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. Basti pensare alla comodità di poter preriscaldare l'abitazione durante il tragitto di ritorno dal lavoro, ottimizzando così tanto il comfort abitativo quanto l'efficienza energetica.

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 democratizzato l'accesso alla casa intelligente. Molti di noi ricordano l'impatto dei primi termostati Nest o delle lampadine Philips Hue, prodotti che hanno reso tangibili i benefici della domotica per le famiglie comuni.

L'integrazione dell'intelligenza artificiale ha rappresentato un ulteriore salto evolutivo. Oggi non ci limitiamo più al semplice controllo via app: le nostre abitazioni imparano dai nostri comportamenti, adattandosi proattivamente alle nostre routine. Gli assistenti vocali come Amazon Alexa o Google Assistant non solo eseguono comandi, ma anticipano le nostre esigenze, suggerendo automatizzazioni personalizzate basate su variabili come orari, condizioni meteorologiche e abitudini consolidate.

L'edge computing costituisce un'innovazione particolarmente rilevante, consentendo l'elaborazione dei dati direttamente a livello locale, eliminando la dipendenza dal cloud. Questo approccio migliora sensibilmente i tempi di risposta: una telecamera di sicurezza con capacità di edge computing può identificare immediatamente un intruso e inviare alert in tempo reale, senza dover attendere l'elaborazione su server remoti.

Le reti di nuova generazione, dal 5G fino al futuro 6G, promettono di sbloccare scenari applicativi finora impensabili. Potremmo presto gestire i nostri dispositivi domestici attraverso interfacce di realtà aumentata o monitorare parametri di salute tramite sensori che comunicano direttamente con i nostri medici. Questi sviluppi, pur offrendo enormi opportunità per comfort ed efficienza, sollevano inevitabilmente nuove questioni relative alla cybersecurity e alla privacy.

Tuttavia, uno degli ostacoli più significativi rimane l'interoperabilità tra dispositivi di produttori diversi. Chiunque abbia tentato di integrare nuovi dispositivi smart nella propria abitazione ha probabilmente sperimentato la frustrazione di dover gestire multiple app e protocolli incompatibili. Fortunatamente, l'emergere di standard aperti come il protocollo Matter sta progressivamente abbattendo queste barriere, facilitando l'integrazione di ecosistemi eterogenei.

La presente tesi si focalizza sull'evoluzione dei protocolli di comunicazione IoT nella domotica residenziale, con particolare enfasi su sicurezza, prestazioni e interoperabilità. Per concretizzare l'analisi teorica, presenterò un caso studio basato su Apple HomeKit, selezionato per la sua usabilità e le robuste caratteristiche di sicurezza.

1.1 Approccio metodologico della ricerca

La mia ricerca adotta un approccio multidisciplinare che combina analisi teorica approfondita con valutazione empirica di dati provenienti da studi esistenti e sperimentazioni pratiche. Ho strutturato il lavoro seguendo una metodologia che integra diverse prospettive:

- **Revisione sistematica della letteratura**: ho condotto un'analisi critica delle pubblicazioni scientifiche e tecniche più rilevanti, privilegiando fonti recenti e autorevoli per garantire l'attualità dei contenuti;
- **Analisi comparativa dei protocolli**: ho sviluppato un confronto sistematico basato su metriche concrete e risultati di test sperimentali, attingendo sia da benchmark consolidati che da valutazioni indipendenti;
- **Studio di casi reali**: ho esaminato soluzioni commerciali esistenti, concentrandomi particolarmente sul sistema Apple HomeKit come esempio paradigmatico di integrazione sicura e user-friendly;
- **Prototipazione pratica**: ho realizzato un sistema domotico multimarca per validare empiricamente le considerazioni teoriche e identificare problematiche concrete nell'implementazione quotidiana.

Questo approccio metodologico integrato mi ha permesso di sviluppare una panoramica completa e aggiornata della domotica residenziale, bilanciando rigore accademico e applicabilità pratica. L'obiettivo è fornire non solo un quadro teorico solido, ma anche spunti concreti per chiunque desideri avvicinarsi consapevolmente al mondo della casa intelligente.

1.2 Obiettivi della ricerca

Il presente lavoro persegue obiettivi articolati su più livelli, che riflettono la complessità intrinseca del panorama domotico contemporaneo:

- **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 e sostenibili 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.

Questi obiettivi riflettono la mia convinzione che la ricerca accademica debba coniugare profondità teorica e utilità pratica, contribuendo tanto all'avanzamento della conoscenza quanto al miglioramento dell'esperienza utente nel mondo reale.

Capitolo 2

La Domotica Residenziale

2.1 Definizione e principi fondamentali

La domotica residenziale indica l'integrazione delle tecnologie elettroniche e informatiche per automatizzare, controllare e ottimizzare gli impianti e i dispositivi presenti nelle abitazioni. Questo campo applicativo sfrutta in maniera determinante l'Internet of Things (IoT), consentendo agli utenti un controllo sia locale che remoto degli ambienti domestici (Wikipedia contributors 2024). I principi fondamentali della domotica comprendono automazione, integrazione, personalizzazione e interoperabilità, aspetti che sono cruciali per il funzionamento efficace di un sistema intelligente.

2.2 Vantaggi della domotica: efficienza energetica, sicurezza e comfort abitativo

L'impiego della domotica in contesti residenziali porta numerosi vantaggi, tra cui spiccano l'efficienza energetica, l'aumento della sicurezza e il miglioramento del comfort abitativo. Sistemi intelligenti avanzati permettono, ad esempio, di ottimizzare automaticamente l'illuminazione e la climatizzazione sulla base di parametri ambientali e comportamenti abituali degli utenti, riducendo così significativamente i consumi energetici (International Electrotechnical Commission 2020). Sul fronte della sicurezza, sensori intelligenti e telecamere integrate consentono una sorveglianza continua, intervenendo autonomamente in caso di emergenze o situazioni anomale (Standards e Technology 2022). Il comfort è garantito da interfacce intuitive, quali app per dispositivi mobili e assistenti vocali, che rendono semplice e immediata la gestione personalizzata degli ambienti domestici.

