

**Evoluzione dello Smart Home**

**L’impatto dell’IOT negli ambienti domestici: stato dell’arte e sviluppi futuri**

*Mattia Gatto 182926*

*Francesco Maria Granata 182669*

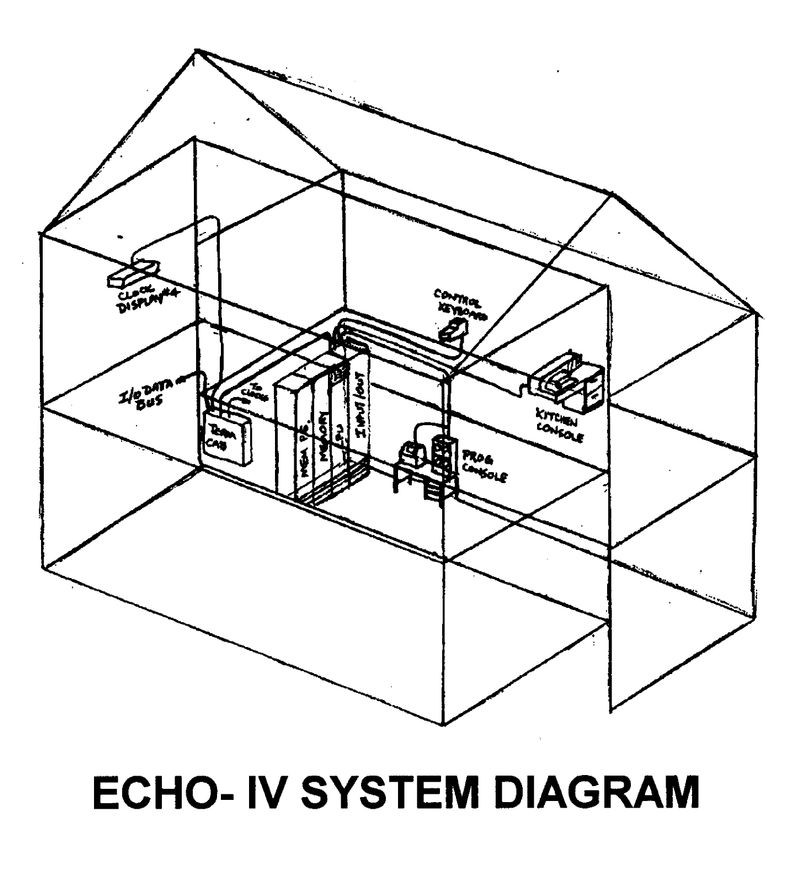
*Riccardo Bova 185268*

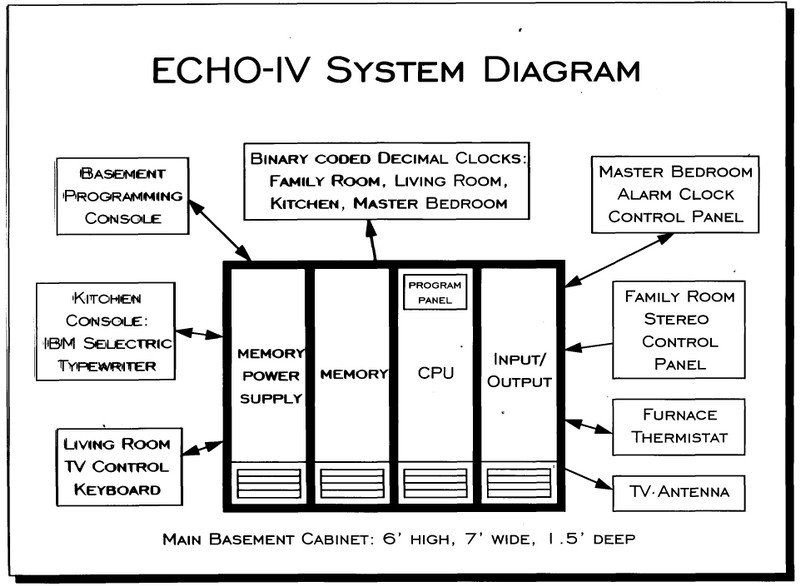
*Francesco Mandarino 183721*

Non risulta per niente facile parlare di un argomento così vasto e complesso come quello dello Smart Home. Sin dalle sue origini si sviluppa a cavallo fra diverse discipline ingegneristiche quali l’automazione e l’elettronica fino ad arrivare ai giorni nostri dove, grazie all’evoluzione sfrenata delle nuove tecnologie di telecomunicazione, sbarca nel campo degli oggetti cognitivi e dell’IOT. Senza dilungarci troppo in introduzioni partiamo, come è giusto che sia, dalla sua nascita.

Sebbene non sia concorde con l’idea di Smart Home odierna è necessario ricordare che un primo passo nella direzione giusta è stato effettuato all’inizio del ventesimo secolo con l’invenzione dell’aspirapolvere. L’idea di poter automatizzare quella che era un’azione “onerosa” di tutti i giorni è già un’introduzione ad un paradigma di intelligenza domestica che senza dubbio diede un grande impulso a sviluppi futuri. Pochi anni dopo si assiste all’invenzione dei frigoriferi, delle lavatrici e di tutti quegli elettrodomestici che al giorno d’oggi sono una realtà quotidiana.

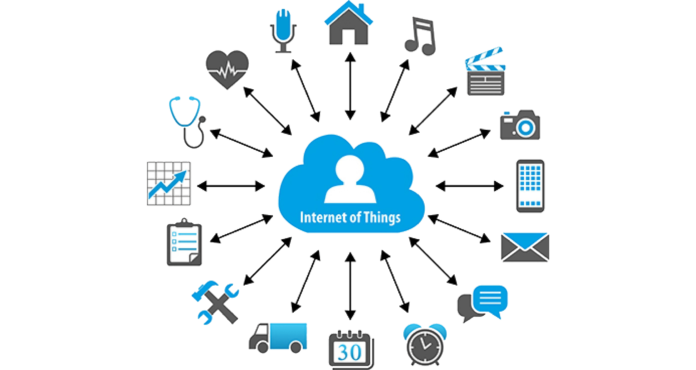
Da dove veniamo…

Nel 1966 viene reso operativo il primo operatore domestico computerizzato della storia: ECHO IV. Grazie ad esso era resa possibile, tra l’altro, l’interazione fra i vari membri della casa tramite terminali collocati in diverse stanze. Tali terminali potevano controllare sveglie, temperatura della casa e televisione; un terminale in cucina era predisposto per elaborare testi (ad es. liste della spesa) che potevano essere stampati ed inoltre vi era un’interfaccia di I/O alla quale potevano essere collegati stereo, termostato e antenna TV.



