INTERNET DE LES COSES

Protocols d'Internet

Jordi Bru Carci
Universitat Politècnica de Barcelona
Protocols d'Internet - FIB
30/5/2022

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat d'Informàtica de Barcelona

FIB

INDEX

Introducció

Si fem una ullada al nostre entorn segurament trobarem almenys un element que tingui connectivitat a internet; des del nostre telèfon mòbil, una televisió o fins i tot, una nevera. El terme que engloba els objectes que comparteixen aquesta funcionalitat, s'anomena "l'internet de les coses", més conegudament com *"Internet of Things (iot)"*. En poques paraules, l'internet de les coses és la capacitat d'un objecte físic de connectar-se a internet, emmagatzemar i intercambiar dades amb altres dispositius o sistemes d'internet, mitjançant sensors, software i altres tecnologies que es detallaran en profunditat al llarg del treball.

Cal esmentar que un dels punts d'interés del tema, no és només la seva gran utilitat, també el gran marge de millora que pot assolir juntament amb els avenços tecnològics. Per tant, si actualment ja és una gran millora de la nostre qualitat de vida, cal preguntar-se com com de vital serà l'internet de les coses en un futur pròxim.

El present treball s'emmarca dins de l'objectiu principal de entendre i donar a conèixer l'internet de les coses i la seva implicació en la vida quotidiana. Com a objectius secundaris s'estableixen els següents aspectes: anàlisi en profunditat de com s'implementa aquesta tecnologia i el seu funcionament. Ademés tractarem com afecta la privacitat i seguretat l'internet de les coses i s'esmentaran diverses solucions per resoldre aquest problema. Amb tot això es pretén obtenir una idea clara de en què consisteix aquesta tecnologia i entendre les millores que pot permetre en el nostre dia a dia amb una bona implementació i suficients recursos.

La metodologia emprada es basa en la cerca, anàlisis i síntesis d'un conjunt d'articles pertanyents al camp d'estudi de la tecnologia de l'internet de coses.

L’internet de les coses. Definició

“L’internet de les coses” (IoT) és un sistema de dispositius interrelacionats, capaços d’emetre i intercanviar informació entre ells sense que hi hagi cap humà que interfereixi [1].

Aquesta tecnologia té un objectiu clar: interconnectar digitalment a tota la societat mitjançant els objectes que ens rodegen per fer les nostres vides molt més còmodes [16]. Fins al punt de que, per exemple, qualsevol persona amb un smartphone, pot mirar pel·lícules, parlar amb gent, consultar pàgines web, comprar; i tot des del sofà.

Les “coses” que son capaces de complir aquest objectiu són objectes físics que poden ser assignats per adreces de direccions IP i que ademés poden transmetre i recollir dades de l’entorn a la xarxa mitjançant sensors i processadors [16].

L’internet de les coses i la seva infraestructura es troba en constant desenvolupament i creixement amb un gran marge de millora. Actualment, les xarxes inalàmbriques estan construïdes en tecnologia 4G, que provoca, tot i tenir moltes funcionalitats, que l’IoT no obtingui el seu màxim potencial. Davant aquesta situació, l’actual integració de tecnologia 5G, esdevindrà en una nova generació amb una connexió inalàmbrica més ràpida, amb menys latència i sobretot l’augment del número que dispositius que la poden suportar [10]. Així doncs, aquesta evolució fa que l’imapacte que pugui tenir sigui molt més gran.

Figura 1. Descripció gràfica d’un món interconnectat. Font: Wikipedia

Impacte en la actualitat

Està clar el creixement i el gran marge que existeix. Conseqüentment, suposa un gran impacte pels sectors d'avui dia, ja que estan constantment rebent nova informació, i d'aquesta, un valor afegit per portar les infraestructures a un alt nivell. Gràcies a tot aquest constant seguiment, una empresa pot mantenir un control a temps real de tot el seu sistema i així, poder operar més eficientment. Degut a aquest alt nivell de control, les empreses tenen la capacitat d'automatitzar la major part de processos i ademés de poder prendre les millors decisions en tot moment [1].