2.3 Componenti principali di un sistema domotico

Un sistema domotico completo ed efficace è composto da diversi elementi essenziali che interagiscono costantemente tra loro (International Electrotechnical Commission 2020):

- **Sensori intelligenti**: dispositivi in grado di rilevare parametri ambientali (temperatura, umidità, luminosità, movimento), fornendo dati essenziali per le automazioni;

- **Attuatori**: dispositivi che trasformano i comandi ricevuti in azioni concrete, come l'accensione o lo spegnimento di luci, regolazione di tapparelle o riscaldamento;
- **Unità centrale di controllo (hub o gateway)**: componente centrale del sistema che gestisce le regole di automazione, interpreta i dati dei sensori e coordina gli attuatori;
- **Interfacce utente**: comprendono applicazioni mobili, assistenti vocali o pannelli di controllo fisici, permettendo agli utenti di interagire facilmente con il sistema;
- **Rete di comunicazione**: infrastruttura di rete che collega i dispositivi domotici, solitamente basata su protocolli cablati (es. KNX) o wireless (es. Wi-Fi, Zigbee, Thread o Matter).

2.4 Sfide aperte nella domotica residenziale

Nonostante gli evidenti vantaggi, permangono diverse sfide cruciali per una diffusione più ampia e sostenibile della domotica, tra cui l'interoperabilità tra sistemi multimarca, la sicurezza informatica e l'affidabilità delle soluzioni implementate. Questi temi saranno approfonditi nei capitoli successivi, analizzando nello specifico l'importanza della sicurezza IoT e le prestazioni dei vari protocolli di comunicazione utilizzati nel contesto domestico.

Capitolo 3

Evoluzione dei Protocolli di Comunicazione IoT

3.1 Introduzione ai protocolli IoT

I protocolli di comunicazione IoT sono il vero e proprio "linguaggio" che permette ai dispositivi intelligenti di casa nostra di parlarsi e collaborare. Pensate a quando accendete la luce dal vostro smartphone o regolate il termostato senza alzarvi dal divano: tutto questo è possibile grazie a protocolli che gestiscono la comunicazione tra dispositivi diversi, spesso di marche e tecnologie differenti. Nel tempo, questi protocolli si sono evoluti per rispondere a nuove esigenze, come consumi energetici più bassi, maggiore sicurezza e facilità d'uso. Possiamo dividerli 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 pionieri della domotica e ancora oggi sono molto usati, soprattutto in contesti dove la stabilità della comunicazione è fondamentale.

KNX è uno standard internazionale molto affidabile e flessibile. Immaginate un grande edificio, come un hotel o un ufficio, dove luci, riscaldamento, tende e sistemi di sicurezza devono funzionare in modo coordinato e senza intoppi. KNX permette di collegare tutti questi dispositivi con un unico sistema cablato, garantendo che tutto funzioni senza problemi. Il vantaggio principale per l'utente è la grande affidabilità e la possibilità di personalizzare il sistema in base alle esigenze specifiche. Tuttavia, l'installazione richiede un intervento tecnico specializzato e può risultare costosa, il che lo rende meno adatto per case più piccole o soluzioni fai-da-te.

RS-485, invece, è spesso usato in contesti industriali o in impianti domestici più semplici. Per esempio, in un'abitazione con un sistema di allarme o controllo accessi, RS-485 può garantire una comunicazione stabile anche su lunghe distanze e in ambienti con molte interferenze elettriche. Dal punto di vista dell'utente, questo si traduce in un sistema robusto che raramente perde il segnale. Tuttavia, come KNX, richiede cablaggi e competenze tecniche per l'installazione.

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

Con l'avvento delle tecnologie wireless, la domotica è diventata più accessibile e flessibile, permettendo installazioni più semplici e meno invasive.

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. Questo significa che anche in case grandi o con muri spessi, la comunicazione resta stabile. Gli utenti apprezzano il basso consumo energetico, che permette ai sensori di durare anni con una singola batteria. Lo svantaggio può essere la necessità di un hub centrale e qualche difficoltà iniziale nella configurazione.

Z-Wave è simile a Zigbee ma spesso preferito in ambito residenziale per la sua semplicità. Molti utenti lo trovano intuitivo per collegare dispositivi come serrature smart o controller per tapparelle. La sicurezza integrata è un punto forte, 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 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. L'utente comune apprezza la facilità d'uso, ma spesso si scontra con l'alto consumo energetico, che limita l'uso di Wi-Fi in dispositivi alimentati a batteria, e con problemi di congestione della rete domestica.

Bluetooth Low Energy (BLE) è ideale per dispositivi a corto raggio e a bassissimo consumo, come smartwatch, fitness tracker o sensori di prossimità. Per esempio, potete usare BLE per sbloccare la porta di casa automaticamente quando vi avvicinate con il telefono. Il vantaggio è il risparmio energetico e la semplicità, ma la portata limitata lo rende inadatto per coprire tutta la casa senza dispositivi aggiuntivi.

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

Gli utenti di domotica spesso si trovano frustrati perché dispositivi di marche diverse non "parlano" tra loro facilmente. Thread e Matter sono protocolli pensati per risolvere questo problema.

Thread è una rete mesh basata su IPv6 che permette ai dispositivi di comunicare direttamente tra loro senza passare per un hub centrale. Immaginate di avere luci, sensori e termostati che si connettono in modo autonomo e stabile, anche se un dispositivo si spegne o perde la connessione: la rete si auto-ripara. Gli utenti notano una maggiore affidabilità e una configurazione più semplice rispetto a Zigbee o Z-Wave. Come svantaggio, è ancora relativamente nuovo e non tutti i dispositivi lo supportano.