L’ evoluzione delle Smart home è strettamente collegata a quella dell’IOT che a sua volta è largamente influenzato dallo sviluppo delle reti mobili.  
Nel 1960 in Svezia nasce il primo dispositivo mobile. La prima generazione di telefonia mobile sviluppa anche le prime infrastrutture e reti nazionali che nascono in Giappone nel 1980. La nascita della tecnologia mobile di seconda generazione (1990) crea le basi per introdurre gli SMS e i servizi di download. Successivamente passiamo alla terza generazione mobile (il 3G) che nasce ad ottobre 2001 in Giappone e che rende in poco tempo il 2G una tecnologia obsoleta. Da qui in poi si trasforma in modo radicale il mondo della telefonia mobile rendendo possibile l’uso diffuso dei dispositivi mobili per accedere al web e per la trasmissione di servizi televisivi e radiofonici.

Siamo ai giorni nostri con la quarta generazione (4G) che trasforma l’internet mobile in qualcosa di molto simile all’internet usato da casa su computer fissi, con una velocità molto superiore a quella usata precedente. Il 5G, cioè la reti di quinta generazione, arriveranno ufficialmente a partire dal 2020, e consentiranno di collegare milioni di dispositivi in tutto il mondo ad alta velocità e con basso ritardo(latenza), permettendo così la realizzazione di progetti avanzati come le auto connesse, l’Internet of Things, le Smart City e le Smart Home della nuova generazione. Il concetto di IOT definisce un nuovo approccio alla tecnologia.

L’idea dell’Internet of Things, risale almeno agli anni Novanta, quando ne venne data una prima descrizione da Kevin Ashton, (ricercatore britannico cofondatore dell’Auto-ID Center del Massachusetts Institute of Technology (MIT)). Nel 1999 Ashton definì l’Internet of Things come l’insieme di: «tutte le cose che sono connesse con Internet attraverso sensori, come ad esempio il Radio Frequency Identification (RFID), per raggiungere sistemi intelligenti di identificazione e management». L’Internet of Things può essere considerata “una famiglia di tecnologie il cui scopo è rendere qualunque tipo di oggetto, anche senza una vocazione digitale, un dispositivo collegato ad Internet, in grado di godere di tutte le caratteristiche che hanno gli oggetti nati per utilizzare la rete”.

Le due grandi proprietà degli oggetti connessi sono essenzialmente di due tipi: monitoraggio e controllo. Per monitoraggio si intende la capacità dell’oggetto di operare come sensore, e di conseguenza di produrre informazioni relative a sé e all’ambiente (come ad esempio un lampione Internet of Things che può, non solo, rivelare se la propria lampada è funzionante oppure no, ma anche analizzare il livello di inquinamento dell’aria) mentre per controllo si intende invece la possibilità di gestire a distanza gli oggetti attraverso il solo utilizzo di Internet. Per quanto riguarda il futuro prossimo l’IOT (Internet of Things) rappresenta la prossima evoluzione di Internet, con un notevole miglioramento della capacità di raccogliere, analizzare e distribuire dati convertibili in informazioni e conoscenza. Per far accadere tutto ciò, è necessario governare molte tecnologie spesso non compatibili. Per quanto riguarda l’ambito delle Smart Home dovremmo regolare gli aspetti del controllo, del risparmio energetico e dei sensori.

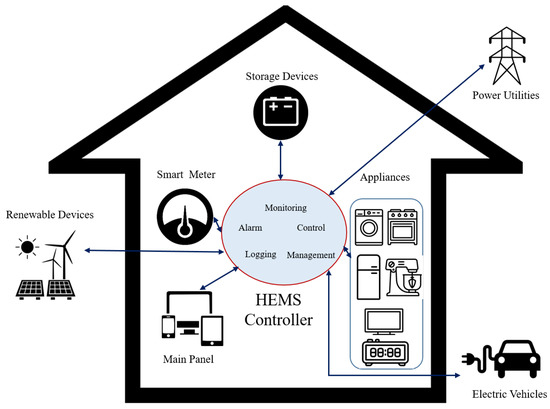
**GESTIONE DELL’ ENERGIA**

Le smart home sono caratterizzate tra le altre cose da un approccio differente alla gestione dell’energia:

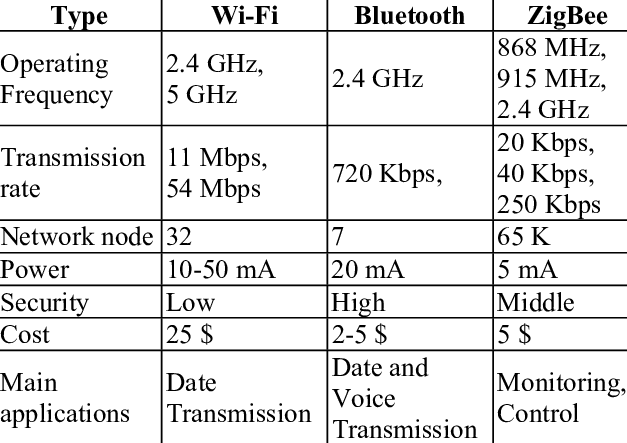
adottano dei sistemi anch’essi “smart” che consentano di ottimizzare l’efficienza energetica (SHEMS) che non sono altro che l’evoluzione dei tradizionali sistemi di gestione dell’energia (EMS).

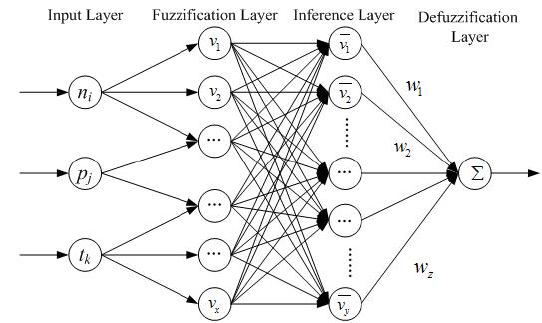
L’ evoluzione degli EMS parte già da inizio ‘900 con i termostati notturni come forma di automatizzazione della gestione dell’energia ma fu solo con la diffusione dei computer, di sistemi operativi come Unix, Gnu/Linux, Windows e successivamente lo sviluppo dei moderni sistemi embedded che venne fatto un notevole passo in avanti.

