Università degli Studi eCampus

Tesi di Laurea

Domotica Residenziale

Evoluzione dei Protocolli di Comunicazione IoT e Gestione di Dispositivi Multimarca

Relatore: Prof. Christian Callegari
Candidato: Michele Rota Biasetti
Matricola nº 1518870

Anno accademico 2024/2025

Indice

Capitolo 1

Introduzione

Negli ultimi anni, le tecnologie legate all'Internet of Things (IoT) hanno trasformato radicalmente il nostro modo di vivere gli spazi domestici. La casa tradizionale, un tempo costituita semplicemente da strutture fisiche e arredi, si è evoluta in un ambiente intelligente e interconnesso, capace di rispondere dinamicamente alle nostre necessità quotidiane attraverso la domotica. Pensiamo ad esempio a quanto sia comodo accendere il riscaldamento mentre si sta tornando a casa dal lavoro, così da trovare la casa già calda e risparmiare anche energia.

Le radici della domotica affondano negli anni '80, quando i primi sistemi cablati, seppur rudimentali come il protocollo X10, permettevano già il controllo remoto di luci ed elettrodomestici. Il decennio successivo ha segnato un'accelerazione significativa: l'introduzione di sistemi più sofisticati come KNX e l'avvento delle reti wireless (Zigbee, Z-Wave) hanno reso la casa intelligente accessibile a tutti. Molti di noi ricordano l'impatto dei primi termostati Nest o delle lampadine Philips Hue, prodotti che hanno fatto capire alle persone comuni quanto può essere utile la domotica in casa.

L'arrivo dell'intelligenza artificiale ha ulteriormente ampliato le possibilità ed accelerato il cambiamento in atto. Oggi le nostre case non si limitano a rispondere ai nostri comandi: è come se ci conoscessero e si adattassero a noi. Per esempio, dopo qualche settimana il sistema capisce che di solito accendiamo le luci del salotto verso le 19:00 e inizia a farlo automaticamente. Gli assistenti vocali come Alexa, Google o Siri non sono più semplici esecutori di ordini: a volte ci sorprendono suggerendo cose utili tipo "Hey, sta per piovere, vuoi che chiuda le finestre?" oppure "È ora di andare a dormire, spengo le luci?". È un po' come avere un maggiordomo digitale che impara a conoscerti giorno dopo giorno.

L'edge computing rappresenta una ulteriore innovazione rilevante che consentendo l'elaborazione dei dati direttamente a livello locale riduce ed in alcuni casi elimina la dipendenza dal cloud. Con questo nuovo approccio si migliorano sensibilmente i tempi delle risposte: una telecamera di sicurezza con le funzionalità e la capacità di edge computing può identificare immediatamente un intruso e inviare alert in tempo reale, senza così dover attendere l'elaborazione su server remoti.

Le tecnologie di rete continuano a evolversi e questo porterà sicuramente nuove possibilità per la casa intelligente. Già oggi vediamo come il miglioramento delle connessioni

permetta di controllare i dispositivi con maggiore affidabilità e velocità. Nel prossimo futuro, potremmo vedere interfacce più intuitive e una maggiore integrazione con servizi esterni. Naturalmente, ogni innovazione porta con sé nuove sfide legate alla sicurezza e alla protezione dei dati personali.

Tuttavia, una delle sfide più rilevanti nel settore della domotica residenziale riguarda l'interoperabilità tra dispositivi di differenti produttori. L'esperienza comune di molti utenti che si approcciano alla domotica nella propria abitazione sono le difficoltà legate alla gestione di applicazioni multiple e protocolli di comunicazione non compatibili, oltre alla necessità di acquisire componenti hardware dedicate per ciascun ecosistema proprietario (Hub per la gestione dei diversi dispositivi per ogni marca). Tuttavia l'introduzione di standard aperti come il protocollo Matter rappresenta un'evoluzione significativa in questa direzione, favorendo una maggiore integrazione tra soluzioni di produttori diversi e la possibilità di avere un unico Hub centrale in grado di gestire dispositivi di marche differenti.

La presente tesi sarà incentrata sul passi evolutivi nei protocolli di comunicazione IoT per la domotica residenziale, con un focus su alcuni aspetti, quali la sicurezza, le prestazioni e l'interoperabilità, sarà presentato anche caso studio per passare dalla ateoria alla pratica. Il caso stusdio sarà basato su Apple HomeKit, selezionato in questo caso per la sua usabilità, per le sue caratteristiche di sicurezza integrata e per la facilità di condivisione delle imporstazioni con i componenti della famiglia.

1.1 Approccio metodologico

Il lavoro presentato in questa tesi nasce dall'esigenza di comprendere a fondo il mondo della domotica residenziale, combinando diversi punti di vista per offrire una visione il più possibile completa e pratica.

- **Esplorazione della letteratura**: ho consultato numerose pubblicazioni tecniche e articoli specializzati, cercando di selezionare le fonti più recenti e significative per mantenermi aggiornato sugli sviluppi del settore;
- **Confronto tra protocolli**: ho messo a confronto le diverse tecnologie disponibili, basandomi su informazioni pubblicamente accessibili e opinioni di esperti del settore, per capire punti di forza e debolezza di ciascuna soluzione;
- **Osservazione di esempi concreti**: ho dedicato particolare attenzione ai sistemi già presenti sul mercato, con un focus su Apple HomeKit come caso interessante di tecnologia ben integrata nell'esperienza quotidiana degli utenti;
- **Esperienza diretta**: ho avuto modo di sperimentare personalmente con alcuni dispositivi di marche diverse, toccando con mano le sfide che si incontrano quando si cerca di far dialogare prodotti di aziende differenti.

Attraverso questo percorso ho potuto esplorare il mondo della domotica da diverse angolazioni, cercando di capirne pregi e difetti. Lo scopo è offrire spunti pratici e considerazioni concrete a chi vuole iniziare a rendere la propria casa più intelligente, andando oltre la semplice teoria.

1.2 Obiettivi della ricerca

Questa tesi si propone diversi obiettivi, che nascono dalla natura complessa e variegata del mondo della domotica oggi:

- **Analisi evolutiva**: tracciare un quadro completo dell'evoluzione storica e tecnologica dei protocolli IoT nel contesto domotico, evidenziando le forze trainanti del cambiamento e le tendenze emergenti;
- **Valutazione critica della sicurezza**: esaminare approfonditamente le vulnerabilità specifiche dei sistemi IoT domestici, proponendo strategie di mitigazione pratiche semplici e gestibili per l'utente finale;
- **Comparazione prestazionale**: sviluppare una valutazione sistematica delle performance dei protocolli principali attraverso metriche quantitative significative (latenza, throughput, consumo energetico, scalabilità);
- **Studio dell'interoperabilità**: identificare e descrivere strategie concrete per l'integrazione efficace di dispositivi eterogenei, con particolare attenzione alle sfide pratiche di implementazione;
- **Validazione empirica**: fornire un esempio tangibile attraverso l'implementazione pratica con Apple HomeKit, dimostrando l'applicabilità dei principi teorici discussi.

Questo lavoro di tesi è un mix di teoria e pratica, cerca di essere utile sia per chi studia questi argomenti sia per chi vuole semplicemente migliorare la propria casa con la tecnologia.

Capitolo 2

La Domotica Residenziale

Negli ultimi decenni, l'evoluzione delle tecnologie digitali ha profondamente trasformato il nostro modo di vivere la casa, dando origine al concetto di casa intelligente. Questo processo ha permesso che la domotica residenziale sia diventata una realtà tangibile, non più solamente in scenari futuristici o in prototipi sperimentali. L'automazione dei dispositivi domestici, la possibilità di controllarli da remoto e la loro capacità di apprendere dai nostri comportamenti e dalle nostre preferenze, oggi è una realtà presente in molte abitazioni moderne.

La domotica rappresenta una trasformazione a 360 gradi del modo in cui vengpono progettati gli ambienti domestici, vissuti e gestiti, non è solamente un'insieme di gadget tecnologici. Attraverso l'integrazione tra le diverse componenti, sensori, attuatori, interfacce utente e protocolli di comunicazione, l'abitazione si delinea come un ecosistema digitale interconnesso, orientato al miglioramento dell'efficienza energetica, della sicurezza, del comfort e dell'accessibilità.

2.1 Definizione e principi fondamentali

2.1.1 Cos'è davvero la domotica?

«Il termine *domotica* è l'unione del termine latino *domus* (casa) e dal termine *informatica*. Indica l'integrazione di tecnologie elettroniche, informatiche e di telecomunicazione per automatizzare, controllare e ottimizzare i sistemi presenti in un'abitazione. Il suo scopo principale è migliorare il comfort, la sicurezza, l'efficienza energetica e l'accessibilità degli ambienti domestici»[1].

2.1.2 I pilastri della casa intelligente

I principi fondamentali che guidano un sistema domotico efficace ed efficiento sono:

[1] Wikipedia contributors Domotica. *Domotica*. Accesso il 10 aprile 2025. 2024. URL: `https://it.wikipedia.org/wiki/Domotica`.

- **Automazione**: la casa esegue azioni senza un intervento diretto da parte dell'abitante della casa, basandosi su orari, sensori o scenari predefiniti;
- **Integrazione**: tutti i dispositivi cooperano in modo sinergico all'interno di un ecosistema condiviso;
- **Personalizzazione**: la casa si adatta alle abitudini, alle preferenze e alle necessità specifiche dei suoi abitanti;
- **Interoperabilità**: i dispositivi dei diversi produttori comunicano tra loro in modo coerente, riducendo frammentazione e complessità.

2.2 Componenti principali di un sistema domotico

Un sistema domotico può essere paragonato ad esempio a un organismo vivente, dove abbiamo i sensori che percepiscono l'ambiente, gli attuatori che compiono le azioni, una rete nervosa che serve per la comunicazione e un cervello centrale che riesce a coordinare il tutto.

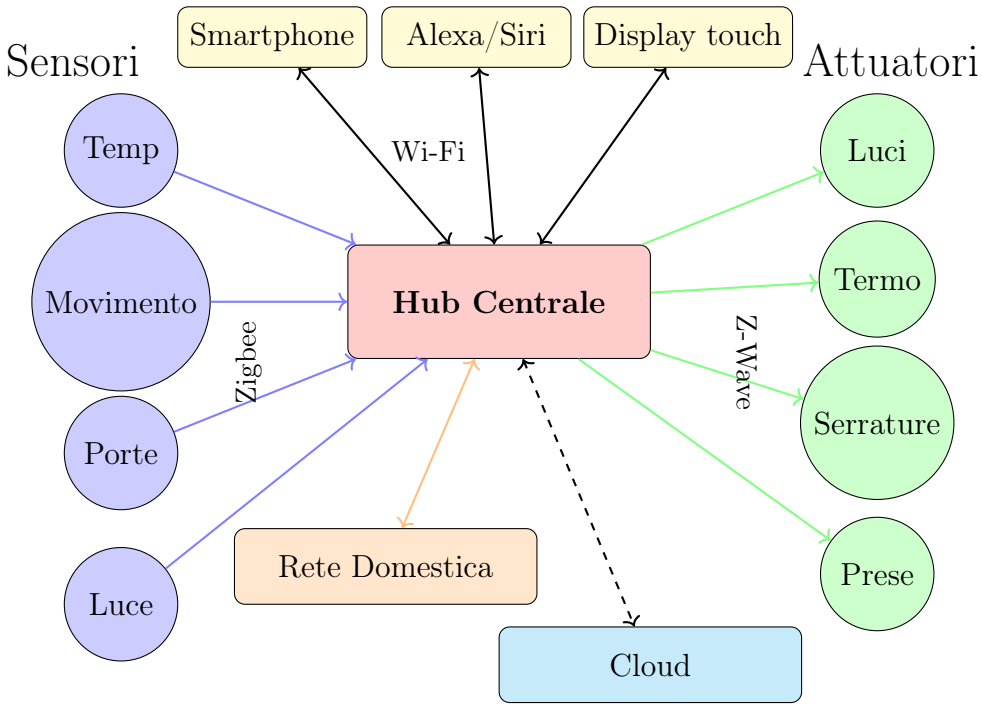

Figura 2.1: Architettura tipica di un sistema domotico residenziale

2.2.1 Sensori

I sensori servono a raccogliere le informazioni sull'ambiente circostante come ad esempio:

- misuratorazione dell'ambiente (per la temperatura, l'umidità, la luminosità, la qualità dell'aria, etc.);

- rilevamento di movimento/presenza (PIR, microonde, ultrasuoni);
- controlli di sicurezza (controllano l'apertura porte/finestre, la presenza di fumo, gas, fuiriuscite di acqua);
- misuratorazione del consumo energetico.

2.2.2 Attuatori

Gli attuatori sono i dispositivi che trasferiscono i comandi ricevuti in azioni fisiche:

- per accensione/spegnimento di luci e dispositivi;
- per il controllo di tapparelle, tende e infissi motorizzati;
- per la regolazione di riscaldamento e condizionamento;
- per la gestione di elettrodomestici e impianti multimediali.

2.2.3 Controller e hub

L'unità centrale (hub) è il vero e proprio cervello del sistema, deve gestire le regole di automazione, interpretare i dati e coordinare le azioni sugli attuatori. In alcuni casi può essere un dispositivo fisico dedicato, un assistente vocale (es. Alexa, Google Home) o un server locale (es. Home Assistant su Raspberry Pi).

2.2.4 Interfacce utente

Gli utenti possono interagire con il sistema tramite:

- App mobili;
- Interfacce vocali;
- Dashboard web;
- Pulsanti intelligenti o pannelli touch.

2.2.5 Reti di comunicazione

La rete collega tutti i dispositivi tra di loro. Può essere cablata (es. KNX) o wireless (es. Zigbee, Z-Wave, Wi-Fi, Thread). I protocolli scelti influenzano la scalabilità, l'efficienza e la sicurezza del sistema.

2.3 I vantaggi della domotica

2.3.1 Efficientamento energetico

La domotica permette di gestire in maniera più consapevole i consumi energetici che vengono utilizzati dalla casa, tra questi possiamo avere:

- la gestione e ottimizzazione del sistema di riscaldamento e del sistema di raffrescamento;
- il monitoraggio dei dispositivi inutilizzati e lo spegnimento automatico di luci;
- poter costruire una dashboard per monitorare i consumi in tempo reale.

2.3.2 Sicurezza

Grazie all'utilizzo dei sensori e alle automazioni è possibile ricevere notifiche rendendo la casa più sicura:

- rilevamento intrusioni o incidenti (fumo, acqua, CO);
- gestione remota e controllo in tempo reale;
- registrazione video e notifiche intelligenti.

