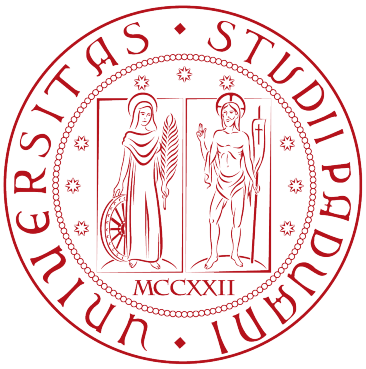

Università degli Studi di Padova

Dipartimento di Diritto pubblico, internazionale e comunitario

Dipartimento di Ingegneria dell'Informazione

Corso di Laurea in Diritto e Tecnologia

Internet of Medical Things: sfide e opportunità in tema di sicurezza

Relatrice:
Dott.ssa Sara Baldoni

Candidata:
Anna Variati
Matricola 2038937

Anno Accademico 2023-2024

Sommario

L'Internet of Medical Things (IoMT) rappresenta una cruciale innovazione nel settore sanitario: combina le tecnologie Internet of Things (IoT) con i servizi sanitari per supportare il monitoraggio e il trattamento dei pazienti in tempo reale e a distanza.
Questa Tesi esplora le tecnologie utilizzate, l'architettura dell'IoMT e fornisce esempi pratici di applicazione.
Una particolare attenzione è dedicata alla sicurezza, in quanto l'interconnessione dei dispositivi medici con altri sistemi crea nuove opportunità per gli avversari remoti.
Verranno analizzati lo stato dell'arte, le potenziali vulnerabilità e nuove tecniche di protezione.
Infine, verrà approfondito un caso di studio allo stato dell'arte.

Ringraziamenti

A mia mamma, che con infinita pazienza mi ha ascoltato ripetere innumerevoli volte prima degli esami, voglio dire grazie dal profondo del cuore.
A mio papà, la mia stella che brilla.
A Diego, che è sempre stato al mio fianco nei momenti più difficili. Grazie per avermi, come dici tu, sopportato e supportato, per avermi fatto ridere quando tutto sembrava andare storto e per non aver mai smesso di credere in me.
A chi mi vuole bene e a chi mi ha aiutato a raggiungere questo traguardo.
E soprattutto a me stessa, per tutte le volte in cui ho creduto di non farcela, per poi ricredermi, alla mia determinazione che non mi ha mai abbandonata, e ai miei sogni che, nonostante tutto, ho continuato a inseguire.

Indice

Capitolo 1

Introduzione

L'IoMT rappresenta un'importante evoluzione nel settore sanitario, in quanto combina le potenzialità dell'IoT con le esigenze del mondo medico.
Grazie all'uso di questi dispositivi, indossabili o impiantabili, i professionisti sanitari possono accedere a una vasta gamma di dati biometrici e contestuali, migliorando la precisione delle diagnosi, l'efficienza delle terapie e la gestione dei pazienti.

Tuttavia, nonostante i numerosi aspetti positivi, ci sono numerosi aspetti critici in termini di *privacy* e sicurezza: l'interconnessione di dispositivi medici con altri dispositivi e sistemi informatici, espone i pazienti a numerosi rischi, come la manomissione dei dispostivi stessi o dei dati da essi raccolti.

In questa Tesi verranno analizzate le principali tecnologie alla base dell'IoMT ed esplorate le problematiche di sicurezza ad esse associate. Attraverso l'utilizzo delle soluzioni attualmente disponibili, come la crittografia, l'intelligenza artificiale e la *blockchain*, si mira a identificare le migliori pratiche per proteggere i dati sensibili dei pazienti e garantire la resilienza dei sistemi IoMT.

Infine, verrà discusso un *framework* di sicurezza per mitigare i rischi e migliorare l'affidabilità dei dispositivi IoMT.

L'elaborato è strutturato come segue:

- Nel capitolo 1 viene fornita una panoramica generale

- Nel capitolo 2 si approfondiscono i fondamenti dell'IoMT, le sue tecnologie e l'architettura, con una particolare attenzione ai protocolli e alle sfide legate all'interoperabilità, all'efficienza energetica e alla sicurezza.

- Nel capitolo 3 ci si concentra sulle problematiche di sicurezza, analizzando le principali vulnerabilità e le soluzioni disponibili per proteggere i dispositivi IoMT dagli attacchi informatici.
- Nel capitolo 4 si affronta la questione relativa alla *privacy* esaminando i dati sensibili coinvolti nei sistemi IoMT e i relativi quadri normativi, come il Regolamento generale sulla protezione dei dati (GDPR) e l'Health insurance portability and accountability act (HIPAA).
- Nel capitolo 5 viene analizzato un *framework* di sicurezza per valutare e mitigare le vulnerabilità dei dispositivi IoMT in modo efficace, tenendo conto delle risorse limitate.
- Nel capitolo 6 vengono tratte le conclusioni, con un riepilogo delle sfide future e delle opportunità per migliorare ulteriormente la sicurezza e la privacy dei dispositivi IoMT.

