plain]

plain]

ETSETB – Grau en Enginyeria de Tecnologies i Serveis de Telecomunicació

[

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Tècnica Superior d'Enginyeria
de Telecomunicació de Barcelona

# Deployment of a security testbed for IoT

Treball de Fi de Grau
presentat a l'Escola Tècnica Superior
d'Enginyeria de Telecomunicació de Barcelona
de la Universitat Politècnica de Catalunya
per

Joel Otero Masplà

En compliment parcial
dels requisits per a l'obtenció del
**Grau en Enginyeria de Tecnologies i Serveis de Telecomunicació**

Director/a: Olga León Abarca
Ponent: *{Nom del ponent (si s'escau)}*

Barcelona, Maig de 2025

# Resum

Cada exemplar del Treball de Fi de Grau (TFG) ha de contenir un Resum, que és un breu extracte del TFG. En termes d'estil, el Resum hauria de ser una versió reduïda del projecte: una introducció concisa, un compendi dels resultats i les principals conclusions o arguments presentats en el projecte. El Resum no ha de superar les 150 paraules i cal que estigui traduït al català, castellà i anglès.

# Resumen

Cada ejemplar del Trabajo de Fin de Grado (TFG) debe incluir un Resumenque es un breve extracto del TFG. En cuanto al estilo, el Resumen debería ser una versión reducida del proyecto: una introducción breve, un resumen de los resultados principales y las conclusiones o argumentos principales presentados en el proyecto. El Resumen no debe exceder las 150 palabras y debe estar traducido al catalán, castellano e inglés.

# Summary

Each copy of the Bachelor's Thesis (TFG) must include a Summary, which is a concise abstract of the TFG. In terms of style, the Summary should be a condensed version of the project: a brief introduction, a summary of the main results, and the conclusions or key arguments presented in the project. The Summary should not exceed 150 words and must be translated to catalan, spanish and english.

*Podeu incloure una pàgina de Dedicatòries just abans de la pàgina d'Agraïments, però no és un requisit.*

# Agraïments

És apropiat, però no obligatori, declarar l'extensió de l'ajuda aportada per persones de l'*staff*, companys/companyes d'estudis, tècnics/ques o altres en la col·lecció de dades, disseny i construcció del prototip, l'anàlisi de dades, l'execució dels experiments i la preparació del projecte (incloent l'ajuda editorial). A més a més, és apropiat reconèixer la supervisió i la direcció donada pel tutor/a.

# Historial de revisió i aprovació

| Revisió | Data | Autor(s) | Descripció |
|---|---|---|---|
| 1.0 | dd/mm/yyyy | AME | Creació del document |
| 1.1 | dd/mm/yyyy | AME, JPV | Correcció d'errors |
| 2.0 | dd/mm/yyyy | AME, MLO | Versió revisada |
| 4.0 | dd/mm/yyyy | AME | Versió final |
| | | | |

**LLISTA DE DISTRIBUCIÓ DEL DOCUMENT**

| Rol | Cognom(s) i Nom |
|---|---|
| [Estudiant] | |
| [Director del projecte] | |
| [Director 2 (si aplica)] | |

| **Escrit per:** | | **Revisat i aprovat per:** | |
|---|---|---|---|
| Data | dd/mm/yyyy | Data | dd/mm/yyyy |
| Nom | Xxxxxxx Yyyyyyy | Nom | Xxxxxxx Yyyyyyy |
| Rol | Autor del projecte | Rol | Director del projecte |

# Índex

# Índex de figures

# Índex de taules

# Sigles i acrònims

[

CAPÍTOL 1

# Introducció

Una Introducció que estableix clarament la justificació de la tesi que inclogui:

1. Objectius del treball.
2. Requisits i especificacions.
3. Mètodes i procediments, citant si aquest treball és una continuació d'un altre projecte o utilitza aplicacions, algoritmes, programari o maquinari desenvolupat anteriorment per altres autors.
4. Pla de treball amb tasques, fites i un diagrama de Gantt.
5. Descripció de les desviacions del pla inicial i incidències que poden haver ocorregut.

Els capítols mínims que aquest document de TFE hauria de tenir es descriuen a continuació; no obstant això, poden tenir noms diferents i es poden afegir més capítols.

## 1.1 Objectius del treball

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

## 1.2 Requisits i especificacions

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

## 1.3 Mètodes i procediments

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

## 1.4 Pla de treball

Normalment les figures i taules es col·loquen en els entorns `\figure` i `\table`, que poden flotar lliurement en el document. Pots identificar cada flotant amb un `\label`

CAPÍTOL 2

# Estat de l'art

## 2.1 Internet of Medical Things (IoMT)

L'Internet of Medical Things (IoMT) és una branca específica de l'Internet de les Coses (IoT) aplicada a l'àmbit sanitari. Consisteix en una xarxa creixent de dispositius mèdics intel·ligents que poden recopilar, processar i transmetre dades clíniques amb l'objectiu de millorar la qualitat assistencial, facilitar el monitoratge de pacients i optimitzar els processos hospitalaris.

Aquest ecosistema connectat inclou una gran varietat de dispositius, que poden ser tant portables com fixes, i que cobreixen des del seguiment de signes vitals fins al control automatitzat de tractaments. Alguns exemples habituals són:

- **Monitors cardíacs:** permeten controlar l'activitat del cor de manera contínua.
- **Pulsòmetres i termòmetres intel·ligents:** ofereixen dades precises i fàcilment accessibles.
- **Inhaladors i bombes d'insulina intel·ligents:** poden registrar l'ús i ajudar a ajustar el tractament.
- **Implants mèdics connectats:** permeten registar l'estat d'un pacient a temps complert. Per exemple marcapassos o neuroestimuladors.
- **Sistemes de dosificació automàtica de medicació:** especialment útils en pacients amb malalties cròniques.
- **Equips hospitalaris intel·ligents:** com llits monitoritzats o sistemes de seguiment de pacients dins d'unitats de cures intensives.

El creixement de l'IoMT s'ha vist impulsat per diversos factors, com la miniaturització dels sensors, el progrés tecnològic en dispositius mèdics, l'augment de la digitalització sanitària, i la necessitat creixent de models d'atenció centrats en el pacient i orientats a la prevenció i el seguiment continuat. A més, la pandèmia de la COVID-19 va accelerar

l'adopció de solucions de monitoratge remot, que han consolidat l'ús d'aquest tipus de dispositius fora dels entorns hospitalaris convencionals.

L'ús generalitzat d'aquesta tecnologia permet una atenció més personalitzada i basada en dades, alhora que facilita la detecció precoç de complicacions i una millor gestió dels recursos sanitaris. També contribueix a reduir la necessitat de desplaçaments i hospitalitzacions, millorant l'accessibilitat a l'atenció mèdica, especialment en zones rurals o amb menys infraestructures.

Amb una adopció creixent tant en entorns clínics com domèstics, s'espera que l'IoMT sigui una peça clau en la transformació digital del sistema sanitari en els pròxims anys, aportant beneficis tant per als pacients com per als professionals de la salut. [6]

## 2.2 Seguretat en entorns IoMT

Donat el creixement de l'us de dispositius IoMT, aquesta mateixa expansió comporta un augment significatiu de la superfície d'exposició a ciberatacs. A més a més, s'espera que a mesura que avança la seva adopció, aquests dispositius siguin més determinants en les tasques mèdiques, la qual cosa pot impilcar una major criticitat en cas de ciberatac.

A diferència dels sistemes informàtics convencionals, els dispositius IoMT sovint operen en entorns amb recursos computacionals limitats (processador, memòria, energia), i moltes vegades han estat dissenyats amb una orientació funcional, no pas de seguretat. Això els fa especialment vulnerables a atacants que poden es poden aprofitar de configuracions per defecte, manca d'actualitzacions, credencials febles o vulnerabilitats en els protocols de comunicació. A més, la connexió d'aquests dispositius mitjançant xarxes Wi-Fi o altres canals sense fils exposa el sistema a atacs com l'escolta (sniffing), suplantació de dispositius (spoofing), atacs de denegació de servei (DoS) entre altres.

