Anàlisi de vulnerabilitats i gestió de riscos de dispositius Internet of BioNano Things

Sara Giménez

TFM - Seguretat en la internet of things

Seguretat en la internet of things

Tutor/a de TF
Isaac Guasch Garcia
Professor/a responsable de l'assignatura
Victor Garcia Font

Gener 2024

Universitat Oberta de Catalunya

Universitat Oberta de Catalunya uoc.edu

FITXA DEL TREBALL FINAL

Títol del treball:	*Anàlisi de vulnerabilitats i gestió de riscos de dispositius Internet of BioNano Things*
Nom de l'autor:	*Sara Giménez Guillén*
Nom del consultor/a:	*Isaac Guasch Garcia*
Nom del PRA:	*Victor Garcia Font*
Data de lliurament (mm/aaaa):	*01/2024*
Titulació o programa:	*Màster Universitari en Ciberseguretat i Privadesa*
Àrea del Treball Final:	*Seguretat en la internet of things*
Idioma del treball:	*Català*
Paraules clau	*IoBNT, ODS, 2030*

Resum del Treball

Aquest treball té com a finalitat fer un anàlisi de les vulnerabilitats i la gestió de riscos davant possibles ciberatacs dels dispositius d'Internet of BioNano Things existents actualment en el sector de la Salut Pública, en concret, en l'aplicació en el tractament de l'aigua.

Per la realització d'aquest inventari es farà un anàlisi descriptiu dels diferents dispositius existents en l'actualitat en l'àmbit de les IoBNT aplicables al tractament de l'aigua per finalitats de Salut Pública. S'establiran les vulnerabilitats detectades i la gestió de riscos establerta.

El resultat serà un estat de l'art de vulnerabilitats i la gestió de riscos de dispositius IoBNT utilitzats en el tractament de l'aigua en el sector de Salut Pública.

Les conclusions d'aquest treball dirimiran si és possible mitjançant una visió actualitzada d'aquest estat de l'art d'aquests dispositius IoBNT en quant a ciberseguretat, es poden impulsar iniciatives de millora que permetin incrementar el grau d'acompliment de l'ODS 3, 6 i 13 de l'Agenda 2030 per al Desenvolupament Sostenible de les Nacions Unides.

Abstract

This work aims to make an analysis of the vulnerabilities and risk management in the face of possible cyberattacks of the Internet of BioNano Things devices currently existing in the Public Health sector, specifically, in the application in water treatment.

For the realization of this inventory, a descriptive analysis of the different devices currently existing in the field of IoBNTs applicable to water treatment for Public Health purposes will be carried out.

The vulnerabilities detected and the risk management established will be established.

The result will be a state-of-the-art vulnerability and risk management of IoBNT devices used in water treatment in the Public Health sector.

The conclusions of this work will decide if possible through an updated vision of this state of the art of these IoBNT devices in terms of cybersecurity, improvement initiatives can be promoted to increase the degree of compliance with SDG 3, 6 and 13 of the 2030 Agenda for Sustainable Development of the United Nations.

Índex

Llista de Taules

Llista de Figures

1 Introducció

L'aigua és la base de la vida. El component principal del cos de tots els éssers vius.

Experts de l'Organització Mundial de la Salut (OMS) han descobert que el 80% de totes les malalties i el 50% de les morts infantils a tot el món estan relacionades amb la qualitat de l'aigua potable i les violacions de les normes d'higiene i sanejament del subministrament d'aigua [6].

En un moment en què el creixement de la població, la urbanització i la industrialització contaminen les fonts d'aigua existents i les malalties transmeses per l'aigua estan en augment, la recerca de nous mètodes de tractament de l'aigua és un repte pel món científic.

L'aplicació de la nanotecnologia i la bionanotecnologia, així com, el disseny de sistemes artificials IoBNT ofereixen una oportunitat per millorar l'eficiència dels processos de sanejament i gestió de l'aigua.
Per tant, la seguretat en aquestes tecnologies i en els sistemes IoBNTs esdevé de vital importància. La ciberseguretat té un paper primordial, ja que les conseqüències de patir ciberatacs en sistemes IoBNTs destinats a tractament de l'aigua poder arribar a ser fatals per a la població.

1.1. Context i justificació del Treball

1.1.1 Conceptes previs

El terme **IoBNT** és l'acrònim d'Internet of BioNano Things. És un camp relativament nou que combina les eines de biologia sintètica, la nanotecnologia i que preveu xarxes col·laboratives heterogènies de dispositius funcionals nanobiològics naturals i artificials perfectament integrats a la infraestructura d'Internet.[1]

La **Salut Pública** és el conjunt d'activitats organitzades per les Administracions públiques, amb la participació de la societat, per prevenir la malaltia així com per protegir, promoure i recuperar la salut de les persones del territori o regió, tant en l'àmbit individual com en el col·lectiu i mitjançant accions sanitàries, sectorials i transversals.[2]

ODS és l'acrònim de Objectius de Desenvolupament Sostenible. A l'any 2015, tots els Estats Membres de les Nacions Unides van aprovar 17 Objectius com a part de l'Agenda 2030 per al Desenvolupament Sostenible [3], en la que es va establir un pla per assolir els Objectius en 15 anys.

1.1.2 Context i justificació

Diferents sectors es beneficien de la utilització dels dispositius IoBNTs. Les aplicacions es poden classificar en 3 grans categories [4] segons la tipologia de IoBNTs existents actualment:

- *Biomedicina*: Els dispositius IoBNT són capaços de recollir informació relacionada amb la salut i transmetre-la a l'exterior cap a equips d'atenció mèdica a través d'Internet. Els dispositius IoBNT també poden encarregar-se de reparar o evitar fallades en les comunicacions entre els nostres òrgans interns.
- *Ramaderia i Agricultura intel·ligent:* La salut dels animals com el bestiar boví i l'aviram també poden ser monitoritzats per IoBNT per garantir la qualitat de productes com la carn, la llet i els ous. A l'agricultura, a través del monitoratge de les plantes mitjançant BNTs desplegats a les plantes o al sòl es pot mesurar la seva salut. Això també pot ser amb el suport de BNTs que monitoritzen i controlen el reg intel·ligent sistemes, fertilitzant activament el sòl i dissuadint fauna salvatge que danyen els cultius.
- *Control i neteja ambiental*: Els dispositius IoBNT es despleguen en el medi ambient i són utilitzats per verificar la presència d'agents tòxics i contaminants. Una vegada identificats, poden arribar a encarregar-se de transformar aquests agents contaminants mitjançant tècniques de descontaminació.

La connexió de l'entorn biològic amb el domini cibernètic a través de nano-dispositius bio-electrònics proporciona als ciberdelinqüents una oportunitat d'idear nous mecanismes per atacar de forma remota i a nivell de nano escala (10^{-9}).

L'aplicació ambiental de les IoBNT a la que s'enfoca aquest treball és la relacionada amb el tractament de l'aigua per a:

a) purificació/desinfecció
b) descontaminació d'aigües residuals domèstiques i industrials (tèxtil, petroquímica, automotriu, metal·lúrgica, minera, begudes)
c) dessalinització
d) sensors de qualitat de l'aigua

Aquest treball es centra en els dispositius IoBNT utilitzats en el tractament de l'aigua del sector de la Salut Pública i en analitzar les vulnerabilitats existents i la gestió de riscos que es realitza. Addicionalment aquest treball proporciona una visió de com aquests IoBNTs contribueixen en l'assoliment dels ODS 3, 6 i 13 (3 Salut i benestar, 6 Aigua neta i sanejament, 13 Acció pel clima). [5]

Els accessos maliciosos a sistemes de tractament de l'aigua a través d'Internet per a sabotatge són potencialment molt perillosos o inclús mortals per la població.

Les IoBNT plantegen un repte en l'àmbit de la seguretat, tant biològica com cibernètica. La nano biotecnologia connectada a internet fan que la seguretat es plantegi com una necessitat des de l'inici.

1.2 Objectius del Treball

L'objectiu principal del present treball és:

Elaborar un estat de l'art de la ciberseguretat de dispositius d'IoBNT de tractament de l'aigua en el marc del sector de la Salut Pública per millorar l'assoliment dels ODS 3, 6 i 13.

Altres objectius secundaris:

- Llistat de vulnerabilitats de dispositius IoBNT
- Descripció la gestió de riscos en dispositius IoBNT
- Establir un punt de partida per al futur disseny i desenvolupament de solucions efectives de seguretat en entorns on els dispositius IoBNT per a tractament de l'aigua participin en el marc de Salut Pública.

1.2.1 Objectius principal i secundaris

L'objectiu principal d'aquest treball es descriure l'estat actual de la seguretat dels dispositius IoBNTs respecte els objectius de seguretat: Confidencialitat, Integritat, Disponibilitat i Autenticitat.

Addicionalment, es centrarà en:

- Descriure la tecnologia dels dispositius IoBNT relacionats amb tractament de l'aigua.
- Descriure l'arquitectura de sistemes on s'utilitzin els dispositius IoBNT
- Identificar i avaluar les vulnerabilitats dels sistemes descrits
- Realitzar un estudi de la gestió de riscos d'aquests sistemes
- Argumentar com la millora en ciberseguretat d'aquests dispositius aporta millora en els ODS 3, 6 i 13

Els tipus d'atacs que són objectiu d'aquest treball són: (classificats segons el nivell d'atac on es produeixen)

- Atacs a nivell de la Bio-nanoxarxa
  - Escoltes
  - Atac de forat negre o Balckhole
  - Atacs sentinelles
- Atacs a nivell de la Interfície Bio-cibernètica
  - Escoltes
  - Atac de reproducció
  - Atac Man-In-The-Middle (MITM)
  - Esgotament de recursos
  - Atacs d'injecció
  - Manipulació de dispositius
  - Atac de denegació de servei (DoS)
  - Atacs de malware
  - Atacs de firmware

Per aquests atacs/amenaces que els dispositius IoBNTs poden patir, tant a nivell intern com extern, es descriuran les mesures de gestió de riscos establertes fins al moment actual.

A partir d'aquest escenari es deriva un punt de partida per a dissenyar sistemes més segurs basats en dispositius IoBNTs destinats al tractament de l'aigua directament per millorar els ODS 3, 6 i 13 de l'Agenda 2030, ja que contribuint en l'assoliment de mesures incloses en aquests ODS.

1.2.2 ODS 3 - Salut i Benestar

Aquest ODS té com a finalitat:

> Garantir una vida sana i promoure el benestar en totes les edats és essencial per al desenvolupament sostenible.

Abans de la pandèmia de la COVID-19, es van aconseguir grans avenços en la millora de la salut de milions de persones. Sobretot es van assolir en augmentar l'esperança de vida i reduir algunes de les causes de mort comunes associades amb la mortalitat infantil i materna.

Tanmateix, es necessiten més esforços per erradicar per complet una gran varietat de malalties i abordar un gran nombre de problemes de salut, tant constants com emergents.

A través d'un finançament més eficient dels sistemes sanitaris, un major sanejament i higiene, i un major accés al personal mèdic, es podran aconseguir avenços significatius a l'hora d'ajudar a salvar les vides de milions de persones.

Les fites de l'ODS3 són:

> 3.1 Per al 2030, reduir la taxa mundial de mortalitat materna a menys de 70 per cada 100.000 nascuts vius
>
> 3.2 Per al 2030, posar fi a les morts evitables de nounats i de nens menors de 5 anys, aconseguint que tots els països intentin reduir la mortalitat neonatal almenys fins a 12 per cada 1.000 nascuts vius, i la mortalitat de nens menors de 5 anys almenys fins a 25 per cada 1.000 nascuts vius
>
> 3.3 Per al 2030, posar fi a les epidèmies de la SIDA, la tuberculosi, la malària i les malalties tropicals desateses i combatre l'hepatitis, les malalties transmeses per l'aigua i altres malalties transmissibles
>
> 3.4 Per al 2030, reduir en un terç la mortalitat prematura per malalties no transmissibles mitjançant la prevenció i el tractament i promoure la salut mental i el benestar
>
> 3.5 Enfortir la prevenció i el tractament de l' abús de substàncies addictives, inclòs l'ús indegut d' estupefaents i el consum nociu d'alcohol
>
> 3.6 Per al 2020, reduir a la meitat el nombre de morts i lesions causades per accidents de trànsit al món
>
> 3.7 Per al 2030, garantir l' accés universal als serveis de salut sexual i reproductiva, inclosos els de planificació de la família, informació i educació, i la integració de la salut reproductiva en les estratègies i els programes nacionals
>
> 3.8 Aconseguir la cobertura sanitària universal, en particular la protecció contra els riscos financers, l'accés a serveis de salut essencials de qualitat i l'accés a medicaments i vacunes segurs, eficaços, assequibles i de qualitat per a tothom

3.9 Per al 2030, reduir substancialment el nombre de morts i malalties produïdes per productes químics perillosos i la contaminació de l' aire, l'aigua i el sòl

3.a Enfortir l'aplicació del Conveni Marc de l'Organització Mundial de la Salut per al Control del Tabac a tots els països, segons escaigui

3.b Donar suport a les activitats de recerca i desenvolupament de vacunes i medicaments per a les malalties transmissibles i no transmissibles que afecten primordialment els països en desenvolupament i facilitar l'accés a medicaments i vacunes essencials assequibles de conformitat amb la Declaració de Doha relativa a l'Acord sobre els ADPIC i la Salut Pública, en la qual s' afirma el dret dels països en desenvolupament a utilitzar al màxim les disposicions de l' Acord sobre els Aspectes dels Drets de Propietat Intel·lectual Relacionats amb el Comerç pel que fa a la flexibilitat per protegir la salut pública i, en particular, proporcionar accés als medicaments per a tothom

3.c Augmentar substancialment el finançament de la salut i la contractació, el desenvolupament, la capacitació i la retenció del personal sanitari als països en desenvolupament, especialment als països menys avançats i als petits estats insulars en vies de desenvolupament

3.d Reforçar la capacitat de tots els països, en particular els països en vies de desenvolupament, en matèria d' alerta primerenca, reducció de riscos i gestió dels riscos per a la salut nacional i mundial

Es ressalta la fita 3.9 on el present treball pot millorar l'assoliment del ODS.