Capitolo 2

Fondamenti dell'IoMT

2.1 Definizioni e concetti chiave

Il termine IoT si riferisce alla rete interconnessa di vari dispositivi dotati di sensori, attuatori e altre tecnologie che consentono loro di raccogliere ed elaborare dati, per poi scambiarli con altri dispositivi e con l'ambiente circostante [1].
Kevin Ashton propose per la prima volta il concetto di IoT nel 1999 [2], e lo definì come insieme di oggetti connessi tra loro, univocamente identificabili, con la tecnologia *Radio Frequency Identification (RFID).*
La connettività avanzata di questi dispositivi li rende versatili e applicabili in una vasta gamma di settori, spaziando dall'automazione domestica all'industria, dalle città intelligenti all'assistenza medica e sanitaria. È proprio in quest'ultimo ambito che trovano una delle loro applicazioni più promettenti, dando vita al concetto di IoMT [3].
L' IoMT si basa sulla possibilità di integrare dispositivi intelligenti nel contesto medico che raccolgono, trasmettono e analizzano dati biometrici e contestuali in tempo reale, consentendo ai professionisti sanitari di monitorare le condizioni dei pazienti da remoto ed intervenire prontamente in caso di emergenza.
Il potenziale di questa tecnologia emergente è enorme: può trasformare radicalmente la pratica medica, migliorando la qualità dell'assistenza, della diagnosi, del trattamento dei pazienti e riducendo tempi e costi sanitari.
L'IoMT si riflette in una vasta gamma di applicazioni, che spaziano dall'assistenza domiciliare a quella ospedaliera, dalla gestione dei farmaci al monitoraggio delle condizioni croniche e perfino alla prevenzione sanitaria.
I dispositivi IoMT possono essere di due tipologie: dispositivi medici impiantabili (IMDs)

oppure dispositivi indossabili (IoWDs) come descritto di seguito [4]:

- **Dispositivi Medici Impiantabili (IMDs):** questi dispositivi, inseriti nel corpo umano, hanno lo scopo di sostituire, supportare o migliorare una struttura biologica.
  Negli ultimi anni sono stati sviluppati IMDs senza fili per evitare problemi legati alle infezioni o alla rottura dei cavi.
  Data la loro posizione all'interno del corpo umano, gli IMDs devono essere estremamente compatti, consumare poca energia e garantire una lunga durata della batteria, poiché spesso rimangono in sede per diversi anni.
  Un esempio di IMDs, è il pacemaker che regola i ritmi cardiaci anomali.

- **Dispositivi Indossabili (IoWD):** questi dispositivi monitorano diversi parametri biometrici per migliorare la salute complessiva di chi gli indossa.
  Un esempio può essere lo *smartwatch* che consente il monitoraggio continuo della frequenza cardiaca e dei movimenti.
  Questi dispositivi sono utili per rilevare eventuali anomalie cardiache oppure possono supportare funzionalità come il rilevamento delle cadute o il conteggio dei passi effettuati.
  Nonostante questo, gli IoWD spesso presentano limitazioni per quanto riguarda la precisione dei sensori e la durata della batteria, il che li rende meno adatti per utilizzi in contesti critici rispetto agli IMDs.

L'interconnessione di questi dispositivi consente di creare un ecosistema sanitario efficiente, che offre ai pazienti un monitoraggio continuo e personalizzato e una migliore gestione del loro percorso di cura. Questo non solo migliora l'esperienza complessiva del paziente, ma permette anche ai professionisti sanitari di intervenire tempestivamente, ottimizzando l'efficacia delle terapie.
Inoltre, l'integrazione dei dispositivi IoMT con sistemi di intelligenza artificiale e analisi avanzata dei dati permette di predire e prevenire emergenze mediche, ottimizzando l'utilizzo delle risorse sanitarie e migliorando ancora di più la precisione diagnostica.
Tutto questo può contribuire a garantire la sicurezza e il benessere dei pazienti, consentendo interventi mirati e tempestivi che possono salvare vite.

2.2 Architettura e tecnologie principali

2.2.1 L'architettura

Attualmente non è ancora presente un modello di riferimento per l'architettura dei dispositivi IoMT, ma esistono numerosi progetti e proposte che mirano a svilupparne uno condiviso.
Un punto di partenza ampiamente adottato è rappresentato dal semplice modello a 3 strati: *Application Layer, Network Layer e Perception Layer*, che possiamo trovare raffigurato in Figura 2.1. [5].

- **Lo strato di percezione** (*perception layer*), costituisce le fondamenta dell'architettura IoT.
  Si tratta del livello più basso che si occupa di raccogliere e trasformare i dati provenienti dai sensori in un formato digitale, per poi trasmetterli al livello successivo.
  Questo strato sfrutta tecnologie a corto raggio come RFID, Bluetooth, Near-Field Communication (NFC) e Low Power Personal Area Network (6LowPan) per identificare e comunicare con gli oggetti.
  Nel contesto dell'IoMT, il livello di percezione è costituito dall'insieme di sensori, impiantati o indossati, che raccolgono i dati biometrici del paziente.

- **Lo strato di rete** (*network layer*), qui, i dati provenienti dai sensori vengono trasmessi direttamente ai dispositivi degli utenti, come gli *smartphone*.
  Questi dispositivi, dotati di potenza di calcolo e memoria, possono eseguire operazioni di pre-elaborazione. Ciò consente la validazione e l'analisi dei dati in loco, prima di inviare solo le informazioni essenziali al *cloud* per ulteriori elaborazioni e archiviazione.
  In questo modo, il *network layer* permette una gestione più efficiente dei dati.

- **Lo strato di applicazione** (*application layer*) permette un'interazione intuitiva e semplice tra utenti e applicazioni.
  In particolare, nell'IoMT, facilita l'interazione tra medici e pazienti, presentando in modo chiaro e comprensibile i dati, consentendo ai medici di fornire consulenze e raccomandazioni, e ai pazienti di tenere monitorato il loro stato di salute.
  Oltre alla visualizzazione dei dati, questo livello supporta azioni pratiche come la prescrizione di farmaci e la regolazione dei dosaggi in base alle informazioni ricevute.