2.3.3 Comfort e accessibilità

L'automazione è alla base per la semplificazione la vita quotidiana:

- scenari personalizzati (es. "buongiorno", "cinema");
- controllo vocale per utenti con disabilità;
- adattamento dinamico dell'ambiente alle esigenze familiari.

2.4 Sfide attuali e prossimi capitoli

Nonostante il progresso tecnologico ed alla riduzione dei costi, persistono però numerosi ostacoli ad un'adozione diffusa:

- **Interoperabilità**: i dispositivi di marche diverse spesso non comunicano bene tra di loro
- **Sicurezza e privacy**: i dispositivi connessi devono proteggere i dati e gli accessi non autorizzati
- **Affidabilità**: un sistema domestico deve funzionare anche in caso di disconnessioni dalla rete o in caso di guasti di alcune sue componenti

Nel prossimo capitolo analizzeremo più da vicino le tecnologie di comunicazione che rendono possibile tutto questo, confrontando protocolli cablati e wireless in termini di prestazioni, consumo e compatibilità.

Capitolo 3

L'evoluzione dei Protocolli di Comunicazione per l'IoT

3.1 Introduzione ai protocolli per l'IoT

I protocolli di comunicazione per l'IoT possiamo immaginarli come il vero e proprio "linguaggio" che rende possibile ai dispositivi intelligenti della nostra casa di parlarsi e di collaborare. Pensiamo a quando accendiamo la luce grazie all'utilizzo del nostro smartphone o regoliamo il termostato per riscsaldare la casa prima di arrivare, tutto questo azioni sono possibili grazie ai protocolli di comunicazione che gestiscono per l'appunto la comunicazione tra dispositivi diversi, spesso di marche e con tecnologie differenti. Nel corso del tempo, questi protocolli si sono via via evoluti per poter rispondere alle nuove esigenze del mercato, come ad esempio avendo una miglior gestione dei consumi, una maggiore sicurezza ed una miglior facilità d'uso. I variprotocollik possono essere divisi in due grandi famiglie, quelli cablati come KNX e RS-485, e quelli wireless come Zigbee, Z-Wave, Wi-Fi, Bluetooth Low Energy, Thread e Matter.

3.2 Protocolli cablati: KNX e RS-485

I protocolli cablati sono stati i primi protocolli utilizzati nella domotica, residenziale e industrile, ed ancora oggi vengono molto utilizzati, soprattutto in quei progetti dove la stabilità della comunicazione è fondamentale.

«**KNX** è uno standard aperto per la building automation, definito a livello internazionale come ISO/IEC 14543-3. È stato sviluppato per garantire l'interoperabilità tra dispositivi e sistemi di diversi produttori, con applicazioni che spaziano dall'illuminazione al riscaldamento, fino alla sicurezza e al controllo degli elettrodomestici. KNX è un sistema standardizzato a livello mondiale per la domotica e la gestione tecnica degli edifici»[1]. Un suo utilizzo classico è ad esempio in un grande edificio, come può essere un'hotel, dove le luci, il riscaldamento, le tende ed i sistemi di sicurezza deveono poter funzioanre senza problemi. Tuttavia un suo impiego in ambieti più piccoli come nelle case presenta de-

[1] Wikipedia contributors KNX. *KNX (standard).* `https://it.wikipedia.org/wiki/KNX_(standard)`. Accessed: 2025-08-25. 2025.

gli svantaggi economici, per la necessita dell'intervento di tecnici specializzati, ed inoltre successivi ampliamenti richiederanno nuovi lavori edili se non previsti in fase iniziale di progettazione

RS-485, invece, è spesso usato in contesti industriali o in impianti domestici più semplici per risolvere specifici problemi, come ad esempio un sistema di allarme o controllo degli accessi. «RS-485 è uno standard di comunicazione seriale definito dall'EIA/TIA, progettato per consentire trasmissioni affidabili in sistemi multipunto e su lunghe distanze. RS-485 definisce le caratteristiche elettriche dei driver e dei ricevitori per l'uso in sistemi digitali bilanciati multipunto»[2].

RS-485 può garantire una comunicazione stabile anche su lunghe distanze e in ambienti con molte interferenze elettriche, questo si traduce in un sistema robusto che raramente perde il segnale. Tuttavia, come KNX, richiede cablaggi e competenze tecniche per l'installazione, inoltre ache in questo caso sono onerosi i successivi ampliamenti e modifiche se non previste nella prima fase di progettazione.

3.3 I protocolli wireless: Zigbee, Z-Wave, Wi-Fi e Bluetooth Low Energy

Con l'arrivo e la diffusione delle tecnologie wireless, la domotica è potuta diventata più accessibile e flessibile, permettendo così alle nuove installazioni di essere più semplici e meno invasive.

«**Zigbee** è un protocollo di comunicazione wireless a basso consumo energetico, progettato per applicazioni che richiedono trasmissione di dati a corto raggio e con bassa velocità. Basato sullo standard IEEE 802.15.4, Zigbee è stato sviluppato e mantenuto dalla *Connectivity Standards Alliance* (già Zigbee Alliance) con l'obiettivo di favorire l'interoperabilità tra dispositivi di diversi produttori e garantire soluzioni affidabili e scalabili per l'automazione domestica e industriale»[3].

Zigbee è molto popolare per dispositivi come sensori di movimento, termostati smart e lampadine intelligenti. Ad esempio, in una casa, i sensori Zigbee possono comunicare tra loro formando una rete mesh, se un dispositivo è lontano dal router il segnale passa attraverso altri dispositivi fino a raggiungerlo. Questa tecnica permette di poter installare anche in case di grandi dimensioni o con muri spessi che schermerebbero il segnale, diversi dispositivi. Un vantaggio è che la comunicazione tra i dispositivi e l'hub centrale resta stabile, a questo si aggiunge il basso consumo energetico, che permette ai sensori di durare anni con una singola batteria. Lo svantaggio è la necessità di un hub centrale per ogni marca di dispositivi e la difficoltà nella configurazione e nei successivi momenti di aggiornamento del firmware dei singoli dispositivi.

[2]Wikipedia contributors RS-485. *RS-485*. `https://it.wikipedia.org/wiki/RS-485`. Accessed: 2025-08-25. 2025.

[3]Connectivity Standards Alliance. *Zigbee Technology Overview*. `https://csa-iot.org/all-solutions/zigbee/`. Accessed: 2025-08-25. 2025.

«**Z-Wave** è un protocollo wireless progettato specificamente per applicazioni di domotica e automazione residenziale. Utilizza frequenze sub-GHz per garantire una copertura più ampia e minori interferenze rispetto al Wi-Fi o al Bluetooth. Lo standard è gestito dalla *Z-Wave Alliance*, che promuove l'interoperabilità tra dispositivi di diversi produttori e assicura la certificazione dei prodotti conformi»[4].
Z-Wave è simile a Zigbee ma spesso preferito in ambito residenziale per la sua semplicità di configurazione iniziale, i wizard di installazione e configurazione sono intuitivi e permettono di collegare dispositivi come serrature smart o controller per tapparelle. Un'ulteriore caratteristica è la sicurezza integrata, così come la compatibilità tra marche diverse, tuttavia, la velocità di trasmissione è limitata rispetto al Wi-Fi, il che lo rende meno adatto a trasmettere grandi quantità di dati.

«**Wi-Fi** è una famiglia di tecnologie di rete wireless basate sullo standard IEEE 802.11. È progettato per consentire connessioni a banda larga senza fili, garantendo interoperabilità e compatibilità tra dispositivi di diversi produttori. La *Wi-Fi Alliance*, l'organizzazione che gestisce il programma di certificazione, assicura che i prodotti conformi possano comunicare tra loro in modo sicuro ed efficiente»[5].

Wi-Fi è probabilmente il protocollo più familiare, essendo quello usato per connettere smartphone, computer e smart TV a internet, molti dispositivi IoT, come videocamere di sicurezza o assistenti vocali, usano il Wi-Fi perché garantisce alta velocità e non richiede hub aggiuntivi. Lo svantaggio principale sta nell'alto consumo energetico, che limita l'uso di Wi-Fi nei dispositivi alimentati a batteria, altre problematiche riguradano la sicurezza di questi dispositivi e la congestione della rete Wi-Fi domestica.

«**Bluetooth Low Energy (BLE)** è una variante a basso consumo dello standard Bluetooth, introdotta con la specifica Bluetooth 4.0 e sviluppata dal *Bluetooth Special Interest Group (SIG)*. È progettata per applicazioni che richiedono comunicazioni wireless a corto raggio e con un consumo energetico minimo, come sensori, dispositivi indossabili e soluzioni IoT. Grazie alla sua diffusione e compatibilità, BLE è diventato uno dei protocolli più utilizzati nella connettività tra dispositivi intelligenti»[6].

Il BLE è utilizzato prevalentemente quindi nei dispositivi a corto raggio e con bassissimo consumo energetivco, come ad esempio gli smartwatch, i fitness tracker o i sensori di prossimità. Un suo utilizzo classico è quello per lo sblocco di una porta quando ci si avvicina con uno smartphone o con un Tag BLE. Il suo grande vantaggio è il risparmio energetico e la sua semplicità, il suo problema principale riguarda la portata limitata del segnale che lo rende inadatto per coprire tutta la casa senza dispositivi aggiuntivi.

[4]Z-Wave Alliance. *Z-Wave Technology Overview*. `https://z-wavealliance.org/z-wave/`. Accessed: 2025-08-25. 2025.

[5]Wi-Fi Alliance. *Discover Wi-Fi*. `https://www.wi-fi.org/discover-wi-fi`. Accessed: 2025-08-25. 2025.

[6]Bluetooth SIG. *Bluetooth Low Energy*. `https://www.bluetooth.com/learn-about-bluetooth/tech-overview/low-energy/`. Accessed: 2025-08-25. 2025.

3.4 Thread e Matter: verso l'interoperabilità e l'unificazione

Chi si avvicina alla domotica spesso scopre con disappunto che i dispositivi di marche diverse faticano a comunicare tra loro. È frustrante comprare una lampadina smart di un brand e scoprire che non funziona con l'hub di un altro. Thread e Matter sono protocolli nati proprio per risolvere questa babele tecnologica.

«**Thread** è un protocollo di rete wireless basato su IPv6, sviluppato per dispositivi IoT a basso consumo energetico. Utilizza IEEE 802.15.4 come livello fisico e supporta topologie mesh per garantire affidabilità, sicurezza e auto-riparazione della rete. Lo sviluppo e la promozione dello standard sono gestiti dal *Thread Group*»[7].

Thread permette ai dispositivi quali le luci, i sensori e i termostati di connettersi tra di loro creando una ragnatela di nodi, questo rende possibile qualora una lampadina si spegne o perde il segnale, che gli altri dispositivi trovino automaticamente percorsi alternativi per comunicare, aumnetando la stabilità rispetto ai protoicolli precedenti. La configurazione è generalmente più semplice e immediata. Il principale problema rigurda al diffusione essendo ancora una tecnologia giovane, è poco integrata o supportata dai vari produttori di dispositivi

«**Matter** è uno standard aperto di connettività per la smart home, sviluppato congiuntamente da un consorzio di aziende guidato dalla *Connectivity Standards Alliance*. Il suo obiettivo è garantire un livello elevato di interoperabilità tra dispositivi e piattaforme diverse, riducendo la frammentazione del mercato e semplificando l'esperienza d'uso per i consumatori. Matter si basa su protocolli IP come Wi-Fi ed Ethernet per la comunicazione ad alta velocità e su Thread per scenari a basso consumo»[8].

Matter quindi rappresenta forse l'iniziativa più ambiziosa nell'intero settore della domotica, nasce dall'idea di stabilire un protocollo di comunicazione universale tra dispositivi intelligenti di differenti produttori. Questo nuovo standard si pone alla base per la soluzione delle problematiche di interoperabilità che caratterizzano l'attuale panorama della smart home, in cui i dispositivi appartenenti a ecosistemi diversi presentano impossibilità tecniche o limitazioni significative per l'integrazione reciproca. L'adozione di Matter consente ai diversi dispositivi certificati di poter operare contemporaneamente su piattaforme differenti, come i principali hub commerciali (Alexa, Apple, Google, Samsung), tale standardizzazione garantisce una semplificazione nella configurazione della casa domotica, permettendo di fare delle scelte basate su criteri qualitativi e funzionali piuttosto che su vincoli di compatibilità.

Nonostante le promettenti prospettive, l'adozione del protocollo si trova ancora in fase di espansione, con una progressiva ma non ancora completa diffusione nel mercato. È importante sottolineare che il protocollo Matter non consente l'integrazione di qualsiasi tipologia di dispositivo, ma definisce specifiche categorie supportate attraverso le pro-

[7] Thread Group. *About Thread*. `https://www.threadgroup.org/`. Accessed: 2025-08-25. 2025.

[8] Connectivity Standards Alliance. *Matter: The Foundation for Connected Things*. `https://csa-iot.org/all-solutions/matter/`. Accessed: 2025-08-25. 2025.

prie direttive tecniche. Questo approccio selettivo garantisce l'affidabilità e la coerenza dell'ecosistema, limitando tuttavia l'universalità inizialmente prospettata.

3.5 Criteri di selezione dei protocolli

Quando si deve scegliere un protocollo per la nostra casa intelligente, bisogna prendere in considerazione diversi aspetti pratici:

- **Consumo energetico**: Se avete dispositivi alimentati con delle batterie, come i sensori o le serrature, è fondamentale scegliere dei prodotti che abbiamo dei protocolli a basso consumo energetico per evitare continui ricambi delle batteria.
- **Portata e copertura**: In case grandi o con muri spessi, protocolli con rete mesh come Zigbee, Thread o Z-Wave possono garantire una copertura migliore.
- **Velocità e latenza**: Per le applicazioni che necessitanod di avere delle risposte immediate, come sono le videocamere o i sistemi di allarme, è meglio scegliere dei dispositivi che supportino i protocolli veloci come il Wi-Fi.
- **Facilità d'uso e integrazione**: Per far funzionare insieme dispositivi di produttori diversi, è essenziale verificare che supportino gli stessi protocolli di comunicazione, preferendo standard aperti che facilitino la configurazione e garantiscano una reale interoperabilità.
- **Sicurezza e privacy**: Per proteggere la propria rete domestica è poi fondamentale sceglere dispositivi che supportino i protocolli che offrono le più solide misure di sicurezza.

Nel prossimo capitolo approfondiremo proprio questi aspetti di sicurezza e privacy nei protocolli IoT domestici, fornendo consigli pratici per mantenere la vostra casa intelligente protetta e affidabile.