1.2.3 ODS 6 – Aigua neta i Sanejament

Aquest ODS té com a finalitat:

Garantir la disponibilitat d' aigua i la seva gestió sostenible i el sanejament per a tothom

Encara hi ha milers de milions de persones (principalment en àrees rurals) que no tenen accés a aigua potable i sanejament.
A tot el món, una de cada tres persones no té accés a aigua potable salubre, dues de cada cinc persones no disposen d'una instal·lació bàsica destinada a rentar-se les mans amb aigua i sabó, i més de 673 milions de persones encara fan les seves necessitats a l'aire lliure.

La pandèmia de la COVID-19 ha posat de manifest la importància vital del sanejament, la higiene i un accés adequat a aigua neta per prevenir i contenir les malalties.
D'acord amb l'Organització Mundial de la Salut, el rentat de mans és una de les accions més efectives que es poden dur a terme per reduir la propagació de patògens i prevenir infeccions, inclòs el virus de la COVID-19.
Tot i així, hi ha milers de milions de persones que no tenen accés a aigua salubre i sanejament, i els fons destinats a millorar-ho són insuficients.

Les fites de l'ODS 6 són:

6.1 D' aquí a 2030, assolir l'accés universal i equitatiu a l'aigua potable a un preu assequible per a tothom

6.2 D' aquí a 2030, assolir l'accés a serveis de sanejament i higiene adequats i equitatius per a tothom i posar fi a la defecació a l'aire lliure, tenint especial cura en les necessitats de les dones i les nenes, i les persones en situacions de vulnerabilitat

6.3 D' aquí a 2030, millorar la qualitat de l'aigua reduint la contaminació, eliminant l'abocament i minimitzant l'emissió de productes químics i materials perillosos, reduint a la meitat el percentatge d'aigües residuals sense tractar i augmentant considerablement el reciclat i la reutilització sense riscos a nivell mundial

6.4 D'aquí al 2030, augmentar considerablement l'ús eficient dels recursos hídrics en tots els sectors i assegurar la sostenibilitat de l' extracció i l'abastament d' aigua dolça per fer front a l'escassetat d' aigua i reduir considerablement el nombre de persones que pateixen manca d'aigua.

6.5 D'aquí al 2030, implementar la gestió integrada dels recursos hídrics a tots els nivells, fins i tot mitjançant la cooperació transfronterera, segons escaigui

6.6 D'aquí al 2020, protegir i restablir els ecosistemes relacionats amb l'aigua, inclosos els boscos, les muntanyes, els aiguamolls, els rius, els aqüífers i els llacs

6.a D'aquí a 2030, ampliar la cooperació internacional i el suport als països en desenvolupament per a la creació de capacitat en activitats i programes relatius a l'aigua i el sanejament, com els de captació d'aigua, dessalinització, ús eficient dels recursos hídrics, tractament d'aigües residuals, reciclat i tecnologies de reutilització

6.b Donar suport i enfortir la participació de les comunitats locals en la millora de la gestió de l'aigua i el sanejament

1.2.4 OBS 13 – Acció pel clima

Aquest ODS té com a finalitat:

Adoptar mesures urgents per combatre el canvi climàtic i els seus efectes.

Els nivells de diòxid de carboni (CO_2) i d'altres gasos d'efecte hivernacle a l'atmosfera van augmentar fins a nivells rècord el 2019.

El canvi climàtic està afectant tots els països de tots els continents. Està alterant les economies nacionals i afectant diferents vides. Els sistemes meteorològics estan canviant, els nivells del mar estan pujant i els fenòmens meteorològics són cada vegada més extrems.

Cal prendre mesures urgents per abordar l'emergència climàtica per tal de salvar vides i mitjans de subsistència.

Les fites de l'ODS 13 són:

13.1 Enfortir la resiliència i la capacitat d' adaptació als riscos relacionats amb el clima i els desastres naturals a tots els països

13.2 Incorporar mesures relatives al canvi climàtic en les polítiques, estratègies i plans nacionals

13.3 Millorar l' educació, la sensibilització i la capacitat humana i institucional respecte de la mitigació del canvi climàtic, l' adaptació a ell, la reducció dels seus efectes i l' alerta primerenca

13.a Complir el compromís dels països desenvolupats que són parts en la Convenció Marc de les Nacions Unides sobre el Canvi Climàtic(*) d'aconseguir per a l'any 2020 l'objectiu de mobilitzar conjuntament 100.000 milions de dòlars anuals procedents de totes les fonts a fi d'atendre les necessitats dels països en desenvolupament respecte de l'adopció de mesures concretes de mitigació i la transparència de la seva aplicació, i posar en ple funcionament el Fons Verd per al Clima capitalitzant-lo al més aviat possible

13.b Promoure mecanismes per augmentar la capacitat per a la planificació i gestió eficaços en relació amb el canvi climàtic als països menys avançats i els petits Estats insulars en desenvolupament, fent particular èmfasi en les dones, els joves i les comunitats locals i marginades

(*) La Convenció Marc de les Nacions Unides sobre el Canvi Climàtic és el principal fòrum intergovernamental internacional per negociar la resposta mundial al canvi climàtic.

1.3 Abast del Treball

Aquest treball es limita a analitzar els punts especificats en els objectius establerts.

Queda fora de l'abast d'aquest treball:

- Avaluar aspectes dels dispositius que no siguin estrictament els relatius a ciberseguretat.
- Fer un treball d'investigació científica sobre aspectes biològics, químics o físics del tractament de l'aigua. Per exemple: no es presenten solucions a problemes bioquímics de descontaminació.
- Disseny de nous dispositius IoBNT.

1.4 Impacte en sostenibilitat, ètic-social i de diversitat

Aquest treball pretén, mitjançant la seva contribució a la millora de la ciberseguretat de dispositius IoBNT per al tractament de l'aigua en l'àmbit de la Salut Pública, millorar la consecució dels ODS 3, 6 i 13, per la qual cosa el seu impacte en sostenibilitat és positiu,

ja que intrínsecament ja contempla uns objectius sostenibles i no suposa el malbaratament de recursos (ni escassos ni abundants).

L'aigua és un recurs universal i necessari per a tot ésser viu del planeta. Aquest treball té un impacte ètic-social positiu, perquè té un compromís amb la humanitat, ja que la seva comesa contribueix a millorar la ciberseguretat de dispositius IoBNT que intervenen en el tractament de l'aigua en l'àmbit de la Salut Pública.

I en l'àmbit de la diversitat, l'impacte és positiu, perquè aquest treball està adreçat a tothom i beneficia a tothom, sense fer distincions de gènere, raça, religió, nivell cultural o social. És un treball dirigit a tot el planeta i que beneficia a tots els éssers vius.

1.5 Enfocament i mètode seguit

El mètode seguit per realitzar aquest treball és l'anàlisi descriptiu de les vulnerabilitats i la gestió de riscos d'utilització de dispositius d'IoBNT en aplicacions de tractament de l'aigua en el marc del sector de la Salut Pública.
Les vulnerabilitats en ciberseguretat identificades fins el moment actual en els dispositius d'IoBNT no apareixen en l'inventari de vulnerabilitats de programes com CVE.org[Z903] o organitzacions com l'INCIBE[Z904].
El mètode utilitzat per fer la recopilació de vulnerabilitats ha estat analitzar la bibliografia existent sobre aspectes de seguretat de dispositius IoBNT de varis autors i extreure'n aquelles vulnerabilitats que poden afectar a la cibersegureta. [48] [50] [51]

Anàlogament, el mètode seguit per a analitzar la gestió de riscos ha estat el mateix que per les vulnerabilitats sobre seguretat en dispositius IoBNT, però copsant-ne els riscos i contramesures identificats pels autors que afecten o poden afectar a la gestió de riscos en ciberseguretat. [48] [50] [51]

Aquest document pretén representar un punt de partida per al futur disseny i desenvolupament de solucions efectives de seguretat, en entorns on els dispositius IoBNT per a tractament de l'aigua participin en el marc de Salut Pública.

1.6 Planificació del Treball

La planificació, a alt nivell, prevista per a la realització del TFM és la següent:

Tasques	**Jornades**
Estudi previ i identificació dels aspectes rellevants de la proposta de TFM	7
Definició d' objectius sobre seguretat d'IoBNT	2
Definició de la metodologia, planificació temporal i de recursos	4
Anàlisi de requeriments de seguretat d'IoBNT	7
Elecció d' eines, tecnologies i fonts d' informació adequades relatius a dispositius IoBNT de tractament de l'aigua	10
Disseny de la proposta de TFM	8

Redacció de la proposta TFM	50
Anàlisi i tractament de l' impacte ètic-social, de sostenibilitat i de diversitat del anàlisi de seguretat de dispositius IoBNT de tractament de l'aigua	6
Preparar entregues parcials (PACs)	12
Conclusions i discussió dels resultats obtinguts del anàlisi de seguretat de dispositius d'IoBNT de tractament de l'aigua	12
TOTAL	**118**

Taula 1. Estimació de jornades previstes (elaboració pròpia)

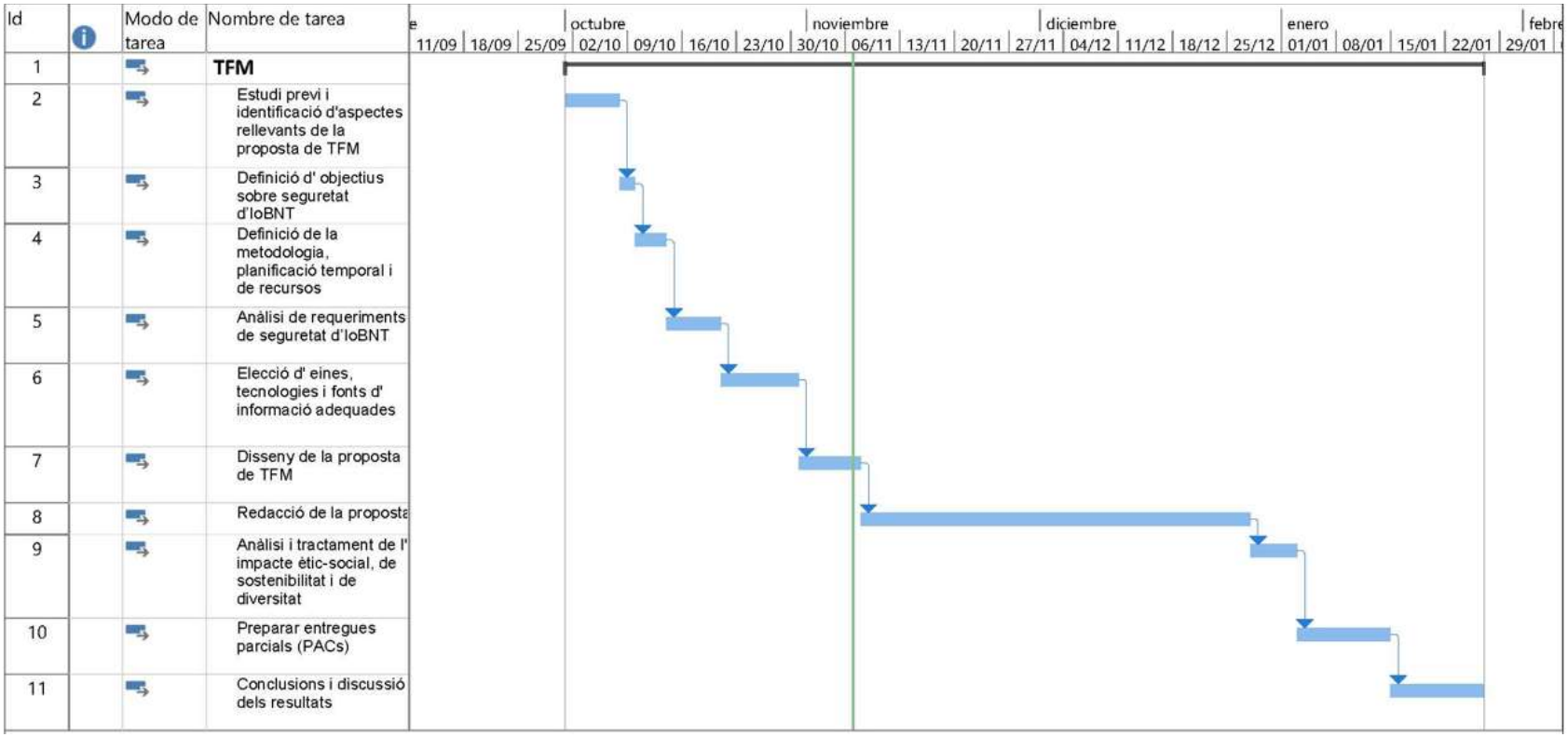

Figura 1. Planificació TFM

1.7 Breu descripció dels altres capítols de la memòria

Els diferents capítols del treball consisteixen en:

- Descripció de les nanotecnologies i bio-nanotecnologies actuals que intervenen en el procés de tractament de l'aigua.
- Descripció dels components que intervenen en l'arquitectura general IoBNT per tenir una visió general de com és l'arquitectura d'un sistema que interactua amb dispositius d'IoBNT que pot ser susceptible de patir un ciberatac.
- Identificar les necessitats de seguretat de dispositius IoBNT per la qual cosa es realitzarà:
    - Anàlisi descriptiu de les amenaces i vulnerabilitats de dispositius IoBNT.
    - Identificar tipus d'atacs dels dispositius d'IoBNT i descriure el mecanisme de l'atac.
    - Establir mesures de mitigació segons els atacs identificats

2 Materials i mètodes

2.1 Noves tecnologies per al tractament de l'aigua

L'aplicació de la nanotecnologia i bio-nanotecnologia en el tractament d'aigües ofereix una oportunitat per millorar l'eficiència i l'assequibilitat dels tractaments mitjançant l'ús de nanomaterials i bio-nanomaterials.
El potencial de les nanotecnologies per transformar la purificació de l'aigua aplana el camí cap a recursos hídrics més nets i sostenibles, i suposa un revulsiu en el camp del tractament d'aigües.

2.1.1 Principals nanotecnologies en el tractament de l'aigua

Aprofitant tècniques científiques com: fotocatàlisi, nanofiltració i nanoadsorció, s'han manipulat àtoms i molècules, que han permès crear nanomaterials (o nanopartícules) amb precisió que combinats amb tècniques aplicades a escala nano en resulta una funcionalitat extraordinària en el camp del tractament d'aigües.

Les diferents nanotècniques aplicades en el tractament de l'aigua són [7]:

- Fotocatàlisi: és eficaç per eliminar contaminants orgànics, metalls pesants i microbis
- Nanofiltració: utilitza materials basats en nanopartícules com nanomaterials de carboni, òxids metàl·lics i zeolites per a l'eliminació precisa de contaminants;
- Nanoadsorció: nanopartícules com nanosorbents de carboni, biosorbents, nanosorbents d'òxid metàl·lic, zeolites i ferro valent Nano Zero adsorbeixen una àmplia gamma de contaminants per a la seva posterior eliminació.

Mitjançant la integració d'aquestes tecnologies de nanopartícules, la gestió de les aigües residuals aconsegueix un enfocament integral per abordar, per exemple, diversos contaminants.

Les nanopartícules o nanomaterials desenvolupats i usats internacionalment per al tractament d'aigües són:

- Nanosemiconductors per a fotocatàlisi, com el TiO2 (Diòxid de Titani) o el ZnO (Òxid de zinc).
- Nanomaterials per a nanofiltració
    - Nanotubs de carboni (CNT) [Z7]
    - Zeolites.
    - Òxids metàl·lics
- Nanomaterial per a nanoadsorció:
    - Nanotubs de carboni
    - Biosorbents
    - Zeolites com adsorbents
    - Ferro valent nano zero

D'altra banda, s'han desenvolupat nanodispositius per a monitoritzar la qualitat de l'aigua:

- Nanobiosensors[8] [9]

La figura 2 il.lusta una visió de l'ús de nanopartícules i nanotècniques en l'àmbit de la gestió i tractament d'aigües residuals.

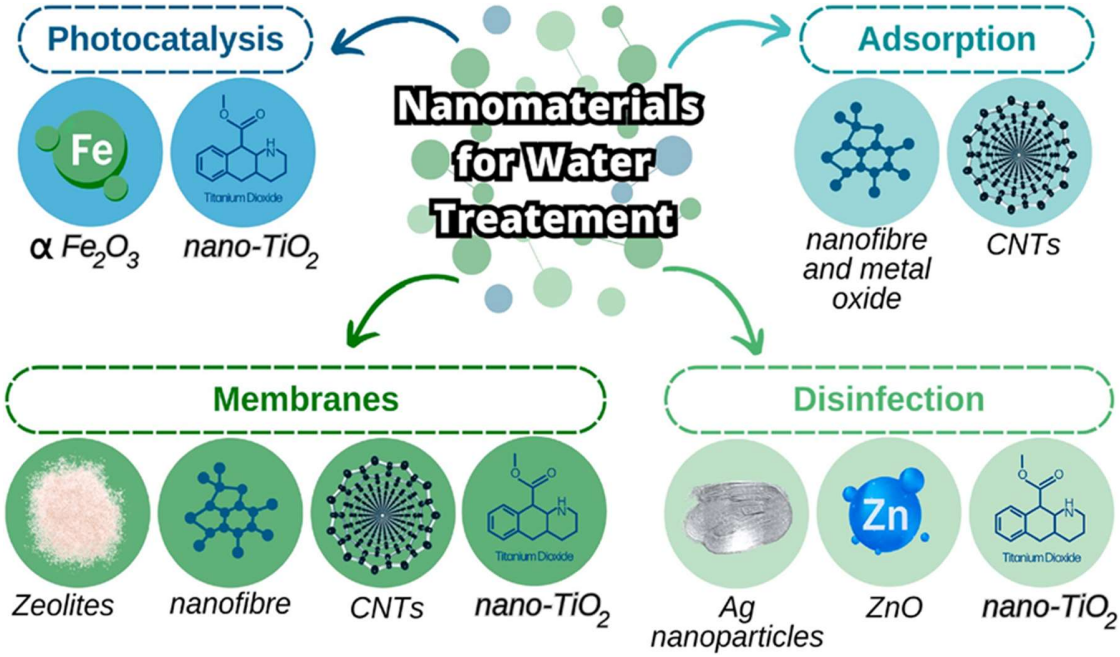

Figura 2. Esquema de l'ús de nanopartícules en la gestió d'aigües residuals

2.2 Els dispositius IoBNTs

Els sistemes naturals IoBNT com nanoxarxes biològiques home-cos, nanoxarxes nervioses, nanoxarxes bacterianes o xarxes de comunicació vegetal, són els que inspiren als investigadors en el disseny de sistemes artificials IoBNT i en la investigació de diversos tipus de BNT, incloent-hi BNT basats en cèl·lules d'enginyeria, màquines moleculars i nanomàquines autoassamblades. [10]

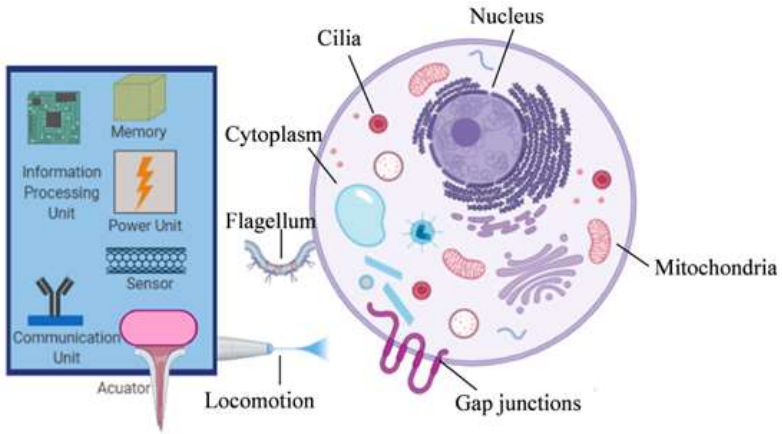

Figura 3. Bio-nano cosa (BNT): Analogia entre els components d'un dispositiu de computació típic d'IoT i els elements d'una cèl·lula biològica

El concepte de bio-nanomàquina [11] sorgeix com una abstracció de les eines disponibles per programar, controlar i interactuar amb estructures computacionals en l'entorn biològic.

En particular, una bio-nanomàquina s'identifica amb una cèl·lula programable [12], que és possible gràcies als últims desenvolupaments en biologia sintètica i nanotecnologia..

Mentre que la biologia sintètica proporciona eines per aprofitar el codi genètic de les cèl·lules biològiques, permetent la manipulació del comportament i les funcionalitats cel·lulars [13], la nanotecnologia possibilita el desenvolupament de cèl·lules artificials des de zero [14].

Per tant, la utilització de les eines d'ambdues disciplines permeten construir bio-nanomàquines.

Els components primaris d'una bio-nanomàquina són les unitats funcionals bàsiques utilitzades per les cèl·lules, és a dir, molècules orgàniques (àcids nucleics, proteïnes, etc.). Aquests s'organitzen entre si per formar estructures i interaccionar mitjançant reaccions químiques.

En concret, com mostra la figura 4, gràcies a les tecnologies esmentades, podem comparar els elements moleculars d'una cèl·lula amb els elements d'una nanomàquina.

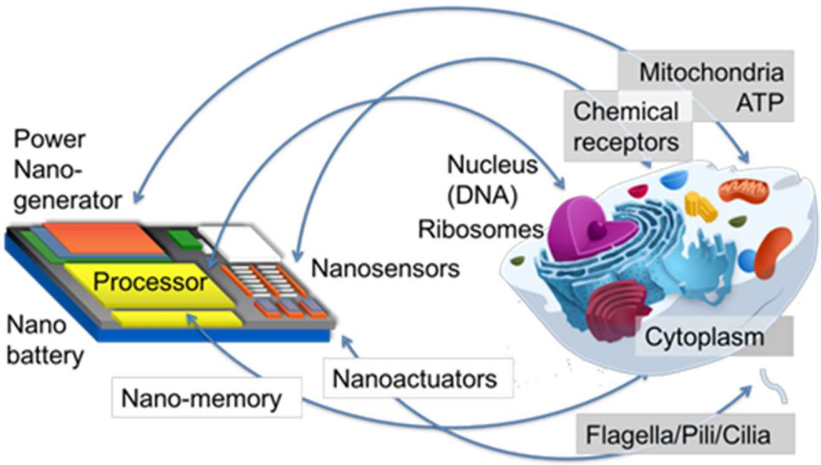

Figura 4.Relació funcional entre elements d'una nanomàquina i una cèl·lula biològica

És a dir:

- El processador de la nanomàquina són: les molècules, les reaccions químiques i les estructures moleculars (per exemple, els ribosomes) que permeten que la informació de l'ADN s'expressi en proteïnes o comportaments cel·lulars.
- La nanomemòria correspon al contingut molecular de tota la cèl·lula.
- La nanobateria és la reserva de la molècula de trifosfat d'adenosina (ATP) gestionada per altres estructures moleculars, els mitocondris.
- Els nanosensors i nanoactuadors corresponen a les molècules i a l'estructura molecular capaces de reaccionar o interactuar amb l'entorn extern.
- Finalment, les cèl·lules es comuniquen entre sí i amb l'entorn principalment mitjançant l'intercanvi de molècules a nanoescala, és a dir, comunicació molecular (Molecular Communication, MC). Un concepte que s'explica més endavant.

2.2.1 Coses BioNano (BioNano Things, BNT)

En el marc d'IoBNT, les coses bionano (BNT) es defineixen com a unitats estructurals i funcionals bàsiques que operen a escala nano dins de l'entorn biològic [10]. Les BNT tenen funcionalitats típiques dels dispositius informàtics incrustats en IoT, com ara detecció, processament, actuació i comunicació.