Actualment, tenir un control sobre les dades és clau pels sectors d'avui en dia. Segons l'article de la *International Data Corporation* (IDC) publicant recentment, "Worldwide Global DataSphere IoT Device and Data Forecast, 2021-2025" [3], s'estima que pel 2025 hi haurà 41.6 mil milions de dispositius iot connectats que generaran 79.4 zettabytes de dades. És per això que cada cop les empreses confien més en aquesta tecnologia.

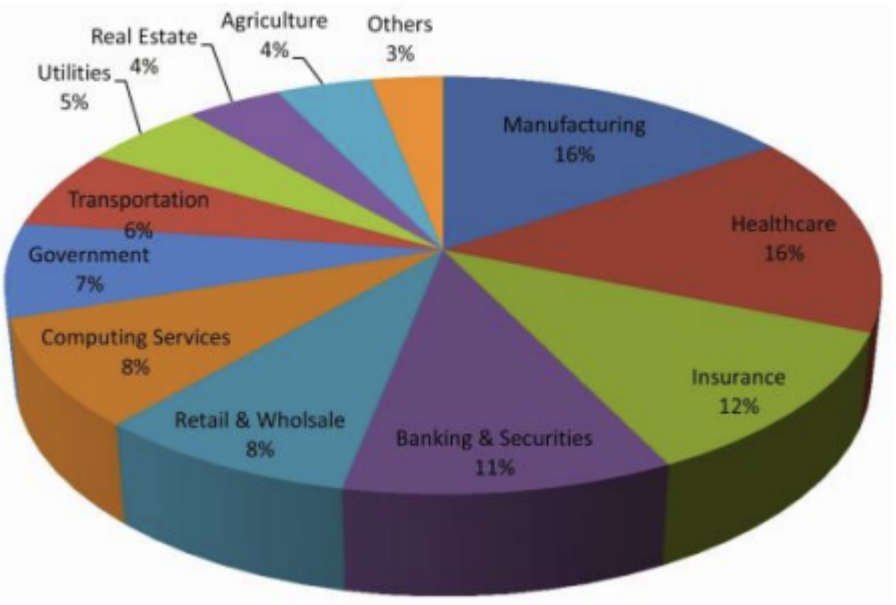

Figura 2. Projecció de la repartició de les aplicacions dominants en diferents sectors i dominis. Font: Fuente: monacotrades.com

Amb una robusta implementació de sistemes i dispositius iot, empreses i sectors poden recopilar, analitzar i distribuir informació amb més facilitat per així d'obtenir nova informació i coneixements com a fonament dels projectes relatius a aquesta tecnologia. A continuació, donarem èmfasi a sectors que han implementat aquesta tecnologia i així entendre la suposada millora de les seves infraestructures.

El sector agrari

Un dels principals reptes de l'actualitat és transformar tecnològicament l'agricultura com a resposta del creixement demogràfic a escala mundial. Segons un article publicat per la ONU [4], s'estima que la població de la terra assoleixi els 10 mil milions d'habitants l'any 2050. En aquest escenari, l'agricultura és i serà un dels medis per abastir a gran part de la població mundial. Tal com menciona la Organització de les Nacions Unides per l'Alimentació i la Agricultura (FAO) en un informe del 2017 [5], "La mecanización agrícola es crucial porque mejora el rendimiento de otros insumos. Al aumentar la demanda de maquinaria, incluso en las pequeñas explotaciones agrícolas, los mercados de arrendamiento y el uso compartido a través de cooperativas agrícolas se han convertido en elementos clave para el éxito de la mecanización".

És aquí on l'aplicació de l'Internet de les coses té un paper important per canviar el paradigma. Aquesta tecnologia, garanteix l'augment de la producció de manera eficient mentre es redueix tot procés manual. Això és degut a dispositius i sensors intel·ligents que permeten tenir un control del clima i una supervisió constant de tots els processos [6]. Segons un estudi de l'implementació d'aquesta tecnologia a Ecuador, no només s'aconsegueix un augment de la productivitat, sinó que també una millor gestió dels recursos, com és una reducció del consum d'aigua gràcies a estratègies amb sistemes hidràulics [17].