Figura 2.1: Architettura IoMT [6]

2.2.2 Protocolli livello di percezione

I dispositivi per il monitoraggio dei pazienti raccolgono una vasta quantità di dati , fondamentali per il trattamento medico. Affinché questi dati siano utilizzati in modo efficace, è necessario trasmetterli al sistema centrale per effettuare varie computazioni, attraverso le quali , sarà possibile effettuare previsioni sul trattamento medico di un individuo.
Questa trasmissione di dati richiede l'impiego di protocolli specifici, ma è cruciale considerare che non tutti i protocolli IoT sono adatti per l'implementazione nei dispositivi IoMT, nonostante IoMT sia parte integrante dell'ecosistema IoT.
Nel livello di percezione, dove avviene la raccolta dei dati dai sensori, vengono utilizzati diversi protocolli, spesso basati sullo standard IEEE 802.15.4, noto per la sua bassa complessità e il consumo energetico ridotto. Questi dati saranno poi inviati a un computer, un *hub* o un *gateway*, dove vengono analizzati [7] [3] [8] .

- **Infrarossi**

  La tecnologia infrarossa proposta dall'*Infrared Data Association* (IrDA) viene utilizza come protocollo di comunicazione a breve raggio, permettendo la trasmissione di dati in modo rapido e sicuro tra dispositivi, senza la necessità di una connessione fisica diretta. È comunemente utilizzata in dispositivi come termometri e telecamere mediche che possono sfruttare le capacità di rilevamento della temperatura di IrDA. [9]

- **RFID** (*Radio Frequency Identification*)

  Questa tecnologia consente l'identificazione e il tracciamento degli oggetti utilizzando segnali radio. I dispositivi RFID includono un lettore che invia segnali radio per identificare i tag RFID presenti sugli oggetti.

  Un esempio di utilizzo di RFID è presentato da Saradha *et al.* [10], i quali propongono il controllo automatico intelligente dei semafori per velocizzare il transito delle ambulanze: si crea un'applicazione in grado di connettere sia l'ambulanza che la stazione dei semafori utilizzando una rete cloud e la tecnologia RFID, con l'obiettivo di ridurre al minimo il ritardo delle ambulanze causato dal traffico.

- **NFC** (*Near Field Communication*)

  La tecnologia NFC supporta la comunicazione a distanze molto brevi, di solito entro pochi centimetri.

  Si basa sull'accoppiamento induttivo tra il dispositivo trasmettitore e quello ricevente. È utilizzato principalmente per trasferire dati tra dispositivi mobili e per scopi di autenticazione.

  Un esempio di utilizzo è la proposta di J.Bravo *et al.* [11] per migliorare l'assistenza infermieristica. Essa prevede il posizionamento di *tag*, ad esempio sui polsi dei pazienti, sui letti, e sulle medicine, mentre gli infermieri utilizzano telefoni cellulari abilitati NFC. Gli infermieri devono solo toccare il *tag* del paziente con il telefono cellulare per identificare i farmaci prescritti e le dosi, nonché per visualizzare lo stato di salute del paziente.

- **Bluetooth/Bluetooth Low Energy (BLE)**

  Il Bluetooth è una tecnologia di comunicazione *wireless* ampiamente utilizzata per trasferire dati tra dispositivi a breve distanza.

  La versione a basso consumo energetico, BLE, è particolarmente adatta per dispositivi alimentati a batteria, come dispositivi indossabili e sensori IoT, poiché consuma meno energia.

  Un esempio di utilizzo, lo possiamo trovare in [12] dove è stato sviluppato uno strumento per rilevare in modalità *wireless* la respirazione, il battito cardiaco e la temperatura, durante il triage nei reparti di emergenza. Questo dispositivo potrebbe consentire una valutazione rapida e continua dei segni vitali dei pazienti, riducendo al contempo il carico di lavoro sul personale infermieristico e migliorando la capacità di identificare rapidamente i pazienti che necessitano di cure urgenti.

2.2.3 Protocolli livello di rete

I protocolli di rete gestiscono il modo in cui i dati vengono instradati e inviati tra dispositivi, garantendo sicurezza nella trasmissione. [8]

- **ZigBee**

  ZigBee è un protocollo di comunicazione wireless a basso costo, a bassa velocità e a basso consumo energetico. È particolarmente adatto per le Reti di Area Personale (PAN) e supporta varie topologie di rete, tra cui stella, albero e mesh, consentendo fino a 65.000 nodi in una rete. ZigBee ha un consumo energetico molto basso, che lo rende ideale per dispositivi alimentati a batteria o che richiedono un funzionamento a lungo termine con risorse limitate, come i dispositivi in questione.
  Lee *et al.* descrivono uno scenario IoMT che implementa il protocollo Zigbee per misurare il livello di glucosio nel sangue e i risultati dell'Elettrocardiografia (ECG) [13].

- **WiFi**

  Wi-Fi è una delle tecnologie di comunicazione *wireless* più utilizzate. Consente una rapida e sicura trasmissione dei dati, tuttavia ha un consumo di energia abbastanza elevato, che lo rende meno adatto ai dispositivi IoMT.
  Per questo è stato sviluppato Wi-Fi HaLow [14], che opera in frequenze più basse e consuma meno energia.
  Nello studio di Jia *et al.* [15] viene indicato come si possa sviluppare un dispositivo che utilizza il Wi-Fi per misurare il livello di attenzione di un guidatore. In questo caso specifico, il dispositivo andrà a misurare l'affaticamento del conducente senza utilizzare dispositivi indossabili, ma basandosi sul respiro e su movimenti riconducibili all'affaticamento.

- **Long Range Wide Area Network (LoRaWAN)**

  LoRaWAN, è un protocollo di rete che consente la comunicazione *wireless* a basso consumo energetico, tra dispositivi a lunga distanze.
  Proprio grazie al suo ampio *range* di copertura è stato scelto come protocollo nell'implementazione di *device* per il controllo remoto di pazienti.
  In particolare Taleb *et al.* [16] hanno sviluppato un sistema dove i dati vengono inviati solo in caso di criticità e non in modo continuo, in modo da utilizzare più efficientemente le risorse e avere una risposta rapida in caso di emergenza.

