication, attackers can publish fake messages to the same topic.



# DEMONSTRATION

07/10

## SECURING MQTT WITH TLS (MQTTSS)

Wireshark capture of **MQTT over TLS**. The payload and topics are fully encrypted, preventing any readable data from being intercepted on the network.

```
Version: TLS 1.2 (0x0303)
Length: 51
Encrypted Application Data: 00000000000000011daaa960d61f10776eaf67d1c3e685de343bc78eb82c408c820fd...
[Application Data Protocol: MQ Telemetry Transport Protocol]

0000 08 01 00 00 42 13 37 55 aa 01 24 0a c4 00 01 10 .....B·7U ·$.....
0010 42 13 37 55 aa 01 40 01 aa aa 03 00 00 00 08 00 B·7U ·@.....·
0020 45 00 00 60 00 11 00 00 40 06 88 26 0a 0a 00 02 E···` .. ·@ ·&.....
0030 36 24 b2 31 c8 d6 22 b3 fc c9 47 29 c3 f4 db c4 6$·1 ·" .. ·G).....
0040 50 18 11 03 32 ed 00 00 17 03 03 00 33 00 00 00 P···2 .. ··3 ·...
0050 00 00 00 00 01 1d aa a9 60 d6 1f 10 77 6e af 67 ···· ··` .. ·wn ·g
0060 d1 c3 e6 85 de 34 3b c7 8e b8 2c 40 8c 82 0f da ····4; ·· ··, @ ·· ··
0070 70 49 ce ac 40 74 b4 20 e0 63 bc e5 e6 5c 29 b9 pI ··@t ·· ·c ·· \) ··
```



# MQTT VS. MQTTS - BEFORE AND AFTER

08/10

Aspect	MQTT (Unencrypted)	MQTTS (TLS)
Payload	Readable in plaintext	Encrypted
Topic	Visible	Hidden
Sniffing	Easy to intercept	Not readable
Authentication	No authentication	TLS authentication
Confidentiality	Compromised	Restored

# CONCLUSION



Communication is the most important aspect of any IoT system, but using MQTT alone puts the data at risk. Without encryption, all messages and topics can be intercepted or modified by attackers.

This is why securing MQTT with TLS is essential, as it encrypts the communication and protects both payloads and topics, greatly improving the security of IoT systems.



THANK  
YOU!