A més a més, un dels mecanismes més destacables introduïts recentment gràcies a l'internet de les coses és la "Ramaderia Intel·ligent". Aquest nou concepte consisteix en tenir sensors que permeten controlar en tot moment els moviments, la salut i la capacitat de reproducció del bestiar. Aquesta tecnologia també permet tenir el

bestiar localitzat amb els sistemes GPS per quan es dongui el cas d'alguna pèrdua o fins i tot d'un robatori [7].

Cal recalcar com tots aquests processos acaben superant els obstacles que sempre han existit en aquest sector de manera sostenible, com l'ús de infraestructures insostenibles i una mala gestió dels recursos. Ademés s'assoleixen amb balanços positius en estalvi d'energia.

Figura 3. Representació del control de processos en l'agricultura gràcies a l'internet de les coses. Font: "What is IoT and what does it mean for farmers?", Youtube.

El sector sanitari

Un altre sector que surt clarament beneficiat és el sector sanitari. En els darrers anys, el sector ha rebut una gran transformació centrat principalment en tres factors: pacients, personal mèdic i infraestructura [8].

L'internet de les coses ha permès monitorar constantment l'estat dels pacients per poder centrar-se en la prevenció i la rehabilitació. La rehabilitació ha suposat grans reptes degut al temps i mitjans que s'han de dedicar per seguir endavant i aquesta tecnologia és la indicada per totes les funcionalitats que contempla que veurem a continuació [9].

De la mateixa manera, ha proporcionat sistemes pel quals equips de sanitaris poden accedir per comunicar-se a temps real amb altres equips o pacients. Assolir aquest repte, actualment, és esencial, ja que agilitza qualsevol procés que giri entorn a la salud de les persones. Conseqüentment, dóna la possibilitat d'obrir un canal metge-pacient eficient i ràpid.

Gràcies a sensors i dispositius iot, més enllà de de monitoritzar pacients, també es pot monitorar material i equip mèdic amb un objectiu clar: obtenir la optimització del dimensionamient de les organitzacions i, així maximitzar l'eficiència de les operacions [9].

Figura 4. Representació de l'implementació de sistemes IoT en els sector sanitari. Font: [24]

El sector industrial

El sector de la industria ha crescut gràcies a l'internet de les coses fins al punt de començar a mencionar el terme d'una Quarta Revolució Industrial (Industria 4.0) [9]. Aquest nou concepte fa que el factor clau que mou aquest sector no siguin les parts o peces que la completen, sinó la complexitat de sistemes que la engloben. Degut al conjunt de dispositius i sensors que formen aquesta tecnologia permet gestionar operacions que el passat eren més aviat un repte.

Posan un exemple, un dels conceptes a destacar és el manteniment preventiu que proporciona l'internet de les coses. L'ús de sensors connectats a la maquinària, permet tenir un control a temps real del funcionament i les condicions de les màquines (temperatura, nivell de combustible, qualitat de neteja,...). Gràcies a aquest nivell de control, les empreses del sector, poden identificar irregularitats abans de que succeeixin i així poder reaccionar a temps [10].

Altres sectors i dominis

Els alts nivells d'escalabilitat i de complexitat de l'internet de les coses fa que sigui una tecnologia tan versàtil en la que pot formar part qualsevol domini o sector. Altres sectors on les aplicacions IoT han deixat petjada son el sector del transport i la logística, i sobretot en el domini que abarca aspectes de la societat en la que vivim per facilitar el nostre dia a dia com a conseqüència d'un entorn intel·ligent [10].

Tots els sectors que formen part dels dominis mencionats, venen marcats per les aplicacions que aquesta tecnologia permet. No només es busca que el procesos siguin el més eficient possibles i que es puguin reduir els costos, sinó que a més a més,es realitza sota una mirada que tingui cura de la sostenibilitat i el medi ambient.