- **6LowPan**

  6LowPan è uno standard sviluppato da Internet Engineering Task Force (IETF) con l'obiettivo di supportare lo standard IPv6 anche in dispositivi a basso consumo energetico. Prevede inoltre la compressione degli *header* e l'incapsulamento dei pacchetti per ridurre la loro dimensione. Può essere anche integrato con altri standard come *Bluetooth Low Energy* e *Wi-Fi*.

2.2.4 Protocolli livello applicativo

I protocolli a livello applicativo si occupano dell'interpretazione e della gestione dei dati da parte delle applicazioni. In altre parole si trasformano i dati grezzi in informazioni utili.

- **Hypertext Transfer Protocol (HTTP)**

  HTTP è un protocollo di comunicazione utilizzato per il trasferimento di informazioni sul *World Wide Web*.

  È un protocollo *client-server* senza stato, il che significa che ogni richiesta del *client* al *server* è indipendente dalle richieste precedenti, e ogni risposta del *server* al *client* è indipendente dalle risposte precedenti.

  Rispetto ad altri protocolli viene utilizzato in maniera minore in quest'ambito perchè non soddisfa le esigenze di comunicazione dei dispositivi IoT con risorse limitate.

- **Message Queue Telemetry Transport (MQTT)**

  MQTT è un protocollo che utilizza il modello di pubblicazione/sottoscrizione (*publish/-subscribe*), il quale permette agli utenti di inviare lo stesso messaggio a più destinatari contemporaneamente, mentre i destinatari possono scegliere quali argomenti (*topic*) sottoscrivere, in modo da ricevere solo messaggi rilevanti per i loro interessi.

  Per risparmiare memoria, i messaggi vengono cancellati appena dopo essere stati inviati, a meno che non abbiano una *retain flag*.

  MQTT-SN è una versione ottimizzata di MQTT specifica per lavorare con dispositivi con risorse limitate, come i dispositivi IoT: viene utilizzato ad esempio nello studio di Alshammari *et al.* [17] come mezzo di trasmissione per consentire il monitoraggio remoto, inviando dati in tempo reale.

- **Constrained application protocol (COAP)**

  Il COAP [8] è un protocollo leggero e funzionale a livello applicativo che ricopre le stesse funzionalità di HTTP, per dispositivi IoT con risorse limitate, come potenza e spazio di

archiviazione.

Il COAP sfrutta il protocollo User Datagram Protocol (UDP) anziché il Transmission Control Protocol (TCP), poiché UDP è più semplice e ha una dimensione e una struttura dei messaggi ridotta.

Tuttavia presenta alcuni svantaggi, tra cui un aumento del ritardo di comunicazione, un'instabilità nella consegna dei pacchetti e l'incapacità di trasferire dati complicati che richiedono una gestione complessa e una maggiore affidabilità e stabilità della connessione per essere trasmessi correttamente [18].

2.3 Problematiche e sfide

L'IoT sta avendo sempre più impatto nelle nostre vite, nonostante questo, la sua rapida crescita non è immune a sfide e problemi. Tra le principali troviamo:

2.3.1 Interoperabilità e standardizzazione

L'interoperabilità rappresenta la capacità di diversi dispositivi e sistemi di comunicare, cooperare e scambiarsi informazioni.
Questa rappresenta una sfida significativa per l'IoT e ancora di più per l'IoMT, dove i dispositivi devono lavorare in sinergia avendo un impatto diretto sulla salute dei pazienti.
L'ecosistema IoT è, infatti, caratterizzato da una vasta quantità di dispositivi eterogenei: in un panorama così diversificato, garantire che i dispositivi possano interagire tra loro in modo efficiente diventa molto difficile.
È rilevante anche l'aspetto dell'interoperabilità semantica, ossia i dati scambiati devono essere scritti in una forma comprensibile da tutti i dispositivi.

La standardizzazione copre un ruolo fondamentale per il raggiungimento di interoperabilità tra i dispositivi: stabilendo degli standard, si definirebbe un modo condiviso di comunicare. La standardizzazione non migliora solo l'interoperabilità, ma anche la sicurezza tra dispositivi, che si possono connettere in modo più sicuro e proteggersi meglio da eventuali attacchi. Al momento mancano degli standard specifici a livello di IoMT. Tuttavia, ci sono delle organizzazioni che stanno lavorando a questo proposito come l'IETF, l'Iot Security Foundation (IoTSF) e l'Industrial Internet Consortium (IIC). [19] [20]

2.3.2 Efficienza energetica

I dispositivi IoMT, e in generale i dispositivi IoT, dispongono di risorse energetiche limitate, anche se una lunga autonomia sarebbe cruciale in molte applicazioni, come nel monitoraggio continuo necessario per alcune patologie.
Molti di questi dispositivi utilizzano batterie per il loro funzionamento e questo comporta che in caso di esaurimento sia necessario l'intervento umano.
Per ovviare questo problema, si stanno sviluppando delle soluzioni, ad esempio integrare ai dispositivi IoT dei sistemi di energia rinnovabile, tuttavia anche questi non sono completamente affidabili, si pensi ad esempio ai pannelli solari che durante la notte non producono energia.
Un'altra possibile soluzione è usare metodi che permettano di salvaguardare più energia possibile, come il *duty cycle*, nel quale il dispositivo rimane in stato di risparmio energetico per la maggior parte del tempo e si *sveglia* periodicamente per trasmettere e ricevere dati.