I SHEMS hanno il compito finale di minimizzare i costi totali relativi all’energia sfruttata dal consumatore nel lungo periodo e sono divisi in 5 parti:

1. I sistemi di misurazione che servono per raccogliere dati sui consumi;
2. I sensori che controllano i parametri desiderati in diverse zone della casa;
3. Sistema che consente la comunicazione tra i sistemi di misurazione, i sensori e l’unità di controllo;
4. Gli elettrodomestici “Smart” che devono essere loro stessi efficienti dal punto di vista energetico;
5. Il vero e proprio sistema di gestione dell’energia che ha il compito di dare informazioni sui dati, coordinare, controllare le componenti precedentemente dette;

Gli SHEMS sono elemento fondamentale delle Smart grids (ovvero reti elettriche migliorate attraverso le nuove tecnologie nel campo dell’informazione e delle comunicazioni) che li comprendono.  
La tecnologia wireless più utilizzata per quanto riguarda gli SHEMS è la ZigBee perché consuma poca energia ed è economica, inoltre supporta una raccolta di dati centralizzata ed è soggetta a poca interferenza. In questa immagine vediamo la ZigBee in comparazione con le altre tecnologie wireless di uso comune.



Un elemento fondamentale nel sistema di gestione dell’energia di una Smart home sono i dati che possono essere usati da algoritmi di apprendimento automatico al fine di gestire al meglio i consumi, ad esempio possono essere utilizzate delle reti neurali con logica fuzzy per gestire il tempo di utilizzo di un elettrodomestico e la quantità di energia da esso usata.

La peculiarità di questi algoritmi è che sono in grado di modellare la gestione dei consumi sul comportamento degli abitanti della SH che vengono appresi attraverso i dati.

Ottimizzare l’utilizzo dell’energia da parte di elettrodomestici intelligenti può voler dire due cose:

1. Riduzione dei consumi;
2. Shifting dei consumi ovvero schedulare l’utilizzo di elettrodomestici in modo da bilanciare il carico di energia richiesta durante il giorno;

Per lo scheduling sono utilizzati oltre agli algoritmi di apprendimento automatico precedentemente menzionati anche algoritmi di ottimizzazione euristici.

In futuro la ricerca relativa a questo ambito dovrà risolvere alcuni problemi:

1. L’incapacità dei sistemi attuali di gestire le incertezze, ovvero l’incapacità di adattarsi ad improvvisi cambiamenti della temperatura della casa o cambiamenti dei comportamenti del consumatore;
2. La difficoltà nel regolare le priorità delle attività in presenza di più utenti.
3. Difficoltà nel raggiungere un compromesso tra la comodità dell’utente e il risparmio energetico;
4. Difficoltà di mettere d’accordo le esigenze di più utenti quindi prendere decisione sulla base di input molteplici;

**Sensori**

I sensori sono gli occhi e le orecchie della rete domestica. Esistono sensori per una vasta gamma di applicazioni come la misurazione di temperatura, umidità, luce, liquidi e gas e la rilevazione di movimento o rumore.

Per soddisfare le esigenze delle persone in un ambiente domotico vi è bisogno di identificare gli utenti e le loro posizioni per la realizzazione di progetti e applicazioni Ambient Intelligence (AmI).

I progetti di ricerca mirano a realizzare un ambiente basato sull'intelligenza artificiale in grado di migliorare la qualità della vita degli utenti apprendendo le loro abitudini e anticipando i loro bisogni. Questo ambiente fa parte di un framework adattativo, sensibile al contesto, progettato per rendere interoperabili i sistemi domotici eterogenei incompatibili. Al livello più alto di queste infrastrutture, la struttura di Ambient Intelligence, integrata con i sensori domotici, può consentire al sistema di riconoscere qualsiasi situazione insolita o pericolosa e anticipare problemi di salute o esigenze speciali degli utenti in un ambiente di vita tecnologico, come una casa o uno spazio pubblico.

L'implementazione del paradigma AMI (Ambient Intelligence) richiede la progettazione e l'integrazione di ambienti intelligenti che si incentrano su ricerche che descrivono un'integrazione e una convalida di più sensori eterogenei con ragionatori ibridi che supportano il processo decisionale al fine di monitorare i dati personali e ambientali in una casa intelligente in modo privato. Possiamo vedere vari esempi di framework e sensori come:

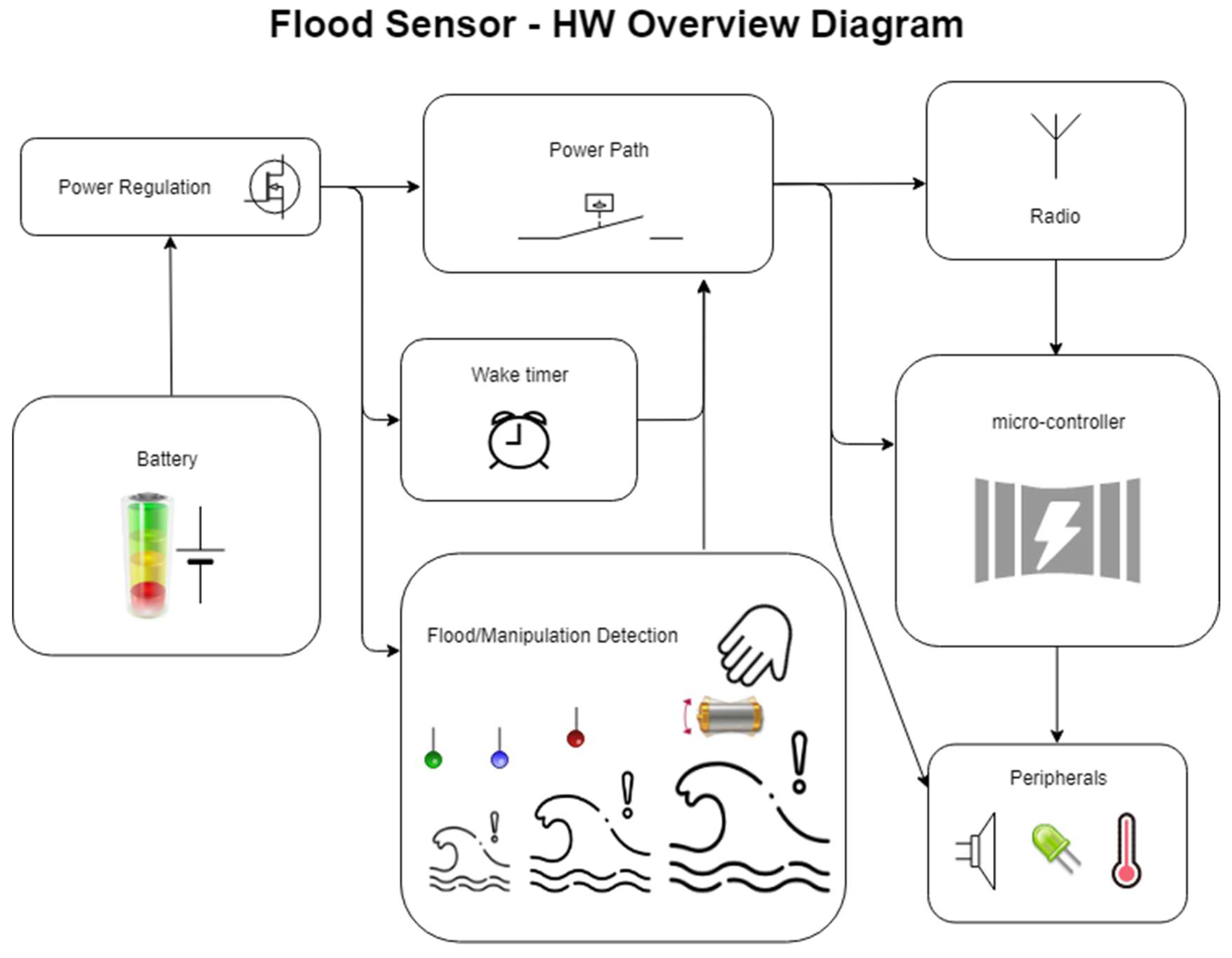
**TALISMAN +**

È un framework AmI implementato su piattaforme basate sulla conoscenza, sensori distribuiti, oggetti connessi, metodi di accessibilità e autenticazione per promuovere la vita indipendente per gli anziani. TALISMAN +, integra quattro sottosistemi nella casa intelligente:

1. una piattaforma mobile di tele monitoraggio biomedico per fornire ai pazienti anziani una gestione continua della malattia e aggiornamenti su questa;
2. un middleware di integrazione che consente la cattura del contesto da sensori eterogenei per programmare la reazione dell'ambiente;
3. un sistema di visione per il monitoraggio intelligente delle attività quotidiane in casa;
4. una piattaforma di ragionamento integrata per attivare azioni locali e gestire le informazioni private nella casa intelligente.

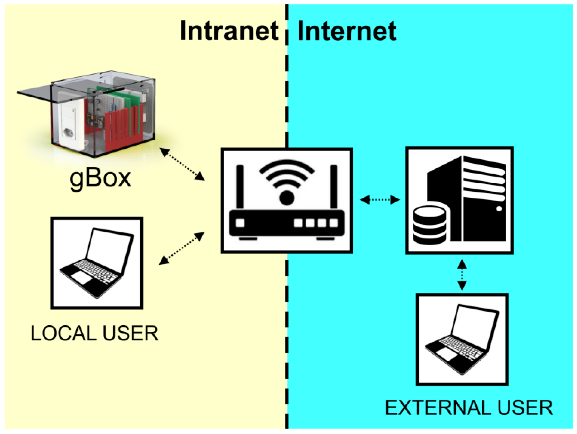
**Sensore di inondazione**

È un tipo di Sensore wireless a basso consumo per sistemi Smart Home in grado di rilevare la presenza di acqua sui pavimenti domestici, fornendo un allarme tempestivo delle perdite d'acqua.

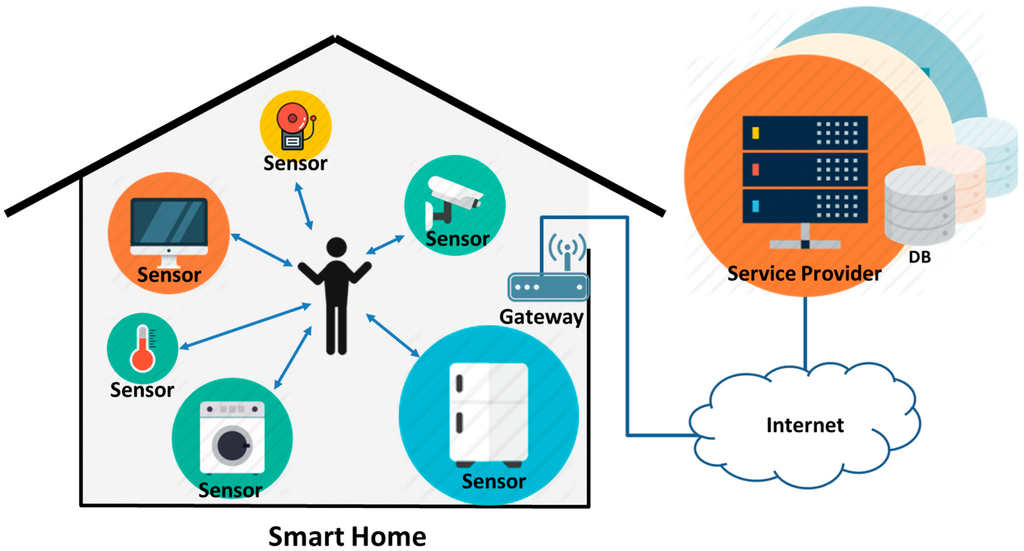


Il sistema di controllo in figura coordina la rete ed elabora i dati. Gli utenti possono richiedere da remoto la presenza di acqua, lo stato delle batterie per un nodo specifico, il tipo di liquido e le informazioni sulla sua funzionalità e sugli allarmi, grazie a un'applicazione software proprietaria. Gli avvisi vengono anche comunicati all'utente all'interno della casa tramite una sirena udibile. Il dispositivo progettato è ottimizzato in termini di costi, facilità di implementazione e manutenzione, rendendolo così ampiamente accettabile per gli utenti finali.