Capitolo 4

Sicurezza e Privacy nella Domotica Residenziale

4.1 Introduzione alla sicurezza IoT nella domotica residenziale

La tecnologia nella domotica ha trasformato le nostre case in case più comode e più facili da gestire, dal controllo del riscaldamento, dalla gestione delle luci in base alle ore del giorno. Assieme a questi benefici però ci sono anche aspetti meno visibili, uno di questi è la grande quantità di dati personali che questi sistemi raccolgono e trattano ogni giorno.

È interessante riflettere sulla quantità di informazioni che fluiscono attraverso una casa intelligente: orari di presenza, preferenze climatiche, abitudini di illuminazione, fino ad arrivare ai dati biometrici raccolti dalle telecamere di ultima generazione. Ogni componente del sistema - dal termostato intelligente all'assistente vocale - rappresenta contemporaneamente un'opportunità e una potenziale vulnerabilità.

Ogni nuovo dispositivo connesso aggiunge un "punto d'ingresso" alla nostra rete domestica. Non dobbiamo più pensare alla sicurezza di un solo apparecchio, ma di un sistema dove tutto comunica con tutto, spesso anche con servizi online. Questa rete invisibile all'occhio dell'utente richiede strategie di protezione completamente riviste.

L'approccio più efficace prevede l'integrazione della sicurezza fin dalle fasi iniziali di progettazione - il cosiddetto principio del *security by design*. Questo significa implementare protezioni a più livelli: cifratura dei dati in transito e a riposo, gestione granulare dei permessi, meccanismi di difesa adattivi capaci di rispondere a minacce in evoluzione.

4.2 Minacce e vulnerabilità comuni

Le minacce alla domotica hanno dinamiche tutte loro, diverse da quelle della sicurezza informatica "classica". Capire queste differenze è il primo passo per proteggere davvero la propria casa smart.

4.2.1 Intrusioni e accessi non autorizzati

Un aspetto sorprendentemente critico riguarda la presenza di credenziali di default nei dispositivi IoT che non vengono aggiornate. Nonostante anni di sensibilizzazione, numerosi produttori continuano a distribuire dispositivi con combinazioni username/password facilmente reperibili attraverso una semplice ricerca online. Questa pratica, unita alla tendenza degli utenti a non modificare tali credenziali, crea vulnerabilità immediate e facilmente sfruttabili.

La situazione è aggravata dalla mancanza di meccanismi che obblighino l'utente a personalizzare le credenziali al primo utilizzo - una misura semplice che potrebbe eliminare gran parte di questi rischi.

4.2.2 Malware specifici per dispositivi embedded

I dispositivi IoT, caratterizzati da risorse computazionali limitate e sistemi operativi minimali, presentano un profilo di vulnerabilità unico. I malware progettati per questi ambienti sfruttano proprio queste limitazioni: la scarsa capacità di implementare antivirus tradizionali, l'impossibilità di monitorare in tempo reale i processi in esecuzione, la difficoltà nell'applicare patch di sicurezza.

Questi software malevoli possono operare inosservati per periodi prolungati, trasformando dispositivi apparentemente innocui in strumenti per la raccolta di dati sensibili o in nodi di botnet per attacchi distribuiti.

4.2.3 Vulnerabilità nei protocolli di comunicazione

L'eterogeneità dei protocolli wireless nella domotica - ZigBee, Z-Wave, Wi-Fi, Bluetooth - introduce sfide specifiche di sicurezza. Gli attacchi di tipo Man-in-the-Middle rappresentano una minaccia particolarmente insidiosa in questo contesto. Un attore malevolo può posizionarsi nel percorso di comunicazione tra dispositivi, intercettando e potenzialmente alterando i comandi trasmessi. Consideriamo l'esempio di una serratura intelligente: l'intercettazione dei segnali di controllo potrebbe permettere l'apertura della casa in un secondo momento.

4.2.4 Il caso Mirai: una lezione da non dimenticare

L'epidemia del botnet Mirai nel 2016 rimane un caso di studio fondamentale per comprendere le vulnerabilità sistemiche dell'IoT. Questo malware ha dimostrato come la combinazione di credenziali predefinite e mancanza di aggiornamenti di sicurezza possa trasformare centinaia di migliaia di dispositivi domestici in armi per attacchi DDoS di scala globale. La semplicità dell'attacco - basato essenzialmente sul tentativo sistematico di credenziali note - evidenzia come problemi apparentemente banali possano avere conseguenze devastanti[1].

[1] M. Antonakakis, T. April e M. et al. Bailey. *Understanding the Mirai Botnet*. 2017. URL: `https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis`.

4.3 Best practice per garantire sicurezza e privacy

Per difendere un ambiente domotico serve una strategia a più livelli, che unisca soluzioni tecniche, buone pratiche e formazione degli utenti. Insieme, questi elementi creano un sistema capace di reagire e adattarsi ai rischi che cambiano nel tempo.

4.3.1 Aggiornamenti e patch management

La gestione sistematica degli aggiornamenti rappresenta la prima linea di difesa contro vulnerabilità note. Questo processo, apparentemente semplice, presenta sfide pratiche significative nell'ambito IoT: molti dispositivi non implementano meccanismi di aggiornamento automatico, richiedendo interventi manuali periodici. La creazione di una routine di verifica - magari calendarizzata mensilmente - può trasformare questa attività da sporadica emergenza a pratica consolidata.

4.3.2 Segmentazione della rete

L'isolamento logico dei dispositivi tramite la segmentazione della rete rappresenta una delle misure di sicurezza più efficaci, poiché permette di ottenere benefici significativi con un impegno tecnico e organizzativo relativamente ridotto. In questo configurazione della rete, la rete domestica può essere suddivisa in più ambienti con delle funzioni distinte. Ad esempio, si puo avere una rete principale che può essere riservata ai dispositivi che gestiscono dati sensibili o ai sistemi IoT considerati più affidabili, mentre una seconda rete separata e isolata può essere destinata agli ospiti della casa, così da impedire accessi indesiderati alle risorse critiche. Una configurazione di questo tipo contribuisce non solo a contenere la propagazione di eventuali compromissioni, ma anche a semplificare l'attività di monitoraggio del traffico anomalo.

4.3.3 Firewall e sistemi di monitoraggio

Negli ultimi anni hanno avuto uno sviluppo importante anche i router destinati all'uso domestico, integrando nuove funzioni di sicurezza che in passato erano tipiche solo dei router professionali. I principali produttori come ASUS, Netgear o AVM (Fritz!Box) oggi includono nei loro dispositivi delle soluzioni che spaziano dai sistemi di prevenzione delle intrusioni fino ad analisi del traffico, oltre a servizi in continuo aggiornamento sui filtri del traffico per contenuti potenzialmente malevoli. A tutte queste funzioni si aggiungono poi anche sistemi di notifica in grado di segnalare all'utente eventi di sicurezza rilevanti. Infine alcuni provider della connettività hanno iniziato a proporre direttamente dispositivi preconfigurati con queste funzionalità già attive, rendendo ancora più immediata l'adozione da parte degli utenti meno esperti.

4.3.4 Gestione degli accessi e autenticazione forte

L'implementazione di politiche di accesso robuste richiede un bilanciamento tra sicurezza e usabilità:

- **Principio del privilegio minimo**: assegnare solo i permessi strettamente necessari per ogni utente o dispositivo

- **Autenticazione multi-fattore (MFA)**: integrare fattori di autenticazione aggiuntivi, bilanciando sicurezza e praticità d'uso
- **Gestione centralizzata delle credenziali**: l'utilizzo di password manager facilita l'adozione di credenziali complesse e uniche
- **Rotazione programmata**: stabilire intervalli regolari per l'aggiornamento delle credenziali critiche

4.3.5 Educazione e consapevolezza degli utenti

La componente umana rimane fondamentale in qualsiasi strategia di sicurezza. La formazione degli abitanti della casa, soprattutto per gli utenti con ruoli di gestione amministrativa dei dispositivi, dovrebbe coprire:

- Riconoscimento di tentativi di phishing specifici per dispositivi IoT
- Comprensione dell'importanza degli aggiornamenti di sicurezza
- Capacità di verificare l'autenticità di app e servizi collegati
- Identificazione di comportamenti anomali nei dispositivi

Sessioni informative periodiche, magari integrate con esempi pratici e simulazioni, possono trasformare ogni membro della famiglia in un elemento attivo del sistema di sicurezza.

4.4 Tecniche di crittografia e autenticazione nei protocolli IoT

L'implementazione di meccanismi crittografici in ambienti con risorse limitate rappresenta una delle sfide tecniche più interessanti della sicurezza IoT.

4.4.1 Crittografia end-to-end nei sistemi domotici

La protezione crittografica dei dati deve essere garantita lungo l'intero percorso di trasmissione, dal dispositivo Ioy fino al nostro smartphone. Le limitazioni hardware dei dispositivi IoT impongono scelte oculate nell'implementazione:

- **AES-128**: uno degli standard più diffusi, usato perché offre un buon equilibrio tra sicurezza e velocità. Protegge bene senza pesare troppo sulle prestazioni o sulla batteria.
- **Crittografia a curve ellittiche (ECC)**: garantisce lo stesso livello di protezione di altri sistemi ma con chiavi più corte, quindi più veloce e adatta anche ai dispositivi più piccoli.
- **Suite crittografiche leggere**: algoritmi come ChaCha20-Poly1305, pensati apposta per l'IoT, che mantengono alta la sicurezza anche su hardware con risorse limitate.

4.4.2 Protocolli di comunicazione sicura

L'adattamento dei protocolli di sicurezza tradizionali alle necessità e caratteristiche dei dispositivi IoT ha prodotto soluzioni innovative:

- **DTLS (Datagram TLS)**: una versione di TLS pensata per funzionare bene con il protocollo UDP, utile per dispositivi che si connettono in modo intermittente o con reti non stabili.
- **Protocolli sicuri a livello applicativo**: come CoAP-DTLS e MQTT-TLS, che integrano le funzioni di sicurezza direttamente nel protocollo usato dai dispositivi per comunicare.
- **Meccanismi di attestazione**: sistemi che controllano l'integrità e l'autenticità del dispositivo prima di consentire lo scambio di dati, così da evitare comunicazioni con unità compromesse.

4.4.3 Standard di autenticazione nell'era IoT

La tendenza all'adozione di standard aperti ha reso sempre più semplice l'interoperabilità tra i dispositivi di produttori differenti, garantendo allo stesso tempo i livelli di sicurezza. Tra queste tecnologie oggi tra le più significative rientrano:

- **OAuth 2.0 e OpenID Connect**: questi protocolli consentono di autorizzare un servizio esterno per poter accedere solo a specifiche risorse, senza dover condividere la password principale. Con questo metodo l'utente riesce a mantenere un controllo più granulare sui propri dati.
- **JWT e CBOR Web Tokens**: si tratta di formati molto leggeri che racchiudono al loro interno tutte le informazioni necessarie all'autenticazione, riducendo la dipendenza da database centrali e semplificando la gestione delle varie sessioni.
- **FIDO2 e WebAuthn**: è lo standard che l'agestisce l'utenticazione senza password, utilizzando i metodi biometrici come l'impronta digitale o il riconoscimento facciale dei nostri smartphone.

La scelta dei vari dispositivi che integrano queste tecnologie ci permette di gestire al meglio la protezione contro accessi non autorizzati, e costituisce anche una garanzia per la compatibilità con le soluzioni future, favorendo ecosistemi più eterogenei e flessibili.

4.5 Analisi di casi di violazione della sicurezza in ambito domestico

L'esame di incidenti reali fornisce informazioni preziose per la prevenzione di future compromissioni.

4.5.1 Il caso delle telecamere IP compromesse

L'incidente del 2020 che ha esposto migliaia di feed video domestici rappresenta un caso emblematico e su vasta scala:

- Persistenza di credenziali di accesso di default
- Nessun aggiornamento del firmware da diversi anni
- Esposizione diretta delle porte di gestione dei servizi critici direttamente su Internet
- Assenza di cifratura per lo stream dei video

L'analisi successiva ha rivelato come la concatenazione di vulnerabilità apparentemente minori possa creare brecce di sicurezza maggiori.

4.5.2 L'incidente Ring e le implicazioni sulla privacy

Il caso Ring del 2019 ha evidenziato come la sicurezza debba estendersi oltre il dispositivo stesso. Gli hacker hanno sfruttato diversi punti di vulnerabiltà:

- Riutilizzo di credenziali compromesse in precedenti data breach per lo stesso account personale
- Mancata adozione di MFA nonostante fosse disponibile
- Scarsa attenzione degli utenti agli indicatori di compromissione

La risposta di Amazon - rendere obbligatoria l'autenticazione a due fattori dopo l'azione legale collettiva - dimostra come la pressione regolatoria e sociale possa accelerare l'adozione di misure di sicurezza basilari ma efficaci.

4.5.3 Lezioni apprese e raccomandazioni

L'analisi degli incidenti esaminati finora mette in evidenza una serie di aspetti ricorrenti che possono essere considerati vere e proprie lezioni. Da questi incidenti emergono alcune raccomandazioni utili per poter rafforzare la sicurezza dei nostri sistemi domotici e quindi della nostra casa: 1. Security by default. La configurazione iniziale di un dispositivo dovrebbe già garantire un livello di protezione adeguato, non deve richiedere all'utente interventi aggiuntivi, anche perchè spesso questi non vengono effettuati. 2. Trasparenza proattiva. È fondamentale che gli utenti siano informati in maniera chiara su quali dati vengono raccolti e in che modo questi dati vengono trattati e protetti. 3. Responsabilità condivisa. La sicurezza non può essere gestita da un solo attore: deve richiede la collaborazione continua tra tutti i diversi produttori, dai provider di servizi e dagli utilizzatori finali. 4. Resilienza operativa. La predisposizione di piani di risposta agli incidenti, testati periodicamnete, riduce in maniera significativa l'impatto di eventuali violazioni.

4.6 Conclusioni e prospettive future

Nel contesto della domotica residenziale, la sicurezza deve essere intesa come un processo dinamico e in costante evoluzione. Ogni nuovo progresso tecnologico porta con sé nuove opportunità di miglioramento, ma introduce anche nuove potenziali vulnerabilità che richiedono un aggiornamento continuo delle strategie di difesa. Solo mantenendo un approccio proattivo e adattivo tra i diversi attori sarà possibile garantire un equilibrio sostenibile tra l'innovazione e la protezione.