2.3.3 Sicurezza e privacy

L'utilizzo di dispositivi medici, siano essi indossabili o impiantabili, comporta numerosi benefici per il monitoraggio e il trattamento di condizioni sanitarie , tuttavia la sicurezza delle reti e dei dispositivi è un aspetto fondamentale da tenere in considerazione, in quanto questi dispositivi comportano rischi e pericoli per la sicurezza stessa del paziente.
L'eterogeneità di questo sistema lo rende più suscettibile agli attacchi informatici.
La principale motivazione per un attacco ai sistemi IoMT è il valore dei dati; si stima che il costo medio di tali dati sia 50 volte superiore rispetto ad altri settori. [21]
Come detto in precedenza, si tratta di dispositivi con risorse limitate, questo rende ancora più difficile l'implementazione di sistemi di sicurezza robusti.
L'*hacking* di tali reti potrebbe mettere a rischio la salute dei pazienti, o comunque la loro privacy, per questo è importante implementare strategie di accesso robuste e sicure come verrà trattata nel Capitolo 3.

Capitolo 3

Sicurezza nell'IoMT

3.1 Introduzione alla sicurezza nei dispositivi IoMT

L'evoluzione tecnologica in ambito sanitario, a cui hanno contribuito anche i dispositivi IoMT, ha migliorato significativamente le cure mediche. Tuttavia, è importante tenere anche in considerazione gli aspetti relativi alla sicurezza, molto delicati per questi dispositivi.
Dato che questi dispositivi raccolgono, trasmettono e analizzano dati estremamente sensibili, come informazioni personali e dati clinici, un'inadeguata protezione può portare a violazioni della privacy, compromissioni dei dati e persino rischi per la salute dei pazienti.
In questo capitolo si esploreranno le principali minacce alla sicurezza, lo stato dell'arte e possibili opportunità future.

3.1.1 Importanza della sicurezza nei dispositivi IoMT e rischi associati

L'importanza della sicurezza nei dispositivi IoMT è dovuta principalmente al fatto che i dati trattati sono altamente sensibili, inclusi dettagli sulle condizioni di salute dei pazienti, trattamenti in corso e storie cliniche: una compromissione di questi dati può avere conseguenze devastanti, non solo in termini di privacy, ma anche per la sicurezza dei pazienti stessi.
Ad esempio, la manipolazione non autorizzata di un dispositivo medico connesso può portare a diagnosi errate o trattamenti inappropriati, mettendo a rischio la vita dei pazienti.
Inoltre, un'eventuale violazione di sicurezza può danneggiare gravemente la reputazione di un'istituzione sanitaria, portando a una perdita di fiducia da parte dei pazienti.
Per questi motivi quindi è molto importante investire nella sicurezza di questi dispositivi.

3.2 Stato dell'arte

3.2.1 Requisiti

Per garantire un adeguato livello di sicurezza, i dispositivi devono soddisfare 11 requisiti, i quali sono stati sviluppati basandosi sul principio CIANA (*Confidentiality, Integrity, Availability, Non-repudiation, Authentication*) [4]:

1. **Confidenzialità:** i dati devono rimanere privati mentre vengono raccolti, trasmessi o memorizzati. Inoltre, devono essere accessibili solo agli utenti autorizzati.
   Per soddisfare questo requisito si possono utilizzare, per esempio, la crittografia e il controllo degli accessi.

2. **Integrità**: i dati devono essere protetti da qualsiasi manomissione e alterazione.

3. **Disponibilità**: i sistemi IoMT devono essere mantenuti continuamente operativi e i dati devono essere sempre disponibili per gli utenti autorizzati.

4. **Non ripudio**: ogni utente autorizzato è responsabile delle proprie azioni, questo requisito garantisce che qualsiasi interazione nel sistema non possa essere negata.
   Questo requisito può essere raggiunto utilizzando tecniche come la firma digitale.

5. **Autenticazione**: ci si riferisce alla capacità di convalidare l'identità di un utente che accede al sistema.

6. **Autorizzazione**: gli utenti autenticati possono svolgere solo le azioni per cui sono autorizzati.

7. **Anonimato**: questo requisito riguarda la capacità di mantenere nascoste alcune infomazioni, come le identità di pazienti e medici, da utenti non autorizzati quando interagiscono con il sistema.

8. **Segretezza progressiva/regressiva**: la segretezza progressiva garantisce che anche se un aggressore riesce a compromettere le chiavi crittografiche correnti, non sarà in grado di decifrare le comunicazioni passate.
   Un metodo comune per ottenere la segretezza progressiva è l'uso di protocolli di scambio chiave come il Diffie-Hellman effimero, che genera chiavi temporanee per ogni sessione di comunicazione.

La segretezza regressiva assicura il contrario, ovvero, che se anche le chiavi crittografiche attuali vengono compromesse, le comunicazioni e le chiavi future non siano a rischio. In altre parole, l'attaccante che riesce ad accedere alle chiavi correnti non sarà in grado di utilizzare tali chiavi per compromettere le comunicazioni future. [22]

9. **Scambio sicuro delle chiavi**: è la capacità di condividere in modo sicuro le chiavi tra i nodi nel sistema.

10. **Resilienza al *Key-Escrow***: il *key-escrow* è una tecnica mediante la quale le chiavi crittografiche (o una copia di esse) vengono affidate a una terza parte fidata [23].
    L'obiettivo di questo sistema è permettere a tale autorità di accedere alle comunicazioni cifrate in caso di necessità. Tuttavia questo può generare delle problematiche come: abuso di potere da parte del detentore delle chiavi e la creazione di un unico punto vulnerabile, cosicché, se la terza parte venisse compromessa, l'attaccante potrebbe accedere a tutte le informazioni da essa detenute.
    Un sistema resistente al *key-escrow* è progettato per minimizzare i rischi che possono derivare dalla conservazione delle chiavi da parte di terzi, ad esempio l'amministratore del sistema non può impersonare un altro utente del sistema, fornendo così protezione dalle minacce interne.
    Utilizzando chiavi asimmetriche, che assicurano che solo il destinatario autorizzato possa accedere ai dati crittografati, assieme ad una funzione di *hash* crittografico (CHF), che garantisce che i dati non siano stati modificati durante il trasferimento, il sistema può stabilire un sistema sicuro di autenticazione prevenendo accessi non autorizzati.