Per construir BNT, un enfocament és miniaturitzar dispositius elèctrics amb nanotecnologia i encapsular aquests dispositius per a la biocompatibilitat. No obstant això, a una mida tan petita, els BNT elèctrics miniaturitzats pateixen falta d'espai per a les bateries per proporcionar suficient potència i antena que generi freqüències utilitzables.[15]

Un altre enfocament per construir BNT és utilitzar unitats biològiques com substrats, com ara cèl·lules, que es poden considerar dispositius independents que poden recollir la seva energia del medi ambient [16]

Una altra classe important de BNT són les màquines moleculars i les nanomàquines autoassamblades, que són petits dispositius artificials amb mides entre 1 i 100 nm [17],[18]:

- Les màquines moleculars són sistemes moleculars sintètics que consisteixen en una o unes poques molècules que poden experimentar un moviment mecànic després d'una estimulació que desencadena una tasca útil [19].

- Les nanomàquines autoassamblades són dispositius a nanoescala que es construeixen a partir d'una organització autònoma o programada de molècules, i poden realitzar funcions similars a màquines moleculars, normalment a escales de major longitud.[20]

Un altre enfoc són les nanomàquines inorgàniques híbrides. Es tracta de dispositius inferiors a 100 nanòmetres de mida que poden estar fets de metall, òxid metàl·lic o nanopartícules híbrides [20].
En comparació amb les nanomàquines autoassamblades i les màquines moleculars, que involucren components biomoleculars "tous", les nanomàquines inorgàniques híbrides tendeixen a ser més rígides estructuralment, però, menys biocompatibles. A més, la seva interacció amb estímuls externs, com la llum, camps magnètics i elèctrics, també tendeixen a ser molt més forts, la qual cosa les fa més interessants per a aplicacions controlades externament [20].

2.2.2 Mètodes de comunicació per a IoBNT

Les formes convencionals de comunicacions electromagnètiques (EM) no es consideren adequades per connectar BNTs, principalment a causa de les limitacions de mida de l'antena, problemes de biocompatibilitat i l'atenuació severa dels senyals electromagnètics en medis fisiològics rellevants per a aplicacions IoBNT[10]. A causa d'aquests entrebancs, s'han investigat mètodes alternatius de comunicació.

Es poden classificar els mètodes de nanocomunicació en dos tipus principals:
(i) Comunicacions Moleculars (MC, sigles en anglès)[21]
(ii) Electromagnètica de banda THz (THz-band EM, en anglès) [23]

També s'han investigat altres tècniques basades en acoblament magnètic, transferència de calor, etc, però l'enfocament de comunicació molecular es considera el millor mètode de nanocomunicació per habilitar IoBNT.

(i) *Comunicacions Moleculars:*
És una tècnica bio-inspirada de comunicació que utilitza molècules per transferir informació.

En concret, s'utilitzen característiques físicament distingibles de les molècules (per exemple, el seu tipus o la concentració), per codificar informació. El moviment molecular aleatori en un canal fluid s'utilitza com a mitjà de propagació de senyals per a la transferència d'informació. Per tant, els missatges es codifiquen en les pròpies molècules, i després es transmet al receptor a través de la propagació molecular en un canal fluid.

La informació es pot codificar en la concentració, el tipus, el temps d'alliberament o l'estat electrònic de les molècules [22]. D'entre els diferents tipus de mètodes de propagació de missatges moleculars, el que resulta més atractiu és la difusió passiva, ja que no requereix consum energètic i s'adapta perfectament a les limitacions energètiques de les nanomàquines.

Un parell d'escenaris de MC entre parells de nanomàquines s'il·lustren a la Figura 5, on els missatges es codifiquen en la concentració de molècules, i després es transmet al receptor a través de la propagació molecular en un canal fluid.

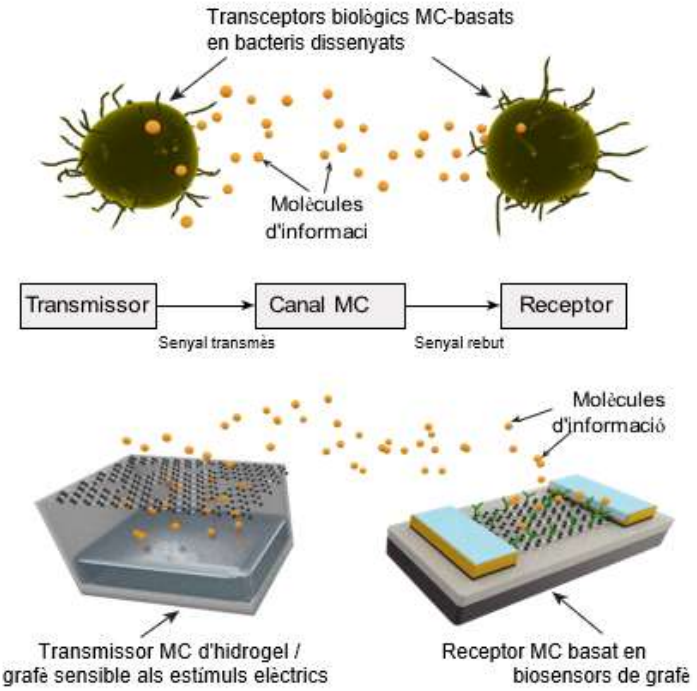

Figura 5. Components d'un sistema MC amb enfocaments biològics i basats en el disseny de transmissors i receptors MC basats en nanomaterials

(ii) *Nanocomunicació electromagnètica en banda THz*
La comunicació electromagnètica convencional (EM) no es considera adequada per a IoBNT perquè la mida de les BNT fa necessària freqüències de funcionament molt altes [23].

Això ha fet que es desenvolupin dissenys de nanoantenes incorporant grafè basades en plasmons [24] (plasmó es una quasipartícula que, tècnicament, es poden definir com oscil·lacions de la densitat d'electrons). Els plasmons són considerats medis de transmissió d'informació que poden assolir altes freqüències (de fins a 100 THz) [25], per tant, es poden tenir nanoxarxes EM de BNT basats en nanomaterials que utilitzen aquesta tècnica de comunicació EM d'escala nano.[26]

2.2.3 Interfície Biocibernètica

La interfície biocibernètica, també anomenada Interfície Bio-Ciber Nano-Macro, és el dispositiu més sofisticat en les aplicacions IoBNT.

La majoria de les aplicacions IoBNT previstes requereixen una interfície nano-macro bidireccional que pugui connectar perfectament les nanoxarxes a les xarxes convencionals externes (per exemple, Internet), i viceversa [27].

Tenint en compte que la comunicació molecular (MC) és el millor mètode a utilitzar per a IoBNT, la interfície és capaç de realitzar la conversió entre senyals bioquímics i altres formes de senyal que es puguin processar i comunicar fàcilment a través de xarxes convencionals, com ara electromagnètiques, elèctriques i òptiques.

Es consideren diverses tècniques per habilitar aquesta interfície nano-macro.

2.2.3.1 Interfícies elèctriques

Aquests són els dispositius que poden transduir senyals moleculars en senyals elèctrics, i viceversa.

Els biosensors elèctrics poden servir fàcilment per a la funció de convertir senyals MC en senyals elèctrics[28], però la conversió de senyals elèctrics a senyals moleculars és més difícil en segons quines aplicacions, per exemple intracos, a causa del problema de mantenir la generació o subministrament continu de molècules un cop es detecta el senyal elèctric.[29]

També es pot tenir una interfície macro-nano que pugui connectar IoBNT a la xarxa de comunicació externa, amb la integració d'antenes de comunicació, com antenes d'identificació per radiofreqüència (RFID). [30] Encara que existeix un repte en la miniaturització d'aquests dispositius així com el seu funcionament continu.

2.2.3.2 Interfícies òptiques

La llum representa una modalitat alternativa per interactuar IoBNT amb xarxes externes. En el cas que la comunicació molecular (MC), aquesta interfície òptica es pot realitzar amb l'ajuda de proteïnes sensibles a la llum i proteïnes bioluminescents / fluorescents.[31]

El control òptic de cèl·lules excitables, (per exemple, neurones i cèl·lules musculars), es pot aconseguir mitjançant una tècnica anomenada optogenètica [32].

2.2.3.3 Altres mètodes d'interfície

Depenent de la modalitat de comunicació utilitzada en IoBNT, hi ha alguns altres mètodes d'interacció nano-macro com, per exemple, l'ús de nanopartícules magnètiques (MN) com a portadores d'informació en un sistema de comunicació molecular (MC), tenint un detector de nanopartícules magnètiques portable en forma d'anell per connectar la comunicació molecular (MC) a una retroalimentació basada en radiofreqüència (RF). [33].

Un altre modalitat és el control de senyals de comunicació molecular (MC) basats en nanopartícules magnètiques (MN) en canals microfluids amb camps magnètics externs [34].

2.2.4 Arquitectura IoBNTs

En termes generals, els components de l'arquitectura IoBNT [35] són els següents:

- Nanonodes (coses Nano o BNT)
- Nanorouters
- Interfície Biocibernètica
- Passarel.la (o gateway)
- Servidor d'aplicació

La taula 2 mostra una breu descripció de cada un [36]. En apartats anteriors ja s'han detallat característiques i funcionament d'alguns d'ells:.

Components	**Descripció**
Nanonodes	Són nanodispositius senzills formats per BNTs que realitzen tasques com ara detecció de dades, transmissió i computació.
Nanorouters	Dispositius més avançats que els nanonodes en termes d'informàtica i emmagatzematge. S'encarreguen de recollir informació dels nanonodes i controlar els nanonodes amb ordres de control senzilles (p.ex: on/off, sleep, read value, etc.).
Interfície biocibernètica	Dispositiu híbrid que converteix el senyal bioquímic rebut de nanoxarxes en senyal elèctric per al seu processament per xarxes externes i viceversa.
Passarel·la	Dispositius híbrids que es poden utilitzar tant en xarxes clàssiques com nanoxarxes a escales micro i macro. Aquests dispositius permeten el control remot de les xarxes IoBNT dissenyades a través d'Internet.
Servidor d'aplicació	Aquests dispositius s'encarreguen de l'emmagatzematge, anàlisi, monitoratge en temps real de la informació procedent de nanoxarxes.

Taula 2. Components d'arquitectura IoBNT

La Figura 6 il·lustra un exemple d'arquitectura d'IoBNT de l'entorn sanitari.

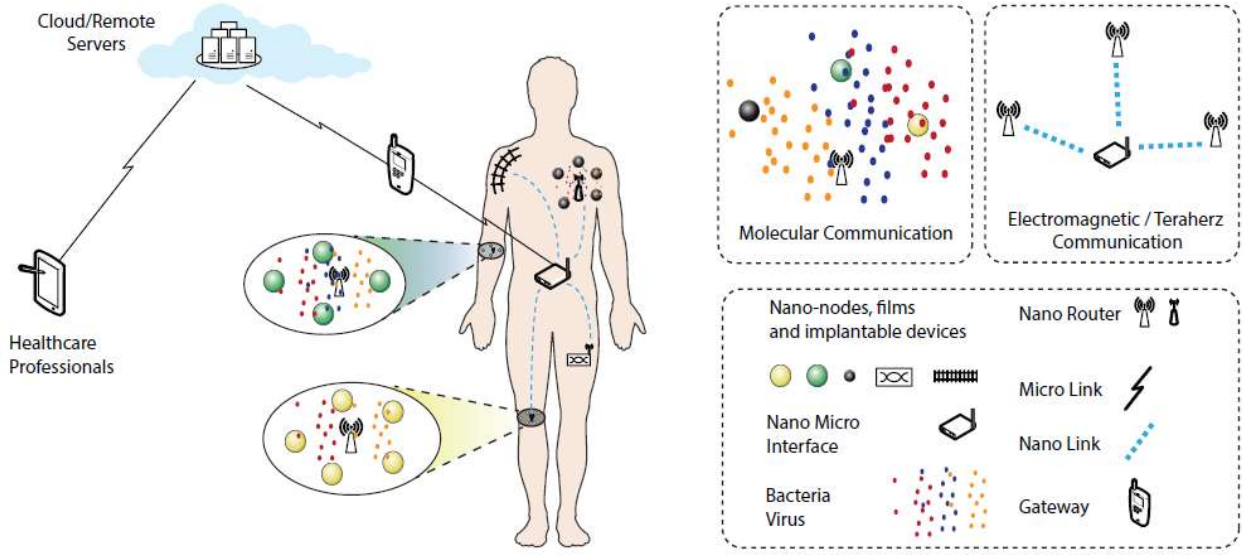

Figura 6. Una arquitectura de xarxa típica IoNT i IoBNT per a aplicacions sanitàries

2.2.4.1 Xarxa Nano o Nanoxarxa

La xarxa nano o nanoxarxa consta de diversos dispositius (per exemple, nanonodes, nanorouter,...) a escala nano (1-100 nm), interconnectats que treballen en col·laboració per realitzar tasques exclusives i col·laboratives de manera distribuïda com detecció, actuació, monitorització i control.