Matter è il progetto più ambizioso, nato per creare un linguaggio comune per tutti i dispositivi smart, indipendentemente dal produttore. Se avete mai avuto difficoltà a far dialogare un dispositivo Amazon Alexa con uno Google Home, Matter promette di risolvere questo problema. Grazie a Matter, sarà possibile integrare facilmente nuovi dispositivi nel proprio ecosistema domestico senza preoccuparsi della compatibilità. Per

gli utenti, questo significa meno stress e più libertà di scelta. Al momento, però, l'adozione è in crescita e non tutti i prodotti sul mercato lo supportano ancora.

3.5 Criteri di selezione dei protocolli

Quando scegliete un protocollo per la vostra casa intelligente, dovete considerare diversi aspetti pratici:

- **Consumo energetico**: Se avete dispositivi alimentati a batteria, come sensori o serrature, è fondamentale scegliere protocolli a basso consumo per evitare continui cambi di 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 applicazioni che richiedono risposte immediate, come videocamere o sistemi di allarme, è meglio optare per protocolli veloci come Wi-Fi.
- **Facilità d'uso e integrazione**: Se non siete esperti, è importante scegliere protocolli supportati da dispositivi facili da configurare e che funzionano bene insieme.
- **Sicurezza e privacy**: Proteggere la propria rete domestica è fondamentale, quindi è bene preferire protocolli che offrono 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.

—

Nuovi termini introdotti da aggiornare nel glossario:

- **Rete mesh**: Una rete in cui ogni dispositivo si connette direttamente ad altri dispositivi vicini, migliorando copertura e affidabilità.
- **IPv6**: La versione più recente del protocollo Internet, che consente un numero praticamente illimitato di indirizzi IP.
- **Hub centrale**: Un dispositivo che funge da punto di controllo e coordinamento per altri dispositivi in una rete domotica.

Capitolo 4

Sicurezza e Privacy nella Domotica Residenziale

4.1 Introduzione alla sicurezza IoT domestica

La sicurezza in ambito IoT residenziale è cruciale poiché i dispositivi intelligenti raccolgono e condividono continuamente dati sensibili degli utenti, come informazioni personali, abitudini domestiche e dati biometrici. La crescente diffusione di dispositivi connessi, quali termostati intelligenti, telecamere di sorveglianza, assistenti vocali e sensori ambientali, aumenta la superficie di attacco potenziale. È quindi fondamentale adottare strategie di sicurezza integrate che includano la protezione dei dati in transito e a riposo, la gestione degli accessi e la resilienza contro attacchi informatici (Roman, Zhou e Lopez 2013; Sicari et al. 2015).

4.2 Minacce e vulnerabilità comuni

Le minacce tipiche nel contesto IoT domestico includono intrusioni non autorizzate, attacchi malware specifici per dispositivi embedded, e vulnerabilità nei protocolli di comunicazione wireless come ZigBee, Z-Wave, Wi-Fi e Bluetooth. Ad esempio, attacchi di tipo Man-in-the-Middle (MitM) possono intercettare e manipolare dati sensibili, mentre exploit di buffer overflow possono compromettere i firmware dei dispositivi. Inoltre, la presenza di dispositivi con password di default o aggiornamenti mancanti facilita l'accesso illecito. Un caso noto è stato l'attacco Mirai, che ha sfruttato dispositivi IoT vulnerabili per generare un vasto botnet DDoS (Antonakakis, April e Bailey 2017).

4.3 Best practice per garantire sicurezza e privacy

Per garantire sicurezza e privacy è consigliabile implementare una serie di misure preventive e protettive. Tra queste, l'applicazione regolare di aggiornamenti firmware e patch di sicurezza è fondamentale per correggere vulnerabilità note. La segmentazione della rete domestica, ad esempio tramite VLAN o reti Wi-Fi separate per dispositivi IoT e dispositivi personali, riduce il rischio di compromissione trasversale. L'uso di firewall e sistemi di rilevamento delle intrusioni (IDS) consente di monitorare il traffico e bloccare attività sospette. Inoltre, l'adozione di politiche di gestione degli accessi basate su principi

di minimo privilegio e autenticazione multifattoriale (MFA) rafforza la protezione degli account. Infine, la sensibilizzazione degli utenti su pratiche di sicurezza, come la modifica delle password di default, è un elemento chiave (Sicari et al. 2015; Yang et al. 2017).

4.4 Tecniche di crittografia e autenticazione nei protocolli IoT

La protezione dei dati in ambienti IoT si basa su tecniche di crittografia end-to-end, che garantiscono la riservatezza e l'integrità delle comunicazioni tra dispositivi e server cloud. Il protocollo TLS/SSL è ampiamente utilizzato per cifrare le comunicazioni su IP, mentre protocolli specifici per IoT, come DTLS, sono adottati per ambienti con limitate risorse computazionali. L'autenticazione a due fattori (2FA) e l'uso di certificati digitali migliorano la sicurezza degli accessi, riducendo il rischio di compromissione da password deboli. La gestione sicura delle credenziali, tramite hardware security modules (HSM) o Trusted Platform Modules (TPM), è essenziale per prevenire furti di chiavi crittografiche. Inoltre, l'adozione di standard come OAuth 2.0 e MQTT con autenticazione integrata facilita un controllo granulare degli accessi (Sicari et al. 2015; Yang et al. 2017).

4.5 Analisi di casi di violazione della sicurezza in ambito domestico

Diversi casi concreti evidenziano le conseguenze di violazioni della sicurezza in ambito domestico. Un esempio è l'hacking di telecamere IP domestiche che ha portato alla diffusione di video privati online, sfruttando vulnerabilità nelle credenziali di default e firmware obsoleti (The Washington Post 2019). Un altro caso riguarda la compromissione di assistenti vocali che, una volta controllati da attaccanti, possono intercettare conversazioni o attivare dispositivi senza consenso (TechCrunch 2019). Tali studi contribuiscono a definire linee guida per la progettazione di sistemi più sicuri e resilienti.