Funcionament IoT

Un sistema que implementa l'internet de les coses se li atribueix el nom de "Wireless Sensor Networks" (WSN). Això és degut a la seva arquitectura, composada per sensors capaços d'intercanviar-se inalàmbricament informació amb la finalitat d'obtenir un sistema centralitzat [11].

Els nodes d'aquest sistema, és a dir, els sensors són els responsables d'obtenir la informació, processar-la i empaquetar-la, per finalment poder transmetre-la a internet gràcies al *gateway* i així, poder arribar a la destinació final: l'usuari o l'empresa a càrrec.

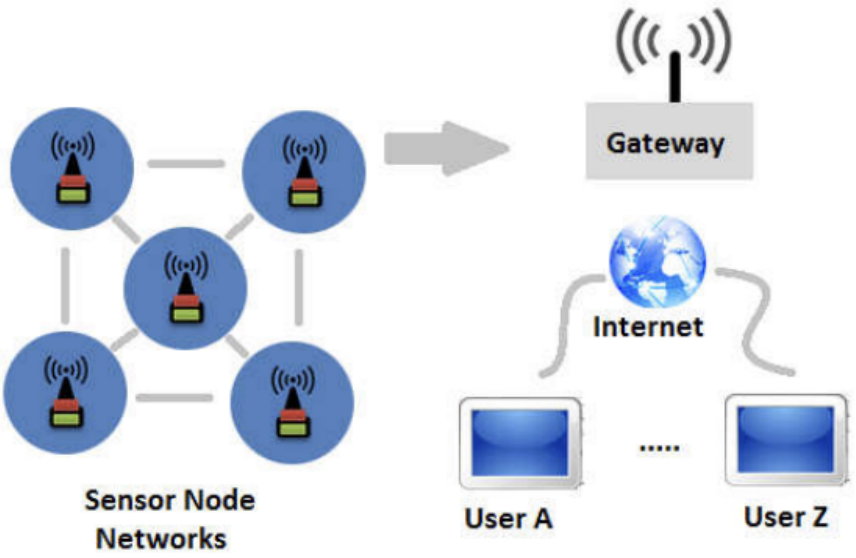

Figure 5. Mapa conceptual del funcionament d'un sistema WSN. Font: [11]

Tecnologia darrere IoT

Els sensors són dispositius que acostumen a ser de proporcions petites i amb un rendiment bastant limitat. Encara que existeixin aquestes limitacions, el que es busca és que sigui "low cost" en temes de consumició d'energia per a que siguin suficientment sostenibles i duraders [11].

Per a que els dispositius puguin processar les dades que s'obtenen de les unitats sensorials, tenen una CPU integrada composada per un microprocessador i una memoria flash. El microprocessador té l'objectiu de prendre les decisions correctes i dur a terme funcionalitats de la CPU, i la memoria flash té el rol d'emmagatzemar tota la informació generada fins que arribi a la capacitat màxima. Un cop arriba a aquest límit, el microprocessador decideix empaquetar la informació i transmetre-ho via broadcast a altres nodes o a internet (ho desenvoluparem més endavant). És així com realment es crea una topologia entre els nodes d'un sistema. S'ha de tenir present que el radi de transmissió per broadcast sol ser aproximadament d'uns 30 metres degut a les limitacions de recursos que tenen [13].

Cada dispositiu té implementat una font d'alimentació per poder suministrar la energia necesària a la CPU i als sensors integrats per poder dur a terme totes les funcionalitats necessàries. Els recursos per obtenir energia, pot anar des d'unes bateries convencionals com son piles AA, bateries que es carreguen amb llum solar o fins i tot bateries intel·ligents [12]. Per a que els sensors tinguin una autonomia duradera, els sensors solen estar un 99% del temps en estat "sleep" i s'activen solament quan és realment necessari i així tenir un gestió més eficient dels recursos.