2.2.4.2 Dispositius passarel·la

Els dispositius passarel.la o gateway són una part integral de la majoria de les aplicacions d'IoT, on funcionen com un dispositiu de retransmissió entre sensors i Internet i garanteix una recepció eficient del senyal de tecnologies de baix rang de transmissió (NFC, RFID, Bluetooth LE, etc.).

El punt d'accés pot ser un punt d'accés WiFi, que ajuda a encaminar el trànsit del sensor al servidor.

2.2.4.3 Servidor d'aplicació

El servidor actua com un repositori en on s'emmagatzemen, analitzen i processen totes les dades recollides dels dispositius d'IoBNT.

Aquest servidor també pot actuar com un terminal per al monitoratge en temps real i continu on, donat el cas, es maneguen situacions crítiques mitjançant l'enviament de missatges d'alerta.

Només les entitats autoritzades haurien de poder accedir a aquest servidor per enviar instruccions i analitzar les dades recollides.

2.3 Dispositius IoBNT per al tractament d'aigua

Els dispositius IoBNT incorporen tecnologia a nivell nanoescala per detectar, purificar i monitoritzar la qualitat de l'aigua en aspectes d'agents contaminants, nivell de pH, presència de metalls pesants, patògens, etc,,, Estan basats en les nanotecnologies explicades en l'apartat 2.1.1 del present treball.

- Nanorobots depuradors: Robots d'escala nano que identifiquen i eliminen contaminants presents a l' aigua, contribuint així a la purificació del recurs hídric. [66]

- Nanosensors de monitoratge remot: Sensors connectats a la IoBNT que permeten la supervisió en temps real de paràmetres ambientals i del sistema de tractament d'aigua. [67]

- Nanofiltrants: Materials nanoestructurats utilitzats en sistemes de filtració per eliminar impureses i millorar l'eficiència del tractament de l'aigua. [68]

- Nanomembranes: Membranes nano-optimitzades per a processos d'osmosi inversa i filtració, millorant l'eficiència de la purificació de l'aigua. [69]

- Nanocomunicadors moleculars: dispositius per a comunicació mitjançant senyals biomoleculars per coordinar accions i optimitzar processos de detecció en temps real. [70]

- Nanodesinfectants: nanodispositius que empren propietats antimicrobianes per desinfectar l'aigua, eliminant bacteris i altres patògens. [71]

- Nanoabsorbents: Materials nanoestructurats dissenyats per absorbir i retenir contaminants químics presents a l' aigua. [72]

Aquesta relació reflecteix la diversitat de dispositius IoBNT aplicats al tractament de l'aigua, aprofitant la nanotecnologia per millorar l'eficiència, precisió i sostenibilitat dels processos de purificació.

2.4 Característiques de seguretat dels dispositius IoBNT

Un dels principals reptes relacionats de les aplicacions IoBNT és la realització d'una interfície pràctica i segura entre la bionano xarxa i Internet.[37]

Els dispositius d'IoBNT no estan exempts de patir atacs, usos malintencionats o accessos maliciosos.

Un esquema general que representa una interfície bio-cibernètica es presenta a la Figura 7. L'arquitectura consta d'un mòdul de comunicació sense fils per connectar amb Internet i un transductor per permetre la transformació cibernètica de la informació biològica i viceversa.[38]

Una arquitectura d'interfície bio-cibernètica segura depèn del lloc i funció on s'apliqui, així com de la naturalesa física/aquosa/cel·lular de la implementació electromagnètica.

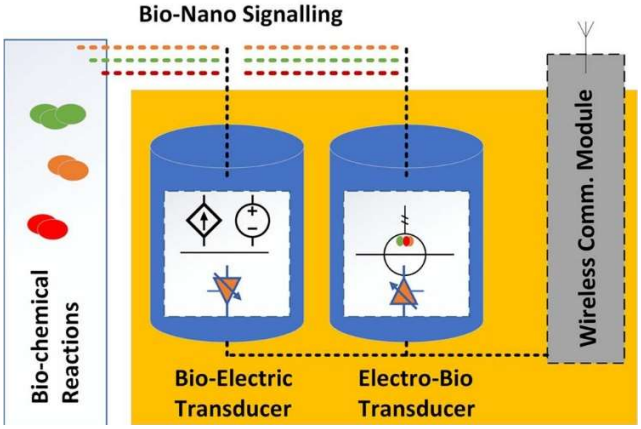

Figura 7. Esquema genèric d'interacció bio-cibernètica

En aquest apartat s'analitzarà les necessitats de seguretat per a nano xarxes i interfícies bio-cibernètiques.

Els objectius de seguretat, independentment de les variacions tecnològiques inherents, són el mateixos que altres entorns no IoBNT [39]

L'enfocament d'amenaces STRIDE [40] modela les amenaces de seguretat contra IoBNT on cada categoria d'amenaça està relacionada amb un objectiu de seguretat tal i com es reflecteix a la Taula 3.

Amenaça	**Objectiu Seguretat**	**Possible Escenari IoBNT**
Spoofing	Autenticació	Bretxa de seguretat per intercepció de la comunicació entre el dispositiu d'IoBNT i la resta del sistema
Manipulació	Integritat	En escenaris de purificació i descontaminació, el comportament del dispositiu pot ser alterat per part de l'atacant durant la transmissió
Repudiació	No-Repudiació	Supressió dels registres d'accés per eliminar rastres d'activitats malicioses dels usuaris
Divulgació informació	Confidencialitat	Bretxa de seguretat per intercepció de la comunicació entre dispositiu IoBNT i la resta del sistema
Denegació del servei	Disponibilitat	En escenaris de detecció de contaminants, incapacitat per transmetre valors de nivells irregulars d'agents contaminants en controls de cabdals d'aigua que depenen exclusivament de dispositiu IoBNT per a la comunicació amb la resta del sistema.
Elevació de privilegis	Autorització	Un atacant intern pot abusar del privilegi d'accés per robar o manipular informació

Taula 3. Categories de models d'amenaces STRIDE, objectius de seguretat relacionats i possibilitats d'atac a IoBNT

2.4.1 Les vulnerabilitats

Les vulnerabilitats en ciberseguretat identificades fins el moment actual segons la bibliografia analitzada:

- Consum d'aigua essencial per la vida: aquesta vulnerabilitat en una xarxa de bionanosensors que monitoritzen i rastregen la presència d'agents contaminants, un accés maliciós pot crear un greu problema de salut pública.

- Seguretat física: a causa de la seva petita mida, els dispositius IoBNT són vulnerables a manipulacions físiques i a patir danys.

- Exposició a internet: degut a la petita mida, els dispositius IoBNT tenen capacitats de càlcul i memòria limitades, i sense funcions (o amb funcions molt limitades) de seguretat integrades, això els fa vulnerables davant d'internet.

- Manca d'encriptació: hi ha manca de xifratge a la majoria dels IoBNT a causa de la seva mida reduïda i capacitats de càlcul limitades.

- Seguretat de la xarxa: els dispositius IoBNT es comuniquen a través de xarxes sense fils, que poden ser vulnerables a la pirateria informàtica i altres ciberamenaces. Garantir la seguretat d'aquestes xarxes és essencial per protegir les dades transmeses pels dispositius IoBNT.

- Protecció de dades: les dades recopilades pels dispositius IoBNT poden ser sensibles i protegir aquestes dades de l'accés no autoritzat es considera essencial. Això inclou tant les dades transmeses pel dispositius com les dades emmagatzemades en ells

- Vulnerabilitats del programari: el programari que s'executa en dispositius IoBNT està subjecte a vulnerabilitats que poden ser explotades pels pirates informàtics. Garantir que aquests dispositius es mantinguin al dia la data amb els últims "patches" de seguretat és important per prevenir.

- Seguiment i vigilància de la ubicació: alguns dispositius IoBNT utilitzats per al monitoratge de l'aigua poden estar equipats amb GPS o una altra tecnologia de seguiment de la ubicació. Això podria aprofitar-se per utilitzar-ho per fer seguiment d'individus, violant potencialment la seva privacitat.

- Susceptibilitat dels dispositius IoBNT als quimioatraients: la *quimiotaxi*[1] positiva fa que el IoBNT es vegi arrossegat cap a la substància química que l'atrau dins el medi que comparteixen. Un excés de substàncies quimioatraients pot fer canviar el comportament de certs dispositius IoBNTs cap una finalitat errònia.

- Susceptibilitat dels dispositius IoBNT als quimiorepel·lents: la quimiotaxi negativa fa que el IoBNT s'allunyi de la substància química que el repel·leix dins el medi que comparteixen. Un

[1]Quimiotaxi és un fenomen on les cèl·lules d'organismes uni/pluricel·lulars dirigeixen els seus moviments segons la concentració de certes substàncies químiques dins el medi ambient compartit.

excés de substàncies quimiorepel·lents pot fer canviar el comportament de certs dispositius IoBNTs allunyant-los de la seva finalitat.

- Manca de regulació: actualment hi ha una manca de regulació específica al voltant de l'ús de dispositius IoBNT.

2.4.2 Els riscos

Respecte els riscos als que estan sotmesos els dispositius o sistemes amb IoBNTs, la bibliografia avaluada n'identifica els següents:

- Dispersió d'agents contaminants: aprofitar una xarxa dispositius IoBNTs de monitoratge de qualitat d'aigua per col·locar-ne d'aliens amb agents contaminants.

- Manipulació física no autoritzada dels IoBNTs: facilitat d'accés físic als dispositius degut a la seva reduïda mida.

- Ciberamenaces o ciberatacs per manca de seguretat integrades als dispositius IoBNT davant d'internet.

- Ciberamenaces o ciberatacs per manca de seguretat de la xarxa sense fils per on es comuniquen els dispositius IoBNT.

- Informació sensible accessible per manca d'encriptació
- Accés no autoritzat a dades sensibles recopilades o trameses pels dispositius IoBNT per manca de seguretat.

- Errades del programari per manca de d'actualització nivell de seguretat del programari dels dispositius IoBNT.

- Violació de privacitat o seguiment d'individus per ús inadequat de GPS dels dispositius IoBNTs que en disposin.

- Alteració de comportament dispositius IoBNT desviant-lo cap a una finalitat no autoritzada o maliciosa mitjançant substàncies quimioatraients.

- Alteració de comportament dispositius IoBNT allunyant-los de la seva finalitat mitjançant substàncies quimiorepel·lents..

- Impunitat dels atacants, reiteració del delicte i complicacions per obtenir la prova forense de delictes a dispositius IoBNT o utilitzant dispositius IoBNT.

2.4.3 Tipus d'atacs

En l'àmbit IoBNT els atacs es poden produir a nivell de bio-nanoxarxa o d'interfície bio-cibernètica.

Nivell d'atac	Atac
Atacs a la Bio-Nanoxarxa	Escoltes
	Blackhole o atac de forat negre
	Atacs sentinella
Atacs a la Interfície Bio-cibernètica	Escoltes
	Atac de reproducció
	Atac Man-In-The-Middle (MITM)
	Esgotament de recursos
	Atacs d'injecció
	Manipulació de dispositius
	Atac de denegació de servei (DoS)
	Atacs de malware
	Atacs de firmware

Taula 4. Tipologia d'atacs a dispositius IoBNT

En els apartats subsegüents es descriuen com es produeixen aquests atacs identificats fins el moment.

2.4.3.1 Atacs a la Bio-nanoxarxa

2.4.3.1.1 Escoltes

Es refereix a interceptar la transmissió entre dos nodes. La informació interceptada (escoltada) pot ser emmagatzemada i posteriorment utilitzada maliciosament per llençar atacs.

Les escoltes en nanoxarxes poden tenir lloc quan:

> Dues nanomàquines (o nodes) legítimes intercanvien molècules missatgeres i una nanomàquina (o node) maliciosa propera intercepta les molècules missatgeres de manera silenciosa.

La nanomàquina (o node) maliciosa activa podria absorbir les molècules missatgeres en el cas que s'utilitzi comunicació molecular (MC) com a mitjà de comunicació,

El node maliciós actiu podria absorbir les molècules missatgeres en el cas en que s'utilitzi MC com a mitjà de comunicació, aquest atac es podria prevenir mitjançant la capacitat de secretisme [44].

2.4.3.1.2 Atac de forat negre o Balckhole

L'atac de forat negre es refereix a l'atac on nodes maliciosos propaguen molècules atraients per dirigir (atraure) el tràfic de la xarxa cap a una ubicació diferent de l'objectiu.

L'atac de blackhole és similar a l'atac de sinkhole (en català, dolina) a les xarxes de sensors inalàmbrics (WSN en anglès, Wireless Sensor Network), però l'atac sinkhole interromp el procés d'encaminament mentre que el blackhole allunya físicament els nodes legítims de l'objectiu.

Els atacs de forats negres són un tipus d'atac DoS (Denial of Service).