Capitolo 5

Analisi delle Prestazioni e Affidabilità dei Protocolli

5.1 Indicatori chiave di performance

Gli indicatori chiave per valutare le prestazioni dei protocolli IoT sono molteplici e fondamentali per determinare l'idoneità di un protocollo in specifici contesti applicativi. Tra i principali si annoverano la latenza, il consumo energetico, la larghezza di banda, l'affidabilità della trasmissione e la capacità di gestione della rete.

La latenza rappresenta il tempo necessario affinché un pacchetto dati venga trasmesso da un nodo sorgente a un nodo destinazione. In applicazioni critiche come il controllo industriale o la domotica in tempo reale, una bassa latenza è essenziale per garantire risposte tempestive. Ad esempio, Zigbee tipicamente offre latenze nell'ordine di qualche decina di millisecondi, mentre Wi-Fi può garantire latenze inferiori ma a costo di consumi energetici più elevati **ZigbeeLatencyStudy**.

Il consumo energetico è un indicatore cruciale, soprattutto per dispositivi alimentati a batteria. Protocollo come Z-Wave e Thread sono progettati per ottimizzare l'efficienza energetica, permettendo una durata della batteria di mesi o anni in condizioni normali di utilizzo **EnergyEfficientProtocols**.

La larghezza di banda determina la quantità di dati che possono essere trasmessi in un dato intervallo di tempo. Wi-Fi, ad esempio, offre larghezze di banda significativamente superiori rispetto a Zigbee o Z-Wave, rendendolo adatto a scenari che richiedono il trasferimento di grandi quantità di dati, come il video streaming **WiFiBandwidth**.

Infine, l'affidabilità della trasmissione e la capacità di gestione della rete, che includono la tolleranza ai guasti e la scalabilità, sono indicatori fondamentali per garantire il corretto funzionamento della rete IoT in ambienti dinamici e complessi.

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

Il confronto tra i protocolli Zigbee, Z-Wave, Wi-Fi, Thread e Matter si basa su diverse metriche chiave. Zigbee e Z-Wave operano su bande di frequenza sub-GHz o 2.4 GHz, offrendo un buon compromesso tra portata e consumo energetico. Zigbee supporta velocità

fino a 250 kbps, mentre Z-Wave arriva a circa 100 kbps, con una portata tipica di 30-100 metri **ZWaveVsZigbee**.

Wi-Fi, invece, opera su bande a 2.4 GHz e 5 GHz con velocità che possono superare i 100 Mbps, ma con un consumo energetico significativamente più elevato, rendendolo meno adatto per dispositivi a bassa potenza **WiFiVsIoT**.

Thread è un protocollo IP-based progettato per reti mesh a bassa potenza, con supporto per IPv6 e sicurezza integrata. Offre una latenza inferiore rispetto a Zigbee e una migliore interoperabilità grazie all'uso di standard aperti **ThreadProtocol**.

Matter, recentemente sviluppato, mira a unificare i protocolli esistenti per garantire interoperabilità tra dispositivi di diversi produttori. Utilizza Thread e Wi-Fi come tecnologie di trasporto e si distingue per un elevato livello di sicurezza e facilità di configurazione **MatterWhitePaper**.

Un esempio pratico di confronto è la gestione di una rete domestica complessa: mentre Zigbee e Z-Wave sono adatti per sensori e attuatori a bassa potenza, Wi-Fi è preferibile per dispositivi ad alta richiesta di banda come videocamere IP, e Thread/Matter offrono un equilibrio tra efficienza energetica e interoperabilità.

5.3 Scalabilità dei protocolli in ambienti domestici complessi

La scalabilità è un aspetto critico nella progettazione di reti IoT, soprattutto in ambienti domestici complessi con numerosi dispositivi interconnessi. Zigbee e Thread supportano reti mesh che permettono di estendere la copertura e migliorare la robustezza della rete attraverso il routing dinamico.

Zigbee può gestire fino a 65.000 dispositivi in una singola rete, ma in pratica la gestione di un numero elevato di nodi può introdurre problemi di congestione e ritardi nella comunicazione **ZigbeeScalability**. Thread, grazie all'architettura IP-based e al supporto per il routing efficiente, offre una migliore scalabilità e gestione del traffico.

Z-Wave, pur supportando un numero inferiore di dispositivi (fino a 232 nodi per rete), è noto per la sua affidabilità in ambienti domestici, grazie a un protocollo di routing semplice e robusto **ZWaveScalability**.

Wi-Fi, pur offrendo alta capacità di banda, può incontrare difficoltà nella gestione di un elevato numero di dispositivi IoT a causa del consumo energetico e della congestione della rete, soprattutto nelle bande a 2.4 GHz molto utilizzate.

L'adozione di protocolli come Matter, che sfruttano Thread e Wi-Fi, consente di combinare la scalabilità di reti mesh a bassa potenza con la capacità di banda di Wi-Fi, facilitando la gestione di ambienti domestici complessi e favorendo l'interoperabilità tra dispositivi di diversi produttori.

5.4 Strumenti e metodologie di test per le performance IoT

Per valutare in modo efficace le prestazioni e l'affidabilità dei protocolli IoT, sono disponibili numerosi strumenti software e hardware, oltre a metodologie di test specifiche.

Tra gli strumenti software, Wireshark è ampiamente utilizzato per l'analisi del traffico di rete, permettendo di monitorare pacchetti, latenza e perdite di dati **WiresharkTool**. Per testare il consumo energetico, strumenti come Power Profiler Kit di Nordic Semiconductor consentono di misurare con precisione l'assorbimento di corrente dei dispositivi **PowerProfiler**.

Le metodologie di test includono test di stress, che simulano un carico elevato di traffico per valutare la robustezza della rete; test di latenza e throughput, che misurano i tempi di risposta e la capacità di trasmissione dati; e test di interoperabilità, fondamentali per protocolli come Matter che puntano a garantire la compatibilità tra dispositivi di diversi produttori **IoTTestingMethods**.

Inoltre, simulazioni tramite software come NS-3 permettono di modellare reti IoT complesse e prevedere il comportamento dei protocolli in scenari realistici, riducendo i costi e i tempi di sviluppo **NS3Simulator**.