Le direzioni future più promettenti includono:

- **Intelligenza artificiale per la sicurezza adattiva**: sistemi che apprendono pattern comportamentali per identificare anomalie in tempo reale
- **Tecnologie distributed ledger**: blockchain e simili per garantire integrità e non ripudiabilità dei dati IoT
- **Crittografia post-quantistica**: preparazione proattiva all'era del quantum computing

Vogliamo abitazioni intelligenti che offrano tutti i vantaggi della tecnologia, ma senza sacrificare la sicurezza e la riservatezza dei dati e l'usabilità dei dispositivi. E' un traguardo possibile grazie all'adozione di pratiche consolidate, all'uso di consapevole di soluzioni innovative per la sicurezza e alla formazione continua di chi le utilizza.

Capitolo 5

Analisi delle Prestazioni e Affidabilità dei Protocolli

5.1 Introduzione

Nel contesto della domotica residenziale, la selezione del protocollo di comunicazione rappresenta un passaggio cruciale, capace di incidere in modo determinante sulle prestazioni complessive del sistema, sull'affidabilità delle connessioni tra i dispositivi e, non da ultimo, sull'esperienza d'uso percepita dagli utenti finali. Questo capitolo si propone di esplorare in modo approfondito le caratteristiche tecniche e operative dei principali protocolli IoT impiegati in ambito domestico, offrendo strumenti concreti per orientare la scelta verso la soluzione più adeguata in funzione delle specifiche esigenze progettuali.

L'evoluzione tecnologica degli ultimi anni ha favorito la diffusione di una molteplicità di protocolli, ciascuno sviluppato per rispondere a determinati requisiti funzionali o vincoli strutturali. Nessuno di essi può essere considerato intrinsecamente "migliore" in senso assoluto: la decisione finale deve necessariamente derivare da un'attenta analisi comparativa, che tenga conto di fattori quali la scalabilità, il consumo energetico, la latenza, la sicurezza, la compatibilità con ecosistemi preesistenti e il grado di complessità richiesto per l'integrazione.

5.2 Indicatori chiave di performance

Per capire davvero quanto un protocollo di comunicazione IoT sia efficace all'interno di un'abitazione intelligente, non basta leggerne le specifiche tecniche ma è fondamentale considerare alcuni indicatori chiave di performance, definiti con il nome Key Performance Indicators abbreviato in (KPI), questi indicatori oggettivi ci aiutano a valutare in modo concreto e comparabile il comportamento di ciascuna tecnologia nelle situazioni reali di abitazioni comuni.

5.2.1 Latenza: il tempo di risposta del sistema

Uno degli aspetti che più influisce sull'esperienza d'uso quotidiana è la **latenza**, ovvero il tempo che passa tra l'invio di un comando e la sua esecuzione. In altre parole,

quanto velocemente la casa "risponde" quando chiediamo qualcosa. È un po' come premere l'interruttore della luce: se dopo averlo fatto ci vogliono più di 200-300 millisecondi perché la lampada si accenda, la sensazione immediata è che qualcosa non funzioni a dovere – anche se tecnicamente tutto è sotto controllo. Questo breve ritardo può sembrare irrilevante, ma oltre una certa soglia diventa fastidioso e può minare la fiducia nel sistema.

Ogni protocollo si comporta in maniera diversa, ad esempio **Zigbee** è generalmente molto reattivo quando si tratta di comunicazioni dirette, con una latenze comprese tra i 15 e i 30 millisecondi. Tuttavia, all'aumentare della complessità della rete, come nel caso di una struttura mesh con più passaggi intermedi (multi-hop), il tempo di risposta può allungarsi fino a 50-100 millisecondi.

Il **Wi-Fi**, se ottimizzato per applicazioni in tempo reale, può offrire prestazioni ancora migliori, arrivando a latenze inferiori ai 10 millisecondi. Ma c'è un prezzo da pagare: questi risultati richiedono un consumo energetico decisamente più elevato, rendendo il Wi-Fi meno adatto per dispositivi alimentati a batteria, come sensori o piccoli attuatori che devono funzionare per anni senza manutenzione.

In definitiva, la scelta del protocollo deve sempre tenere conto di un equilibrio tra velocità, efficienza energetica e caratteristiche dell'ambiente domestico in cui verrà implementato. La reattività è importante, ma lo è altrettanto la capacità del sistema di durare nel tempo senza interventi continui.

5.2.2 Consumo energetico: la sfida dell'autonomia

Quando parliamo di smart home, una delle sfide più rilevanti riguarda la gestione dei consumi energetici dei diversi dispositivi. Non è affatto un aspetto marginale: molti dispositivi smart installati nelle nostre abitazioni, come i sensori di movimento, i sensori di temperatura o i sensori di apertura di porte e di finestre, devono poter funzionare per lunghi periodi senza la necessità di interventi di manutenzione. In generale, questi dispositivi sono alimentati da batterie di piccole dimensioni che dovrebbero durare diversi anni. Appunto in questo scenario, l'efficienza energetica deve rappresentare un requisito imprescindibile per garantire sia la sostenibilità d'uso sia l'affidabilità complessiva dell'ecosistema domotico.

I protocolli di comunicazione IoT si distinguono nettamente per quanto riguarda l'impatto energetico, in funzione del loro design, delle modalità di trasmissione e della gestione dei cicli di attività e standby. Di seguito, una panoramica comparativa delle principali soluzioni:

- **Z-Wave**: Progettato fin dalle origini per applicazioni a basso consumo, Z-Wave offre consumi estremamente contenuti in modalità standby (inferiori a 1 µA) e una richiesta energetica in trasmissione intorno ai 30–40 mA, limitata a brevi istanti. Queste caratteristiche lo rendono ideale per dispositivi alimentati a batteria.

- **Zigbee**: Anch'esso particolarmente efficiente, Zigbee utilizza modalità "sleep" avanzate con assorbimenti inferiori ai 3 µA. Il tempo di riattivazione è molto contenuto (meno di 15 ms), garantendo un buon compromesso tra reattività e risparmio energetico.

- **Thread**: Questo protocollo eredita l'approccio efficiente di Zigbee, ma introduce ulteriori ottimizzazioni per supportare il routing basato su IPv6, consentendo una gestione energetica ancora più flessibile e scalabile, pur mantenendo consumi contenuti.
- **Wi-Fi**: Tradizionalmente meno adatto ai dispositivi a basso consumo, anche nelle sue versioni più recenti – come Wi-Fi 6 – continua a presentare assorbimenti elevati, con consumi in standby nell'ordine dei millesimi di ampere (mA), decisamente superiori rispetto agli standard sopra citati.

Per rendere il confronto più concreto, si consideri un sensore di temperatura basato su Z-Wave, configurato per trasmettere dati ogni 5 minuti: in condizioni ottimali, può operare per un periodo compreso tra i 5 e i 7 anni con una singola batteria tipo CR2032. Al contrario, un dispositivo Wi-Fi equivalente richiederebbe una ricarica mensile o un'alimentazione continua, fattore che limita fortemente la sua applicabilità in scenari stand-alone.

5.2.3 Larghezza di banda: quanto possono davvero "parlare" i dispositivi

Un altro parametro importante da considerare, soprattutto in certi scenari, è la **larghezza di banda**, ovvero la quantità di dati che possono essere trasmessi attraverso la rete in un dato intervallo di tempo. Anche se molti dispositivi domotici scambiano solo piccoli pacchetti di dati (ad esempio, un comando on/off o la lettura di un sensore), esistono casi d'uso che richiedono una capacità di trasferimento ben più ampia.

Alcuni esempi includono:

- Lo *streaming video* in tempo reale da telecamere di sicurezza
- Gli *aggiornamenti firmware over-the-air*, fondamentali per la manutenzione remota
- Il trasferimento di *log diagnostici* da dispositivi complessi
- Il controllo e la sincronizzazione di *impianti audio multi-room*

In questi contesti, la banda disponibile fa la differenza. I protocolli IoT presentano valori molto diversi in termini di velocità massima e throughput reale, come evidenziato nella tabella seguente:

Protocollo	**Velocità massima**	**Throughput reale stimato**
Z-Wave	100 kbps	40–60 kbps
Zigbee	250 kbps	100–150 kbps
Thread	250 kbps	100–150 kbps
Wi-Fi 4	600 Mbps	100–200 Mbps
Wi-Fi 6	9.6 Gbps	1–2 Gbps

Tabella 5.1: Confronto tra velocità teoriche e throughput pratico dei principali protocolli IoT

Come si osserva, **Wi-Fi** domina nettamente per capacità di banda. Tuttavia, nella maggior parte degli impianti domotici, questa potenza risulta sovradimensionata: un

semplice comando per accendere una luce o inviare una lettura della temperatura richiede pochi byte, rendendo il Wi-Fi inefficiente in termini energetici per compiti così semplici[1].

In altre parole, voler utilizzare il Wi-Fi per trasmettere pochi dati è come voler utilizzare un camion per consegnare una cartolina, si funziona, ma è chiaramente uno spreco.

5.2.4 Affidabilità e resilienza: quando la rete deve sapersela cavare da sola

Perché un sistema domotico possa davvero definirsi affidabile, non basta che funzioni "quando tutto va bene": deve essere in grado di reagire e adattarsi anche quando qualcosa non va come previsto. È in queste situazioni che entrano in gioco due concetti fondamentali: **affidabilità** e **resilienza**.

In termini pratici, un protocollo di comunicazione non si limita solo a trasmettere dati, ma deve anche essere in grado di adattarsi a condizioni che non sono sempre ideali quando si calano nelle nostre case. Alcune delle loro caratteristiche diventano quindi fondamentali. Per esempio, la capacità di gestire le interferenze è fondamentale in un ambiente domestico, dove Wi-Fi, Bluetooth e altri segnali convivono uno stesso spazio, un protocollo deve essere in grado si mantenere stabile la comunicazione senza avere interruzioni percepibili.

Un altro aspetto è la ritrasmissione automatica dei pacchetti andati persi, in questo modo l'utente non si accorgersi di eventuali errori o malfunzionamenti. Allo stesso modo, la rete deve poter ricalcolare i percorsi dei messaggi in maniera dinamica: se un nodo smette di funzionare o viene rimosso, il traffico deve trovare da sé una strada alternativa. Infine, per alcune applicazioni è necessario introdurre meccanismi di prioritizzazione del traffico (*Quality of Service*), che permettano di dare precedenza ai messaggi più critici rispetto a quelli meno urgenti.

Le reti *mesh* basate su **Zigbee** e **Thread** rispondono esattamente a queste esigenze. Grazie ad algoritmi di instradamento intelligente, sono in grado di auto-organizzarsi e di reindirizzare i messaggi anche quando un dispositivo viene scollegato, sostituito o risulta temporaneamente non disponibile[2]. Questa caratteristica rende tali soluzioni particolarmente robuste e affidabili nel tempo.

Anche **Z-Wave**, pur avendo una struttura mesh meno estesa, offre un vantaggio rilevante: opera su frequenze **sub-GHz**, in particolare intorno agli 868 MHz in Europa, una banda meno affollata rispetto alla classica 2.4 GHz utilizzata da molti altri protocolli. Ciò si traduce in una maggiore immunità alle interferenze, che spesso rappresentano un problema negli ambienti domestici saturi di dispositivi wireless[3].

---

[1] Wi-Fi Alliance. *Wi-Fi CERTIFIED 6 Technology Overview*. Accessed: 2025-08-05. 2022. URL: `https://www.Wi-Fi.org/discover-Wi-Fi/Wi-Fi-certified-6`.

[2] Connectivity Standards Alliance. *Zigbee Specification*. Accessed: 2025-08-05. 2024. URL: `https://csa-iot.org/all-solutions/zigbee/zigbee-direct/`; Thread Group. *Thread Technical Overview*. Accessed: 2025-08-05. 2023. URL: `https://www.threadgroup.org/What-is-Thread/Overview`.

[3] Z-Wave Alliance. *Z-Wave Specification*. Accessed: 2025-08-05. 2023. URL: `https://z-wavealliance.org/technology-overview/`.

Per quanto riguarda il **Wi-Fi**, nonostante la sua ampia diffusione e le elevate prestazioni in termini di velocità, si dimostra talvolta meno resiliente in ambienti particolarmente congestionati. La stabilità complessiva della rete Wi-Fi dipende fortemente dalla qualità dell'infrastruttura (router, access point, gestione dei canali), e in caso di sovraccarico o malfunzionamenti può mostrare latenze elevate o perdita di pacchetti[4].

Come illustrato nella Figura 5.1, le reti mesh consentono a ogni nodo di fungere da ponte per altri dispositivi, garantendo comunicazione anche in caso di guasti o disconnessioni.

[4] Alliance, *Wi-Fi CERTIFIED 6 Technology Overview*.

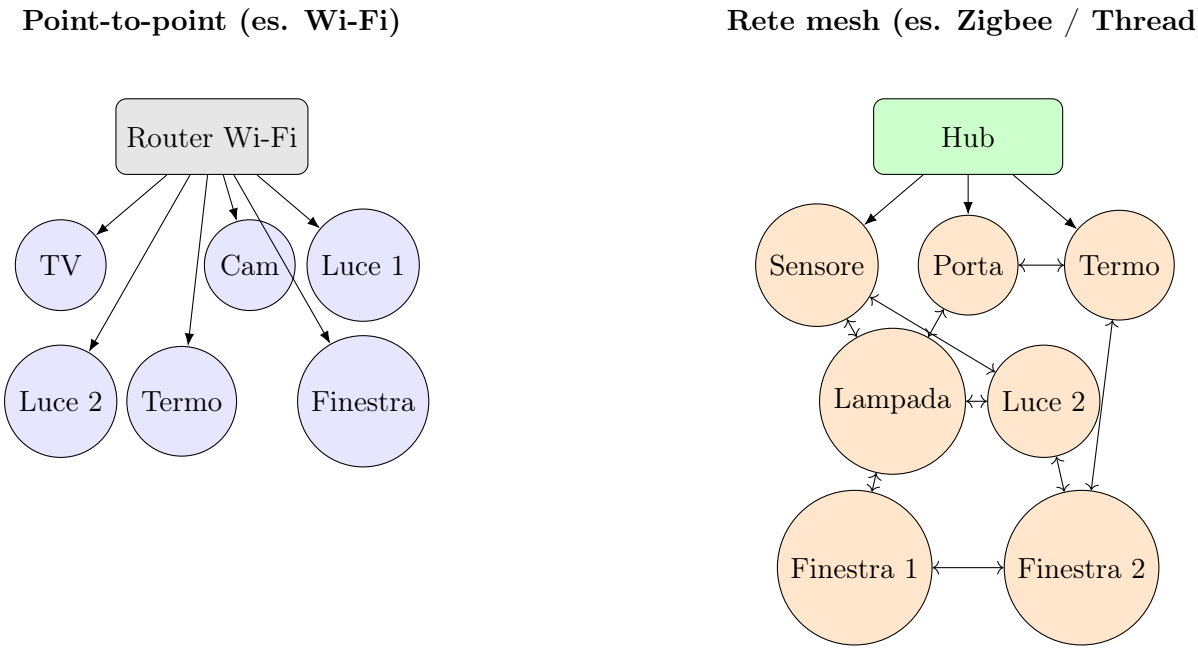

Figura 5.1: Confronto tra rete point-to-point (Wi-Fi) e rete mesh (Zigbee/Thread).