2.4.3.1.3 Atacs sentinelles

Els atacs sentinelles són oposats als atacs de forats negres, on els nodes (nanomàquines) legítimes són empeses lluny de l'objectiu, a causa d'un gran nombre de molècules repel·lents repartides per nodes maliciosos al voltant de l'objectiu.

2.4.3.2 Atacs a la Interfície Bio-cibernètica

Garantir la protecció d'extrem a extrem de les aplicacions IoBNT, implica la seguretat dels dispositius bionanoelectrònics.
Els vectors d'atac es descriuen en l'àmbit de les xarxes de sensors sense fils [49].

L'objectiu principal d'un dispositiu bionanoelectrònic en aplicacions IoBNT de tractament de l'aigua és permetre la comunicació bidireccional entre la bio-nanoxarxa i una xarxa externa (per exemple, internet).

La interfície bio-cibernètica tampoc està exempta de patir atacs. Els identificats fins el moment actual es descriuen en els subsegüents apartats.

2.4.3.2.1 Escoltes

Les escoltes es poden realitzar durant la comunicació de dispositius bionanoelectrònics amb nanonets biològics i durant la comunicació amb els dispositius passarel·la.

2.4.3.2.2 Atac de reproducció

Aquest tipus d'atac es pot llançar després d'un intent reeixit de caiguda d'escoltes.

La seqüència d'autenticació escoltada dels dispositius legítims es pot reproduir per obtenir accés il·legítim al canal de comunicació. A més, un atacant pot copiar ordres enviades prèviament d'usuaris legítims per reproduir el missatge de nou.

2.4.3.2.3 Atac Man-In-The-Middle (MITM)

Un atac MITM es projecta a través de dispositius il·legítims quan passen a formar part de la comunicació entre dispositius transmissors legítims, i els dispositius legítims són falsificats per creure que s'estan comunicant amb el dispositiu autoritzat.

Des de la perspectiva de la comunicació, l'atac MITM es pot aconseguir reproduint la seqüència d'autenticació legítima per accedir al canal de comunicació. MITM és el tipus d'atac d'escolta

actiu on l'atacant no només escolta la comunicació, sinó que també altera la seqüència de dades i comunicació.

2.4.3.2.4 Esgotament de recursos

Els dispositius bio-nanoelectrònics tenen limitació de recursos en termes d'espai, consum d'energia i complexitat de càlcul, degut a la seva reduïda mida.

L'atacant pot causar esgotament de recursos enviant múltiples missatges d'autenticació amb credencials incorrectes per ocupar i col·lapsar el processador. Cada sol·licitud d'autenticació ocupa la memòria per crear registres d'accés i consumeix bateria.

2.4.3.2.5 Atacs d'injecció

L'atac d'injecció pot ser realitzat pels usuaris il·legítims de tres maneres, inserció, alteració i replicació [56]:

- Inserció, l'atacant genera nous paquets de dades aparentment legítims al canal de comunicació.
- Alteració, l'atacant captura el paquet de dades de l'enllaç de comunicació i manipula els valors.
- Rèplica, l'atacant torna a enviar ordres prèviament executades al sistema.

La comunicació no segura entre dispositius bio-nanoelectrònics i els dispositius passarel·la poden provocar un atac d'injecció.

2.4.3.2.6 Manipulació de dispositius

Aquest atac és llançat principalment en els dispositius bionanoelectrònics per atacants propers, a causa del baix rang de transmissió dels dispositius. El dispositiu es pot reprogramar o substituir físicament per realitzar les tasques malicioses.

Aquest atac també es pot llançar accedint al dispositiu de forma remota mitjançant l'enviament d'actualitzacions falses del firmware que alteren la configuració del programari del dispositiu per realitzar l'ús maliciós. [59]

2.4.3.2.7 Atac de Denegació de Servei (DoS)

L'atac de denegació de servei provoca la interrupció i el bloqueig del flux d'informació entre les parts legítimes comunicants.

Un atacant intenta suspendre els serveis del dispositiu bionanoelectrònic, perquè no estigui disponible per a la comunicació i el processament. És possible aclaparar/col·lapsar la disponibilitat de potencials nodes IoBNT mitjançant el lliurament de missatges falsos.

2.4.3.2.8 Atacs de Programari Maliciós (Malware)

L'atac de malware és un altre tipus d'atac de xarxa que és comú en aplicacions basades en IoT.

L'atac de programari maliciós s'utilitza per controlar remotament un dispositiu llunyà de manera maliciosa, robar informació sensible d'un dispositiu i utilitzar-la per llançar més atacs de programari maliciós.

Els atacs de malware específics de les aplicacions IoBNT poden ser botnets, rootkit, ransomware i keylogger:

- Botnets: En aquest tipus d'atacs, l'atacant obté accés a diversos dispositius interconnectats llançant programari maliciós i controlant-los per robar informació, llançar un atac DDoS (Denegació de Servei Distribuïda) per llançar temps d'inactivitat del sistema no planificat i, fins i tot, vendre accés a la xarxa a altres ciberdelinqüents.

- Ransomeware: L'atacant s'apodera del dispositiu xifrant les dades de l'usuari i bloqueja el dispositiu, restringint així l'accés del propietari al dispositiu. L'atacant exigeix una quantitat de rescat.

- Keylogger: És un tros maliciós de codi que registra les pulsacions de tecles de l'usuari per accedir a ID i contrasenyes. Aquest atac és més perillós que els atacs de força bruta i les contrasenyes segures no proporcionen protecció contra aquest malware.

- Rootkit: S'instal·la un fragment de codi maliciós al dispositiu IoBNT que amaga la seva identitat per robar dades, reconfigurar el dispositiu o controlar el sistema executant comandes malicioses. Aquest tipus d'atac és més perillós, ja que eludeix tots els mecanismes de seguretat i amaga amb èxit la seva presència.

2.4.3.2.9 Atacs de Microprogramari (Firmware)

Les actualitzacions del firmware són necessàries per garantir el correcte funcionament del dispositiu.

Les actualitzacions del firmware es poden fer de forma remota.

Normalment, s'emet un anunci a la xarxa cada vegada que hi ha disponible una nova versió de l'actualització del firmware. Els atacants poden enviar sol·licituds falses d'actualització de firmware per tal d'accedir al firmware i programar-lo amb codi maliciós.

2.4.4 Estratègies de mitigació

En aquest apartat es detallen les accions per a mitigar i contramesures actuals als atacs descrits de la nanoxarxa com de la interfície bio-cibernètica.

2.4.4.1 Estratègies de mitigació per a la Bio-Nanoxarxa

2.4.4.1.1 Mitigació d'atacs d'Escolta

Com a mecanismes de detecció es tenen:

- El node maliciós passiu pot ser detectat en nanoxarxes per un mecanisme tal com la geometria estocàstica o tècniques d'estimació de distàncies [41].

- S'han postulat altres propostes per detectar la ubicació d'escoltes i assegurar la nanocomunicació:
  - Proposta d'un canal segur per a la comunicació molecular [42]. En primer lloc, s'intercanvia una clau segura basada en l'algorisme Diffie-Hellman entre la nanomàquina emissora i la nanomàquina receptora. A continuació, el xifratge del maquinari es realitza mitjançant la clau secreta. Encara que la seguretat general es compromet, ja que MC necessita models matemàticament més resistents per a la seguretat.
  - Proposta de un model matemàtic per a la detecció i localització d'intrusos en un passeig aleatori pel canal [43]. Aquest és l'únic treball en MC que considera la detecció d'un receptor maliciós absorbent en un passeig aleatori pel canal.

Com a mecanismes de prevenció d'escoltes previstos s'inclouen: beamforming[45], game theory [46] i generació de soroll [45].

Darrerament, s'ha proposat una mesura de prevenció mitjançant l'autenticació de capa física per a la Comunicació Molecular basada en Bifusió (DbMC, sigles en anglès) [47].

2.4.4.1.2 Mitigació d'atac de Forat negre

La contramesura a l'atac blackhole consisteix en:

Establir, als nodes legítims, un llindar de concentració de molècules atraients a partir del qual, quan els nodes legítims detecten concentracions de molècules atraients (dels nodes maliciosos) que superin el llindar, aleshores els nodes legítims generen les seves pròpies molècules atraients per desplaçar a les molècules atraients malicioses i redreçar l'encaminament cap a l'objectiu.

El mètode per decidir el llindar a considerar té dos enfocaments possibles: la regla de Bayes i l'enfocament llindar simple [48].

2.4.4.1.3 Mitigació de l'atac sentinella

La mitigació a l'atac sentinella també passa perquè els nodes legítims emetin molècules atraients capaces de redreçar el tràfic.

El mètode per decidir el llindar a considerar té els dos enfocaments possibles: la regla de Bayes i l'enfocament llindar simple [48].

2.4.4.2 Estratègia de mitigació per a la Interfície Bio-cibernètica

2.4.4.2.1 Mitigació de l'atac d'Escoltes

La mitigació de l'atac és: El xifratge.

Per a dispositius amb restriccions de recursos, com els IoBNT, s'ha demostrat que els esquemes de xifratge lleugers com la criptografia Elliptic Curve són eficaços [52] [53].

2.4.4.2.2 Mitigació de l'Atac de reproducció

La mitigació de l'atac de reproducció seria: Esquemes d'autenticació, Detecció d'intrusions o Delegar autenticació en dispositius externs. [61][64]

2.4.4.2.3 Mitigació de l'atac Man-In-The-Middle

La mitigació de l'atac de Man-In-The-Middle seria: Esquemes de xifrat amb esquema lleuger [54] d'encriptació adequat a les limitacions de recursos. [52] [53]

2.4.4.2.4 Mitigació de l'atac d'Esgotament de recursos

La mitigació d'atacs d'esgotament d recursos serien: Mecanismes de control d'accés, sistema de detecció d'anomalies i ús de font d'energia recarregable.

A més, també es pot aconseguir amb l'ús de mitjans de comunicació sense fils passius com senyals de radiofreqüència (RF) i l'ús de noves tècniques de preservació d'energia com ZPD (ZeroPower Defence) [55].

2.4.4.2.5 Mitigació de l'atac d'Injecció

Per a aquest tipus d'atacs, es necessiten estratègies de mitigació acurades que incloguin protocols d'autenticació [57], mecanismes de control d'accés [58] i detecció d'intrusos, validació d'entrada i tècniques d'autorització.

2.4.4.2.6 Mitigació de l'atac de Manipulació de Dispositius

Les estratègies per a mitigar aquest atac són: Prova de manipulacions i autodestrucció, enduriment del dispositiu i funció físicament no clonable [63] (PUF, Physically Unclonable Function).[2]

2.4.4.2.7 Mitigació de l'atac DoS

La mitigació d'aquest tipus d'atac és la Detecció d'intrusions. [61] [65]

2.4.4.2.8 Mitigació de l'atac de Malware

[2] Physically Unclonable Function (PUF): és una funció que afegeix soroll al IC (Intergrated Circuit) del dispositiu. El PUF és inclonable i a prova de manipulacions. A més, els PUF tenen una identificació i autenticació d'objectes únics que poden detectar canvis no desitjats en el IC.

Les estratègies de mitigació per aquests tipus d'atac serien: Control d'accés, monitorització del sistema, Antivirus, Detecció d'intrusions. [62][65]

2.4.4.2.9 Mitigació de l'atac de Firmware

Com a estratègia de mitigació per aquests tipus d'atac es tindria: Xifrat del firmware, actualitzacions periòdiques del firmware, detecció de firmware maliciós. [62]

3 Resultats

3.1 Resultats de l'anàlisi de vulnerabilitats i gestió de riscos

El resultat de l'anàlisi sobre vulnerabilitats, riscos, atacs i mitigació realitzat en apartats anteriors s'il·lustra amb la informació representada en les taules següents, on es reflecteix l'estat de l'art dels dispositius IoBNT en matèria de ciberseguretat respecte els objectius de seguretat de Confidencialitat, Integritat, Disponibilitat i Autenticació.

La taula 5 reflecteix les diferents vulnerabilitats identificades en dispositius IoBNT i quins riscs poden suposar pel que respecta a la ciber/seguretat.