L'integrazione di questi strumenti e metodologie consente di ottenere una valutazione completa delle prestazioni dei protocolli IoT, guidando la scelta del protocollo più adatto in base alle esigenze specifiche dell'applicazione.

Capitolo 6

Prospettive Future nella Domotica Residenziale

6.1 Il ruolo dello standard Matter e dei protocolli basati su IP

Matter rappresenta una svolta fondamentale nel panorama della domotica residenziale: è uno standard aperto sviluppato dalla Connectivity Standards Alliance (CSA), precedentemente nota come Zigbee Alliance, con l'obiettivo di garantire l'interoperabilità tra dispositivi di produttori diversi. Basato su protocolli IP come IPv6 e UDP, Matter consente una comunicazione sicura, affidabile ed efficiente tra dispositivi domestici smart, eliminando molte delle barriere imposte dai sistemi proprietari e frammentati.

L'architettura di Matter si fonda su un modello client-server e utilizza tecnologie di crittografia avanzate come TLS 1.3 per garantire la sicurezza end-to-end. Inoltre, supporta diversi livelli di connettività, inclusi Ethernet, Wi-Fi, Thread e BLE (Bluetooth Low Energy), permettendo una flessibilità di implementazione che si adatta a molteplici scenari d'uso. Ad esempio, Thread, un protocollo mesh basato su IPv6, consente una comunicazione a bassa potenza tra dispositivi, aumentando l'affidabilità della rete domestica.

L'adozione su larga scala di Matter potrebbe uniformare il mercato, facilitare l'integrazione di dispositivi di marche diverse e semplificare le configurazioni per l'utente finale, riducendo la necessità di hub multipli e applicazioni separate. Numerosi produttori di dispositivi smart home, tra cui Apple, Google, Amazon e Samsung, hanno già annunciato il supporto a Matter, sottolineando il potenziale impatto sul settore (**zillner2022matter**; Connectivity Standards Alliance 2024).

6.2 Sviluppi tecnologici emergenti

6.2.1 Intelligenza artificiale e apprendimento automatico nella smart home

L'integrazione dell'intelligenza artificiale (IA) e dell'apprendimento automatico (machine learning) nelle smart home sta rivoluzionando il modo in cui i sistemi domotici interagiscono con gli utenti e l'ambiente circostante. Algoritmi di machine learning possono

analizzare grandi quantità di dati provenienti da sensori ambientali, dispositivi indossabili e sistemi di controllo, per riconoscere pattern comportamentali e prevedere le esigenze degli utenti.

Ad esempio, un sistema basato su IA può apprendere gli orari di presenza degli abitanti, regolando automaticamente l'illuminazione, la climatizzazione e la sicurezza, ottimizzando il consumo energetico. Sistemi avanzati utilizzano reti neurali profonde (deep learning) per il riconoscimento vocale e il controllo gestuale, migliorando l'interazione naturale con l'ambiente domestico. Inoltre, l'IA può rilevare anomalie, come intrusioni o guasti, e attivare allarmi o interventi correttivi in tempo reale.

Un caso concreto è rappresentato da assistenti vocali intelligenti che, integrati con piattaforme domotiche, consentono di personalizzare scenari complessi, come la preparazione della casa per il rientro degli abitanti o la gestione automatica delle risorse in base alle condizioni meteo esterne (**chen2023smart**; Ray 2016).

6.2.2 Reti mesh e Wi-Fi 6

Le reti mesh stanno diventando la soluzione preferita per migliorare la copertura e l'affidabilità delle comunicazioni wireless in ambito domestico. A differenza delle reti tradizionali che dipendono da un singolo punto di accesso, le reti mesh utilizzano una topologia distribuita in cui ogni nodo può comunicare con più altri nodi, creando percorsi ridondanti che aumentano la resilienza della rete.

In particolare, il protocollo Thread, fortemente integrato con lo standard Matter, è un esempio di rete mesh basata su IPv6 progettata per dispositivi a bassa potenza e bassa latenza. Questo consente di collegare sensori, attuatori e altri dispositivi smart con consumi energetici contenuti e alta affidabilità.

Parallelamente, la diffusione del Wi-Fi 6 (802.11ax) introduce significativi miglioramenti in termini di velocità, efficienza spettrale e capacità di gestire un elevato numero di dispositivi contemporaneamente. Wi-Fi 6 utilizza tecnologie come OFDMA (Orthogonal Frequency Division Multiple Access) e MU-MIMO (Multi-User Multiple Input Multiple Output) per ottimizzare la trasmissione dati in ambienti densi, tipici delle smart home moderne.

Queste caratteristiche rendono Wi-Fi 6 particolarmente adatto a contesti smart home complessi, dove numerosi dispositivi, quali videocamere di sorveglianza, sensori ambientali, elettrodomestici intelligenti e sistemi di intrattenimento, devono comunicare simultaneamente senza degradare le prestazioni (**zhang2021wifi6**; ETSI 2023).

6.3 Sfide legate alla privacy e alla sicurezza

Con l'aumento esponenziale dei dispositivi connessi nella domotica residenziale, cresce parallelamente il rischio legato alla sicurezza informatica e alla protezione della privacy degli utenti. I sistemi domotici rappresentano potenziali bersagli di attacchi hacker, che possono portare a violazioni di dati sensibili, compromissione dei dispositivi o controllo non autorizzato degli ambienti domestici.

Tra le principali criticità si evidenziano:

- trasmissione non cifrata di dati sensibili, che espone le informazioni a intercettazioni e attacchi di tipo man-in-the-middle;

- vulnerabilità nei firmware dei dispositivi, spesso causate da aggiornamenti ritardati o assenti, che possono essere sfruttate per eseguire codice malevolo;
- accessi non autorizzati tramite reti domestiche compromesse, dovuti a configurazioni deboli o password predefinite.