En els darrers anys, la tecnologia ha crescut ràpidament aportant un gran rang de sensors i transductors nous al ser la part més esencial d'un WSN. La finalitat d'aquests transductors és que puguin convertir tota variable del seu entorn en ràfegues o senyals d'electricitat [13]. Primordialment es poden separar en tres tipus de sensors: temperatura vibració i humitat; però cada cop es van implementat funcionalitats extres a les ja esmentades, com podria ser capturar audio, fer fotografies i un llarg etcetera.

Ja hem mencionat com un sensor pot recollir informació del seu entorn, com la processa i empaqueta però encara ens queda entendre com un sensor pot emetre tota la informació generada i estar interconnectat amb altres nodes. Aquest component és el transmissor [11]. El transmissor pot rebre i emetre mitjançant diferents tipus de medis de comunicació inalàmbrics, com són els raigs infrarojos, làser o freqüències de radio. Preferentment, en un WSN es recomana usar aquest últim degut a la energia, velocitat i el "data rate" requerit [14].

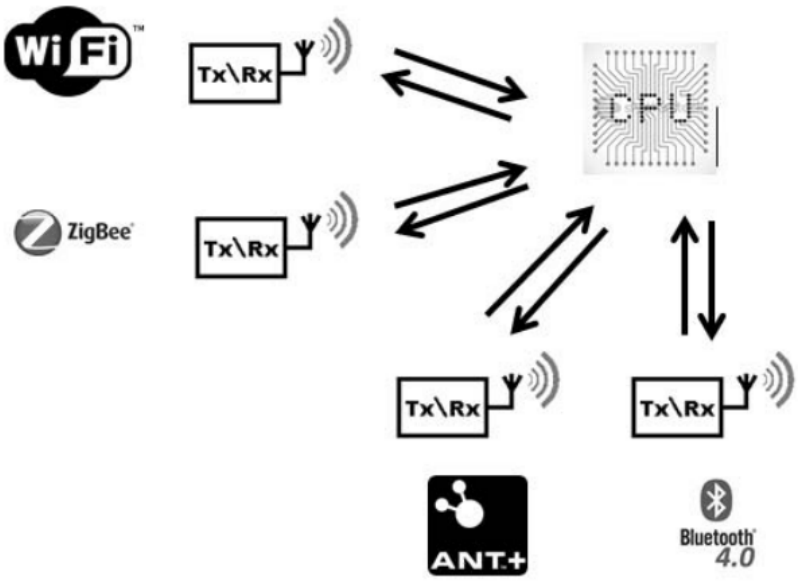

Figure 6. Representació de la interconnexió entre sensors iot. Font: [14]

A part de la comunicació que hi ha entre tots els nodes del sistema, s'ha de tenir en consideració l'altre connexió que han de tenir. Els nodes també han de poder transmetre la informació empaquetada a la seva destinació final, el que pot ser a cap a uns PC personals o també cap uns dispositius d'emmagatzematge de dades conegudament com Personal Data Assistants (PDA). Això serà possible gràcies a una serie de gateways disposats en el sistema.

Per a que aquest procés sigui possible, existeixen diferent mètodes per accedir a la xarxa final. Els més comuns son sense cable via internet o via satèl·lit pel direccionament de les dades i per l'enrutament es poden usar diferents protocols, com per exemple RPL per IPv6 o Trickle [15].

Finalment, l'últim pas de l'aplicació consisteix en com l'usuari rep la nova informació. Com hem mencionat anteriorment, el destí final de la nova data sol ser una estació d'emmagatzematge i l'usuari té accés a ella. En el cas d'un PC, l'usurari es pot connectar presencial o remotament per i així poder recollir les noves mostres i visualitzar-les. Cal recalcar que no només té el permís d'accés a les dades sinó que també pot manar directives per a que la estació es comuniqui amb la resta de dispositius del sistema per modificar i gestionar el seu comportament [13]. Per

exemple, decidir noves estratègies, i fins i tot, manar cap a on enviar tota la informació i decidir com ho farà.