Vulnerabilitat	**Risc**
Consum d'aigua essencial per la vida	Dispersió d'agents contaminants
Seguretat física	Manipulació física no autoritzada dels IoBNTs
	Destrucció de dispositius
Exposició a internet	Accés als dispositius IoBNT mitjançant internet
	Accés no autoritzat a dades sensibles recopilades
Manca d'encriptació	Accés no autoritzat a dades sensibles recopilades
	Alteració de comportament dispositius IoBNT
Seguretat de la xarxa	Accés mitjançant la xarxa sense fils als dispositius IoBNT
Protecció de dades	Accés no autoritzat a dades sensibles recopilades
Vulnerabilitats del programari	Errades del programari
	Alteració de comportament dispositius IoBNT
Seguiment i vigilància de la ubicació	Violació de privacitat o seguiment d'individus
Susceptibilitat dels dispositius IoBNT als quimioatraients	Alteració de comportament dispositius IoBNT
Susceptibilitat dels dispositius IoBNT als quimiorepel·lents	Alteració de comportament dispositius IoBNT
Manca de regulació/legislació específica	Impunitat dels atacants, reiteració del delicte

Taula 5. Vulnerabilitats / Riscos IoBNT (confecció pròpia)

Respecte els diferents tipus d'atacs i el nivell al que es poden produir:

- Per una banda tenim els atacs a la bionano xarxa i les seves estratègies de mitigació (taula 6):

Nivell d'atac	Atac	Estratègia Mitigació
Atacs a la Bio-Nanoxarxa	Escoltes	Mecanismes de geometria estocàstica o tècniques d'estimació de distàncies
		Proposta de canal segur per a la comunicació molecular
		Model matemàtic per detecció i localització d'intrusos en passeig aleatori
		Molecular Beamforming
		Game theory
		Generació de soroll
		Autenticació de capa física per a la Comunicació Molecular basada en Bifusió
	Blackhole o atac de forat negre	Llindar de concentració de molècules atraients segons regla de Bayes o llindar simple
	Atacs sentinella	Llindar de concentració de molècules atraients segons regla de Bayes o llindar simple

Taula 6.Bio-Nanoxarxa: Atac/Mitigació (elaboració pròpia)

També s'identifiquen els objectius de seguretat segons l'amenaça/atac que es pot produir a nivell de Bio-nanoxarxa. Es reflecteixen a la següent taula (taula 7):

Nivell d'atac	Atac	Objectiu de seguretat
Atacs a la Bio-Nanoxarxa	Escoltes	Confidencialitat
	Blackhole o atac de forat negre	Disponibilitat
	Atacs sentinella	Integritat

Taula 7. Objectiu de seguretat per atac a la Bio-nanoxarxa (confecció pròpia)

- Per una altra banda, es tenen els atacs que afecten a la interfície bio-cibernètica i les seves estratègies de mitigació (taula 8):

Nivell d'atac	Atac	Estratègia Mitigació
Atacs a la Interfície Bio-cibernètica	Escoltes	Encriptació o xifratge per esquema lleuger com criptografia Elliptic Curve
	Atac de reproducció	Esquemes d'autenticació
		Detecció d'intrusions
		Delegar autenticació en dispositius externs
	Atac Man-In-The-Middle (MITM)	Encriptació o xifratge per esquema lleuger com criptografia Elliptic Curve
	Esgotament de recursos	Mecanismes de control d'accés
		Sistema de detecció d'anomalies
		Ús de font d'energia recarregable
		Mitjans de comunicació sense fils passius com senyals de radiofreqüència
		Tècniques de preservació d'energia com ZeroPower Defence
	Atacs d'injecció	Protocols d'autenticació
		Mecanismes de control d'accés
		Detecció d'intrusos
		Validació d'entrada
		Tècniques d'autorització
	Manipulació de dispositius	Prova de manipulacions i autodestrucció
		Funció físicament no clonable (Physically Unclonable Function)
	Atac de denegació de servei (DoS)	Detecció d'intrusions
	Atacs de malware	Control d'accés
		Monitorització del sistema
		Antivirus
		Detecció d'intrusions
	Atacs de firmware	Xifrat del firmware
		Actualitzacions periòdiques de firmware
		Detecció de firmware maliciós

Taula 8. Interfície Bio-cibernètica/Atac/Mitigació

I també s'identifiquen els objectius de seguretat per atac a la interfície bio-cibernètica i es reflecteixen en la següent taula (taula 9):

Nivell d'atac	Atac	Objectius de seguretat
Atacs a la Interfície Bio-cibernètica	Escoltes	Confidencialitat
	Atac de reproducció	Integritat
	Atac Man-In-The-Middle (MITM)	Confidencialitat
	Esgotament de recursos	Disponibilitat
	Atacs d'injecció	Integritat
	Manipulació de dispositius	Integritat
		Autenticació
	Atac de denegació de servei (DoS)	Disponibilitat
	Atacs de malware	Confidencialitat
		Integritat
		Disponibilitat
	Atacs de firmware	Integritat

Taula 9. Objectius de seguretat per atac a la interfície bio-mètrica (confecció pròpia)

Es constata que en el desenvolupament i desplegament de tecnologies innovadores com dispositius IoBNTs per al tractament de l'aigua s'aborda els objectius de ciberseguretat de Confidencialitat, Integritat, Disponibilitat i Autenticitat d'aquests dispositius:

- Des del punt de vista de la Confidencialitat, és crucial implementar mecanismes robustos de xifrat i control d'accés per protegir la informació sensible relacionada amb la qualitat de l'aigua i els processos de tractament.

- La Integritat de les dades és essencial per garantir que la informació crítica no sigui manipulada o alterada de manera maliciosa, cosa que podria tenir conseqüències greus per a la presa de decisions i la salut pública.

- La Disponibilitat dels sistemes és fonamental per assegurar que els dispositius IoBNT estiguin operatius en tot moment, especialment en situacions crítiques que requereixen respostes ràpides, com esdeveniments de contaminació de l'aigua.

- L'Autenticitat, per la seva banda, esdevé un element clau per verificar la legitimitat de les dades i la identitat dels actors involucrats en el monitoratge i control dels dispositius.

3.2 Resultats d'assoliment d'ODS 3, 6 i 13

De l'anàlisi realitzat es desprèn que la ciberseguretat de dispositius IoBNT per al tractament de l'aigua esdevé un component molt important en el compliment dels Objectius de Desenvolupament Sostenible (ODS) 3, 6 i 13.

La convergència de la innovació tecnològica i la gestió sostenible dels recursos hídrics exigeix una atenció especial a la seguretat cibernètica per garantir l'èxit d'aquestes iniciatives i abordar els desafiaments associats amb la salut, l'accés a l'aigua potable i l'acció climàtica.

La implementació de dispositius IoBNT contribueix directament a l'ODS 3, que busca garantir una vida saludable i promoure el benestar per a tothom en totes les edats. No obstant això, perquè aquests dispositius siguin efectius en la millora de la salut pública, és essencial assegurar la integritat i confidencialitat de les dades generades i processades. La ciberseguretat, en aquest context, esdevé un pilar fonamental per protegir la informació crítica relacionada amb la qualitat de l'aigua i els processos de tractament.

En relació amb l'ODS 6, que aborda la disponibilitat i gestió sostenible de l'aigua i sanejament, la ciberseguretat dels dispositius IoBNT es presenta com un element clau per garantir la fiabilitat dels sistemes de monitoratge i control. La integritat i autenticitat de les dades són essencials per a la presa de decisions informades en la gestió eficient i sostenible dels recursos hídrics, i la ciberseguretat juga un paper determinant en la preservació de la disponibilitat d'aquests sistemes.

Així mateix, respecte l'ODS 13, centrat en l'acció climàtica, la ciberseguretat dels dispositius IoBNT es converteix en un factor crític per garantir la continuïtat i fiabilitat dels sistemes en entorns climàtics canviants. La resiliència d'aquests dispositius davant possibles amenaces cibernètiques és essencial per mantenir operatius els processos de tractament de l'aigua i, per tant, contribuir a la mitigació dels impactes del canvi climàtic en els recursos hídrics.

4 Conclusions i treballs futurs

En l'anàlisi realitzat s'ha obtingut un estat de l'art de les vulnerabilitats identificades fins el moment actual en dispositius IoBNTs, així com de la gestió dels riscos. S'han identificat els riscos que les amenaces suposen, així com la mitigació de les mateixes. Per tant, s'ha pogut descriure l'estat actual de la seguretat dels dispositius IoBNTs respecte els objectius de seguretat: Confidencialitat, Integritat, Disponibilitat i Autenticitat.

La consideració dels objectius de seguretat Confidencialitat, Integritat, Disponibilitat i Autenticitat en el desenvolupament i aplicació de dispositius IoBNT per al tractament de l' aigua no només garanteix l'efectivitat d'aquestes tecnologies, sinó que també salvaguarda la confiança pública i promou un enfocament segur i sostenible cap a la gestió dels recursos hídrics en l'era de la IoT i la bionanotecnologia.

En aquest treball també s'havien plantejat objectius addicionals pels quals es conclou que s'han assolit tots ells (Tecnologia dels dispositius IoBNT de tractament d'aigua, Arquitectura de dispositius IoBNT, Vulnerabilitats, Gestió de riscos, Millora dels ODS 3, 6 i 13), ja que s'han pogut abordar en diferents apartats. En especial, esmentar que la ciberseguretat dels dispositius IoBNT és una eina que possibilita l'assoliment dels ODS 3, 6 i 13. La protecció de la confidencialitat, integritat, disponibilitat i autenticitat de les dades esdevé un pilar fonamental per garantir l'èxit de les iniciatives que busquen millorar la salut, la gestió de l'aigua i la resiliència climàtica a través de la convergència de la biotecnologia, la nanotecnologia i la connectivitat.

Degut a la novetat que encara suposa l'aplicació de IoBNT en el tractament de l'aigua (i, en general, l'ús de les IoBNT), s'esperaven uns resultats més minsos o inconcrets, però s'han superat les expectatives.

Respecte la planificació i metodologia, s'ha treballat seguint els temps i fites previstos en la planificació inicial amb alguns ajustos en les fases inicials on hi ha hagut més inversió de temps del previst degut a que s'ha demorat la cerca i estudi de la documentació sobre una tecnologia emergent com les IoBNTs, temps que després s'ha recuperat en fases posteriors.
També s'ha introduït algun canvi en l'ordre de redacció dels diferents apartats per donar més continuïtat al treball i fer el tema més entenedor.

Els impactes ètic-socials, de sostenibilitat i de diversitat previstos s'han assolit, ja que els resultats obtinguts en quant a objectius principals i secundaris sobre la ciberseguretat en dispositius IoBNT pel tractament de l'aigua ens apunten beneficis generals para tot ésser viu del planeta.

Com a reflexió cara al futur de la ciberseguretat en IoBNTs, comentar el següent:

> La convergència de IoT i la bionanotecnologia per gestionar els recursos hídrics presenta desafiaments específics en termes de protecció contra amenaces cibernètiques, i la consideració dels objectius de Confidencialitat, Integritat, Disponibilitat i Autenticitat esdevé un imperatiu per garantir l'eficàcia i la confiança en la implementació dels dispositius IoBNT.
>
> En aquest context, es destaca la necessitat d'adoptar enfocaments integrals que incloguin protocols de seguretat des del disseny mateix dels dispositius IoBNT fins a la seva implementació i manteniment continu. A més, la col·laboració entre la comunitat científica,

els fabricants de tecnologia i les entitats reguladores és essencial per establir estàndards i pràctiques de seguretat robustes que mitiguin els riscos associats amb la connectivitat i la digitalització en l'àmbit del tractament de l'aigua.

5 Bibliografia

[1] Kuscu, M., & Unluturk, B. D. (2021). Internet of bio-nano things: A review of applications, enabling technologies and key challenges. arXiv preprint arXiv:2112.09249.

[2]https://www.sanidad.gob.es/ciudadanos/pdf/Estrategia_de_Salud_Publica_2022___Pendiente_de_NIPO.pdf, 29/10/2023

[3] https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/, 01/10/2023

[4] Kuscu, M., & Unluturk, B. D. (2021). Internet of bio-nano things: A review of applications, enabling technologies and key challenges. arXiv preprint arXiv:2112.09249.

[5] https://www.un.org/sustainabledevelopment/es/, 01/10/2023

[6] Lin, L., Yang, H., & Xu, X. (2022). Effects of water pollution on human health and disease heterogeneity: a review. Frontiers in environmental science, 10, 880246.

[7] Joseph, T. M., Al-Hazmi, H. E., Śniatała, B., Esmaeili, A., & Habibzadeh, S. (2023). Nanoparticles and nanofiltration for wastewater treatment: From polluted to fresh water. Environmental Research, 117114.

[8] Diana Soukarié, Vincent Ecochard, Laurence Salomé, DNA-based nanobiosensors for monitoring of water quality, International Journal of Hygiene and Environmental Health, Volume 226, 2020, 113485, ISSN 1438-4639, https://doi.org/10.1016/j.ijheh.2020.113485.

[9] Vikesland, P.J. Nanosensors for water quality monitoring. Nature Nanotech 13, 651–660 (2018). https://doi.org/10.1038/s41565-018-0209-9

[10] I. F. Akyildiz, M. Pierobon, S. Balasubramaniam, and Y. Koucheryavy, “The internet of bio-nano things,” IEEE Communications Magazine, vol. 53, no. 3, pp. 32–40, 2015.

[11] Marzo, J. L., Jornet, J. M., & Pierobon, M. (2019). Nanonetworks in biomedical applications. Current drug targets, 20(8), 800-807.