Un dels aspectes més crítics del risc en entorns IoMT és la naturalesa de les dades que gestionen. Les dades mèdiques són altament sensibles i personals. Un accés no autoritzat pot vulnerar drets fonamentals com la privacitat i tenir conseqüències legals greus per a les institucions sanitàries. En aquest context, la ciberseguretat en l'àmbit IoMT no es pot considerar un afegit posterior al desplegament dels sistemes, sinó un requisit fonamental des de la fase de disseny. Això, és especialment rellevant en entorns on les conseqüències d'un atac poden tenir un impacte directe sobre la salut i la seguretat física dels pacients.

Però, és important destacar que la protecció dels sistemes IoMT també ha de ser escalable i adaptable. L'amenaça no és estàtica, i els vectors d'atac evolucionen constantment.

Davant d'aquesta realitat, la recerca en ciberseguretat per a l'IoMT s'està orientant cada cop més cap a solucions dinàmiques, com ara IDS/IRS basats en aprenentatge automàtic que permetin detectar patrons anòmals de comportament i actuar de forma proactiva. En aquest sentit, la generació de datasets reals que simulin tant trànsit legítim com maliciós en entorns IoMT esdevé una peça clau per entrenar i validar aquestes solucions emergents. Aquestes solucions han estat tractades en artícles com [1]. També la caracterització de

vulnerabilitats connegudes ha estat tractada en artícles com [23] o [20] que han estat utlitzats com a referència per a la recopliació d'atacs i la generació de datasets.

## 2.3 Message Queuing Telemetry Transport (MQTT)

El Message Queuing Telemetry Transport (MQTT) és un protocol de missatgeria lleuger dissenyat per a la comunicació entre dispositius amb recursos limitats en xarxes poc fiables o amb amplada de banda reduïda. Aquest protocol s'ha convertit en un estàndard de facto en moltes aplicacions IoT, inclòs l'àmbit de l'Internet of Medical Things (IoMT), per la seva eficàcia, simplicitat i facilitat de desplegament.

Desenvolupat originalment per IBM l'any 1999, MQTT segueix un model de comunicació publish/subscribe, que afavoreix la desconnexió temporal dels nodes i la minimització de l'ús de la xarxa, dos requisits habituals en xarxes IoT.

En una arquitectura MQTT, el component central és el broker, un servidor que actua com a intermediari entre els dispositius que publiquen dades (publishers) i els que les reben (subscribers). Els dispositius no es comuniquen directament entre ells, sinó que ho fan a través del broker, que rep els missatges publicats en un tema determinat (tòpic) i els redirigeix als clients que s'han subscrit a aquest tema. Aquesta arquitectura desacoblada simplifica el disseny de sistemes escalables i resilients. A l'àmbit IoMT, aquesta estructura és especialment útil per gestionar sensors mèdics que generen dades de manera periòdica, com ara nivells de glucosa, senyals d'electrocardiograma (ECG), o mesures de tensió arterial. Aquests sensors poden publicar lectures de manera eficient al broker MQTT, i altres components del sistema (com bases de dades, aplicacions clíniques o sistemes d'alerta) poden consumir aquesta informació segons les seves necessitats.

El protocol MQTT opera habitualment sobre TCP/IP, utilitzant el port 1883 per a connexions no segures i el port 8883 quan es fa servir TLS (Transport Layer Security) per protegir la transmissió. Entre les característiques tècniques més destacades d'MQTT, podem ressaltar:

- **Qualitat del servei (QoS):** MQTT ofereix tres nivells de abilitat en el lliurament de missatges, cosa que permet ajustar el comportament segons els requisits de l'aplicació.
- **Sessions persistents:** Un missatge es pot marcar com a retained perquè quedi emmagatzemat al broker i sigui enviat automàticament als nous subscriptors del topic. Això permet garantir que les dades més recents estiguin disponibles en tot moment, encara que el dispositiu que les va enviar originalment ja no estigui actiu.
- **Protocol lleuger:** Amb una capçalera mínima de només 2 bytes, MQTT genera molt poca sobrecàrrega, cosa que el fa extremadament ecient per dispositius amb CPU limitada, poca memòria RAM o connexions de xarxa inestables o intermitents.
- **Model desacoblat (publish/subscribe):** Els clients no necessiten conèixer ni l'adreça ni l'estat dels altres dispositius. Això facilita l'escalabilitat i la fexibilitat

del sistema, ja que els rols de publicador i subscriptor poden canviar dinàmicament.

- **Jerarquia de temes (topics):** Els topics MQTT segueixen una estructura jeràrquica cosa que permet l'ús de comodins ("+","#"), fet que proporciona una gran fexibilitat, però també pot ser explotat maliciosament si no es controla adequadament.

Malgrat aquests avantatges, el protocol MQTT no està pensat amb la seguretat com a objectiu principal, cosa que el fa vulnerable en entorns crítics com l'IoMT si no s'hi afegeixen mecanismes de protecció. Les principals limitacions de seguretat inclouen:

- **El broker com a punt crític:** El broker MQTT és un únic punt de fallada. Si és compromès o queda saturat, tota la infraestructura de comunicació es veu afectada.

- **Flooding i sobrecàrrega:** Un ús malitencionat del QoS i grans volums de dades, poden causar sobrecàrregues en el broker i saturar el sistema.

- **Control d'accés deficient:** En moltes implementacions, si no es configuren polítiques d'ACL (Access Control List), qualsevol client pot publicar o subscriure's a qualsevol tema.

- **Manca d'autenticació forta:** MQTT deneix només un sistema bàsic d'autenticació mitjançant username i password, sense mecanismes d'autenticació mútua ni suport nadiu per a protocols d'identitat moderna (com OAuth 2.0). Si el canal de comunicació no es protegeix amb TLS/SSL, tant les dades com les credencials es transmeten en text pla.

- **Lack of message integrity:** Si no s'utilitza TLS, tampoc hi ha garanties que els missatges no hagin estat modificats durant el trànsit.

Donada la seva extensió en entorns IoT i les seves característiques adaptades a dispositius amb recursos limitats, MQTT s'ha triat com a protocol principal per a la simulació de trànsit en aquest treball. El seu ús permet generar escenaris tant de comunicació legítima com maliciosa, en els quals es poden observar comportaments anòmals mitjançant eines d'anàlisi i detecció. Això facilita la creació de datasets realistes per a l'entrenament d'IDS basats en IA.

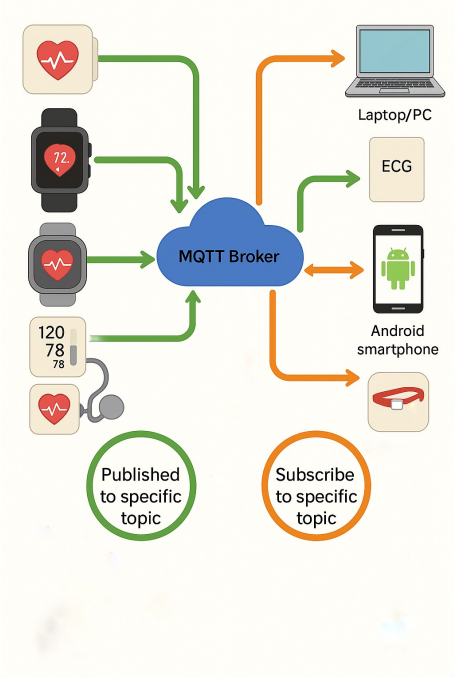


**Figura 2.1:** *Protocol MQTT en un entorn IoMT. Imatge extreta de [7] i adaptada amb intel·ligència artificial.*

## 2.4 Altres protocols en l'entorn IoMT

Pel que fa a altres protocols, tot i que MQTT és el protocol principal emprat en aquest treball, també es considera l'ús del protocol Constrained Application Protocol (CoAP) com a alternativa o complement en la generació de trànsit. CoAP és un protocol pensat específicament per a dispositius amb recursos limitats en xarxes IoT. Funciona sobre UDP, cosa que li proporciona una latència molt baixa i un comportament lleuger, tot i que això també comporta certes limitacions pel que fa a la fiabilitat de la transmissió.