Vediamo che sono state implementate anche interfacce uomo-macchina basate sul tracciamento degli occhi per il controllo e il monitoraggio di una casa intelligente che utilizza IoT.

Le persone con gravi disabilità possono avere difficoltà quando interagiscono con i loro dispositivi domestici a causa delle limitazioni inerenti alla loro disabilità. Semplici attività domestiche potrebbero anche essere impossibili per questo gruppo di persone. Sebbene sia stato dedicato molto lavoro alla proposta di nuove tecnologie assistite per migliorare la vita delle persone con disabilità, alcuni studi hanno rilevato che l'abbandono di tali tecnologie è piuttosto elevato. Questo lavoro presenta un nuovo sistema assistito basato sul tracciamento oculare per il controllo e il monitoraggio di una casa intelligente, basato sull'Internet of Things, che è stato sviluppato seguendo i concetti di design centrato sull'utente e usabilità. Con questo sistema, una persona con gravi disabilità era in grado di controllare le attrezzature di tutti i giorni nella sua residenza, come lampade, televisione, ventilatore e radio. Inoltre, è in grado di monitorare a distanza, tramite Internet, il suo utilizzo del sistema in tempo reale. Inoltre, l'interfaccia utente sviluppata qui ha alcune funzionalità che hanno permesso di migliorare l'usabilità del sistema nel suo complesso. Gli esperimenti sono stati divisi in due fasi. Nella prima fase, il sistema di assistenza è stato assemblato in una casa reale dove sono stati condotti test con 29 partecipanti senza disabilità. Nella seconda fase, il sistema è stato testato con un monitoraggio online per sette giorni da una persona con disabilità grave (utente finale), a casa sua, non solo per aumentare la comodità e il comfort, ma anche perché il sistema potesse essere testato dove sarebbe infatti usato. Alla fine di entrambe le fasi, tutti i partecipanti hanno risposto al questionario SUS (System Usability Scale), e i risultati sono stati positivi.

Possiamo definire che l’infrastruttura della casa intelligente è costituita da sensori, gateway e fornitori di servizi. Nella casa intelligente, questi sensori forniscono un singolo servizio direttamente agli occupanti di casa, utilizzando le informazioni che raccolgono in tempo reale o più servizi attraverso lo scambio di informazioni con altri sensori. Quando i sensori trasmettono le informazioni raccolte a un fornitore di servizi, devono passare attraverso un gateway per comunicare con l'esterno perché hanno scarse risorse per l'uso. Il gateway funziona in due modi: riceve i dati raccolti dai sensori nella Smart Home e invia i dati ai fornitori di servizi o trasmette i dati dai fornitori di servizi ai sensori. Inoltre, il gateway invia direttamente un comando di controllo ai sensori sulla base delle informazioni ricevute e in base al tipo di servizio. Il fornitore dei servizi non è altro che un server registrato prima che un sensore venga distribuito nella Smart Home. Riceve informazioni rilevate da un sensore attraverso il gateway e fornisce un comando o un servizio di controllo, poiché l'infrastruttura della Smart Home è principalmente costruita con sensori, gateway e fornitori di servizi, creando così un ambiente multipiattaforma.



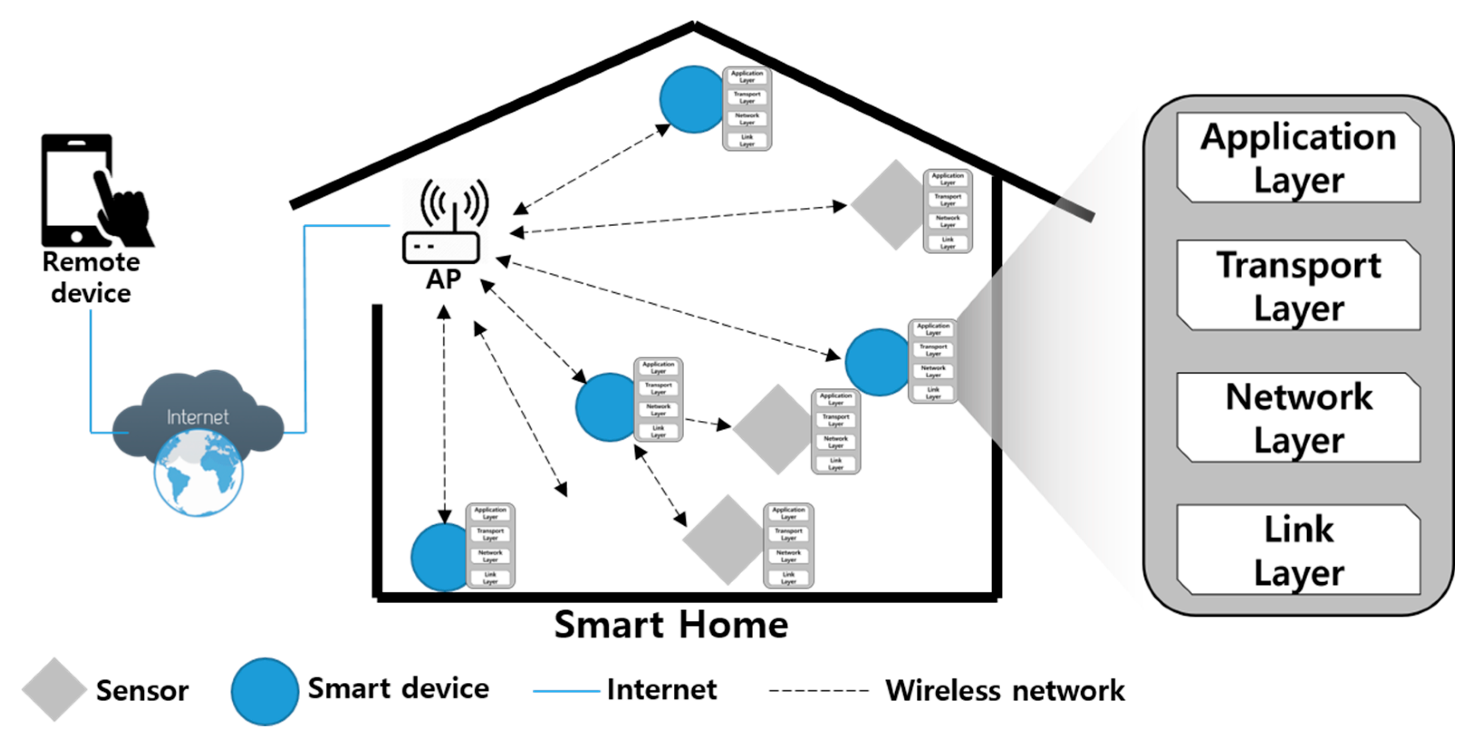
**Sicurezza**

Le Smart Home offrono soluzioni all’avanguardia per quanto riguarda i tradizionali problemi di sicurezza dell’ambiente domestico, tuttavia ne creano potenzialmente degli altri relativi alla cyber security.