In definitiva, quando si progettano sistemi domotici destinati a durare nel tempo e ad adattarsi a contesti mutevoli, scegliere protocolli con meccanismi di recupero e adattamento diventa una garanzia di stabilità e continuità.

5.3 Confronto prestazionale tra Zigbee, Z-Wave, Wi-Fi, Thread e Matter

5.3.1 Zigbee: il veterano delle reti mesh

Zigbee è considerato uno dei protocolli più maturi e diffusi nell'ambito della domotica residenziale. La sua larga diffusione sul mercato con un'ampio supporto da parte dei produttori ne hanno di fatto diventare una scelta quasi "classica" per chi sviluppa soluzioni di automazione residenziale. Dal punto di vista tecnico, si basa sullo standard IEEE 802.15.4 e utilizza principalmente la banda a 2.4 GHz, la stessa su cui operano anche Wi-Fi e Bluetooth.

Punti di forza:

- Ecosistema maturo con ampia disponibilità di dispositivi
- Supporto per reti mesh auto-riparanti fino a 65.000 nodi teorici

- Profili applicativi standardizzati (es. Zigbee Home Automation, Zigbee Light Link)
- Consumi energetici estremamente ridotti

Limitazioni:

- Rischio di interferenze nella banda 2.4 GHz
- Complessità nella gestione di reti molto estese
- Frammentazione tra profili e versioni differenti
- Velocità non adatta a trasferimenti di dati intensivi

Philips Hue, ad esempio, utilizza Zigbee per controllare fino a 50 lampadine con un singolo bridge, offrendo sincronizzazione precisa e latenza impercettibile.

5.3.2 Z-Wave: l'alternativa su frequenze dedicate

Z-Wave si distingue per l'utilizzo di frequenze sub-GHz (868 MHz in Europa, 908 MHz negli USA), che garantiscono una maggiore penetrazione attraverso muri e ridotte interferenze rispetto alla banda 2.4 GHz.

Caratteristiche distintive:

- Interoperabilità certificata tra dispositivi Z-Wave
- Portata estesa fino a 100 metri in campo aperto
- Topologia mesh con routing source-routed ottimizzato
- Limite di 232 nodi per rete, sufficiente per l'ambito residenziale

La sua velocità massima, pari a 100 kbps, lo rende inadatto a carichi di dati elevati, ma perfetto per sistemi di controllo. Un impianto di sicurezza domestica può includere sensori di movimento, contatti magnetici per porte/finestre e sirene ad alta affidabilità.

5.3.3 Wi-Fi: potenza e versatilità

Wi-Fi si distingue dagli altri protocolli soprattutto per la capacità di offrire larghezze di banda elevate e per la sua diffusione ormai capillare. La presenza in ogni casa di router domestici fa sì che non siano necessarie infrastrutture dedicate, un aspetto che ne ha favorito la crescita e l'adozione. Questa sue caratteristica rendeno il Wi-Fi particolarmente adatto ai dispositivi che devono gestire grandi quantità di dati o alle applicazioni che richiedono un throughput elevato, come le videocamere di sorveglianza o sistemi di streaming multimediale.

Vantaggi competitivi:

- Larghezza di banda elevatissima, adatta a video e trasferimenti intensivi
- Infrastruttura già presente nella maggior parte delle abitazioni
- Supporto IP nativo, ideale per integrazione cloud

- Ottimizzazioni recenti in Wi-Fi 6 per dispositivi IoT (es. Target Wake Time)

Sfide operative:

- Consumo energetico elevato, inadatto a dispositivi a batteria
- Degrado prestazionale con molti dispositivi connessi a un singolo access point
- Latenza variabile in presenza di congestione di rete
- Hardware più costoso rispetto ad alternative low-power

Le videocamere IP rappresentano un'applicazione ideale: richiedono banda elevata e sono alimentate da rete elettrica, eliminando il vincolo energetico[5].

5.3.4 Thread: l'evoluzione IP-native

Thread è un protocollo mesh moderno progettato per supportare IPv6 nativamente, con un'architettura leggera e sicura adatta all'era dell'interoperabilità e del cloud.

Innovazioni chiave:

- Supporto IPv6 nativo con instradamento end-to-end
- Sicurezza avanzata con crittografia AES e gestione automatica delle chiavi
- Commissioning semplice via smartphone
- Mesh self-healing con tempi di riconvergenza rapidi

Le sue latenze sono paragonabili a Zigbee (20–50 ms), ma con un'architettura più moderna e scalabile. Dispositivi come Apple HomePod mini o Google Nest Hub fungono da border router per reti Thread, facilitando l'adozione senza componenti aggiuntivi[6].

5.3.5 Matter: l'unificatore dell'ecosistema

Matter vuole essere un livello applicativo universale, progettato per lavorare sopra i protocolli già presenti come Thread, Wi-Fi ed Ethernet. Il suo scopo non è quindi sostituire ciò che esiste, ma andare a fornire uno strato comune superiore in grado di unire mondi spesso frammentati.

Punti di forza:

- Compatibilità trasversale tra Apple, Google, Amazon, Samsung
- Sicurezza integrata nel design, con certificazione obbligatoria
- Commissioning tramite QR code o NFC
- Comunicazione locale senza necessità di cloud

[5]Wi-Fi Alliance. *Wi-Fi and the Internet of Things*. Accessed: 2025-08-05. 2021. URL: `https://www.Wi-Fi.org/internet-things-iot`.

[6]Group, *Thread Technical Overview*.

Matter introduce un overhead minimo (circa 5–10% di latenza aggiuntiva), ma il vantaggio in termini di compatibilità compensa ampiamente. Un termostato compatibile può essere gestito indistintamente da Siri, Google Assistant o Alexa, mantenendo la stessa qualità d'interazione[7].

Parametro	**Zigbee**	**Z-Wave**	**Wi-Fi**	**Thread**	**Matter**
Banda	2.4 GHz	Sub-GHz	2.4/5 GHz	2.4 GHz	-
Topologia	Mesh	Mesh	Point-to-point	Mesh	-
Velocità max	250 kbps	100 kbps	>100 Mbps	250 kbps	-
Energia	Molto bassa	Bassa	Alta	Bassa	Variabile
Interoperabilità	Limitata	Alta (cert.)	Variabile	Alta	Massima

Tabella 5.2: Confronto sintetico tra protocolli e standard IoT in ambito domotico

5.4 Scalabilità dei protocolli in ambienti domestici complessi

Man mano che le abitazioni intelligenti si arricchiscono di sensori, attuatori e dispositivi di controllo, il tema della **scalabilità** diventa centrale. Un sistema domotico moderno non si limita più ad accendere qualche luce o a regolare il termostato: può arrivare a gestire centinaia di elementi distribuiti in ambienti ampi e strutturati. In questo contesto, è fondamentale comprendere come i principali protocolli IoT reagiscano all'aumento della complessità della rete.

5.4.1 Scalabilità per protocollo

5.4.1.1 Zigbee: tra teoria e realtà

Zigbee dichiara, almeno a livello teorico, la possibilità di poter gestire fino a 65.000 dispositivi all'interno della stessa rete. Una cifra davvero impressionante, che evidenzia le potenzialità di espansione di questo protocollo. Nella pratica quotidiana, però, questo valore resta lontano dall'esperienza reale: nelle nostre case difficilmente si supera qualche decina di dispositivi attivi, e già oltre tale soglia emergergono alcuni limiti legati a prestazioni, stabilità o complessità di gestione.wifi6-spec

Già superata la soglia dei 200-300 dispositivi, cominciano a emergere difficoltà pratiche:

- Latenze maggiori dovute al routing tra nodi multipli
- Congestione nella banda a 2.4 GHz, soprattutto in ambienti densi
- Rallentamenti durante aggiornamenti firmware distribuiti
- Complessità crescente nella configurazione e manutenzione

[7] Connectivity Standards Alliance. *Matter Overview White Paper*. Accessed: 2025-08-05. 2023. URL: `https://csa-iot.org/wp-content/uploads/2022/03/Matter_Security_and_Privacy_WP_March-2022.pdf`.

Una strategia spesso adottata è la creazione di **sotto-reti logiche** distinte, ciascuna gestita da un coordinator dedicato, per esempio separando l'illuminazione dalla climatizzazione o dai sistemi di sicurezza.

5.4.1.2 Z-Wave: solido entro i propri limiti

Z-Wave ha un limite teorico molto più contenuto: 232 dispositivi per rete. Tuttavia, per la maggior parte delle abitazioni — anche quelle di grandi dimensioni — si tratta di un numero più che sufficiente. La gestione più semplice e il minor rischio di congestione radio, grazie all'uso della banda sub-GHz, lo rendono una scelta solida e prevedibile.

Un'abitazione con circa 100 dispositivi (tra interruttori, sensori e attuatori) rientra tranquillamente nei limiti del protocollo, offrendo ancora margine per ulteriori espansioni.

5.4.1.3 Thread e Matter: progettati per crescere

Thread è stato pensato fin dall'inizio per reti scalabili, affidabili e facilmente gestibili:

- I router mesh distribuiti bilanciano il traffico in modo dinamico
- L'uso nativo di IPv6 semplifica il routing e la gestione
- La rete si auto-configura e auto-ripara in caso di guasti

Test su installazioni reali mostrano che anche con oltre 200 dispositivi, i tempi di risposta restano sotto i 100 ms nel 95° percentile, con una degradazione molto graduale delle prestazioni all'aumentare del carico.

Matter, appoggiandosi a Thread (e in parte al Wi-Fi), eredita e potenzia questa capacità, offrendo al tempo stesso interoperabilità tra ecosistemi e gestione centralizzata semplificata.

5.4.2 Strategie di progettazione per reti complesse

5.4.2.1 Progettare la rete per livelli

Quando i dispositivi aumentano, progettare in modo gerarchico diventa essenziale. Una buona architettura divide la rete in tre livelli logici:

1. **Livello Edge**: i dispositivi periferici (sensori, attuatori) che eseguono compiti specifici
2. **Livello di Aggregazione**: hub locali o controller di zona che raccolgono e instradano i dati
3. **Livello Core**: un controller principale (o cloud gateway) che integra, elabora e coordina tutto il sistema

Questa suddivisione migliora la stabilità, semplifica la manutenzione e consente di isolare eventuali malfunzionamenti, evitando che si propaghino all'intero sistema.

5.4.2.2 Separare per funzione: la rete è più leggibile

Un'altra strategia efficace è la suddivisione dei dispositivi in reti logiche in base alla loro funzione:

- **Rete Sicurezza**: dispositivi critici come sensori di movimento, allarmi e serrature (dove l'affidabilità è prioritaria)
- **Rete Comfort**: luci, termostati e tapparelle (ottimizzati per reattività e basso consumo)
- **Rete Media**: smart TV, speaker, videocamere (dove la banda e la connessione stabile sono fondamentali)

In questo modo si ottimizzano i protocolli per ciascun gruppo: Z-Wave può essere usato per la sicurezza, Zigbee o Thread per l'illuminazione, e il Wi-Fi per streaming e intrattenimento.

5.4.3 Conclusioni sulla scalabilità

In sostanza quando ci troviamo a realizzazione di sistemi domotici complessi, la prima vera sfida è quella della scalabilità che non si esaurisce nei soli numeri dichiarati dai produttori. Al contrario, deve essere fondamentale che la rete sia in grado di mantenere buoni tempi di risposta, sia semplice nella gestione ed affidabilità, sopratutto quando il numero di dispositivi collegati aumenta sensibilmente.

Ogni protocollo che abbiamo visto finoea presenta caratteristiche diverse in questo scenario.
Zigbee può scalare bene, ma richiede una buona esperienza nella progettazione di rete per evitare colli di bottiglia.
Z-Wave, per la sua semplicità di configurazione e la sua stabilità, ottenuta sfruttando le banda sub-GHz con meno traffico, si adatta perfettamente a contesti residenziali di dimensioni medio-piccole.
Thread e Matter, diversamente dai precedenti, offrono un approccio più moderno e flessibile, risultando particolarmente indicati per installazioni più grandi, complesse e in continua evoluzione, spinto anche dall'innovazione che le proncipali aziende stanno dando a questo protocollo.

In conclusione, per definire il successo di una rete domotica complessa e grande, non bisogna guardare solo dal protocollo che abbiamo scelto, ma soprattutto da come viene disegnata: una buona progettazione, cola presenza di segmentazioni funzionali, la definizione di una organizzazione gerarchica, consentono di ottenere risultati affidabili e duraturi, qualunque sia la tecnologia utilizzata.

Capitolo 6

Prospettive Future nella Domotica Residenziale

6.1 Introduzione

Dopo aver esaminato nel Capitolo 5 le prestazioni, l'affidabilità e la scalabilità dei principali protocolli di comunicazione impiegati nelle abitazioni intelligenti, ora andiamo ad esplorare le tecologie emergenti per le smart home.

Negli ultimi anni, la casa ha smesso di essere solo il nostro spazio abitato, ma si sta trasformando progressivamente in un ecosistema interattivo. Questo cambiamento segue una trasformazione culturale e tecnologica più ampia, che rispecchia ilnostro modo di vivere, oramai siamo abituati a lavoriamo e interagiamo con l'ambiente che ci circonda. La domotica quindinon è più appannaggio di pochi appassionati o early adopter ma è diventata una componente concreta dell'abitare contemporaneo.

Questa evoluzione tuttavia non è lineare né priva di ostacoli. L'interoperabilità tra dispositivi, la protezione dei dati personali, l'efficienza energetica e l'inclusività sono sfide reali. Ma sono anche i punti su cui costruire una nuova idea di casa.

Dopo anni in cui i vari produttori fornivano soluzioni frammentate e proprietarie, oggi una nuova visione orientata sta guidando gli sviluppi concentrandosi su interoperabilità, sostenibilità e intelligenza diffusa. Questa transizione non riguarda soltanto l'arrivo di nuovi dispositivi e nuove tecnologie, ma è un cambiamento più profondo, la casa interagisce con i suoi abitanti impara da loro e si adatta in modo intelligente.

Le abitazioni del futuro quindi saranno case realmente smart, saranno capaci di prevedere i nostri bisogni, sapranno reagire in tempo reale ad eventi, proteggeranno dati sensibili e garantiranno l'accessibilità a tutti. In questo nuovo capitolo andremo ad analizzare le nuove tendenze emergenti, valutandone potenzialità e sfide.