CoAP segueix un model client-servidor similar a HTTP però optimitzat per a entorns embeguts. Utilitza mètodes com GET, POST, PUT i DELETE, i permet observar recursos mitjançant un sistema d'actualitzacions automàtiques (observe). A diferència de MQTT, que és orientat a un model (publish/subscribe), CoAP és més adequat per a interaccions puntuals o consulta de recursos puntuals. En aquest treball, l'ús de CoAP es contempla per generar variabilitat en els escenaris de comunicació i per comparar comportaments de trànsit entre protocols amb estructures diferents. Això pot enriquir el dataset resultant i millorar la capacitat de generalització del sistema d'IA per a la detecció d'intrusions.

En l'entorn mèdic, també són utilitzats altres protocols d'aplicació com HTTP/HTTPS o bé Extensible Messaging and Presence Protocol (XMPP) Pel que fa a protocols de capa física, també es fa servir Bluetooth Low Energy (BLE), Near Filed Communication (NFC) o bé dades cel·lulars com NB-IoT que no seran usats en aquest treball.

## 2.5 Eines per a la simulació i anàlisi de trànsit en entorns IoMT

Per a la realització d'aquest treball s'han emprat diverses eines de codi obert, escollides pel seu suport ampliat en entorns de xarxa, la seva flexibilitat i la possibilitat d'automatitzar proves i captures de trànsit en entorns simulats. Algunes d'aquestes eines tenen un enfocament general i són àmpliament utilitzades en proves de penetració en xarxes IP tradicionals, mentre que d'altres presenten característiques específiques que les fan especialment adequades per a entorns IoT o IoMT. A continuació es descriuen les principals fetes servir en aquest projecte:

### 2.5.1 Mosquitto

Mosquitto és una de les implementacions més conegudes del protocol MQTT. Es tracta d'un broker MQTT lleuger, de codi obert i altament configurable i compatible amb les especificacions MQTT 3.1 i 5.0 que permet la configuració de les funcionalitats bàsiques del protocol com definir tòpics, limitacions en l'ús de recursos, ACLs I encriptat TLS. També permet desplegar clients MQTT mitjançant mosquitto-clients i poder realitzar el procés de subscriure's a un tòpic en un broker concret (mosquitto-sub) on publicar missatges en aquest tòpic (mosquitto-pub). Adicionalment, disposa de les configuracions bàsiques de MQTT com els paràmetres de QoS, retain o presistance. [11]

En l'entorn acadèmic, la seva simplicitat fa que sigui una excel·lent opció per a desplegar laboratoris d'IoMT.

### 2.5.2 Docker

Docker és una plataforma de virtualització lleugera basada en contenidors que permet desplegar entorns complexos de manera ràpida, reproduïble i aïllada. Els seus principals avantatges són: [2]

- **Escalabilitat i control:** És possible desplegar ràpidament desenes de dispositius virtuals, amb configuracions personalitzades, IPs xes i comportaments diferenciats.
- **Ús d'orquestradors:** Gràcies a Docker Compose, es poden definir tots els serveis i la seva configuració en un sol fitxer YAML, cosa que permetent la reproducció exacta de l'escenari en qualsevol màquina o entorn.
- **Monitoratge de xarxa simplificat:** Docker permet definir xarxes virtuals internes, facilitant la simulació d'una infraestructura complexa.

### 2.5.3 Kali Linux

Kali Linux és una distribució basada en Debian orientada específicament a seguretat informàtica i proves de penetració (pentesting). Mantinguda per l'equip d'Offensive Security (OFSEC), Kali proporciona un entorn completament equipat amb centenars

d'eines preinstal·lades per a l'auditoria de xarxes, anàlisi de vulnerabilitats, enginyeria inversa, sniffing, spoofing, explotació i forense digital. [24]

En aquest treball, Kali Linux s'ha utilitzat com a sistema operatiu base per dur a terme les diferents fases de l'atac, simulant el comportament d'un atacant actiu dins la xarxa IoMT. Aquesta elecció es basa en diversos avantatges claus:

- **Gran nombre d'eines incloses:** Kali inclou eines com Nmap, Masscan, Wireshark, tcpdump, Scapy, aprscan i moltes més, facilitant la realització de proves diverses sense necessitat d'instal·lació addicional.
- **Entorn controlat i configurable:** Kali pot executar-se de manera virtualitzada (en aquest treball s'ha utilitzat en contenidors Docker), fet que permet recrear escenaris controlats i aïllats per a la simulació d'atacs sense posar en risc cap sistema real.
- **Actualitzacions contínues i suport actiu de la comunitat:** Es tracta d'una distribució mantinguda amb freqüència, compatible amb la majoria d'arquitectures, i àmpliament utilitzada tant en àmbits acadèmics com professionals.
- **Automatització i scripting:** El seu entorn Unix-like facilita l'ús d'scripts en bash o python per automatitzar atacs, recollir trànsit o llançar seqüències repetitives d'accions

### 2.5.4 Nmap

Nmap (Network Mapper) és una eina de "network reconnaissance" i auditoria de xarxes molt utilitzada en l'àmbit del pentesting. Permet identificar dispositius connectats a una xarxa, descobrir serveis oberts, detectar sistemes operatius i obtenir informació sobre les possibles vulnerabilitats de cada node mitjançant scripts NSE personalitzats. [22]

### 2.5.5 TCPDump

TCPDump és una eina de línia de comandes per a la captura i anàlisi de paquets a nivell de xarxa. Es tracta d'una eina fonamental en entorns de recerca i pentesting, ja que permet registrar amb precisió tot el trànsit que circula per una interfície de xarxa en temps real. [3]

TCPDump permet capturar trànsit benigne i maliciós entre dispositius de la xarxa i crear arxius de captura amb extensió pcap. És una eina similar a Wireshark, però més lleugera, utilitzada a través de terminal i amb capacitat de ser feta servir en automatitzacions.

CAPÍTOL 3

# Metodologia / desenvolupament del projecte

En aquest capítol es detallarà la metodologia emprada en la realització del treball. Té com a objectiu oferir un compte detallat de les aproximacions i tècniques utilitzades, assegurant la replicabilitat i el rigor acadèmic. No només cobrirà els mètodes de recerca i tècniques de mesurament emprats, sinó que també aprofundirà en les especificitats del desenvolupament de programari i maquinari. Tant si el projecte implica anàlisi qualitativa, mesuraments quantitatius, modelatge computacional com prototipatge físic, aquest capítol hauria d'elucidar com contribueix cada component als objectius generals.

A més de descriure els mètodes en si mateixos, el capítol també proporcionarà justificacions per què es van escollir mètodes particulars enfront d'altres. Per exemple, podria explicar la tria d'un llenguatge de programació específic, prova estadística o configuració experimental. El capítol també abordarà les limitacions de la metodologia i com aquestes s'han mitigat o tingut en compte. Els lectors haurien de sortir amb una comprensió clara de com s'ha dut a terme el desenvolupament del projecte, per què s'han escollit determinades opcions i com aquests mètodes serveixen per complir els objectius establerts inicialment.

## 3.1 Escenari utilitzat

L'escenari presentat en aquest treball està inspirat en el que s'utilitza en el Treball: *"«MIoTTA-UPC: Testbed MIoT Configurable para la Evaluacion de Algoritmos de Detección de Ciberataques Basados en Inteligencia Artificial» "* [29] . L'objectiu principal és poder generar un banc de dades que contingui paquets benignes i maliciosos de diferents atcas per a entrenar un sistema de detecció d'intrusions (IDS) basat en intel·ligència artificial que classifiqui si aquest tràfic és benigne o maliciós. La programació, desplegament i entrenament d'aquest IDS no formen part d'aquest treball. Per a generar aquest testbed és necessari simular atacs coneguts per a una infraestructura com utilitzada de manera realista i amb un escenari que reprodueixi adequadament unes condicions reals.