Per affrontare tali sfide, è fondamentale adottare protocolli sicuri come TLS e DTLS per la cifratura delle comunicazioni, implementare meccanismi di autenticazione forte, e garantire aggiornamenti software regolari e automatici per correggere vulnerabilità note. Inoltre, la consapevolezza e l'educazione dell'utente sulle buone pratiche di cybersicurezza giocano un ruolo cruciale, ad esempio evitando l'uso di password deboli e configurando correttamente i dispositivi.

Inoltre, la normativa sulla privacy, come il GDPR in Europa, impone requisiti stringenti sulla raccolta, l'uso e la conservazione dei dati personali, obbligando i produttori a implementare misure di protezione adeguate e trasparenza verso gli utenti (**gdpr2016**; National Institute of Standards and Technology (NIST) 2020).

Infine, l'adozione di tecnologie emergenti come la crittografia omomorfica e le reti neurali federate promette di migliorare ulteriormente la sicurezza e la privacy, permettendo l'elaborazione di dati sensibili senza esporli direttamente (**liu2022homomorphic**).

Capitolo 7

Gestione di Dispositivi Multimarca

7.1 La sfida dell'interoperabilità

Uno dei principali ostacoli alla diffusione della domotica è rappresentato dalla mancanza di interoperabilità tra dispositivi di marche diverse. Le barriere tecnologiche sono spesso dovute all'utilizzo di protocolli proprietari, all'assenza di standard comuni e a una frammentazione dell'ecosistema. Questa situazione genera complessità nella configurazione e nella gestione quotidiana degli impianti domestici, limitando l'esperienza utente e l'adozione su larga scala di soluzioni smart home.

Tuttavia, iniziative come lo standard Matter e le alleanze tra produttori stanno contribuendo a superare tali ostacoli, promuovendo la compatibilità tra dispositivi. Matter, sviluppato dalla Connectivity Standards Alliance (CSA), si propone come un protocollo IP-based aperto e sicuro, progettato per consentire una comunicazione nativa e senza soluzione di continuità tra dispositivi di diverse marche e piattaforme. Grazie all'adozione di tecnologie come Thread per la rete mesh a bassa potenza e l'integrazione con Wi-Fi e Ethernet, Matter rappresenta un passo importante verso un ecosistema IoT domestico veramente interoperabile Connectivity Standards Alliance 2023.

Inoltre, l'adozione di API standardizzate e di framework software comuni facilita lo sviluppo di applicazioni domotiche capaci di gestire dispositivi multimarca in modo trasparente per l'utente finale. L'uso di protocolli come MQTT, CoAP e RESTful API permette la comunicazione e l'integrazione anche in scenari complessi, dove dispositivi legacy e nuovi coesistono.

7.2 Soluzioni generiche per la gestione multimarca

Per garantire la coesistenza e il funzionamento congiunto di dispositivi di produttori diversi, sono state sviluppate soluzioni generiche quali:

- **Gateway universali**: dispositivi hardware/software in grado di tradurre i protocolli tra sistemi differenti, ad esempio un gateway che converte Zigbee in Wi-Fi o Z-Wave in Ethernet. Questi gateway spesso implementano funzioni di bridge e possono includere motori di automazione locali per ridurre la latenza Smith 2022.
- **Piattaforme open-source**: come Home Assistant, OpenHAB e Domoticz, che permettono una personalizzazione spinta e ampia compatibilità grazie a un'architettura modulare basata su componenti e integrazioni. Queste piattaforme supportano

centinaia di protocolli e dispositivi, consentendo agli utenti di creare automazioni complesse e scenari personalizzati Home Assistant 2024.

- **Standard Matter**: protocollo aperto sviluppato da CSA (Connectivity Standards Alliance) per unificare l'ecosistema IoT domestico, garantendo interoperabilità nativa. Matter utilizza tecnologie di trasporto IP, crittografia end-to-end e un modello di dati comune per facilitare la configurazione automatica e sicura dei dispositivi Connectivity Standards Alliance 2023.

Un esempio concreto di implementazione multimarca è rappresentato dall'integrazione di lampadine Philips Hue (Zigbee), termostati Nest (Wi-Fi) e serrature Yale (Z-Wave) all'interno di una piattaforma Home Assistant, che gestisce centralmente le automazioni e la supervisione tramite un'interfaccia web o app mobile.

7.3 Soluzioni native basate sugli smartphone

Numerosi produttori hanno sviluppato piattaforme integrate nei sistemi operativi mobili, che permettono il controllo centralizzato dei dispositivi domestici:

- **Apple HomeKit**: orientato alla sicurezza e alla privacy, con integrazione tramite l'app Casa e l'assistente Siri. HomeKit utilizza un protocollo proprietario basato su crittografia end-to-end e supporta dispositivi certificati con chip specifici per garantire l'affidabilità. L'ecosistema offre anche funzionalità avanzate come automazioni basate su geofencing e scenari personalizzati Apple Inc. 2023b.

- **Google Home**: supporta un'ampia gamma di dispositivi e l'assistente vocale Google Assistant. La piattaforma integra protocolli come Weave e utilizza la rete Wi-Fi per la comunicazione, offrendo un'esperienza utente fluida e supporto per routine personalizzate.

- **Amazon Alexa**: piattaforma versatile con ampia compatibilità e controllo vocale tramite dispositivi Echo. Alexa supporta skill personalizzate per estendere le funzioni dei dispositivi e integra protocolli multipli, inclusi Zigbee tramite hub dedicati.

- **Samsung SmartThings**: combina compatibilità con dispositivi Zigbee/Z-Wave e automazioni intelligenti. SmartThings offre un ecosistema aperto con API per sviluppatori e supporta l'integrazione con assistenti vocali come Bixby, Alexa e Google Assistant Samsung Electronics 2023.

Queste piattaforme native si stanno evolvendo per supportare nativamente Matter, facilitando ulteriormente la gestione multimarca e migliorando la sicurezza e la scalabilità degli impianti.

7.4 Confronto tra soluzioni native

Le piattaforme native presentano caratteristiche differenti in termini di facilità di configurazione, sicurezza, compatibilità e funzioni avanzate. Nella Tabella 7.1 viene proposta una comparazione sintetica.