6.2 Lo standard Matter e i protocolli IP-native

6.2.1 Matter: interoperabilità come fondamento

Matter non è soltanto un nuovo standard, ma è il simbolo di una storica alleanza tra le principali case produttrici dell'industria tecnologica quali Apple, Google, Amazon,

Samsung, per superare i limiti della frammentazione e della interoperatività. Nasce come evoluzione del progetto CHIP (Connected Home over IP), con l'obiettivo di rendere compatibili tra loro dispositivi di diversi produttori.

Il punto di forza di Matter è basato su un modello applicativo standardizzato, che rende possibile un dialogo strutturato e uniforme tra tutti i componenti della rete domestica. La configurazione di nuovi dispositivi avviene in modo semplice e tramite dei wizard attivabili tramite QR code o NFC, supporta inolte il controllo multi-ecosistema, questo rende possibile l'utilizzo dello stesso dispositivo con più assistenti vocali o app differenti, senza conflitti, ad esmpio in casa posso controllare una luce sia da Siri che da Alexa. Inoltre, Matter supporta e privilegia il controllo locale, riuscendo così a garantire continuità anche in assenza di connessione Internet.

Basato sul protocollo di rete IPv6 e rafforzato dall'utilizzo dello standard di crittografia TLS 1.3, **Matter** riesce a coniugare due aspetti spesso difficili da bilanciare: la scalabilità e la sicurezza. In altre parole, il protocollo non solo è pensato per poter crescere e supportare un numero sempre maggiore di dispositivi, ma garantisce anche che lo scambio di informazioni tra i dispositivi avvenga in modo sicuro e protetto, riducendo così al minimo i rischi legati a possibili vulnerabilità o accessi non autorizzati.

6.2.2 Thread: architettura distribuita e resiliente

Il protocollo Thread, spesso utilizzato in abbinamento con Matter, è un protocollo basato su rete mesh IP-native, progettato specificatamente per l'utilizzo in ambiente IoT. Tra le sue caratteristiche principali, ogni nodo ha un indirizzo IP univoco, la rete si auto-configura e si auto-ripara, senza necessità di un coordinatore centrale. In caso di guasto del'Hub centrale leader, un nuovo leader viene eletto automaticamente, garantendo affidabilità e continuità.

Thread, come già analizzato per la sua architettura mesh e sicurezza nativa, si afferma ad oggi come la componente centrale per le reti domestiche, in grado di garantire resilienza ed estendibilità, soprattutto in abbinamento allo standard Matter

L'integrazione di Thread in dispositivi come Apple HomePod, Alexa e Google Home ne facilitano l'adozione domestica, senza bisogno di doversi munire di Hub dedicati.

6.3 Tecnologie emergenti per la casa intelligente

6.3.1 Intelligenza artificiale nella vita domestica

L'adozione dell'intelligenza artificiale sta trasformando l'esperienza abitativa da una serie di automatismi e scenari che apprendono, anticipano e si adattano al nostro stile di vita.

Esempio evolutivo: oggi noi quando rientriamo in casa, diciamo "Alexa, accendi la luce"; un domani non tanto lontano, la casa riconoscerà il nostro rientro, rileverà la scarsa luminosità e accenderà automaticamente la luce più adatta, predisponendo l'ambiente secondo le nostre abitudini.

L'adozione del *machine learning on-device* permette l'elaborazione dei dati direttamente sul dispositivo, riducendo la dipendenza dal cloud e la trasmissione di dati. Questo porta benefici concreti come una minore latenza, una maggiore privacy ed una personalizzazione maggiore.

6.3.1.1 Apprendimento federato

Attraverso il *federated learning*, i dispositivi intelligenti elaboreranno i dati localmente e comunicheranno solo gli aggiornamenti del modello, così garantiranno che nessuna informazione sensibile verrà mai trasferita o memorizzata nel cloud.

6.3.2 Reti mesh e Wi-Fi di nuova generazione

Dopo aver evidenziato i benefici di una rete mesh nel capitolo precedente, le reti mesh oggi evolvono con l'integrazione dei nuovi standard Wi-Fi e Thread, abilitando così scenari più reattivi e modulari.

Le versioni più recenti dello standard **Wi-Fi** hanno segnato tappe decisive nell'evoluzione delle reti domestiche e aziendali. Con **Wi-Fi 6**, ad esempio, sono state introdotte tecnologie come OFDMA, TWT e BSS Coloring, pensate per aumentare l'efficienza delle trasmissioni e ridurre la latenza, soprattutto in ambienti molto congestionati. La successiva estensione, **Wi-Fi 6E**, ha aperto l'accesso alla banda a 6 GHz, liberando nuovi canali e offrendo maggiori possibilità di connessione ai dispositivi dedicati alla smart home. Infine, la nuova **Wi-Fi 7**, ancora in fase di diffusione, promette prestazioni senza precedenti, con velocità teoriche fino a 46 Gbps e latenze ultra-basse[1].

Per chiarezza espositiva, una tabella comparativa può riassumere i principali miglioramenti introdotti da ciascuna versione.

Versione	Anno	Banda	Caratteristiche principali
Wi-Fi 5	2014	2.4 / 5 GHz	Alta velocità, no ottimizzazioni IoT
Wi-Fi 6	2019	2.4 / 5 GHz	OFDMA, TWT, efficienza migliorata
Wi-Fi 6E	2020	6 GHz	Nuovi canali, meno interferenze
Wi-Fi 7	2024	2.4 / 5 / 6 GHz	MLO, latenza bassa, throughput massimo

Tabella 6.1: Evoluzione dello standard Wi-Fi per ambienti smart home

6.3.3 Edge e fog computing domestico

L'elaborazione locale dei dati, resa possibile dal paradigma del **fog computing**, introduce diversi vantaggi rispetto a un approccio interamente basato sul cloud. Innanzitutto, consente di ottenere risposte in tempo reale, riducendo la latenza e garantendo un controllo immediato sui dispositivi domestici. Un altro aspetto rilevante è la resilienza: anche in assenza di connessione a Internet, i sistemi possono continuare a funzionare in autonomia, senza dipendere da server esterni.

Inoltre, mantenere i dati vicino alla fonte aumenta il livello di protezione delle informazioni sensibili, limitando l'esposizione verso l'esterno. Non va poi trascurato il beneficio economico: elaborare localmente riduce il traffico generato verso il cloud e, di conseguenza, i costi associati.

In questa direzione si collocano progetti come **K3s**, una distribuzione leggera e semplificata di Kubernetes progettata per scenari IoT. Grazie a soluzioni di questo tipo, diventa possibile orchestrare microservizi direttamente sugli hub domestici, trasformando ogni

[1] Alliance, *Wi-Fi CERTIFIED 6 Technology Overview*.

stanza della casa in un nodo intelligente e autonomo, capace di cooperare con gli altri per offrire un ambiente realmente distribuito.

6.4 Privacy, sicurezza e fiducia digitale

6.4.1 Le nuove sfide dell'abitazione intelligente

L'impiego dell'intelligenza artificiale nelle abitazioni connesse promette di trasformare radicalmente il modo in cui viviamo la nostra casa, offrendo livelli di automazione ed efficienza impensabili fino a pochi anni fa. Tuttavia, a fronte di questi nuovi benefici emergono anche delle nuove sfide. Per poter funzionare in maniera efficace, i nuovi sistemi intelligenti hanno bisogno di raccogliere e analizzare una gran quantità di dati personali: dagli orari in cui noi siamo presenti o assenti in casa, fino alle nostre preferenze in termini di comfort e consumo energetico.

Tutte queste informazioni, se da un lato consentono di ottimizzare i servizi e anticipare i nostri bisogni, dall'altro lato delineano un quadro delicato in termini di sicurezza e riservatezza. La dipendenza dai dati rende indispensabile un approccio responsabile alla loro gestione, che includa misure tecniche avanzate, ma anche pratiche di trasparenza e consapevolezza da parte dei fornitori.

In Europa, il *General Data Protection Regulation* (GDPR) stabilisce i principi fondamentali per la protezione dei dati personali[2]. Linee guida specifiche per l'IoT e la smart home sono state elaborate anche dall'*European Union Agency for Cybersecurity* (ENISA), che sottolinea l'importanza di criteri di sicurezza fin dalla fase di progettazione (*security by design*)[3]. Negli Stati Uniti, il *National Institute of Standards and Technology* (NIST) ha pubblicato raccomandazioni per la gestione dei rischi in sistemi IoT, offrendo un quadro di riferimento utile anche in contesti internazionali[4].

In questo contesto, la protezione dei dati non riguarda soltanto l'integrità delle infrastrutture digitali, ma diventa una condizione essenziale per mantenere la fiducia degli utenti verso le soluzioni di domotica. Senza fiducia, infatti, anche le tecnologie più evolute rischiano di essere percepite come troppo invasive, rallentandone così la diffusione e l'adozione su larga scala.

6.4.2 Strategie di protezione

Per affrontare le sfide legate alla sicurezza dei sistemi domotici, negli ultimi anni si sono affermati diversi approcci tecnologici. Uno dei più rilevanti è la **Zero Trust Architecture**, che si fonda sul principio secondo cui nessuna richiesta deve essere considerata affidabile a priori: ogni accesso, anche proveniente dall'interno della rete domestica, deve essere verificato e validato.

[2]European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*. `https://eur-lex.europa.eu/eli/reg/2016/679/oj`. Accessed: 2025-08-25. 2016.

[3]European Union Agency for Cybersecurity (ENISA). *Guidelines for Securing the Internet of Things*. `https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things`. Accessed: 2025-08-25. 2020.

[4]National Institute of Standards and Technology (NIST). *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. `https://doi.org/10.6028/NIST.IR.8228`. Accessed: 2025-08-25. 2020.

Un'altra strategia utile è la **segmentazione delle reti**, che consiste nel suddividere l'infrastruttura in più porzioni isolate tra loro. In questo modo, qualora un dispositivo venga compromesso, i danni rimangono circoscritti e non si propagano a tutta la rete.

In ambito più sperimentale, la **crittografia omomorfica** rappresenta un'innovazione promettente: essa permette di elaborare i dati mantenendoli cifrati, evitando che debbano essere decifrati in fase di analisi. Infine, l'impiego della **blockchain** può fornire un registro distribuito e immodificabile delle operazioni compiute, utile a garantire la tracciabilità e a rafforzare i meccanismi di audit trail.

6.5 Inclusività come principio guida

6.5.1 Tecnologia accessibile a tutti

Un'altra sfida cruciale per la domotica residenziale del futuro è quella dell'**inclusività**, ovvero la capacità delle soluzioni tecnologiche di adattarsi alle esigenze di utenti molto diversi tra loro, con abilità e conoscenze tecnologiche variegate, senza lasciare indietro nessuno. Rendere la tecnologia accessibile a tutti significa, innanzitutto, progettare delle interfacce realmente intuitive e **adattive**, capaci di supportare gli anziani e le persone con disabilità.

Strumenti di interazione alternativi, come i comandi **vocali**, **gestuali** o persino **aptici**, possono facilitare di molto l'uso quotidiano della casa smart. Allo stesso tempo, è importante non dimenticare le abitazioni già esistenti: le soluzioni deveono essere il più possibile **retrofit**, permettendo di integrare componenti intelligenti senza dover rifare completamente gli impianti, questi punti rappresentano un passaggio fondamentale in questa direzione.

Infine, la promozione dell'**open source** e del **fai-da-te** offrono la possibilità di sperimentare e personalizzare le soluzioni in base alle proprie esigenze, ampliando il grado di partecipazione degli utenti finali e rendendo la domotica un fenomeno inclusivo e condiviso.

6.6 Conclusioni: la casa come alleata

Non si tratta più solo di rendere la casa "smart", ma di saper costruire un ambiente che sia in grado di ascoltare, apprendere e rispondere in modo etico e personalizzato. Il futuro della domotica non si misura dal numero di dispositivi installati in una casa, ma dalla loro capacità di adattarsi all'ambiente domestico in cui sono inseriti, di rispettare e migliorare la vita dei suoi abitanti.

Capitolo 7

Gestione di Dispositivi Multimarca

7.1 Introduzione

Il Capitolo precedente ha evidenziato come le prospettive future della domotica residenziale si stiano progressivamente orientando verso modelli sempre più aperti, interoperabili e intelligenti. Tuttavia, affinché queste buone promesse si possano tradurre in un'esperienza fluida e semplice per l'utente finale, è necessario affrontare una delle sfide più complesse del settore: la gestione di dispositivi di marche e protocolli differenti all'interno dello stessa casa.

Immagina di essere in un negozio di elettronica. Vuoi poter rendere la tua casa più smart e finalmente ti decidi: una bella lampadina connessa, magari Philips. Poi noti un termostato intelligente, quello della Nest ti convince. La serratura smart più sicura? Yale. E già che ci sei, aggiungi anche un paio di telecamere Arlo, che sembrano avere ottime recensioni.

A casa al momento di configurare il tutto iniziano i primi problemi, ogni dispositivo richiede la sua app, bisogna creare il suo account e necessita del suo hub. Le lampadine non parlano con il termostato, la serratura ignora le telecamere, e si inizia a pensare che più che in una casa intelligente, ci stiamo trovando in una casa complicata. In pratica è come se ogni dispositivo parlasse una lingua diversa, e l'utente dovesse improvvisarsi come un traduttore simultaneo passando da un'app all'altra.

Ecco il paradosso della domotica moderna: abbiamo si più scelta ma è più difficile mettere tutto insieme e farlo comunicare in maniera semplice. Questo capitolo entra nel cuore di questa sfida. Perché far dialogare dispositivi di marche diverse non è solo un problema tecnico: significa garantire coerenza nell'esperienza d'uso, mantenere sicurezza e affidabilità, e soprattutto dover riconfigurare quasi tutto quando si aggiunge un nuovo dispositivo.

7.2 La sfida dell'interoperabilità

7.2.1 Le radici del problema

Quando pensiamo all'interoperabilità nella domotica, potremmo immaginarla come un semplice problema tecnico da risolvere. Ma nella realtà è molto più complesso, questa

frammentazione nasce da anni di scelte industriali, non avendo al centro l'utente, ma per rafforzare la posizione di mercato del proprio dispositivo. Ogni azienda ha costruito il proprio ecosistema proprietario, dove tutto funziona bene finché utilizzi i suoi dispositivi, ma diventa complicato appena provi a integrare qualcosa di altri produttori.

7.2.1.1 La Torre di Babele dei protocolli

La situazione attuale assomiglia a una moderna Torre di Babele: ogni produttore parla la propria lingua, rendendo difficile far comunicare dispositivi diversi tra loro, se non utlizzaando complicati workaround.