**Problemi cyber security**

Nell'ambiente domestico intelligente per la comodità dell'utente, numerose quantità e tipi di dati vengono trasmessi tra una varietà di dispositivi intelligenti, gateway IoT e utenti. Quindi, i dati dovrebbero essere applicati con misure di sicurezza per impedire l'esposizione esterna, sia che si tratti di informazioni semplicemente rilevate, o la voce, l'immagine e le informazioni personali relative agli utenti, direttamente o indirettamente; quindi, si dovrebbero soddisfare i seguenti requisiti di sicurezza:

1. privacy: Esistono vari tipi di dispositivi domestici intelligenti nelle SM e ciascuno di essi ha diversi tipi di input e output. Sebbene i dati semplici, come i vari log, i documenti, le immagini, le animazioni e così via, che vengono scambiate dai dispositivi possano non avere un significato importante, possono contenere informazioni sensibili che dovrebbero essere protette. Pertanto, è necessario stabilire adeguate comunicazioni di sicurezza affinché le informazioni personali dell'utente non vengano esposte.
2. Registrazione di dispositivi Smart certificati: Se il processo di registrazione del dispositivo nella casa è vulnerabile, un dispositivo “malevolo” può essere registrato nella Smart Home. Solo gli utenti autorizzati dovrebbero essere in grado di registrare i propri dispositivi domestici intelligenti nella SH tramite un processo protetto.
3. Autenticazione utente: Gli utenti possono accedere fisicamente ai dispositivi smart home quando sono nella casa intelligente. Quando sono fuori gli utenti accedono alla casa intelligente da remoto. Ovviamente bisogna impedire che utenti non autorizzati accedano da remoto, c’è bisogno quindi di un processo di autenticazione per bloccare gli utenti malevoli. Esistono sistemi di accesso che utilizzano sessione / cookie; scambio di chiavi autenticate basato su password a tre parti (3PAKE); biometrica; e così via. Tuttavia, sono necessari nuovi metodi di autenticazione contro minacce quali ad esempio l'acquisizione di sessioni e le API vulnerabili.



Come detto è necessaria un'interazione sicura e semplice tra i vari dispositivi della SH. Push Button Configuration (PBC) è una delle tecnologie proposte per una facile configurazione di una sessione sicura tra tecnologie dell’informazione e dispositivi consumer. Sebbene la specifica Wi-Fi Direct affermi esplicitamente che tutti i dispositivi devono supportare il metodo PBC, la sua applicabilità è molto limitata. Questo perché la vulnerabilità della sicurezza di PBC può essere sfruttata maliziosamente in modo che gli aggressori possano effettuare sessioni illegittime con dispositivi consumer. Per affrontare questo problema, si è pensato di utilizzare un nuovo schema PBC (SePBC) con sicurezza avanzata con il quale possiamo scoprire dispositivi sospetti o malevoli. Il meccanismo proposto ha diverse caratteristiche. Primo, sviluppiamo un protocollo sicuro per la misurazione della distanza dell’handshake impedendo ad un avversario seduto fuori dalla regione di manipolare maliziosamente la sua distanza. In secondo luogo, è compatibile con l'originale PBC Wi-Fi senza introdurre una metodologia nuova di zecca. Infine, SePBC utilizza operazioni leggere senza calcolo della crittografia intensivo della CPU e impiega hardware poco costoso. Inoltre, ha bisogno di incorrere in un piccolo overhead quando non vi è alcun attacco.

**Gestione protocolli**

Nello Smart Home un elemento chiave, forse il più importante, è quello della comunicazione fra i vari Smart Object. Se da una parte un progresso fondamentale si è raggiunto già nel momento in cui gli oggetti, le cose, sono stati capaci di elaborare informazioni al loro interno, dall’altra la comunicazione e la condivisione di dati all’interno dell’ambiente domestico fra gli stessi può facilmente essere considerata come una vera e propria rivoluzione tecnologica. Si parla Home Area Network, Internet Of Things (IOT); le “cose” che comunicano sono destinate a cambiare radicalmente la nostra vita e in parte lo hanno già fatto: basti pensare ai sistemi di comunicazione healtcare, alla gestione efficiente dell’energia, alla condivisione multimediale e alla sorveglianza e sicurezza. A questo punto però sorgono spontanee delle domande: come comunicano gli Smart Object? Quali sono i protocolli utilizzati? Quando sono nati e come si sono evoluti?

Considerato che le specifiche di comunicazione nello Smart Home sono relativamente nuove e si stanno ancora sviluppando, la maggioranza dei protocolli utilizzati sono stati creati prima che il paradigma stesso di Smart Home nascesse. Conseguentemente la ricerca mira (anche) a capire se tali protocolli sono effettivamente utilizzabili [1]. Ma facciamo qualche passo indietro. Il concetto di Home Area Network (HAN) emerge come risultato della drammatica crescita di Internet alla fine degli anni ’90. Una Home Area Network è una rete di computer che opera nel raggio di una casa o di un ufficio che connette i vari devices al suo interno [2]. Considerato che gli Smart Object da collegare sono molti, l’idea metterli in comunicazione tramite un intricato sistema di cavi è piuttosto scoraggiante ed è il motivo per cui buona parte dei protocolli che si sono sviluppati nella storia dello Smart Home sono orientati a tecnologie e standard wireless. Quelli adottati oggi e largamente utilizzati sono: Wi-Fi, ZigBee, le tecnologie RFID, Bluetooth e Z-Wave [3].