## 3.2 Topologia general

Per a la generació i captura del tràfic de xarxa en un IoMT (Internet of Medical Things), s'ha dissenyat i desplegat un escenari experimental que simula una habitació d'hospital interconnectada amb un servidor central i altres dispositius de suport clínic. Aquest entorn busca reproduir amb fidelitat un ecosistema típic d'atenció sanitària digitalitzada, incloent-hi sensors mèdics, passarel·les de comunicació, equips de monitoratge i possibles actors maliciosos.

L'escenari està basat en una xarxa LAN Wi-Fi irradiada amb un Access Point, en la qual s'hi connecten tots els dispositius, encara que també pot contenir trams Ethernet si és necessari. Entre els dispositius utilitzats es considera:

- **Clients MQTT:** Aquests clients són sensors com ara oxímetres, monitors de ritme cardíac, bombes d'infusió, sensors de glucosa, tensiòmetres o altres sensors utilitzats en l'entorn mèdic. Aquests clients poden actuar tant transmetent informació a altres dispositius com esperant rebre'n o ambdues a la vegada. Una part d'aquests dispositius, s'implementarà de forma simulada i injectada a la xarxa a través d'un node comú, ja que es tracta de dispositius amb gran cost econòmic. En aquest treball s'utilitzarà Docker com és explicat en apartats posteriors.

- **Broker MQTT:** Connectat a la xarxa, es disposa d'un servidor o broker MQTT amb el el qual s'hi connecten sigui per enviar o rebre informació tots els clients de la xarxa. Actua com un organisme central de la informació i un punt crític de la xarxa.

- **Atacant:** Dintre aquesta xarxa Wi-Fi, se suposa que es connecta un dispositiu atacant, el qual realitza diversos atacs cap als altres components de la xarxa.

- **Monitor de trànsit:** S'hi connecta un monitor que captura tot el trànsit dins la xarxa visible des de la seva posició. Aquest actua de forma passiva escoltant tot el trànsit que circula i recopilant tota la informació possible per tal generar el *testbed*, que és el principal objectiu del treball.

- **Ordinadors I servidors:** Se suposa que en aquesta xarxa hi poden haver connectats altres dispositius que no són especialment utilitzats en l'entorn IoMT com per exemple altres servidors hospitalaris o ordinadors.

Dintre aquest escenari, el meu treball se centra en l'apartat de la generació de trànsit simulat així com en l'elaboració d'atacs des de la perspectiva de desplegar clients simulats i fer-los interactuar amb la xarxa real. L'objectiu principal del treball no ha estat la implementació d'aquesta xarxa.

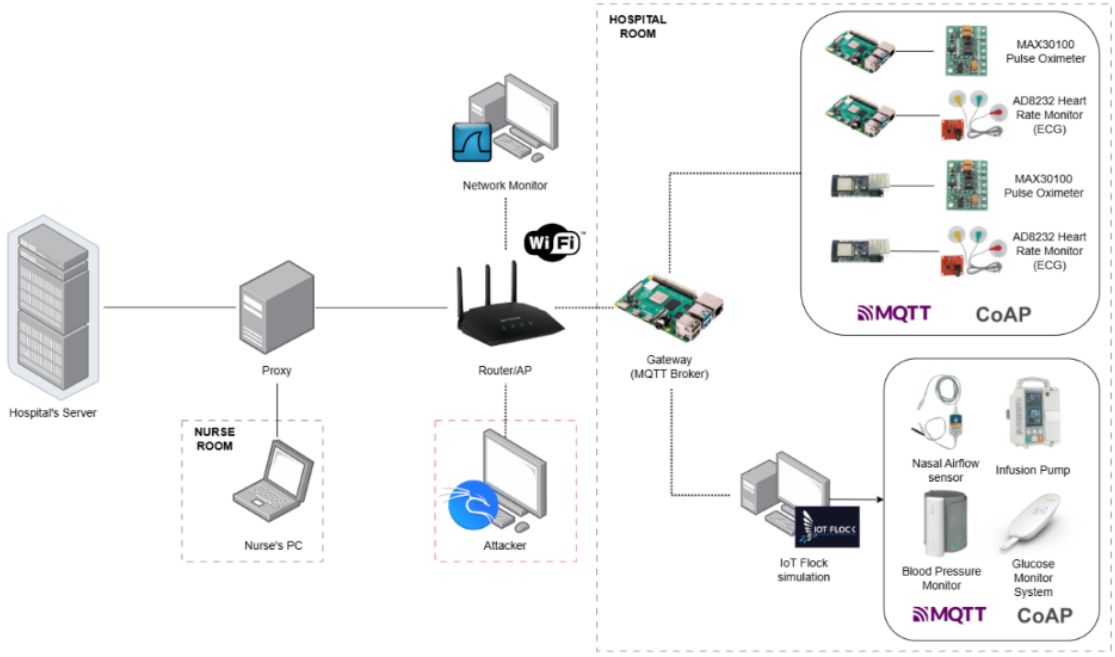


**Figura 3.1:** *Esquema de l'arquitectura utilitzada. Imatge extreta del treball [29].*

## 3.3 Ús del protocol MQTT

Primer de tot, l'elecció del protocol MQTT (Message Queuing Telemetry Transport) està fonamentada en el fet que és un dels protocols més utilitzats en l'àmbit IoT en general i en entorns IoMT en específic.

És un dels protocols amb més rellevància i eficiència per a dispositius amb recursos limitats, com és el cas d'aquest treball, on l'apartat de les comunicacions no és la seva funció principal. Consta d'una arquitectura *publisher – subscriber* centralitzada en un únic servidor, la qual cosa fa que tota la informació estigui centralitzada en un sol dispositiu, aquest fet el fa vulnerable i, per tant, cal prendre les mesures de seguretat adequades. A més a més, és un protocol altament configurable, ja que s'hi poden configurar mesures de seguretat com ara limitacions de trànsit, Access Lists (ACL) o encriptat TLS.

Dintre aquest projecte del grup ISG-UPC també es contempla el protocol CoAP, més enfocat a una arquitectura client -servidor semblant a protocols HTTP, però en aquest treball no serà utilitzat.

## 3.4 Ús de Docker per al desplegament de dispositius

Per al desplegament dels dispositius simulats (clients) i del servidor MQTT (broker), s'ha optat per l'ús de contenidors Docker en lloc de màquines virtuals (VMs). Aquesta decisió s'ha pres tenint en compte diversos criteris tècnics, pràctics i de rendiment, que fan que Docker sigui una opció més adequada per als objectius del projecte.

Docker et permet desplegar contenidors seguint una imatge comuna i configurable. D'aquesta manera, podem desplegar els clients simulats o el servidor en qualsevol entorn i sistema que compleixi uns requisits mínims de hardware I software. També permet mantenir una eficiència de recursos òptima, ja que utilitza el propi kernel del sistema hipervisor.

Alhora, és un sistema aïllat del sistema operatiu principal, per això, podem executar proves de penetració sense veure compromesa realment la seguretat dels nostres equips i amb una gran facilitat de reproduir aquest atac diverses vegades sense haver de configurar novament tot el dispositiu vulnerat, ja que aquests contenidors són fàcilment renovables per còpies idèntiques prèvies a l'atac.

A través del seu orquestrador Docker Compose, podem realitzar desplegaments múltiples de dispositius. Amb aquesta eina, podem desplegar en un sol dispositiu físic una gran quantitat de dispositius simulats que comparteixin unes característiques comunes entre ells.

Dintre dels motius pels quals s'ha escollit aquesta tecnologia, està l'ús de volums, els quals et permeten compartir espai en memòria entre el dispositiu hipervisor i els contenidors. Aquesta funcionalitat ens permet agilitzar la transferència d'arxius entre contenidors, com ara fitxers de configuració, scripts per executar tasques determinades o atacs coordinats (en el cas de contenidors desplegats per l'atacant).

També he utilitzat l'arquitectura de xarxa de Docker Compose per a poder crear infraestructures de xarxa simulades senceres, mantenint una lògica i rigorositat en les adreces de cada contenidor, d'aquesta manera, per a alguns atacs m'és possible simular una arquitectura com ara una gran quantitat de contenidors connectats a un switch o bé com un seguit de serveis del host per fer una arquitectura de microserveis dintre un mateix dispositiu.