- **Protocolli proprietari**: Ogni grande azienda ha sviluppato il proprio "dialetto". Alcuni esempi sono le luci Lutron usano ClearConnect, i sensori Insteon hanno un protocollo dual-band proprietario, i dispositivi Somfy utilizzano RTS o io-homecontrol.Questo si traduce in eccellenti dispositivi, ma incapaci di operare tra loro.

- **Varianti su uno stesso tema**: Anche quando si sceglie lo stesso linguaggio di base, come Zigbee, non è detto che ci sia adottato lo stesso schema di definizione dei protocolli. Philips Hue adotta Zigbee Light Link, altri produttori preferiscono Zigbee Home Automation, si basano sullo stesso standard, ma la struttura e le regole fondamentali del protocollo sono differente.

- **Livelli diversi di astrazione**: Alcuni protocolli lavorano a livello fisico (come Z-Wave), altri a livello di esperienza utente e applicazioni (come HomeKit). Tradurre da uno all'altro è come passare da codice macchina a conversazione naturale: servono interpreti intelligenti.

- **Sicurezza che non si parla**: Anche i modelli di sicurezza variano. Diverse tecniche di crittografia e autenticazione rendono difficile, e talvolta rischioso, mettere in comunicazione dispositivi di produttori diversi senza compromettere la protezione dei dati.

7.2.1.2 L'impatto sull'utente finale

La frammentazione dell'ecosistema domotico diventa nella pratica per l'utente finale un'esperienza spesso frustrante e tutt'altro che "smart":

Troppe app, poca chiarezza: Secondo una ricerca del 2023, l'utente medio di una casa intelligente deve utilizza tra le 8 e le 12 diverse app, per poter controllare i propri dispositivi installati. Ogni produttore inoltre ha una sua interfaccia differente, con logiche diverse e tipologie di notifiche differenti. Il risultato? Lo smartphone diventa un campo di battaglia digitale in cui non si riesce ad avere una visione d'insieme del sistema.

Automazioni che faticano a cooperare: un esempio apparentemente banale, come la regola "quando esco di casa, spegni tutte le luci e abbassa il termostato", può in realtà trasformarsi in una sfida complessa. Ogni elemento della catena – dalle lampadine intelligenti ai sensori di presenza, fino al sistema di riscaldamento – utilizza protocolli diversi e non sempre compatibili tra di loro. Il risultato è che alcune automazioni funzionano correttamente, mentre altre non vengono eseguite come previsto, costringendo l'utente ad intervenire manualmente.

Lentezza imprevista: Ogni volta che un comando deve attraversare più livelli, ad esempio da prima un hub Zigbee, poi ad un bridge proprietario, poi accedere al cloud del produttore, da lì nuovamente accedere ad un altro servizio in cloud ed infine finalmente al dispositivo, così facendo si accumulano ritardi, facendo pensare all'utente che qualche cosa non abbia funzionato. Quello che dovrebbe essere un'azione immediata può impiegare diversi secondi. Non è solo fastidioso, ma anche poco affidabile.

Costi invisibili, ma reali: Oltre al prezzo dei dispositivi, spesso bisogna acquistare hub aggiuntivi, bridge, gateway, e magari anche sottoscrivere abbonamenti per funzionalità cloud avanzate. Una casa "veramente smart" può arrivare a richiedere 3, 4 o 5 hub diversi per funzionare come si desidera.

7.2.2 L'evoluzione verso standard comuni

Per anni, la domotica ha viaggiato su binari paralleli, con ogni produttore convinto di poter costruire il proprio ecosistema proprietario, chiuso e autosufficiente. Tuttavia, col passare del tempo è diventato evidente che questa frammentazione non è utile a nessuno: complica la vita agli utenti, rallenta l'adozione di massa e genera una percezione di tecnologia "instabile" o poco matura. Quando persino i tecnici iniziano a faticare per far dialogare tra loro i dispositivi, è chiaro che serve un cambio di paradigma.

Una parte sempre più ampia del settore infine ha riconosciuto che l'interoperabilità non è solo un vantaggio competitivo, ma è una necessità primaria. Così è iniziata un'evoluzione importante, guidata da due movimenti complementari: uno le comunità open source e l'altro le grandi aziende produttrici di smartphne sulla creazione di standard comuni.

7.2.2.1 Il movimento open source

La community open source ha saputo andare oltre la semplice sperimentazione, creando soluzioni concrete, flessibili e, in molti casi, sorprendentemente sofisticate. In questo ecosistema collaborano sviluppatori indipendenti, maker, professionisti IT e appassionati, accomunati dall'obiettivo di superare le barriere imposte dai singoli produttori e restituire all'utente il pieno controllo della propria casa intelligente.

Il risultato ha creato diverse piattaforme capaci di integrare decine, se non centinaia, di dispositivi eterogenei, mettendoli in comunicazione tra di loro, come se parlassero la stessa lingua. Alcune di queste soluzioni hanno assunto un ruolo centrale nell'interoperabilità domestica:

- **Home Assistant** — Nato nel 2013 come progetto personale di Paulus Schoutsen, si è evoluto fino a diventare il riferimento assoluto per l'integrazione multimarca. Con oltre 2000 integrazioni ufficiali e di terze parti, consente di gestire in un'unica interfaccia luci, termostati, sensori, elettrodomestici e sistemi di sicurezza Home Assistant. *Documentation and Integrations*. Accesso il 10 aprile 2025. 2024. URL: `https://www.home-assistant.io/`. Grazie alle automazioni avanzate e alla compatibilità con protocolli e API proprietarie, riesce a colmare le lacune lasciate anche dai sistemi commerciali più chiusi.

- **OpenHAB** — Storico progetto open source concepito con un'architettura modulare altamente personalizzabile. Supporta logiche complesse scritte in linguaggi come JavaScript, Groovy o Python, risultando particolarmente adatto a installazioni su

larga scala o scenari con esigenze non standard *openHAB - empowering the smart home*. Accessed: 2025-08-07. 2023. URL: `https://www.openhab.org`.

- **Node-RED** — Una piattaforma di programmazione visuale basata su flussi, che consente di collegare dispositivi, API e servizi online attraverso un'interfaccia drag-and-drop. È spesso integrata con Home Assistant per creare automazioni elaborate e monitorare i dati in tempo reale *Node-RED - Flow-based programming for the Internet of Things*. Accessed: 2025-08-07. 2024. URL: `https://nodered.org`.

- **IFTTT** (*If This Then That*) — Servizio web che semplifica l'automazione tra piattaforme e servizi diversi. Pur non essendo open source, è ampiamente adottato anche in contesti di smart home per creare scenari trasversali: ad esempio, accendere una luce Zigbee quando una videocamera Wi-Fi rileva movimento o inviare una notifica Telegram quando il termostato registra un calo improvviso di temperatura.

7.2.2.2 L'alleanza dell'industria: Matter

La collaborazione tra attori globali come Apple, Google, Amazon e Samsung costituisce un passaggio di rilievo strategico nello sviluppo della domotica. Per decenni, tali aziende hanno privilegiato i propri ecosistemi proprietari, limitando l'interoperabilità e alimentando una competizione mirata a consolidare il proprio controllo sul mercato della casa samrt. Tuttavia negli ultimi anni è maturata la consapevolezza che l'innovazione non puo basarsi sull'esclusione reciproca, bensì deve basarsi sulla definizione di standard condivisi e dalla cooperazione tra settori.

Da questo contesto è stato definito **Matter**, uno standard aperto concepito per essere il linguaggio comune per i dispositivi domestici intelligenti. Non è un semplice protocollo, Matter è un cambio di paradigma: i dispositivi possono comunicare direttamente, senza l'uso di hub proprietari, convertitori o complessi meccanismi di integrazione, tutto questo si traduce nella libertà per l'utente che non è vincolato alla scelta di un unico ecosistema.

L'evoluzione che ha portato a Matter è stata graduale:

- **2019**: Nasce *Project CHIP* (Connected Home over IP), inizialmente come iniziativa tecnica congiunta per risolvere i problemi di compatibilità più evidenti.

- **2021**: Il progetto cambia nome in *Matter* e vengono pubblicate le prime specifiche ufficiali.

- **2022**: I primi dispositivi certificati fanno la loro comparsa sul mercato, seguiti da aggiornamenti firmware che permettono anche a dispositivi esistenti di essere compatibili.

- **2023-2024**: Rapida diffusione grazie all'integrazione nei principali ecosistemi (Apple HomeKit, Google Home, Amazon Alexa, Samsung SmartThings) e al crescente supporto di produttori di semiconduttori come Nordic Semiconductor, Silicon Labs e Espressif

La portata innovativa di Matter risiede nella possibilità di utilizzare un medesimo dispositivo su più piattaforme in parallelo. Un sensore di movimento, ad esempio, può essere configurato sia in Apple HomeKit sia in Google Home, rispondendo a comandi da entrambi i sistemi e mantenendo la sincronizzazione degli stati e regole di automazione su

entrambe le piattaforme. Questo approccio permette che sia il sistema ad adattarsi alle esigenze dell'utente e non viceversa.

Dal punto di vista strategico, Matter rappresenta una risposta alla crescente complessità della casa connessa. L'adozione di uno standard aperto riduce il rischio di obsolescenza precoce, semplifica l'integrazione di dispositivi eterogenei e favorisce economie di scala nello sviluppo hardware e software. Inoltre, l'approccio IP-based facilita l'integrazione con servizi cloud e con tecnologie emergenti, come l'Edge Computing e l'Intelligenza Artificiale distribuita, aprendo nuove prospettive per l'automazione predittiva e contestuale.

In sintesi, Matter segna il passaggio da un modello di mercato basato su lock-in tecnologico a uno fondato su interoperabilità e apertura, ponendo le basi per un ecosistema domestico più scalabile, sicuro e sostenibile, e contribuendo a spostare il baricentro dell'innovazione dalla singola piattaforma al sistema complessivo della casa connessa.

Capitolo 8

Caso di Studio: Sistema Domotico Integrato con Apple HomeKit

8.1 Obiettivi e contesto

Questo caso di studio documenta l'implementazione di un sistema domotico per una residenza unifamiliare su due piani, integrato nativamente con Apple HomeKit.

I requisiti riguardano: (i) controllo accessi sicuro; (ii) gestione dell'illuminazione e delle tapparelle; (iii) videosorveglianza perimetrale con notifiche mirate; (iv) monitoraggio ambientale e automazioni meteo; (v) audio multi stanza; (vi) facilità d'uso tramite app Casa e comandi vocali; (vii) riduzione dei consumi energetici senza impattare il comfort.

8.2 Analisi dell'abitazione

Piano terra (100 m^2): ingresso, soggiorno open-space (40 m^2), cucina abitabile (25 m^2), bagno ospiti, studio/ufficio (15 m^2), garage doppio.
Piano primo (100 m^2): camera matrimoniale con bagno, due camere singole, bagno principale, terrazzo (20 m^2).
Esterno: giardino perimetrale, vialetto d'accesso, due accessi carrabili, area barbecue.

Vincoli progettuali: distribuzione su due piani (copertura Wi-Fi e latenza), esposizioni est/ovest (controllo solare), necessità di integrazione non invasiva su impianto esistente e preferenza per controllo nativo da ecosistema Apple. Facilità di gestione e condivisione con i membri della famiglia.

8.3 Architettura del sistema

L'architettura è organizzata su tre livelli: (a) *dispositivi e sensori*; (b) *hub/controller e gateway*; (c) *automazioni e interfacce.*

8.3.1 Rete e infrastruttura

- **LAN IoT dedicata**: VLAN 192.168.20.0/24, SSID dedicato (WPA3), segmentazione del traffico verso la LAN principale.

- **Hub HomeKit**: HomePod in soggiorno come hub primario; HomePod mini in cucina, studio e camera matrimoniale come hub di failover e per audio locale.
- **Gateway BTicino**: modulo DIN collegato alla rete Wi-Fi per la configurazione dei dispositivi su home control e condivisione con HomeKit.

8.3.2 Protocolli e integrazione

- **Bus SCS (BTicino)**: utilizzato per la comunicazione tra moduli Living Now cablati (interruttori, dimmer e comandi tapparelle) e il gateway, quando l'impianto lo prevede. Garantisce bassa latenza e funzionalità anche in assenza di rete IP.
- **Wi-Fi**: impiegato dai dispositivi Living Now connessi *pre-Matter* (installati in questa abitazione), dal Nuki Smart Lock 3.0 Pro, dalle telecamere Netatmo e dalla stazione meteo Netatmo. È il principale canale di comunicazione verso HomeKit in questa configurazione.
- **Thread**: viene utilizzato esclusivamente da dispositivi compatibili con lo standard Matter o nativamente basati su Thread, come ad esempio le *Nanoleaf Lines*. La gestione della rete è affidata ai *Border Router*, già integrati in dispositivi di largo consumo come l'*HomePod mini* e l'*HomePod* di seconda generazione. Questa architettura consente di ottenere comunicazioni a bassa latenza e con un consumo energetico ridotto, due caratteristiche fondamentali per garantire un'esperienza fluida e sostenibile all'interno della smart home.
- **Interruttori BTicino wireless**: modelli da parete privi di cablaggio, alimentati a batteria con comunicazione radio diretta con il gateway via Thread.
- **HomeKit su IP** rappresenta il protocollo applicativo di Apple dedicato all'automazione domestica e al controllo dei dispositivi smart. Si basa su un sistema di cifratura end-to-end, che assicura la protezione dei dati durante tutta la comunicazione, e utilizza un meccanismo di pairing semplice e sicuro tramite codice QR. Questo approccio riduce al minimo i rischi di accesso non autorizzato e rende l'esperienza di configurazione più intuitiva per l'utente finale.
- **HomeKit Secure Video (HKSV)**: per le telecamere Netatmo, con analisi video on-device e registrazione cifrata su iCloud.

8.4 Dotazione installata (per categoria)

Accesso e sicurezza

- **Serratura smart**: Nuki Smart Lock 3.0 Pro (integrazione HomeKit via Wi-Fi). Funzioni: blocco/sblocco, stato porta, automazioni in base a presenza e orario. La gestione delle credenziali ospiti avviene nell'app Nuki; HomeKit fornisce controllo e notifiche.
- **Videosorveglianza esterna**: 4 telecamere Netatmo Outdoor con sirena. In HomeKit Secure Video: rilevamento persone/animali/veicoli, zone di attività, timeline cifrata. Posizionamento: ingresso, garage, giardino posteriore, lato secondario.