11. **Accordo sulla chiave di sessione**: i nodi nel sistema devono utilizzare chiavi di sessione dopo il processo di autenticazione.

3.2.2 Tecnologie e soluzioni attualmente disponibili

Per garantire la sicurezza dei dispositivi, vengono utilizzate alcune delle seguenti tecniche, citate da Bhushan *et al.* in [21]:

3.2.2.1 Funzione *Hash* Crittografica

La funzione di *hash* è un metodo che prende un *input* di lunghezza variabile e produce un *output* di lunghezza fissa, chiamato *hash*.
Questo valore è come un'impronta digitale dell'*input* originale, e ogni cambiamento anche

minimo nell'*input* produrrà un *hash* completamente diverso [24].
Per essere utilizzata nell'ambito IoMT, bisogna innanzitutto raccogliere i dati sanitari attraverso un sensore, a questi dati verrà poi applicata una funzione *hash* crittografica, che genererà una stringa alfanumerica, l'*hash*.
A questo punto l'*hash* viene trasmesso assieme ai dati al *gateway* e ai nodi sensori. Una volta ricevuto, il *gateway* può calcolare di nuovo l'*hash* sui dati ricevuti e confrontarlo con quello inviato dal sensore, per capire se i dati sono stati manipolati. Se gli *hash* coincidono significa che i dati non sono stati alterati.

3.2.2.2 Crittografia a chiave simmetrica

Nei sistemi di crittografia a chiave simmetrica la stessa chiave viene condivisa da entrambi i nodi, che quindi dovranno scambiarsela preventivamente, e la stessa viene utilizzata sia per la cifratura che per la decifratura dei dati.
Nei sistemi IoMT questa tecnica è utile per avviare connessioni sicure e accedere gerarchicamente ai dati del paziente.
Inoltre, consentono l'autenticazione a due fattori, in cui altre tecniche, come il riconoscimento facciale o basato su *pattern*, agiscono come secondo fattore.
Alcuni esempi di tecniche che utilizzano la crittografia simmetrica sono:

- **Accesso Gerarchico**: si tratta di una tecnica di autorizzazione basata su ruoli, ad esempio, nell'ambito sanitario, un infermiere può accedere alla lista dei medicinali da somministrare, ma solo un medico può prescrivere nuovi farmaci. In questa tecnica vengono cifrate le informazioni personali del paziente e ogni utente può decifrare solo una parte dei dati, in base al proprio ruolo e le proprie autorizzazioni.
- **Schema basato sull'andatura**: questo schema genera chiavi simmetriche uniche utilizzando il *pattern* della camminata del soggetto.

3.2.2.3 Crittografia a chiave asimmetrica

In questi sistemi esiste una coppia di chiavi, una pubblica e una privata, dove la chiave pubblica è conosciuta da tutti, mentre la privata è conosciuta solo dal proprietario.
Una chiave verrà utilizzata per la cifratura e l'altra per la decifratura, a seconda dello scopo che si vuole ottenere:

- **Cifratura con chiave pubblica:** il mittente cifra il messaggio utilizzando la chiave pubblica del destinatario. Solo il destinatario, che possiede la chiave privata corrispondente,

sarà in grado di decifrare il messaggio. In questo modo viene garantità la confidenzialità del messaggio.

- **Firma digitale:** il mittente cifra il messaggio (o una firma del messaggio) con la propria chiave privata. Chiunque potrà decifrare il messaggio usando la chiave pubblica del mittente, dimostrando così che il messaggio proviene effettivamente da lui, poiché solo il mittente possiede la chiave privata necessaria per cifrarlo. In questo modo viene garantità l'autenticità e l'integrità del messaggio

Alcuni esempi di tecniche che sfruttano la crittografia simmetrica sono:

- **Crittografia Omomorfica** : la crittografia omomorfica consente di effettuare la computazione su dati criptati senza decriptarli.

- **Firme digitali**: le firme digitali vengono utilizzate per verificare l'autenticità e l'integrità di un messaggio, per garantire quindi da dove proviene e che non sia stato manomesso.
  Si applica un algoritmo di *hash* al documento per creare una sorta di impronta digitale. Questa viene poi cifrata con la chiave privata del mittente per creare la firma digitale.
  Il destinatario, una volta ottenuto il messaggio, utilizza la chiave pubblica del mittente per decifrare la firma. Calcolerà poi un nuovo *hash* sul documento ricevuto: se i due *hash* coincidono la firma è valida e il documento non è stato modificato.

3.2.2.4 Algoritmi senza chiave

Alcune tecniche non richiedono l'utilizzo di chiavi pre-condivise, ad esempio la tecnologia *blockchain*, tecniche *proxy-based* e biometria.

- **Tecnologia *blockchain*:** la *blockchain* può apportare numerosi benefici anche nell'ambito dei dispositivi IoMT, come evidenziato anche da Alkatheiri in [25].
  In particolare, assicura che i dati memorizzati siano immutabili: questo garantisce che una volta che i dati sono stati registrati sulla *blockchain*, non possano essere modificati o cancellati senza che tutti i partecipanti alla rete ne siano consapevoli.
  Inoltre si possono sfruttare i cosidetti contratti intelligenti, i quali si autoeseguono solamente quando determinate condizioni predefinite sono soddisfatte.
  Ad esempio, possono gestire l'accesso ai dati medici sensibili, assicurandosi che solo gli utenti autorizzati possano accedere a queste informazioni.