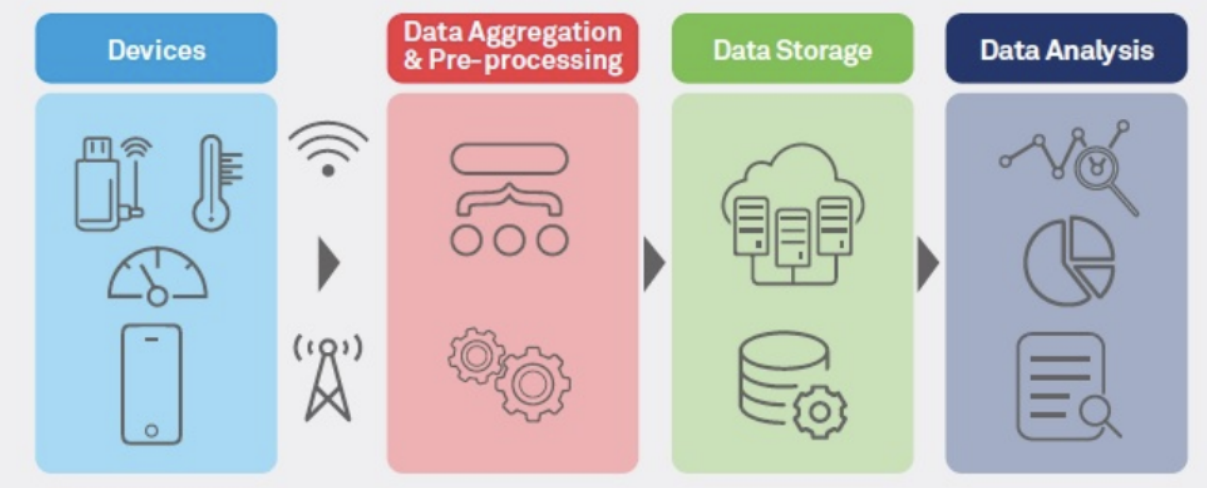

Figura 7. Les quatre estacions d'un sistema que implementa iot. Font: [22]

Privacitat

A conseqüència de l'augment de l'ús i l'èmfasi envers al tractament i processament de les dades gràcies a l'internet de les coses, la privacitat de la informació s'ha acabat convertint en un dels temes més importants avui en dia [18].

Actualment hi ha infinitats de definicions de privacitat però en aquest cas ens centrarem en en els tres punts que ens dóna Jan Henrik Ziegeldorf en el seu article "*Privacy in the Internet of Things: threats and challenges*" [18]:

- "awareness of privacy risks imposed by smart things and services surrounding the data subject."
- "individual control over the collection and processing of personal information by the surrounding smart things."
- "awareness and control of subsequent use and dissemination of personal information by those entities to any entity outside the subject's personal control sphere."

Aquest tres punts recullen en esencia la privacitat: avaluar els riscos de la privacitat personal, prendre les mesures idònies per protegir-la i tenir la seguretat de que s'estigui aplicant més enllà de la esfera de control inmediata [18].

Segons Rabindra Bista [19], hi ha dos tipus de problemes de privacitat en un WSN, la privacitat interna i l'externa. La privacitat interna consisteix en que la informació recollida pels sensors sigui compartida amb altres nodes del sistema que siguin de confiança, és a dir, que siguin compartits amb tercers o altres sensors no contemplats. En canvi, la privacitat externa gira entorn a que les dades obtingudes no estiguin accesibles per tercers ni estranys. Amb poques paraules, que les dades recollides només siguin accesibles pels usuaris contemplats anteriorment.

La intenció és que adversaris no puguin tenir accés ni puguin desxifrar les dades privades obtingudes i només puguin ser rebudes pels usuaris de confiança. A conseqüència, s'ha d'implementar un conjunts de mecanismes per assegurar-nos un control de divulgació de la informació. És per això que és necessari protegir la transmissió de dades privades en cada node del sistema i dels seus respectius nodes veïns. Considerar aquesta implementació és esencial, ja que no només s'ha de centrar en un node en singular, sinó que també el conjunt d'ells. Els nodes veïns poden escoltar tota informació privada i claus privades per xifrar i desxifrar [19].