Lo ZigBee si sviluppa a cavallo fra il 2000 e il 2002 mentre la sua specifica nasce nel 2004 [4]. Si presenta come una delle migliori soluzioni per le applicazioni nello Smart Home grazie al basso consumo di banda e di energia e grazie al basso costo. Al giorno d’oggi è fra le tecnologie più usate nell’ambito IOT. L’architettura ZigBee utilizza un approccio Master-Slave dove i devices ZigBee agiscono da slave e un dispositivo coordinatore di rete da master. Il protocollo ZigBee conta ad oggi 3 diverse versioni: si è partiti con lo ZigBee 2004, a seguire con lo ZigBee 2006 per culminare nello ZigBee PRO 2007 [5]. In particolare, la versione del 2007 garantisce un migliore switching di canale in caso di interferenza ed un miglior routing rispetto alle versioni precedenti [6]. In tutte le versioni la pila protocollare dello ZigBee è divisa fra i livelli appartenenti effettivamente allo ZigBee e i livelli definiti invece dallo standard IEEE 802.15.4 (nato nel 2003). In particolare, il livello fisico e il livello medium access control sono definiti dall’IEEE mentre lo ZigBee definisce tutti i livelli sovrastanti. Lo ZigBee costruisce una rete ad hoc a basa velocità e sfrutta il protocollo di accesso al mezzo CSMA/CA provvedendo un trasferimento di dati affidabile atraverso il mezzo wireless. Lo ZigBee è uno dei protocolli fondamentali nell’IOT ed è quindi sensibilmente apprezzabile il suo impatto storico (e ovviamente non solo) dello Smart Home.

Z-Wave Alliance nasce nel 2005 da un gruppo di produzione di home control insoddisfatto della tecnologia di quel tempo. Dopo aver fondato un contratto con la tecnologia Zensys per lo sviluppo dei suoi prodotti. Il protocollo Z- Wave si basa sulla tecnologia RF ed è uno dei più usati nello Smart Home sin dalla sua nascita all’inizio degli anni 2000. È capace di monitorare, controllare e leggere lo stato delle applicazioni domestiche e probabilmente la sua pervasività aumenterà di molto nel corso degli anni.

La storia del Wi-Fi relativamente allo Smart Home invece cammina parallelamente a quella dello ZigBee. Fondato sullo standard IEEE 802.11 si sviluppa e si sparpaglia ad alta velocità in moltissime applicazioni. Da citare ovviamente è la sua applicazione nelle reti di computer dove la moltitudine di calcolatori da connettere fa sì che una tecnologia non orientata ai cavi sia da preferire. Tuttavia, l’utilizzo del Wi-Fi non si ferma qui. Nell’ambito dello Smart Home svolge un ruolo fondamentale nel tenere collegati tutti i devices e si può considerare come una tecnologia essenziale in quanto grazie alle sue alte prestazioni in termini di velocità può facilmente essere usato per condividere file multimediali, collegare stampanti, fax e altre mansioni dove ci aspetta una risposta pressoché immediata. Moltissimi studi sono stati fatti per collegare al meglio le due realtà, in particolare nel corso della storia dello Smart Home il Wi-Fi si è rivelato ottimo in quanto i suoi segnali si sono mostrati abbastanza sensibili da catturare le dinamiche ambientali. Oltre a questo, nel corso degli ultimi anni è stato proposto da Aditya Virmani e Mahmoud Shahzad (ricercatori dell’università del North Carolina) di utilizzare il segnale Wi-Fi per monitorare le attività umane con l’intento di realizzare un’interfaccia computer-umana per l’automazione Smart Home [9].

La tecnologia RFID (Radio Frequency Identifier) è pervasiva nello Smart Home, non a caso i protocolli ZigBee, Z-Wave e Wi-Fi si basano sulle RF. L’evoluzione e la storia di questa tecnologia in relazione al controllo automatico nello Smart Home è dunque parallela a quella dello Smart Home stesso. Tuttavia, come detto in precedenza considerando che lo Smart Home è un paradigma relativamente nuovo, utilizza tecnologie e protocolli già esistenti antecedentemente ad esso [1] e infatti la tecnologia a RF nasce molto prima. Già nel 1906 Ernst F.W. Alexanderson dimostra l’onda radio continua e muove i primi passi nella comunicazione radio. L’inizio del ventesimo porta all’umanità il radar la cui funzione nella seconda guerra mondiale si rivela cruciale. Utilizzando onde radio che sbattevano contro gli oggetti e che venivano riflesse, poteva determinare posizione e velocità degli stessi [7]. L’importanza del radar venne subito capita dei militari che ne fecero un enorme sviluppo. La RFID nasce proprio da qui, dalla combinazione di tecnologia radio broadcast e dal radar. Dopo numerosi studi da parte di sviluppatori, inventori e istituzioni accademiche la RFID venne completamente implementata nella decade del 1980 mentre il suo utilizzo nelle case comincia intorno al 1990 con l’avvento dei personal computer. Successivamente venne impiegata nelle applicazioni dello Smart Home dell’IOT così come li conosciamo oggi. La RFID utilizza piccoli tag che vengono chiamati passivi (nel senso che non richiedono sorgenti di energia interne). Questi tag sono abbastanza piccolo ed economici da poter essere inseriti negli oggetti di tutti i giorni. Una delle sfide che si pone lo Smart Home con la HAN è quella di aver più cognizione spaziale e temporale delle attività che avvengono nell’ambiente intelligente. I tag RFID possono essere usati per tale scopo sviluppando algoritmi di localizzazione real-time [8].

La tecnologia Bluetooth ha sicuramente svolto un ruolo importante nello Smart Home. In una rete Bluetooth i nodi sono organizzati in piccoli gruppi chiamati piconet. Ogni piconet ha un master e diversi slaves. Un nodo può appartenere a diverse piconet. Ogni piconet può avere massimo 7 membri. Il Bluetooth viene stato usato nello Smart Home nella connessione di devices vicini ma non riveste un ruolo importante come lo ZigBee e il Wi-Fi.

Qualora non bastasse l’enorme mole di innovazioni e benefici in ambito Smart Home e IOT ci si può rallegrare nel fatto che le previsioni per gli sviluppi futuri sono molte e rosee. Lo sguardo dei ricercatori è proiettato verso l’utilizzo di automazioni e intelligenze sempre più complesse. Ad esempio, si potrebbe realizzare quella visione fantascientifica (forse non per molto ancora) di avere operatori robot intelligenti che integrati nella rete possono realizzare diverse funzioni comunicando con i vari Smart devices sulle operazioni svolte. Potrebbe esserci addirittura un controllo molto più complesso dell’ambiente domestico rendendo obsolete tutte quelle mansioni casalinghe che ci portiamo dietro da secoli.