Tabella 7.1: Confronto tra principali soluzioni domotiche native

Piattaforma	**Compatibilità**	**Sicurezza**	**Controllo Vocale**	**Scalabilità**
Apple HomeKit	Alta	Elevata	Siri	Media
Google Home	Molto Alta	Media	Google Assistant	Alta
Amazon Alexa	Alta	Media	Alexa	Alta
Samsung SmartThings	Alta	Alta	Bixby / Alexa	Alta

Ad esempio, Apple HomeKit si distingue per l'elevata sicurezza grazie alla crittografia end-to-end e al controllo rigoroso dei dispositivi certificati, ma può risultare meno flessibile in termini di compatibilità rispetto a Google Home, che supporta un numero maggiore di dispositivi e protocolli diversi. Amazon Alexa e Samsung SmartThings offrono un buon equilibrio tra compatibilità e funzionalità avanzate, con ampio supporto per automazioni vocali e integrazione con altri servizi cloud.

7.5 Esempi concreti di implementazioni multimarca

Un caso di studio significativo riguarda l'installazione di un sistema domotico in un'abitazione con dispositivi di diversi produttori: lampadine Philips Hue (Zigbee), termostati Nest (Wi-Fi), sensori Xiaomi (proprietario e Zigbee), serrature Yale (Z-Wave) e videocamere Arlo (Wi-Fi). Utilizzando Home Assistant come piattaforma centrale, è possibile integrare tutti questi dispositivi tramite componenti specifici, creando automazioni avanzate come l'accensione automatica delle luci al rilevamento di movimento, la regolazione intelligente della temperatura in base alla presenza e la gestione sicura degli accessi tramite notifiche push.

Un altro esempio riguarda l'uso di gateway universali come il dispositivo Hubitat Elevation, che consente di collegare dispositivi Zigbee, Z-Wave e LAN, offrendo una piattaforma locale per l'automazione e riducendo la dipendenza dal cloud. Questa soluzione è particolarmente apprezzata in contesti dove la privacy e la latenza sono critici.

Capitolo 8

Esempio pratico: Sistema Domotico con Apple HomeKit

8.1 Obiettivo della configurazione

Lo scopo di questo capitolo è illustrare un esempio concreto di integrazione domotica attraverso la piattaforma Apple HomeKit. La configurazione prende in esame l'utilizzo combinato di interruttori intelligenti BTicino Living Now e dispositivi di sicurezza Netatmo, il tutto gestito tramite l'ecosistema Apple (Apple Inc. 2023c).

8.2 Componenti utilizzati

Il sistema domotico è stato realizzato impiegando i seguenti dispositivi:

- **Piattaforma centrale**: Apple HomeKit con HomePod Mini come hub (Apple Inc. 2023d);
- **Interruttori intelligenti**: BTicino Living Now con connettività Wi-Fi (BTicino 2023);
- **Dispositivi di sicurezza**: Netatmo Presence (telecamera), sensori per porte/finestre, sirena interna (Netatmo 2023).

8.3 Fasi di configurazione

La configurazione del sistema si articola in tre fasi principali:

1. **Preparazione della piattaforma HomeKit**: configurazione iniziale dell'app Casa su iOS e aggiunta dell'HomePod Mini come hub domestico;
2. **Integrazione degli interruttori BTicino**: installazione fisica e collegamento alla rete Wi-Fi, seguita dall'aggiunta tramite QR code nell'app Casa;
3. **Configurazione dei dispositivi Netatmo**: installazione e associazione via app Netatmo, quindi integrazione in HomeKit tramite HomeBridge ufficiale (Homebridge Project 2023).

8.4 Automazioni e scenari d'uso

Una volta completata l'integrazione, è possibile definire automazioni personalizzate. Tra gli scenari implementabili:

- accensione automatica delle luci al rilevamento di movimento notturno;
- attivazione della sirena in caso di apertura non autorizzata di porte;
- gestione dell'illuminazione tramite comandi vocali a Siri (Apple Inc. 2023a).

8.5 Vantaggi e considerazioni tecniche

Il sistema descritto offre un buon equilibrio tra semplicità di utilizzo, scalabilità e compatibilità. HomeKit garantisce una configurazione intuitiva e un elevato livello di sicurezza dei dati (Apple Inc. 2023e). Tuttavia, va considerata la necessità di dispositivi compatibili con lo standard Apple o l'uso di bridge aggiuntivi per dispositivi non certificati.

Appendice A

Glossario dei termini e degli acronimi

IoT Internet of Things — Insieme di dispositivi interconnessi che comunicano tra loro via rete.

Smart Home Abitazione intelligente in cui dispositivi e impianti sono automatizzati e controllabili a distanza.

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 Framework Apple per l'integrazione e gestione di dispositivi smart home.

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

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

Hub Dispositivo centrale che coordina il traffico e l'automazione dei dispositivi smart.

CSA Connectivity Standards Alliance — Organismo che promuove standard aperti per l'IoT.

NIST National Institute of Standards and Technology — Agenzia USA per standard e tecnologie.

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

NIST IoT Security Linee guida e best practice sulla sicurezza IoT definite dal National Institute of Standards and Technology.

Rete mesh Una rete in cui ogni dispositivo si connette direttamente ad altri dispositivi vicini, migliorando copertura e affidabilità.

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.

Bluetooth Low Energy (BLE) Versione del protocollo Bluetooth a basso consumo energetico, particolarmente adatta per dispositivi IoT con alimentazione a batteria.

VLAN Virtual Local Area Network — Una rete logica separata all'interno della stessa infrastruttura fisica, utilizzata per segmentare e proteggere la rete domestica.

IDS Intrusion Detection System — Sistema di monitoraggio del traffico di rete per individuare attività sospette o non autorizzate.

Firmware Software installato su dispositivi hardware IoT, responsabile della gestione diretta delle funzionalità del dispositivo.