Una de les causes de que hi hagi problemes de privacitat és que la majoria d'interaccions via internet són intrínsecament públiques, és a dir, qualsevol persona o màquina amb els recursos necessaris, pot observar els moviments. Aquí és quan es torna un problema encara més important, ja que en aquests processos s'intercanvien informació privada entre el sistema i l'usuari. Un exemple podria ser, en una ciutat intel·ligent, quan un usuari demani quin és el camí més ràpid per arribar a un hospital en concret. La resposta no hauria de ser exposada públicament per la gent del voltant sinó que sigui personal cap a l'usuari interessat [18].

Una de les solucions vigents són de caire criptogràfic i són útil tan per atacs a la privacitat interns i externs. Aquestes solucions s'enfrenten a un problema quan es tracta de situacions on l'atacant emplea un nivell computacional alt, ja que poden

resoldre els puzzles criptgràfics amb facilitat. Ademés, depenent del WSN que estigui implementat solucions d'aquest caire, poden tenir problemes de rendiment a causa de la creació d'overheads d'aquests procesos. Com a solució, s'implementen solucions criptogràfiques minimalistes per obtenir millors resultats en rendiment [20].

Una altre solució consisteix en implementar proxies com un agent de privacitat, és a dir, que pugui preservar privacitat entre les ISP (Internet Service Providers) i els usuaris. Conseqüentment, les dues bandes reben la informació demanada però s'ha de monitoritzar correctament, ja que pot generar problemes d'escalabilitat i problemes de interconnectivitat en les xarxes iot [21].

També cal mencionar el concepte de cloud computing com a solució. Aquesta tecnologia pot emmagatzemar les dades de manera centralitzada amb diversos controls d'accés, autenticació i gestió d'identitats. El més important d'aquesta solució és que les dues bandes interessades en ella han de pactar prèviament una serie de punts per finalment establir una bona protecció de la privacitat [20].

Actualment, existeixen molts tipus de solucions orientats a protegir la privacitat per així resoldre el problema de que internet és intrínsecament públic. Com hem esmentat anteriorment, aquestes tecnologies estan en constant creixement i evolució, és a dir, cada cop existeixen millores i noves solucions per aquestes xarxes. Però no només es troben noves solucions sinó que també es troben noves maneres de poden violar la privacitat d'una WSN. Tota solució no dóna una resposta absoluta al problema indicat, és per això que per tenir un sistema robust en seguretat, s'ha de implementar un conjunt de solucions orientats a possibles forats de privacitat dels sistemes sense reduir el rendiment d'elles [21] i ademés estar constantment monitoritzant els sistemes per preveure possibles atacs.

Figura 8. Representació de la implementació d'un sistema robust en seguretat. Font: [23]

Conclusions

En aquest treball hem donat a conèixer què és la tecnologia de l'internet de les coses i el seu funcionament. Hem vist com realment, tot i estar, en constant creixement té un gran impacte en la vida quotidiana, tant si ens centrem en el nostre dia a dia com en el món empresarial.

La paraula en la qual resumiria el IoT seria "transformació", ja que hem pogut veure com realment la tecnologia ha afectat en els sectors fonamentals de la nostra societat. Ha aconseguit adaptar les tècniques que coneixem i adaptar-les amb dispositius i sensors per treure un millor rendiment i de manera sostenible. Sobretot sense perdre l'essència del paradigma emprat en cada sector esmentat.

A més, hem pogut entendre amb més detall com funciona un sistema que implementa IoT juntament amb la tecnologia que la fa possible. Com els sensors poden estar relacionats amb altres sensors mentre s'intercanvien informació que van obtenint del seu entorn. Tot perquè finalment, els sensors i nodes veïns acabin enviant la informació rebuda cap al servidor per assolir l'últim pas, el processament i anàlisi de les dades.