Illuminazione e schermature

- **Punti luce e dimmer**: serie BTicino Living Now per 32 punti luce (on/off e dimmerazione). Comandi scenari locali per richiamo rapido.
- **Tapparelle**: 18 motorizzazioni con controllo salita/discesa/stop e posizionamento percentuale; scenari alba/tramonto.

Monitoraggio ambientale e meteo

- **Stazione meteo Netatmo**: modulo interno (temperatura, umidità, CO_2, pressione, rumore) e modulo esterno (temperatura/umidità). Dati usati per automazioni (protezione solare, avvisi vento/calore).
- **Sensori integrati HomePod**: temperatura/umidità ambientale disponibili in HomeKit per regole semplici di comfort.

Audio, interazione e notifiche

- **HomePod / HomePod mini**: audio multi-room, comandi vocali, Intercom, hub HomeKit con failover. Integrazione con scene (es. modalità cinema, sveglia graduale).

Illuminazione decorativa

- **Nanoleaf Lines**: installazione a parete in soggiorno (dietro TV). Integrazione con HomeKit per scene; effetti dinamici per notifiche e modalità cinema. Connessione di rete via Wi-Fi; supporto a protocolli low-latency ove disponibile.

8.5 Implementazione

8.5.1 Fase 1 — Infrastruttura elettrica e di rete

1. Installazione del gateway BTicino su barra DIN e predisposizione protezioni dedicate.
2. Alimentazioni per telecamere esterne.
3. Configurazione VLAN/SSID IoT, indirizzamento statico per dispositivi fissi (telecamere, gateway), WPA3.

8.5.2 Fase 2 — Installazione dispositivi

- Sostituzione interruttori tradizionali con moduli Living Now; configurazione dimmer nelle zone principali; comandi tapparelle.
- Montaggio Nuki su porta blindata con calibrazione.
- Installazione telecamere Netatmo e definizione delle zone di attività.
- Posizionamento HomePod/HomePod mini e installazione Nanoleaf Lines.

8.5.3 Fase 3 — Configurazione HomeKit

1. Aggiunta del gateway BTicino tramite codice HomeKit; rilevamento automatico dei dispositivi collegati.
2. Pairing di telecamere e stazione meteo Netatmo; abilitazione HKSV.
3. Configurazione Nuki via QR e verifica controlli da app Casa.
4. Impostazione HomePod come hub primario e verifica dei servizi remoti.
5. Organizzazione in stanze/piani e definizione di zone (interno/esterno).

8.6 Automazioni rappresentative

Le automazioni sono progettate con logica "*evento-condizione-azione*", utilizzando trigger affidabili e preferendo esecuzione locale quando possibile.

Protezione notturna

```
Trigger: tramonto + 30 min; presenza = true
Azioni: chiusura tapparelle piano terra; accensione luci esterne;
        telecamere in alta sensibilità; blocco automatico serratura.
Notifiche: sintesi eventi su iPhone dei genitori.
```

Arrivo familiare (riconoscimento)

```
Trigger: Netatmo ingresso -> persona riconosciuta; fascia oraria: 18:00-23:00
Azioni: luce ingresso 100% a 3000K; avviso su HomePod (Intercom);
        sblocco manuale facilitato (notifica azionabile da Apple Watch/iPhone).
```

Ottimizzazione solare estiva

```
Trigger: temperatura esterna > 26°C; meteo soleggiato
Condizioni: stagione = estate; qualcuno in casa = true
Azioni progressive: lato est 70% (10:00); lato sud 80% (12:00);
                    lato ovest 70% (15:00); apertura al tramonto.
```

Sveglia graduale

```
Trigger: 07:00 (feriali) / 08:30 (weekend)
Azioni: tapparelle camera 30% con apertura lenta; luce 20% a 2700K (5 min);
        HomePod: riproduzione playlist con volume in fade-in.
```

Modalità cinema

```
Trigger: comando vocale "Ehi Siri, modalità cinema" o pulsante scena
Azioni: chiusura tapparelle soggiorno; spegnimento luci;
        Nanoleaf Lines in Screen/Mirror a 30%;
        HomePod in modalità Home Theater; notifiche familiari silenziate (2 ore).
```

8.7 Gestione utenti, permessi e privacy

- **Ruoli HomeKit**: genitori come amministratori (gestione dispositivi, automazioni, registrazioni video); figli come membri con accesso a luci/tapparelle e audio nelle loro stanze; esclusi controlli su serratura e telecamere.
- **HKSV e dati**: Tra le funzionalità avanzate di HomeKit rientra l'analisi del movimento eseguita direttamente *on-device*, che consente di elaborare i dati in locale senza doverli inviare a server esterni su cloud. I flussi video sono inoltre protetti grazie a una cifratura end-to-end e possono essere archiviati in modo sicuro su iCloud. L'utente ha anche la possibilità di definire **zone sensibili** all'interno dell'inquadratura, riducendo così il numero di notifiche superflue e concentrando l'attenzione solo sugli eventi realmente rilevanti.
- **Accessi ospiti**: gestione credenziali temporanee tramite app Nuki; revoca immediata; log accessi consultabile.

8.8 Conclusioni: vantaggi dell'integrazione multimarca

L'adozione di un'architettura HomeKit in un contesto multimarca, come quello descritto in questo caso di studio, ha permesso di ottenere un impianto coerente, sicuro e facile da gestire.

Principali vantaggi osservati Dall'analisi delle soluzioni integrate in ambiente HomeKit emergono diversi vantaggi rilevanti. Innanzitutto, la possibilità di una **gestione centralizzata** semplifica notevolmente l'esperienza d'uso: dispositivi eterogenei come quelli di BTicino, Netatmo, Nuki o Nanoleaf possono essere controllati da un'unica interfaccia, l'app Casa, evitando la frammentazione in applicazioni separate per ogni produttore.

Un ulteriore beneficio riguarda la **condivisione semplificata**. Grazie alla funzione di Condivisione in famiglia di Apple, l'accesso ai dispositivi può essere esteso automaticamente a tutti i membri della famiglia, senza necessità di configurazioni aggiuntive.

Particolarmente significativo è l'aspetto legato a **privacy e sicurezza**: HomeKit adotta nativamente meccanismi di cifratura end-to-end e automazioni locali. Nel caso dei flussi video, la funzione HomeKit Secure Video assicura che l'analisi venga eseguita direttamente on-device, con archiviazione protetta su iCloud.

La piattaforma contribuisce inoltre alla **riduzione della complessità**, eliminando la necessità di gateway o bridge multipli, e centralizzando sia gli aggiornamenti sia le notifiche di sistema. A ciò si affianca una comprovata **affidabilità operativa**: luci, tapparelle e scenari principali continuano a funzionare anche in assenza di connessione Internet, garantendo continuità all'utente.

L'**esperienza uniforme** rappresenta un ulteriore valore aggiunto, grazie a un'interfaccia coerente e comandi vocali disponibili su tutti i dispositivi Apple (iPhone, iPad, Mac e Apple Watch). Allo stesso tempo, l'ecosistema è orientato alla **scalabilità futura**: la presenza di border router integrati, come quelli degli HomePod, rende la rete pronta ad accogliere dispositivi Matter e Thread.

Non mancano vantaggi in termini di **efficienza energetica**, con automazioni dedicate all'illuminazione e alle schermature solari che permettono di ridurre i consumi migliorando al tempo stesso il comfort abitativo. Infine, l'adozione di pratiche di **sicurezza di rete**,

come la segmentazione VLAN per i dispositivi IoT e l'isolamento del traffico rispetto alla rete principale, contribuisce a rafforzare ulteriormente l'affidabilità dell'intero sistema.
In sintesi, la soluzione implementata dimostra come un ecosistema aperto e interoperabile, basato su standard consolidati come HomeKit, possa integrare tecnologie di produttori diversi garantendo facilità d'uso, sicurezza e possibilità di evoluzione nel tempo.

Appendice A

Glossario dei termini e degli acronimi

Frammentazione Situazione in cui dispositivi, piattaforme e protocolli di comunicazione non sono pienamente interoperabili a causa dell'adozione di standard, profili o implementazioni proprietarie differenti.

IoT Insieme di dispositivi e sensori collegati a Internet, capaci di comunicare autonomamente e rendere intelligenti ambienti e oggetti quotidiani.

BLE Bluetooth Low Energy — Standard wireless a basso consumo energetico.

Zigbee Protocollo wireless basato su IEEE 802.15.4, ottimizzato per reti mesh a corto raggio.

Z-Wave Protocollo wireless a bassa potenza, usato per applicazioni di domotica.

Wi-Fi Wireless Fidelity — Tecnologia di rete locale senza fili basata su IEEE 802.11.

Thread Protocollo di rete IPv6-based pensato per dispositivi IoT.

Matter Standard aperto per l'interoperabilità tra dispositivi smart, sviluppato dalla CSA.

HomeKit Piattaforma sviluppata da Apple per controllare e gestire in maniera semplice e sicura i dispositivi domestici intelligenti tramite dispositivi iOS.

Gateway Dispositivo che consente la comunicazione tra reti o protocolli differenti.

API Application Programming Interface — Interfaccia che permette l'interazione tra software.

Hub Dispositivo che agisce da centro di controllo, permettendo a diversi dispositivi smart di comunicare tra loro e con l'utente.

KNX Standard aperto per l'automazione degli edifici, utilizzato principalmente in sistemi cablati per applicazioni domotiche.

Rete mesh Tipologia di rete in cui ciascun dispositivo è collegato direttamente a più altri, aumentando l'affidabilità e l'efficienza nella comunicazione.

IPv6 Versione più recente del protocollo Internet, che consente un numero quasi illimitato di indirizzi IP.

Hub centrale Dispositivo centrale che coordina e gestisce le comunicazioni tra dispositivi intelligenti in una rete domotica.

RS-485 Standard di comunicazione seriale cablato, resistente alle interferenze e utilizzato principalmente in ambienti industriali e domotici per connessioni su lunghe distanze.

VLAN Rete virtuale che separa logicamente gruppi di dispositivi all'interno della stessa rete fisica, migliorando sicurezza e gestione.

IDS Sistema che monitora il traffico di rete per identificare e segnalare eventuali intrusioni o attività sospette non autorizzate.

Firmware Software fondamentale, installato permanentemente sui dispositivi hardware per controllare direttamente le loro operazioni di base.

DTLS Datagram Transport Layer Security — Protocollo di sicurezza che fornisce comunicazioni cifrate per dispositivi con risorse limitate, basato su UDP.

VLAN Rete virtuale che separa logicamente gruppi di dispositivi all'interno della stessa rete fisica, migliorando sicurezza e gestione.

IDS Sistema che monitora il traffico di rete per identificare e segnalare eventuali intrusioni o attività sospette non autorizzate.

Firmware Software fondamentale, installato permanentemente sui dispositivi hardware per controllare direttamente le loro operazioni di base.

DTLS Datagram Transport Layer Security — Protocollo di sicurezza che fornisce comunicazioni cifrate per dispositivi con risorse limitate, basato su UDP.

Tag Dispositivo utilizzato per attivare automazioni domotiche. Può essere passivo (NFC/RFID, senza batteria, funziona al tocco) o attivo (BLE/beacon, con batteria, rileva la presenza a distanza).

MFA Multi-Factor Authentication – Metodo di autenticazione che richiede all'utente di fornire due o più prove ("fattori") per verificare la propria identità prima di concedere l'accesso a un sistema o servizio

Bibliografia

Alliance, Connectivity Standards. *Matter Overview White Paper*. Accessed: 2025-08-05. 2023. URL: https://csa-iot.org/wp-content/uploads/2022/03/Matter_Security_and_Privacy_WP_March-2022.pdf.

— *Zigbee Specification*. Accessed: 2025-08-05. 2024. URL: https://csa-iot.org/all-solutions/zigbee/zigbee-direct/.

Alliance, Wi-Fi. *Wi-Fi and the Internet of Things*. Accessed: 2025-08-05. 2021. URL: https://www.Wi-Fi.org/internet-things-iot.

— *Wi-Fi CERTIFIED 6 Technology Overview*. Accessed: 2025-08-05. 2022. URL: https://www.Wi-Fi.org/discover-Wi-Fi/Wi-Fi-certified-6.

Alliance, Z-Wave. *Z-Wave Specification*. Accessed: 2025-08-05. 2023. URL: https://z-wavealliance.org/technology-overview/.

Antonakakis, M., T. April e M. et al. Bailey. *Understanding the Mirai Botnet*. 2017. URL: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.

Bluetooth SIG. *Bluetooth Low Energy*. https://www.bluetooth.com/learn-about-bluetooth/tech-overview/low-energy/. Accessed: 2025-08-25. 2025.

Connectivity Standards Alliance. *Matter: The Foundation for Connected Things*. https://csa-iot.org/all-solutions/matter/. Accessed: 2025-08-25. 2025.

— *Zigbee Technology Overview*. https://csa-iot.org/all-solutions/zigbee/. Accessed: 2025-08-25. 2025.

European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*. https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed: 2025-08-25. 2016.

European Union Agency for Cybersecurity (ENISA). *Guidelines for Securing the Internet of Things*. https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things. Accessed: 2025-08-25. 2020.

Wi-Fi Alliance. *Discover Wi-Fi*. https://www.wi-fi.org/discover-wi-fi. Accessed: 2025-08-25. 2025.

Group, Thread. *Thread Technical Overview*. Accessed: 2025-08-05. 2023. URL: https://www.threadgroup.org/What-is-Thread/Overview.

Home Assistant. *Documentation and Integrations*. Accesso il 10 aprile 2025. 2024. URL: https://www.home-assistant.io/.

National Institute of Standards and Technology (NIST). *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. https://doi.org/10.6028/NIST.IR.8228. Accessed: 2025-08-25. 2020.

Node-RED - Flow-based programming for the Internet of Things. Accessed: 2025-08-07. 2024. URL: https://nodered.org.

openHAB - empowering the smart home. Accessed: 2025-08-07. 2023. URL: https://www.openhab.org.

Thread Group. *About Thread*. https://www.threadgroup.org/. Accessed: 2025-08-25. 2025.

Wikipedia contributors Domotica. *Domotica*. Accesso il 10 aprile 2025. 2024. URL: https://it.wikipedia.org/wiki/Domotica.

Wikipedia contributors KNX. *KNX (standard)*. https://it.wikipedia.org/wiki/KNX_(standard). Accessed: 2025-08-25. 2025.

Wikipedia contributors RS-485. *RS-485*. https://it.wikipedia.org/wiki/RS-485. Accessed: 2025-08-25. 2025.

Z-Wave Alliance. *Z-Wave Technology Overview*. https://z-wavealliance.org/z-wave/. Accessed: 2025-08-25. 2025.