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

Man-in-the-Middle (MitM) Tipo di attacco informatico in cui un aggressore intercetta e potenzialmente manipola la comunicazione tra due dispositivi.

VLAN Virtual Local Area Network — Rete logica separata all'interno della stessa infrastruttura fisica, utilizzata per segmentare e proteggere la rete domestica.

IDS Intrusion Detection System — Sistema di monitoraggio del traffico di rete per individuare attività sospette o non autorizzate.

Firmware Software installato su dispositivi hardware IoT, responsabile della gestione diretta delle funzionalità del dispositivo.

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

Man-in-the-Middle (MitM) Tipo di attacco informatico in cui un aggressore intercetta e potenzialmente manipola la comunicazione tra due dispositivi.

Appendice B

Appendice Tecnica: Configurazione di un sistema HomeKit

Esempio di configurazione YAML per Homebridge

```
{
  "bridge": {
    "name": "Homebridge",
    "username": "CC:22:3D:E3:CE:30",
    "port": 51826,
    "pin": "031-45-154"
  },
  "description": "Configurazione base per accessori BTicino e Netatmo",
  "accessories": [],
  "platforms": [
    {
      "platform": "netatmo",
      "name": "Netatmo Platform",
      "client_id": "TUO_CLIENT_ID",
      "client_secret": "TUO_CLIENT_SECRET",
      "username": "email@example.com",
      "password": "password"
    }
  ]
}
```

Schermata di esempio

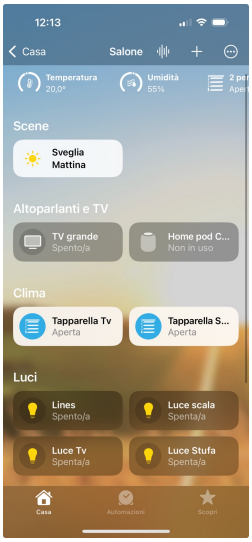

Figura B.1: Interfaccia Apple Home con dispositivi configurati

Bibliografia

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

Apple Inc. (2023a). *Controlla la casa con Siri*. Accesso il 10 aprile 2025. URL: https://support.apple.com/it-it/HT208280.

— (2023b). *HomeKit Accessory Protocol Specification*. Accesso il 10 aprile 2025. URL: https://developer.apple.com/homekit/.

— (2023c). *HomeKit: Tecnologia per la casa intelligente*. Accesso il 10 aprile 2025. URL: https://www.apple.com/it/ios/home/.

— (2023d). *HomePod mini*. Accesso il 10 aprile 2025. URL: https://www.apple.com/it/homepod-mini/.

— (2023e). *Privacy e sicurezza nella casa intelligente*. Accesso il 10 aprile 2025. URL: https://www.apple.com/it/privacy/.

BTicino (2023). *Living Now: Interruttori smart*. Accesso il 10 aprile 2025. URL: https://www.bticino.it/living-now/.

Connectivity Standards Alliance (2023). *Matter Specification Version 1.0*. Accesso il 10 aprile 2025. URL: https://csa-iot.org/all-solutions/matter/.

— (2024). *Matter: The foundation for connected things*. Accesso il 10 aprile 2025. URL: https://csa-iot.org/all-solutions/matter/.

ETSI (2023). *Wi-Fi 6 and Beyond*. Accesso il 10 aprile 2025. URL: https://www.etsi.org/newsroom/news/1941-2023-03-news-wifi6-beyond.

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

Homebridge Project (2023). *Homebridge: HomeKit support for the impatient*. Accesso il 10 aprile 2025. URL: https://homebridge.io.

International Electrotechnical Commission (2020). *IEC and the smart home*. Accesso il 10 aprile 2025. URL: https://www.iec.ch/blog/iec-and-smart-home.

National Institute of Standards and Technology (NIST) (2020). *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. Accesso il 10 aprile 2025. URL: https://csrc.nist.gov/publications/detail/sp/800-213/final.

Netatmo (2023). *Sicurezza domestica: Telecamere e sensori intelligenti*. Accesso il 10 aprile 2025. URL: https://www.netatmo.com/it-it/security.

Ray, P. P. (2016). «Home Health Hub Internet of Things (H3IoT): An architectural framework for monitoring health of elderly people». In: *IEEE Internet of Things Journal* 3.3, pp. 258–268.

Roman, R., J. Zhou e J. Lopez (2013). «On the Features and Challenges of Security and Privacy in Distributed Internet of Things». In: *Computer Networks* 57.10,

pp. 2266–2279. URL: https://www.sciencedirect.com/science/article/abs/pii/S1389128613000054.

Samsung Electronics (2023). *SmartThings Developer Documentation*. Accesso il 10 aprile 2025. URL: https://smartthings.developer.samsung.com/.

Sicari, S. et al. (2015). «Security, Privacy and Trust in Internet of Things: The Road Ahead». In: *Computer Networks* 76, pp. 146–164. URL: https://www.sciencedirect.com/science/article/pii/S1389128614003971.

Smith, J. (2022). «Universal Gateways for IoT: Bridging Protocols in Smart Homes». In: *IEEE IoT Journal* 9.4. Accesso il 10 aprile 2025, pp. 2345–2356. URL: https://ieeexplore.ieee.org.

Standards, National Institute of e Technology (2022). *IoT Security Guidelines*. URL: https://www.nist.gov/itl/applied-cybersecurity/nist-iot-security (visitato il giorno 08/07/2025).

TechCrunch (2019). *Nest thermostat hacked*. URL: https://techcrunch.com/2019/02/18/nest-thermostat-hacked.

The Washington Post (2019). *Ring cameras hacked: Families spied on*. URL: https://www.washingtonpost.com/technology/2019/12/12/hackers-are-breaking-into-ring-cameras/.

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

Yang, Y. et al. (2017). «A Survey on Security and Privacy Issues in Internet-of-Things». In: *IEEE Internet of Things Journal* 4.5, pp. 1250–1258. URL: https://ieeexplore.ieee.org/document/7902207.