La *blockchain* può anche migliorare i meccanismi di autenticazione e autorizzazione, utilizzando firme digitali e metodi di crittografia asimmetrica.
Inoltre non richiede la presenza di una singola autorità centrale, riducendo i rischi associati a un singolo punto di vulnerabilità.

- **Sistemi basati su *proxy*:** questa tecnologia utilizza un intermediario, chiamato *'proxy'*, per gestire e proteggere le comunicazioni tra due parti. Tale intermediario deve essere considerato sicuro, *'trusted'*, da entrambe le parti, perchè ha accesso ai dati in transito. Esso può essere utilizzato per filtrare o monitorare i dati, tuttavia se non vengono applicate tecniche di cifratura, non si potranno utilizzare chiavi crittografiche, quindi la sicurezza deve essere garantita attraverso altri metodi come il filtraggio dei dati, l'autenticazione dei dispositivi e il monitoraggio della rete.

- **Biometria**: l'uso di sensori biometrici è una delle tecniche maggiormente utilizzate per migliorare la sicurezza dei dispositivi IoMT. La biometria si basa sull'uso di caratteristiche fisiche o comportamentali uniche di un individuo per verificarne l'identità.
I sensori basati sull'analisi delle impronte digitali e dell iride sono quelli più diffusi [26].

3.2.3 Tipologie di attacchi

Nonostante vengano utilizzati diversi protocolli e tecniche di protezione, i dispositivi IoMT possono essere suscettibili di attacchi che possono non solo compromettere la privacy del paziente, ma anche causare danni finanziari e reputazionali per l'ente.

Le varie tipologie di attacco vengono distinte da Ioannis *et al.* in [27] e da Deogirikar *et al.* in [28] in quattro categorie: attacchi fisici, di rete, software e crittografici.

3.2.3.1 Attacchi fisici

Questa tipologia di attacchi riguarda i componenti *hardware* dei dispositivi IoMT e l'attaccante deve essere fisicamente vicino o all'interno del sistema per compiere questa tipologia di attacchi.

- **Manomissione del nodo o danno fisico** (*node tampering*) : si verifica quando l'attaccante sostituisce, altera o danneggia un nodo, ad esempio un sensore, in modo da rubare o modificare dati sensibili o causare l'interruzione del servizio.

- **Manipolazione sociale** (*social engineering*): l'attaccante cerca di manipolare un utente del sistema per estrapolare informazioni utili. Anche questo attacco è ritenuto di tipo fisico perché l'attaccante deve interagire fisicamente con un utente.

- **Attacco di privazione del sonno** (*sleep deprivation attack*): questo attacco vuole mantenere i dispositivi attivi per il più lungo tempo possibile in modo da scaricare le batterie che causeranno lo spegnimento.
  Molti dispositivi IoMT incorporano una modalità '*sleep*' o di sospensione per gestire l'uso energetico e prolungare la durata della batteria. Questa modalità consente ai dispositivi di ridurre significativamente il consumo di energia quando non sono in uso. L'attaccante quindi induce il dispositivo a rimanere costantemente attivo, ignorando o disabilitando i cicli di sospensione, causando così l'esaurimento della batteria e conseguente interruzione del servizio.

- **Iniezione di codice malevolo** (*Malicious Code Injection*): l'attaccante infetta i dispositivi con un codice malevolo per accedere al sistema IoT, ad esempio utilizzando una chiavetta USB infetta.

3.2.3.2 Attacchi di rete

Questa tipologia di attacchi riguarda la comunicazione tra i dispositivi IoT e gli altri componenti della rete, come *server* o altri dispositivi.

- **Attacco con intermediario** (*Man-in-the-middle*): l'attaccante si inserisce furtivamente nella comunicazione simulando di essere un intermediario. L'attaccante può intercettare ed eventualmente modificare la comunicazione tra il dispositivo e il destinatario.
  Il suo obiettivo non è solo l'intercettazione: può anche fare da ponte tra l'utente e il vero destinatario, inoltrando messaggi che sembrano legittimi, ma alterati a vantaggio dell'attaccante.
  L'attacco non sempre implica la decifratura dei dati. Tuttavia, quando i dati sono cifrati, l'attaccante può tentare di intercettarli, in forma cifrata, e cercare vulnerabilità per decifrarli, ma se la crittografia è ben implementata, questo processo risulta molto difficile. [29]

- **Interruzione del servizio** (*Denial of service*): consiste nel sovraccaricare il sistema con eccessive richieste, con lo scopo di rendere il servizio inacessibile gli utenti autorizzati. Esiste anche la variante Distributed Denial of Service (DDoS), dove l'attacco proviene

da molteplici fonti simultaneamente.
Un caso documentato è avvenuto nell'ottobre 2016, dove una *botnet*, chiamata *Mirai*, ha condotto un attacco DDoS contro un fornitore di servizi Domain Name System (DNS). In particolare, questo *malware* infettava dispositivi IoT per controllarli, e una volta infetti, questi dispositivi diventano parte di una *botnet* (una rete di dispositivi compromessi controllati da un attaccante) e potevano essere utilizzati per lanciare attacchi coordinati. L'attacco ha causato enormi interruzioni del servizio per molte aziende come Netflix, Reddit, The guardian e CNN. [6]

- **Attacco con false identità** (*sybil attack*): l'attaccante ruba l'identità degli altri nodi o crea identità fittizie con lo scopo di influenzare il sistema, grazie all'alto numero di nodi controllati

- **Attacco di intercettazione** (*sniffing attack*): l'attaccante intercetta e analizza i dati trasmessi.