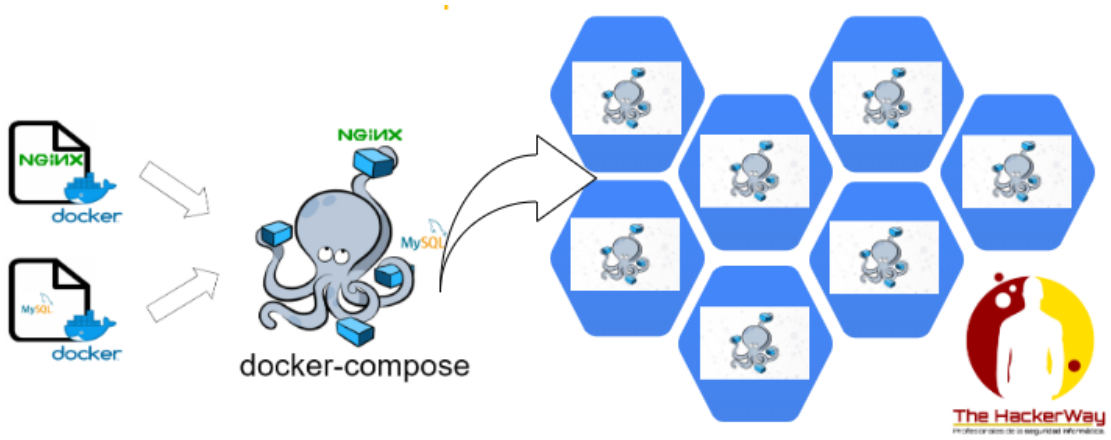


**Figura 3.2:** *Esquema de la generació de contenidors amb Docker Compose. Imatge extreta de The Hacker Way [29].*

## 3.5 Introducció d'expressions matemàtiques

LaTeX és una eina inestimable per a la composició tipogràfica de contingut matemàtic. En aquesta secció mostrem les comandes i entorns LaTeX essencials per a l'escriptura matemàtica. Per a més informació consulteu el capítol 3 de çita borrada".

### 3.5.1 Matemàtiques en línia i aïllades

Per a expressions en línia, utilitzeu `$ ... $` o `\( ... \)`. Escriviu entre `\[ ... \]` les expressions que s'han de mostrar en una línia apart.

```
El polinomi $p(x) = 3x^2+2x-1$
    t\'{e} arrels $x_1=-1$ i
    $x_2=\frac{1}{3}$.

Sigui la funci\'{o} de xarxa:
\[ H(s) = \frac{2\zeta\omega_o
    s}{s^2 + 2\zeta\omega_o s +
    \omega_o^2} \]
```

El polinomi $p(x) = 3x^2+2x-1$ té arrels $x_1 = -1$ i $x_2 = \frac{1}{3}$.
Sigui la funció de xarxa:

$$H(s) = \frac{2\zeta\omega_o s}{s^2 + 2\zeta\omega_o s + \omega_o^2}$$

### 3.5.2 Numeració i agrupació d'equacions

Els entorns `equation`, `gather`, `align` i altres numeren automàticament les equacions. Si definiu una etiqueta dins de l'equació podreu fer referència a ella dins del text usant `\ref{etiqueta}`. Podeu suprimir la numeració amb `\nonumber`.

```
\begin{equation}
  a + b = c   \label{eq:formula}
\end{equation}
Xxxx xxx \ref{eq:formula}.

\begin{gather}
  c = a + b \\
  d + e = f   \nonumber
\end{gather}

\begin{align}
  c &= a + b \nonumber \\
  d + e &= f
\end{align}
```

$$a + b = c \tag{3.1}$$

Xxxx xxx 3.1.

$$\begin{gathered} c = a + b \\ d + e = f \end{gathered} \tag{3.2}$$

$$\begin{aligned} c &= a + b \\ d + e &= f \end{aligned} \tag{3.3}$$

### 3.5.3 Introducció de matrius

```
$A = \begin{pmatrix}
  a & b \\
  c & d
\end{pmatrix}$
```

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

## 3.6 Taules

El paquet `booktabs` ([8]) s'utilitza sovint per crear taules amb un espaiat millor i línies horitzontals més llegibles, i el paquet `array` es pot utilitzar per definir nous tipus de columna. A continuació es mostra un exemple de taula que utilitza aquests paquets i l'entorn `tabular` (consulteu el codi LaTeX del document per a saber com s'ha creat.):

**Taula 3.1:** *Taula d'exemple*

| Element | Quantitat | Descripció |
|---|---|---|
| Mango | 5 | Una fruita taronja |
| Plàtan | 2 | Una fruita groga |
| Cirera | 20 | Una fruita petita, rodona i vermella |

En aquest exemple (consulteu el codi font LaTeX):

- `\toprule`, `\midrule`, i `\bottomrule` del paquet `booktabs` creen línies horitzontals que tenen un espaiat per defecte millor que l'estàndard de LaTeX `\hline`.
- La definició `>{\raggedright\arraybackslash}p{3cm}` del paquet `array` s'utilitza per crear un nou tipus de columna per a la descripció, on el text està alineat a l'esquerra i la columna té una amplada fixa de 3 cm.

Compileu aquest codi amb LaTeX per produir la taula 3.1. La taula hauria de semblar bonica i llegible.

## 3.7 Diagrames

El paquet *TikZ* ([28]) permet dibuixar tot tipus de diagrames i gràfics. Val la pena consultar el seu manual d'ús per tal de conèixer el seu funcionament i poder-ne treure tot el suc possible. Cal no deixar-se intimidar per la seva longitud (1300+ pàgines) ja que la majoria d'espai l'ocupen nombrosos exemples que il·lustren les possibilitats del llenguatge.

Per si això fos poc, també hi ha disponibles una sèrie de biblioteques addicionals que permeten d'augmentar encara més les funcionalitats del *TikZ* amb l'addició d'ordres per

facilitar el dibuix de tot tipus d'objectes, des de xarxes de Petri fins a circuits electrònics, passant per coses tan diverses com calendaris, diagrames d'estats o figures de papiroflèxia.

La figura 3.3 mostra alguns exemples de diagrames creats amb el paquet *TikZ*.