[12] I. F. Akyildiz, M. Pierobon, S. Balasubramaniam, and Y. Koucheryavy, “The internet of bio-nano things,” IEEE Communications Magazine, vol. 53, no. 3, pp. 32–40, 2015

[13] L. J. Kahl and D. Endy, “A survey of enabling technologies in synthetic biology,” Journal of Biol. Eng., vol. 7, no. 1, p. 13, May 2013.

[14] F. Wu and C. Tan, “The engineering of artificial cellular nanosystems using synthetic biology approaches,” WIREs Nanomedicine and Nanobiotech, vol. 6, no. 4, July/August 2014.

[15] Zhang, A., & Lieber, C. M. (2016). Nano-Bioelectronics. Chemical reviews, 116(1), 215–257. https://doi.org/10.1021/acs.chemrev.5b00608

[16] Sonawane, J. M., Mahadevan, R., Pandey, A., & Greener, J. (2022). Recent progress in microbial fuel cells using substrates from diverse sources. Heliyon.

[17] D. A. Leigh, “Genesis of the nanomachines: The 2016 nobel prize in chemistry,” Angewandte Chemie International Edition, vol. 55, no. 47,pp. 14 506–14 508, 2016.

[18] K. Lund, A. J. Manzo, N. Dabby, N. Michelotti, A. Johnson-Buck, J. Nangreave, S. Taylor, R. Pei, M. N. Stojanovic, N. G. Walter et al., “Molecular robots guided by prescriptive landscapes,” Nature, vol. 465, no. 7295, pp. 206–210, 2010.

[19] I. Aprahamian, “The future of molecular machines,” ACS central science, vol. 6, no. 3, pp. 347–358, 2020.

[20] E. Ellis, S. Moorthy, W.-I. K. Chio, and T.-C. Lee, “Artificial molecular and nanostructures for advanced nanomachinery,” Chemical Communications, vol. 54, no. 33, pp. 4075–4090, 2018.

[21] Nakano, T., Suda, T., Okaie, Y., Moore, M. J., & Vasilakos, A. V. (2014). Molecular communication among biological nanomachines: A layered architecture and research issues. IEEE transactions on nanobioscience, 13(3), 169-197.

[22] O. B. Akan, H. Ramezani, T. Khan, N. A. Abbasi, and M. Kuscu, “Fundamentals of molecular information and communication science,” Proceedings of the IEEE, vol. 105, no. 2, pp. 306–318, 2017.

[23] F. Lemic, S. Abadal, W. Tavernier, P. Stroobant, D. Colle, E. Alarcón, J. Márquez-Barja, and J. Famaey, “Survey on terahertz nanocommunication and networking: A top-down perspective,” arXiv preprint arXiv:1909.05703, 2019.

[24] Maier, Stefan A. (2007). Plasmonics: Fundamentals and Applications. Springer US. pp. 5-19. ISBN 978-0-387-33150-8.

[25] Stockmann, Mark (01/02/2011). «Nanoplasmonics: The physics behind the applications». Physics Today. doi:10.1063/1.3554315.

[26] J. M. Jornet and I. F. Akyildiz, “Fundamentals of electromagnètic nanonetworks in the terahertz band,” Foundations and Trends® in Networking, vol. 7, no. 2-3, pp. 77–233, 2013.

[27] F. Al-Turjman, ‘‘A cognitive routing protocol for bio-inspired networking in the Internet of nano-things (IoNT),’’ Mobile Netw. Appl., vol. 25,pp. 1929–1943, Oct. 2017.

[28] M. Kuscu, H. Ramezani, E. Dinc, S. Akhavan, and O. B. Akan, “Fabrication and microfluidic analysis of graphene-based molecular communication receiver for internet of nano things (iont),” Scientific reports, vol. 11, no. 1, pp. 1–20, 2021.

[29] M. Kuscu, E. Dinc, B. A. Bilgin, H. Ramezani, and O. B. Akan, “Transmitter and receiver architectures for molecular communications: A survey on physical design with modulation, coding, and detection techniques,” Proceedings of the IEEE, vol. 107, no. 7, pp. 1302–1341, 2019.

[30] A. Kiourti, “Rfid antennas for body-area applications: From wearables to implants,” IEEE Antennas and Propagation Magazine, vol. 60, no. 5, pp. 14–25, 2018.

[31] L. Grebenstein, J. Kirchner, R. S. Peixoto, W. Zimmermann, F. Irnstorfer, W. Wicke, A. Ahmadzadeh, V. Jamali, G. Fischer, R. Weigel et al., “Biological optical-to-chemical signal conversion interface: A smallscale modulator for molecular communications,” IEEE transactions on nanobioscience, vol. 18, no. 1, pp. 31–42, 2018

[32] K. Deisseroth, “Optogenetics,” Nature methods, vol. 8, no. 1, pp. 26–29, 2011.

[33] S. Kisseleff, R. Schober, and W. H. Gerstacker, “Magnetic nanoparticle based interface for molecular communication systems,” IEEE Communications Letters, vol. 21, no. 2, pp. 258–261, 2016.

[34] W. Wicke, A. Ahmadzadeh, V. Jamali, H. Unterweger, C. Alexiou, and R. Schober, “Magnetic nanoparticle-based molecular communication in microfluidic environments,” IEEE transactions on nanobioscience, vol. 18, no. 2, pp. 156–169, 2019.

[35] Al-Turjman, F. (2020). A cognitive routing protocol for bio-inspired networking in the Internet of nano-things (IoNT). Mobile Networks and Applications, 25(5), 1929-1943.

[36] Akyildiz, I. F., & Jornet, J. M. (2010). The internet of nano-things. IEEE Wireless Communications, 17(6), 58-63

[37] Chude-Okonkwo, U. A., Malekian, R., & Maharaj, B. T. (2016). Biologically inspired bio-cyber interface architecture and model for Internet of bio-nanothings applications. IEEE Transactions on Communications, 64(8), 3444-3455.

[38] Bakhshi, T., & Shahid, S. (2019, November). Securing internet of bio-Nano things: ML-enabled parameter profiling of bio-cyber interfaces. In 2019 22nd International Multitopic Conference (INMIC) (pp. 1-8). IEEE.

[39] Sicari, S., Rizzardi, A., Piro, G., Coen-Porisini, A., & Grieco, L. A. (2019). Beyond the smart things: Towards the definition and the performance assessment of a secure architecture for the Internet of Nano-Things. Computer Networks, 162, 106856.

[40] Camara, C., Peris-Lopez, P., & Tapiador, J. E. (2015). Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of biomedical informatics, 55, 272-289.

[41] Kishk, M. A., & Dhillon, H. S. (2017). Stochastic geometry-based comparison of secrecy enhancement techniques in D2D networks. IEEE Wireless Communications Letters, 6(3), 394-397.

[42] Islam, S. R., Ali, F., Moon, H., & Kwak, K. S. (2017, October). Secure channel for molecular communications. In 2017 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 1-4). IEEE.

[43] Zafar, S., Aman, W., Rahman, M. M. U., Alomainy, A., & Abbasi, Q. H. (2019, August). Channel impulse response-based physical layer authentication in a diffusion-based molecular communication system. In 2019 UK/China Emerging Technologies (UCET) (pp. 1-2). IEEE.

[44] Singh, S. P., Yadav, S., & Mishra, S. (2020, November). Secrecy capacity of diffusive molecular communication under biological spherical environment. In Proceedings of the 1st ACM International Workshop on Nanoscale Computing, Communication, and Applications (pp. 33-38).

[45] Huang, Y., Wen, M., Lin, L., Li, B., Wei, Z., Tang, D., ... & Guo, W. (2023). Physical-Layer Counterattack Strategies for the Internet of Bio-Nano Things with Molecular Communication. IEEE Internet of Things Magazine, 6(2), 82-87.

[46] Koca, C., Civas, M., & Akan, O. B. (2021). Evolutionary Game Theoretic Resource Allocation Simulation for Molecular Communication.

[47] Zafar, S., Aman, W., Rahman, M. M. U., Alomainy, A., & Abbasi, Q. H. (2019, August). Channel impulse response-based physical layer authentication in a diffusion-based molecular communication system. In 2019 UK/China Emerging Technologies (UCET) (pp. 1-2). IEEE

[48] Giaretta, A., Balasubramaniam, S., & Conti, M. (2015). Security vulnerabilities and countermeasures for target localization in bio-nanothings communication networks. IEEE Transactions on Information Forensics and Security, 11(4), 665-676.

[49] Sharma, G., Bala, S., & Verma, A. K. (2012). Security frameworks for wireless sensor networks-review. Procedia Technology, 6, 978-987.

[50] Atlam, H. F., Walters, R. J., & Wills, G. B. (2018, August). Internet of nano things: Security issues and applications. In Proceedings of the 2018 2nd international conference on cloud and big data computing (pp. 71-77).

[51] Alabdulatif, A., Thilakarathne, N. N., Lawal, Z. K., Fahim, K. E., & Zakari, R. Y. (2023). Internet of nano-things (iont): A comprehensive review from architecture to security and privacy challenges. Sensors, 23(5), 2807.

[52] Ye, N., Zhu, Y., Wang, R. C., Malekian, R., & Lin, Q. M. (2014). An efficient authentication and access control scheme for perception layer of internet of things.

[53] Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing, 1-18.

[54] He, D., & Zeadally, S. (2014). An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. IEEE internet of things journal, 2(1), 72-83.

[55] Siddiqi, M. A., & Strydis, C. (2019, April). Towards realistic battery-DoS protection of implantable medical devices. In Proceedings of the 16th ACM international conference on computing frontiers (pp. 42-49).

[56] Abdul-Ghani, H. A., & Konstantas, D. (2019). A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective. *Journal of Sensor and Actuator Networks*, *8*(2), 22.

[57] Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Shamshirband, S. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian informatics journal*, *18*(2), 113-122.

[58] Camara, C., Peris-Lopez, P., & Tapiador, J. E. (2015). Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of biomedical informatics, 55, 272-289.

[59] Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of things: Security and solutions survey. Sensors, 22(19), 7433.

[60] Atlam, H. F., Walters, R. J., & Wills, G. B. (2018, August). Internet of nano things: Security issues and applications. In *Proceedings of the 2018 2nd international conference on cloud and big data computing* (pp. 71-77).

[61] Alabdulatif, A., Thilakarathne, N. N., Lawal, Z. K., Fahim, K. E., & Zakari, R. Y. (2023). Internet of nano-things (iont): A comprehensive review from architecture to security and privacy challenges. Sensors, 23(5), 2807.

[62] Dressler, F., & Kargl, F. (2012). Towards security in nano-communication: Challenges and opportunities. Nano communication networks, 3(3), 151-160.

[63] Manojkumar, S. (2022). Security and possible applications towards internet of nano things in near future. Int. J. Electron. Devices Netw, 3, 36-42.

[64] Nikhat, A., & Yusuf, P. (2020). The internet of nano things (IoNT) existing state and future Prospects. GSC Advanced Research and Reviews, 5(2), 131-150.

[65] Zafar, Sidra, et al. "Securing bio-cyber interface for the internet of bio-nano things using particle swarm optimization and artificial neural networks based parameter profiling." *Computers in Biology and Medicine* 136 (2021): 104707.

[66] Urso, M., Ussia, M., & Pumera, M. (2023). Smart micro-and nanorobots for water purification. *Nature Reviews Bioengineering*, *1*(4), 236-251.

[67] Gupte, T., & Pradeep, T. (2022). Nanosensors for water quality monitoring. In *Separation Science and Technology* (Vol. 15, pp. 37-53). Academic Press.

[68] Sharma, V., Borkute, G., & Gumfekar, S. P. (2022). Biomimetic nanofiltration membranes: Critical review of materials, structures, and applications to water purification. *Chemical Engineering Journal*, *433*, 133823.

[69] Tripathy, D. B., & Gupta, A. (2023). Nanomembranes-Affiliated Water Remediation: Chronology, Properties, Classification, Challenges and Future Prospects. *Membranes*, *13*(8), 713.

[70] Abbas, A. M. (2022, November). Molecular Nano Communication Networks: Architectures, Protocols and Technologies. In *2022 5th International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT)* (pp. 1-5). IEEE.

[71] Bhardwaj, A. K., Sundaram, S., Yadav, K. K., & Srivastav, A. L. (2021). An overview of silver nano-particles as promising materials for water disinfection. *Environmental Technology & Innovation*, *23*, 101721.

[72] El-Sayed, M. E. (2020). Nanoadsorbents for water and wastewater remediation. *Science of the Total Environment*, *739*, 139903.

[Z903] https://www.cve.org ,1/10/2023

[Z904] https://www.incibe.es , 2/10/2023

[Z7] Jain, N., & Kanu, N. J. (2021). *The potential application of carbon nanotubes in water treatment: A state-of-the-art-review. Materials Today: Proceedings, 43,* 2998-3005.