Finalment, hem tractat el tema de la privacitat entorn de la tecnologia de l'internet de les coses, on hem arribat a la conclusió que per acabar tenint un sistema robust i segur s'ha d'implementar diverses solucions amb la finalitat de preveure possibles atacs. És important estar actualitzat, ja que no només la tecnologia evoluciona sinó que els atacants i els seus atacs també.

Aquest tema és molt interessant de tractar, però en un altre context m'agradaria poder prendre altres camps d'estudi i centrar-me en altres ramificacions. Personalment, en un futur, m'agradaria tractar detalladament com afecta IoT en el medi ambient i investigar sobre opcions encara més sostenibles.

Bibliografia

[1] Lopez Research LLC, “An Introduction to the Internet of Things (IoT).”, San Francisco, CA, 2013.
[2] Pramod Dhakal, “Huge impact of IoT in 6 sectors.”, 2020.
[3] Carrie MacGillivray, David Reinsel, “Worldwide Global DataSphere IoT Device and Data Forecast, 2021–2025”, 2021.
[4] ONU, “Una población en crecimiento”, 2019.
[5] FAO, “El estado mundial de la agricultura y la alimentación 2017”, 2017.
[6] Sachin Kumar, Prayag Tiwari, Mikhail Zymbler, “Internet of Things is a revolutionary approach for future technology enhancement: a review”, 2019.
[7] Prieto Ferrer, Miguel Ángel, “Instrumentación inteligente no invasiva para procesos en ganadería y agricultura”, 2021.
[8] Quental, “Tecnología IoT en el Sector Hospitalario”, 2021.
[9] Georgios Lampropoulos, Kerstin Siakas, Theofylaktos Anastasiadis, “INTERNET OF THINGS IN THE CONTEXT OF INDUSTRY 4.0: AN OVERVIEW”, 2019.
[10] Telcel Empresas, “Sectores que aplican internet de las cosas”, 2022.
[11] Mustafa Kocakulak, Ismail Butun, “An overview of Wireless Sensor Networks towards internet of things”, Las Vegas, NV, USA, 2017.
[12] Yinbiao, D., & Lee, D., “IEC White Paper Internet of Things: Wireless Sensor Networks”, International Electrotechnical Commission White Paper, 2014.
[13] A. Holmes, “A Technical Report: Wireless Sensor Networks and How They Work”, University of California Santa Barbara, 2016.
[14] R. Gunasagaran; L. M. Kamarudin; A. Zakaria; E. Kanagaraj; M. S. A. M Alimon; A. Y. M. Shakaff; P. Ehkan; R. Visvanathan; M. H. M. Razali, “Internet of things: Sensor to sensor communication”, Busan, Korea (South), 2016.
[15] Eleonora Borgia, “The Internet of Things vision: Key features, applications and open issues”, 2014.
[16] Cisco, “Internet of Things: La próxima evolución de Internet lo está cambiando todo”, 2011.
[17] Jeannette Alexandra Laverde Mena, Carlos Guillermo Laverde Mena, “Internet de las cosas aplicado en la agricultura ecuatoriana: Una propuesta para sistemas de riego”, 2021.
[18] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, Klaus Wehrle, “Privacy in the Internet of Things: threats and challenges”, 2013.
[19] Rabindra Bista, Jae-Woo Chang, “Privacy-Preserving Data Aggregation Protocols for Wireless Sensor Networks: A Survey”, 2010.
[20] Pawani Porambagem Mika Ylianttila, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov, Athanasios V. Vasilakos, “The Quest for Privacy in the Internet of Things”, 2019.

[21] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions”, 2013.
[22] Wipro, “What can IoT do in Healthcare?”, 2022.
[23] L. Minh Dang, Md. Jalil Piran, Dongil Han, Kyungbok Min, Hyeonjoon Moon, “A Survey on Internet of Things and Cloud Computing for Healthcare”, Sejong University, Seoul 143-747(05006), Korea, 2019.
[24] Sudeep Srivastava, Appinventiv, “Understanding the impact of IoT in healthcare”, 2022.