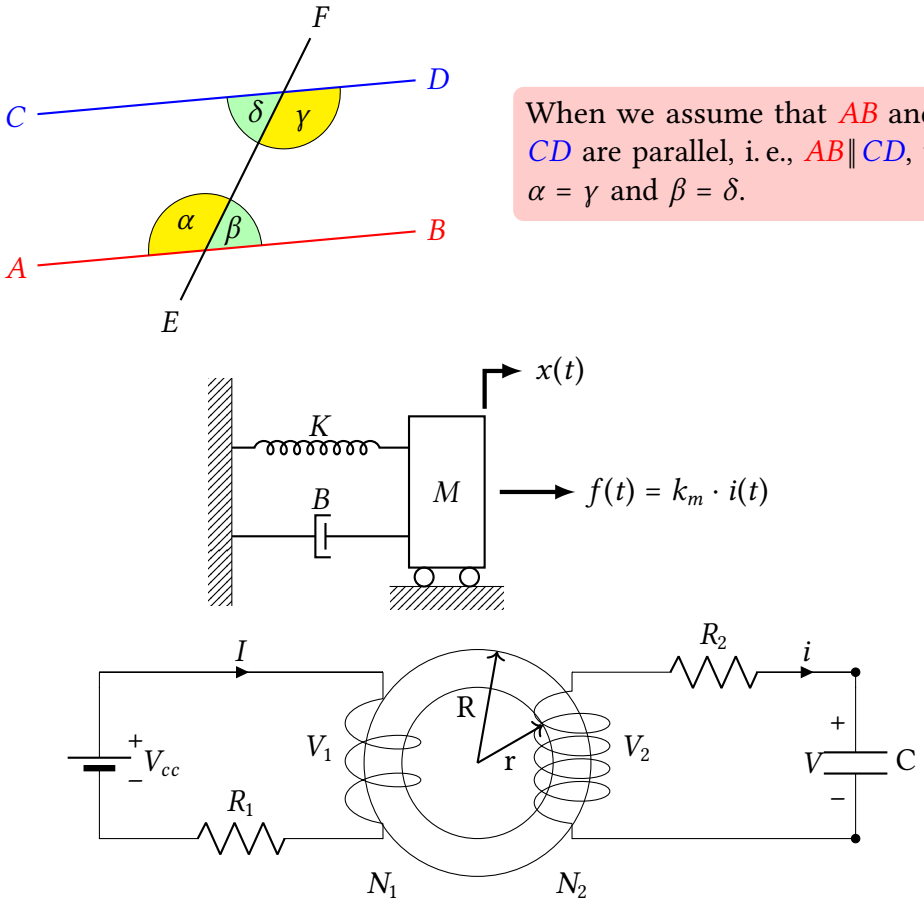


**Figura 3.3:** *Diagrames creats usant les ordres del paquet* TikZ

## 3.8 Gràfiques

Òbviament podeu crear les vostres gràfiques usant un programa informàtic adient, exportant el resultat a algun format gràfic (preferiblement vectorial com ara PDF per no perdre qualitat) i inserint les imatges resultants al document LaTeX en la forma habitual. Aquesta via, però, té l'inconvenient que dificulta aconseguir la coherència i cohesió tipogràfica entre el text del document i el de les imatges. Com a conseqüència, la qualitat del document se'n ressent.

Per tant, si es vol aconseguir la màxima coherència tipogràfica entre el text i les gràfiques, és preferible que sigui el propi LaTeX qui s'encarregui de generar les gràfiques (amb les dades que li proporcionem) ja que en aquest cas usarà les mateixes fonts arreu del document.

A tal efecte al llarg dels anys s'han desenvolupat múltiples paquets i tècniques per aconseguir aquest objectiu. El que aquí us proposem és usar el paquet «**pgfplots**», que utilitza internament el paquet *TikZ* per generar una sèrie de *macros* addicional que faciliten el dibuix de gràfiques. La figura 3.4 mostra un exemple del que es pot arribar a fer amb aquest paquet, però recomanem fermament que consulteu el manual d'instruccions ([9]) on s'il·lustren molts més exemples.

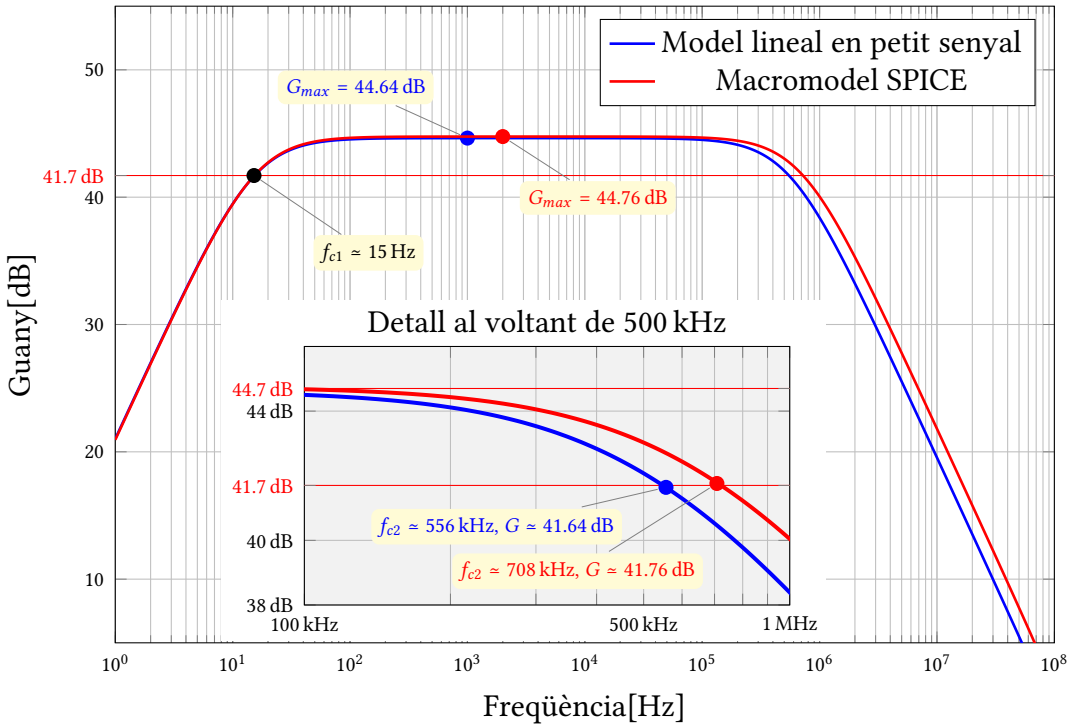


**Figura 3.4:** *Exemple de gràfica complexa dibuixada amb ajut del paquet* pgfplots

## 3.9 Llistats de codi

L'entorn `tcblistings` del paquet `tcolorbox` ([27]) insereix els llistats de codi generats pels paquets `listings` o `minted` dins d'una `tcolorbox`, amb la qual cosa s'aconsegueixen uns llistats molt ben presentats i altament configurables.

Com a exemple d'això, a continuació es mostra el llistat d'un programa en llenguatge Python que implementa l'algorisme del «sedàs d'Eratòstenes» per calcular els nombres primers menors d'un cert nombre donat. Observeu que el paquest «listings» és capaç d'interpretar i ressaltar automàticament la sintaxi del llenguatge.

**Exemple de Python: Sedàs d'Eratòstenes**

```
1 def sieve_of_eratosthenes(limit):
2   primes = []
```

```
  sieve = [True] * (limit + 1)
  for num in range(2, limit + 1):
    if sieve[num]:
      primes.append(num)
      for multiple in range(num*num, limit + 1, num):
        sieve[multiple] = False
  return primes

# Example usage:
if __name__ == "__main__":
  limit = 30
  print(f"The prime numbers up to {limit} are:
          {sieve_of_eratosthenes(limit)}")
```

## 3.10 Unitats

Una de les coses que sovint es menysté a l'hora d'escriure és la correcta representació de valors i unitats, que és essencial en textos científics i tècnics. El paquet `siunitx` de LaTeX s'ajusta al sistema internacional d'unitats (SI) i amb ell els usuaris poden assegurar-se que els nombres i unitats són presentats amb la notació, espaiat i font adequats, tot respectant les diferents convencions internacionals.

A continuació presentem alguns exemples d'ús, però per una presentació exhaustiva de les possibilitats del paquet caldrà que consulteu la seva documentació ([30]).

- **Composició tipogràfica d'unitats senzilles**: Per composar una unitat utilitzant `siunitx`, podeu fer servir la comanda `\si{}`. Per exemple, per composar "metres per segon,"escriuríeu: `\si{\meter\per\second}` que resultaria en «$\mathrm{m\,s^{-1}}$» amb l'espaiament correcte entre ells.

- **Combinació de Nombre i Unitat**: Si voleu incloure un valor amb una unitat, useu la comanda `\SI{}`. Per exemple, per expressar "10 kilo-ohm"escriuríeu: `\SI{10}{\kohm}`, que resulta en 10 kΩ. Aquesta comanda assegura que el nombre i la unitat estan adequadament espaiats.

- **Unitats complexes**: Per unitats més complexes, `siunitx` permet combinar unitats de diverses maneres. Per exemple, per composar «gigawatts per metre quadrat per estereoradian» podeu usar:

  ```
  \si{\giga\watt\per\square\meter\per\steradian}
  ```

  i el paquet treu «$\mathrm{GW\,m^{-2}\,sr^{-1}}$» tenint cura de tota la formatació adequada i la font.

`siunitx` és molt flexible i pot manejar una àmplia gamma d'unitats i opcions de formatatge de nombres, incloent nombres complexos amb unitats, l'alineació en taules,

l'arrodoniment de nombres, i l'establiment d'opcions globals per a la consistència a través d'un document.