È sicuramente vero però che, come in ogni cosa, ci sta il rovescio della medaglia. Sebbene Smart Home e IOT semplifichino notevolmente la nostra vita, è altrettanto vero che i problemi sociali e di sicurezza che ne conseguono possono rivelarsi una brutta spina nel fianco. Ad esempio, potrebbe essere possibile accedere alla rete e modificare lo stato di un device healtcare con conseguenze disastrose se non fatali. I problemi sociali invece nascono ad esempio dal fatto che la parola “smart” così ricorrente possa un po’ stomacare, impaurire e far storcere il naso. È chiaramente una provocazione, ma il punto focale è che non tutte le persone sono in grado di accettare una tale interoperabilità fra oggetti comuni con un’intelligenza così avanzata: le questioni etiche e la paura, purtroppo o per fortuna, sono fra i più acerrimi nemici del progresso scientifico e tecnologico e l’ambito IOT e Smart Home non fanno eccezione alcuna. Oggetti intelligenti e ambienti domestici controllati saranno comunque sempre più all’ordine del giorno e costituiranno un elemento essenziale della nostra vita. Non ci resta quindi che accoglierli con lo stesso entusiasmo e lo stesso sguardo orientato al futuro e all’innovazione che ci ha condotti fino a questo punto fondamentale dell’evoluzione tecnologica.

*Bibliografia*

A. J. Dinusha Rathnayaka, Vidyasagar M. Potdar, Samitha J. Kuruppu:  
 Energy Resource Management in Smart Home: State of art and Challenges Ahead, 2012  
  
A. Mahmood, H. Fakhar, S. H. Ahmed, N. Javaid:  
Home Energy Management in Smart Grid  
  
Giovanni Pau, Mario Colotta, Antonio Ruanu, Jiahu Qin:  
Smart Home Energy Management 2017  
  
Yuanyuan Liu, Bo Qiu, Xiaodong Fan, Haijing Zhu, Bochong Han:  
Review of Smart Home Energy Management Systems  
CUE2016-Applied Energy Symposium and Forum 2016: Low carnon cities & urban energy systems  
  
Wenquan Jin, Israr Ullah ,Shabir Ahmad, Dohyeun Kim:  
Occupant Confort Management Based on Energy Optimization Using an Environment Prediction Model in Smart Homes  
  
Pedro Teixidó, Juan Antonio Gómez-Galán, Fernando Gómez-Bravo, Trinidad Sánchez-Rodríguez, Javier Alcina Juan Aponte:  
Low-Power Low-Cost Wireless Flood Sensor for Smart Home Systems 2018  
  
Vittorio Miori, Dario Russo Cesare Concordia:  
Meeting People’s Needs in a Fully Interoperable Domotic Environment 2012  
  
Miguel Ángel Valero, José Bravo, Juan Manuel García Chamizo, Diego López-de-Ipiña:  
Integration of Multisensor Hybrid Reasoners to Support Personal Autonomy in the Smart Home 2014  
  
Alexandre Bissoli 1, Daniel Lavino-Junior, Mariana Sime, Lucas Encarnação, Teodiano Bastos-Filho:   
A Human–Machine Interface Based on Eye Tracking for Controlling and Monitoring a Smart Home Using the Internet of Things 2019  
  
Junghee Han, Taejoon Park :  
Security-Enhanced Push Button Configuration for Home Smart Control 2017  
  
Namsu Hong, Mansik Kim, Moon-Seog Jun, Jungho Kang:  
A Study on a JWT-Based User Authentication and API Assessment Scheme Using IMEI in a Smart Home Environment 2017  
  
Jungho Kang , Mansik Kim and Jong Hyuk Park:   
A Reliable TTP-Based Infrastructure with Low Sensor Resource Consumption for the Smart Home Multi-Platform 2016  
  
[1] Smart Home Communication Technologies and Applications: Wireless Protocol Assessment for Home Area Network Resources  
Tiago D. P. Mendes,Radu Godina , Eduardo M. G. Rodrigues , João C. O. Matias ,João P. S. Catalão   
Department of Electromechanical Engineering, University of Beira Interior, 6201-001 Covilha, Portugal  
Instituto de Engenharia de Sistemas e Computadores, Investigação e Desenvolvimento em Lisboa (INESC-ID), Instituto Superior Técnico (IST), University of Lisbon, 1049-001 Lisbon, Portugal 20 July 2015

[2] International Journal of Advanced Research in Computer Science and Software Engineering 5 May 2017 Home Area Networks: A Primer Matthew N. O. Sadiku, Mahamadou Tembely, and Sarhan M. Musa

[3] Journal of Communications Vol. 9, No. 9, September 2014. Smart Home Area Networks Protocols within the Smart Grid Context Ayesha Hafeez, Nourhan H. Kandil, Ban Al-Omar, T. Landolsi, and A. R. Al-Ali Computer Science and Engineering Department, American University of Sharjah, UAE

[4] <https://www.zigbee.org/>

[5] Combinatorial Evolution and Forecasting of Communication Protocol ZigBee, Authors: Mark Sh. Levin Russian Academy of Sciences,R. Kistler Lucerne University of Applied Sciences and Arts, Aliaksei Andrushevich Lucerne University of Applied Sciences and Arts, Alexander Klapproth Lucerne University of Applied Sciences and Arts

[6] An Overview of ZigBee Networks Matt Hillman

[7] The history of RFID J. Landt

[8] Exploiting Passive RFID Technology for Activity Recognition in Smart Homes Dany Fortin-Simard, Jean-Sébastien Bilodeau, Kevin Bouchard, Sébastien Gaboury, Bruno Bouchard, and Abdenour Bouzouane, University of Quebec at Chicoutimi

[9]Smart Home Based on WiFi Sensing: A Survey HONGBO JIANG1,2, (Senior Member, IEEE), CHAO CAI1 , XIAOQIANG MA 1,3, (Member, IEEE), YANG YANG4 , AND JIANGCHUAN LIU3 , (Fellow, IEEE)