CAPÍTOL 4

# Desenvolupament d'un entorn IoMT simulat

Per al desplegament d'un entorn IoMT simulat seguint l'arquitectura explicada a 3.2 he elaborat un entorn a través de contenidors Docker i l'orquestrador per defecte Docker Compose.

Per a la realització dels clients, que representen el trànsit benigne, he utilitzat una imatge d'Ubuntu, aquesta ha estat modificada (i renombrada com a mqttclient) on mitjançant el gestor de paquets APT s'ha instal·lat mosquitto-clients 2.0.20 ref imatge. Amb aquesta aplicació podem fer actuar aquest contenidor d'Ubuntu com un client MQTT i tenir les seves funcions principals com subscriure's i publicar a un tòpic d'un broker concret i utilitzar totes les funcionalitats descrites. ref mosquitto

També he instal·lat Python 3.13.2 i Paho-mqtt 2.0.0 [12] per a poder generar paquets de forma personalitzada. Amb aquesta llibreria de Python podem modificar aspectes molt més concrets de les nostres connexions MQTT i paquets, canviant els valors de les dades o la freqüència d'enviament de les publicacions. Gràcies a aquesta eina, al ser una llibreria de Python, podem córrer els clients de manera automatitzada utilitzant les eines pròpies del llenguatge.

També he instal·lat les eines net-tools i iputils per tal de poder monitoritzar l'estat dels contenidors i fer comprovacions de connectivitat.

Pel que fa al Broker, he utilitzat l'imatge oficial de mosquitto anomenada eclipse-mosquitto (versió 2.0.21) [13]. Aquesta permet l'ús del contenidor com a broker MQTT en les seves versions 3.1 i 5.1.1 amb totes les funcionalitats de les quals disposa la versió local 2.5.1.

Respecte a configuració de Docker, he mapejat els ports 1883 i 8883 perquè en establir una connexió TCP a un d'aquests ports de l'hipervisor et dirigeixi al mateix port d'aquest contenidor en concret. També he generat 3 volums compartits amb l'hipervisor:

- Config: on s'ubica el fitxer de configuracions mosquitto.conf
- Data: on opcionalment s'emmagatzemen les dades rebudes en format txt o dintre una base de dades

- Log: on es guarden els logs dels errors ocasionats durant el seu funcionament en fitxers .log

Pel que fa al monitor de trànsit, partint de l'image base Ubuntu (renombrada com a sniffer), s'ha instal·lat tcpdump 4.99.5 i wireshark 4.4.3. Com ha estat explicat a 3.2, la seva funcionalitat és emmagatzemar el trànsit per tal de generar el dataset, que aquest és enregistrat amb tcpdump, però, el mateix contenidor també ha estat utilitzat per a l'elaboració i l'estudi de l'impacte dels diferents atacs, és per això que s'utilitza Wireshark, que perquè pugui ser visualitzat s'ha fet servir el socket de X11 de l'hipervisor i així aquest contenidor pugui fer ús de GUI.

Per l'atacant, parteix de la imatge kalilinux/kali-last-release [14] (renombrada com a atacker) amb l'instal·lació dels paquets kali-linux-headless i que conté les eines més utilitzades de kali linux i depenent de l'atac s'ha instal·lat altres eines de pentesting.

Tots aquests contenidors, s'han integrat mitjançant un fitxer .yaml de Docker-Compose que ens permet definir volums i fer ús de configuracions de xarxa personalitzades. El nombre de clients utilitzats és variable, però tots disposen d'un sol volum vinculat a l'hipervisor.

S'ha creat una xarxa personalitzada (bridge) on es disposen tots els contenidors i tenen connectivitat entre ells com si es tractés d'una xarxa LAN privada. Per utilitzar un model híbrd entre dispositius simulats i dispositius reals (o bé dispositius simulats en hosts diferents), s'ha utilitzat la configuració MACVLAN que permet connectar els contenidors a la xarxa física amb adreces IP i MAC diferent (cal evitar conflictes amb altres adreces de la xarxa física), amb un efecte similar al que tindríem connectant un switch a la xarxa amb tots els seus contenidors. Amb aquesta configuració m'he coordinat amb altres membres del grup ISG-UPC per a poder integrar el meu treball al projecte. Finalment, en diversos atacs, he configurat l'entorn amb el mode IPVLAN (L2) on cada contenidor té una adreça IP diferent. El host realitza NAT col·locant la seva adreça MAC i responent a peticions ARP. Això és mès compatible en xarxes WiFi WPA2.

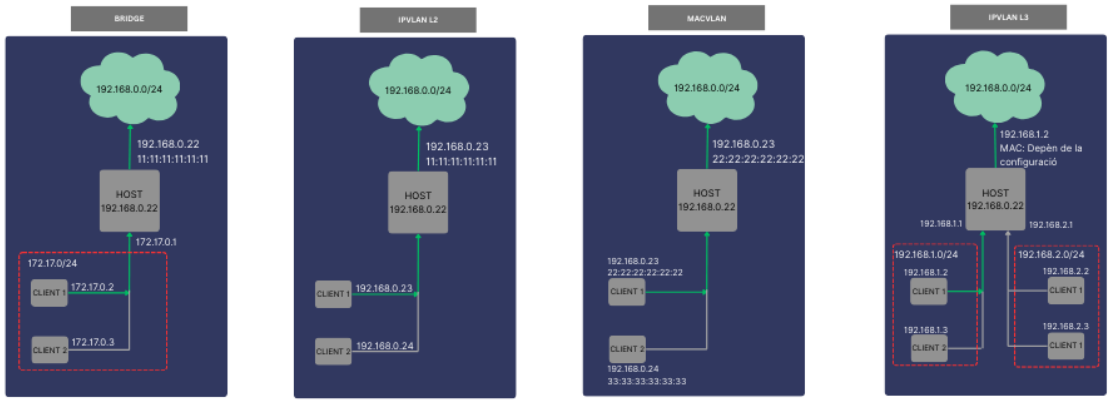


**Figura 4.1:** *La figura mostra el comportament dels diferents drivers de xarxa de Docker (excloent el mode host on directament actua en nom de l'hipervisor).*

CAPÍTOL 5

# Atacs de reconeixmenet

xd

CAPÍTOL 6

# Resultats

Aquest capítol ha d'incloure l'anàlisi de les vostres dades i els resultats obtinguts. A més, incloeu-hi taules, figures i citacions pertinents per donar suport als vostres resultats i interpretacions. Aquí teniu una llista suggerida de temes a tractar:

## 6.1 Experiments i proves

Descriviu els experiments realitzats per provar el rendiment del vostre projecte. Expliqueu com heu recopilat i processat les dades.

## 6.2 Visualització de les dades

Creeu representacions visuals dels resultats (per exemple, gràfics de dispersió, diagrames de barres). Interpreteu les visualitzacions i relacioneu-les amb les preguntes de recerca.

## 6.3 Limitacions

Reconeixeu qualsevol limitació en les dades o l'anàlisi. Expliqueu com aquestes limitacions podrien haver afectat els resultats.

CAPÍTOL 7

# Anàlisi de sostenibilitat i implicacions ètiques

Des del curs 2023-24, la normativa de TFG de l'ETSETB demana la inclusió d'un informe de sostenibilitat a la memòria del treball. Aquesta anàlisi consisteix en una valoració dels impactes ambientals, socials i econòmics, i les possibles implicacions ètiques que ha comportat la realització del TFG. En el cas que el TFG plantegi un producte/servei/sistema/edifici/etc., que podria arribar a implementar-se, l'anàlisi també ha de realitzar-se sobre els impactes que tindria la proposta en la seva execució durant les diferents etapes del seu cicle de vida.

A la plataforma ATENEA trobareu un document separat amb les instruccions detallades de què ha de contenir i com cal confeccionar l'informe de sostenibilitat.

**IMPORTANT: Noteu que l'antic capítol de «Pressupost del projecte» ara queda integrat en l'anàlisi de sostenibilitat, concretament en les cel·les «Econòmic/-Desenvolupament del TFG» i «Econòmic/Execució del projecte».**

CAPÍTOL 8

# Conclusions i Línies Futures

## 8.1 Conclusions

- Resumiu els resultats principals del vostre treball.
- Discutiu el grau d'assoliment en relació amb els objectius marcats a l'inici del treball.
- Destaqueu les contribucions del vostre treball al camp d'estudi.

## 8.2 Línies Futures

- Identifiqueu àrees per a futures investigacions o desenvolupament basades en el vostre treball.
- Discutiu possibles vies per ampliar o millorar el projecte.
- Considereu les preguntes que han quedat sense resposta i les oportunitats per a futures exploracions.

# Bibliografia

El sistema *biblatex* simplifica la gestió de la bibliografia en treballs científics, proporcionant automatització i personalització en el format de les citacions. Això permet a l'autor del document enfocar-se en el contingut sense haver de preocupar-se per l'estil de les referències, estalviant temps i reduint errors.

La base de dades de referències bibliogràfiques és al fitxer «TFG.bib» i és allà on heu d'afegir les vostres referències. Consulteu el manual del `biblatex`, secció «Database Guide», per conèixer els tipus de referències i camps disponibles.

Podeu modificar (o suprimir) aquesta nota editant la macro `\defbibnote` al fitxer «TFG.tex».

---


[1] Héctor Aláiz-Moretón Ángel Luis Muñoz Castañeda José Antonio Aveleira Mata. «Characterization of threats in IoT from an MQTT protocol-oriented dataset». A: *Complex Intelligent Systems* 9.01000 (2023), pàg. 5281 - 5296. DOI: 10.1007/s40747-023-01000-y.

[2] Newtowk Chuck. *Docker Tutorials - NetworkChuck*. 2020. URL: https://www.youtube.com/watchv=eGz9DSaIeY&list=PLIhvC56v63IJlnU4k60d0oFIrsbXEivQo&index=2 (cons. 09-05-2025).

[3] TCPDump Developers. *TCPDump: Manual and Documentation*. 2023. URL: https://www.tcpdump.org/ (cons. 08-05-2025).

[4] Daniel Echeverri. *Docker Stack: Cómo desplegar servicios de Docker Compose en Docker Swarm*. 2021. URL: https://thehackerway.es/2021/11/22/docker-stack-como-desplegar-servicios-de-docker-compose-en-docker-swarm/ (cons. 21-05-2025).

[5] Albert Einstein. «Zur Elektrodynamik bewegter Körper». A: *Annalen der Physik* 322.10 (1905), pàg. 891 - 921.

[6] Alexandria University Elsevier BV on behalf of Faculty of Engineering. *The internet of things healthcare monitoring system based on MQTT protocol*. 2024. URL: https://www.sciencedirect.com/science/article/pii/S1110016823000881 (cons. 08-05-2025).

[7] Mehdi Delrobaei Fatemeh Ghorbani Mohammad Kia. *Evaluating the Possibility of Integrating AugmentedReality and Internet of Things Technologies to HelpPatients with Alzheimer's Disease*. Figura adaptada i modificada amb IA. 2024. URL: https://www.researchgate.net/figure/MQTT-protocol-operation-in-AAL-system_fig1_339906098.

[8] Simon Fear. *booktabs Publication quality tables in LaTeX*. 2020. URL: http://mirrors.ctan.org/macros/latex/contrib/booktabs/booktabs.pdf (cons. 01-11-2023).

[9] Christian Feuersänger. *Manual for Package PGFPLOTS*. URL: http://mirrors.ctan.org/graphics/pgf/contrib/pgfplots/doc/pgfplots.pdf (cons. 03-11-2023).

[10] Richard P. Feynman, Robert B. Leighton i Matthew Sands. *The Feynman Lectures on Physics*. Vol. I-III. Reading, Massachusetts: Addison-Wesley, 1963. ISBN: 978-0201021165.

[11] Eclipse Foundation. *Mosquitto MQTT Broker Documentation*. 2024. URL: https://mosquitto.org/documentation/ (cons. 08-05-2025).

[12] Python Software Foundation. *Paho MQTT Python Packaging Survey*. 2025. URL: https://pypi.org/project/paho-mqtt/ (cons. 23-05-2025).

[13] Docker Inc. *Docker Hub: eclipse-mosquitto*. 2025. URL: https://hub.docker.com/_/eclipse-mosquitto (cons. 23-05-2025).

[14] Docker Inc. *Docker Hub: kalilinux/kali-last-release*. 2025. URL: https://hub.docker.com/r/kalilinux/kali-last-release (cons. 23-05-2025).

[15] Philip Kime, Moritz Wemheuer i Philipp Lehman. *The biblatex Package*. URL: https://ctan.org/pkg/biblatex (cons. 06-11-2023).

[16] Donald Knuth. *Knuth: Computers and Typesetting*. URL: https://www-cs-faculty.stanford.edu/~knuth/abcde.html.

[17] Donald E. Knuth. *The TeXbook*. Reading, Massachusetts: Addison-Wesley, 1986. ISBN: 0-201-13448-9.

[18] Leslie Lamport. *LaTeX: A Document Preparation System, 2nd Edition*. Reading, Massachusetts: Addison-Wesley, 1994. ISBN: 0-201-52983-1.

[19] Frank Mittelbach i Ulrike Fischer. *The LaTeX Companion*. 3a ed. 2 vol. Reading, Massachusetts: Addison-Wesley.

[20] Qasem Abu Al-Haija Mustafa Al-Fayoumi. «Capturing low-rate DDoS attack based on MQTT protocol in software Defined-IoT environment». A: *Sciencie Direct Journal* 19.100316 (2023), pàg. 10. DOI: 10.1016/j.array.2023.100316.

[21] Tobias Oetiker et al. *The Not So Short Introduction to LaTeX*. URL: https://tobi.oetiker.ch/lshort/lshort.pdf (cons. 31-10-2023).

[22] Nmap Project. *Nmap Reference Guide*. 2024. URL: https://nmap.org/book/man.html#man-description/ (cons. 08-05-2025).

[23] Raphael Ferreira Sajjad Dadkhah Euclides Carlos Pinto Neto. «CICIoMT2024: Attack Vectors in Healthcare devices-A Multi-Protocol Dataset for Assessing IoMT Device Security». A: *Preprints.org* 1.0898 (2024), pàg. 30. DOI: 10.20944/preprints202402.0898.v1.

[24] Offensive Security. *Kali Linux Documentation*. 2024. URL: https://www.kali.org/docs/introduction/what-is-kali-linux/ (cons. 11-05-2025).

[25] Claude E. Shannon. «A Mathematical Theory of Communication». A: *The Bell System Technical Journal* 27.3 (1948), pàg. 379 - 423. DOI: 10.1002/j.1538-7305.1948.tb01338.x.

[26] Wolfgang Skala. *Drawing Gantt Charts in LaTeX with TikZ*. URL: http://osl.ugr.es/CTAN/graphics/pgf/contrib/pgfgantt/pgfgantt.pdf.

[27] Thomas F. Sturm. *The `tcolorbox` package*. URL: http://mirrors.ctan.org/macros/latex/contrib/tcolorbox/tcolorbox.pdf (cons. 05-11-2023).

[28] Till Tantau. *The TikZ and PGF Packages*. URL: http://mirrors.ctan.org/graphics/pgf/base/doc/pgfmanual.pdf (cons. 02-11-2023).

[29] Josep Pegueroles Valles. «MIoTTA-UPC: Testbed MIoT Configurable para la Evaluacion de Algoritmos de Detección de Ciberataques Basados en Inteligencia Artificial». A: *The Bell System Technical Journal* 27.3 (1948), pàg. 379 - 423. DOI: 10.1002/j.1538-7305.1948.tb01338.x.

[30] Joseph Wright. *`siunitx` A comprehensive (SI) units package*. URL: https://ctan.org/pkg/siunitx (cons. 08-11-2023).

APÈNDIX A

# Un apèndix

Es poden incloure apèndixs al TFG però no és obligatori.