3.2.3.3 Attacchi di software

Gli attacchi *software* sfruttano le vulnerabilità presenti a livello di *software*.

- **Attacco phishing**: l'attaccante si finge un'altra entità per ingannare le vittime e ottenere informazioni sensibili. Questo può avvenire ad esempio attraverso l'invio di e-mail false e infette.

- ***Malware***: l'avversario infetta il sistema con dei *software* maligni per rubare informazioni, interrompere il servizio o manomettere i dati. Alcuni esempi di *malware* possono essere:

  - *Virus*: con il termine '*virus*', spesso ci si riferisce, impropriamente, a tutti i tipi di *malware*. Un *virus* informatico è un programma malevolo che si attacca ad altri programmi e file, modificandoli e replicandosi. Ha bisogno dell'interazione dell'utente per attivarsi

  - *Worm*: sono simili ai *virus*, ma non necessitano di un 'ospite', come ad esempio un *file*, per replicarsi, possono auto-replicarsi e diffondersi autonomamente. Un *worm* può diffondersi rapidamente all'interno di una rete, infettando ogni dispositivo connesso.

- *Trojan horse*: si tratta di software che si mascherano come legittimi o utili, e una volta all'interno del sistema, consentono all'attaccante di accedere e controllare il dispositivo, installando altri *malware* o rubando dati.
- *Ransomware*: si tratta di un *malware* che cifra i dati di un utente, bloccandone l'accesso, fino a quando non viene pagato un riscatto.

3.2.3.4 Attacchi crittografici

Negli attacchi crittografici, l'attaccante viola il sistema di crittografia, che viene utilizzato dal sistema IoT proprio per garantire la riservatezza, l'integrità e l'autenticità dei dati scambiati.

- **Attacchi a Canale Laterale** *(Side Channel Attacks)*: l'attaccante sfrutta le informazioni che vengono emesse dai dispositivi durante le operazioni di crittografia. Queste informazioni non riguardano né il testo in chiaro né il testo cifrato, ma includono dati su potenza, tempo richiesto per eseguire l'operazione o frequenza di guasti. L'attaccante usa queste informazioni per recuperare la chiave crittografica.
  Esistono diversi tipi di attacchi tramite canali laterali, come gli attacchi temporali, che si basano sul tempo che il dispositivo impiega per compiere le operazioni di crittografia, analisi dei guasti, dove l'attaccante sfrutta eventuali errori o malfunzionamenti, e l'analisi della potenza, dove l'attaccante studia quanta energia il dispositivo consuma durante le operazioni di crittografia.

- **Attacchi di Criptoanalisi** *(Cryptanalysis Attacks)*: in questa tipologia d'attacco, l'attaccante è già in possesso del testo cifrato o del testo in chiaro, e vuole trovare la chiave crittografica usata. A seconda della metodologia utilizzata esistono vari tipi di attacchi:

  - *Ciphertext Only Attack*: in questo caso l'attaccante possiede solo il teso cifrato e cercherà di determinare il testo in chiaro corrispondente.
  - *Known-plaintext attack*: in questo caso l'attaccante conosce il testo in chiaro per alcune parti del testo cifrato. L'obiettivo è decriptare la parte rimantente.
  - *Chosen Plaintext Attack*: in questo caso l'attaccante ha la possibilità di scegliere quale testo in chiaro deve essere cifrato e cerca di trovare la chiave di crittografia.
  - *Chosen Ciphertext attack*): in questo caso l'attaccante, utilizzando il testo in chiaro del testo cifrato scelto, può trovare la chiave di crittografia.

- **Attacco con intermediario** (*Man-in-the-middle*): questo attacco avviene quando due utenti di un sistema si scambiano le chiavi crittografiche; l'avversario intercetta i messaggi che queste due entità si scambiano e cerca di inserirsi nella comunicazione, in modo da eseguire lui stesso lo scambio con le due entità. L'attaccante sarà in grado quindi di decifrare/cifrare qualsiasi dato proveniente da entrambi gli utenti, che invece penseranno di comunicare tra loro.

3.3 Sfide e opportunità future

Il panorama dell'IoMT è in continua evoluzione, andando a integrare tecnologie avanzate, come l'intelligenza artificiale, il *machine learning* e la *blockchain.*
Queste innovazioni non solo promettono di migliorare l'efficienza operativa dei dispositivi, ma aprono anche la strada a nuovi tecniche di sicurezza.

3.3.1 Utilizzo dell'intelligenza artificiale e del *machine learning*

Come descritto da Manickam *et al.* in [30], l'Intelligenza Artificiale (IA) migliora significativamente l'intervento umano nel trattamento e nella diagnosi clinica e può integrarsi ai dispositivi IoMT.
Sebbene l'interesse verso l'IA sia cresciuto negli ultimi anni, grazie alla sua capacità di processare grandi quantità di dati e produrre risultati accurati, il concetto era già stato introdotto da diversi ricercatori alla fine degli anni '40 [31], ponendo le basi per le indagini e gli studi attuali.
Uno dei fattori chiave che hanno favorito l'attuale espansione è il miglioramento della potenza di calcolo delle CPU e l'applicabilità delle GPU, che permettono di eseguire algoritmi complessi in modo rapido ed efficiente. Altro fattore chiave, è la disponibilità di grandi quantità di dati (*big data*), generati dalla crescente domanda degli utenti, necessari per analisi più approfondite e accurate.

Nel contesto medico, il Machine Learning (ML) viene utilizzato per applicazioni come la diagnosi o previsione dell'andamento di malattie sulla base di dati storici dei pazienti, pianificazione dei trattamenti e ricerca e sviluppo di nuovi farmaci.
È stato dimostrato come l'IA possa essere uno strumento di grande utilità nella diagnosi precoce di alzhaimer, cancro, diabete e problemi cardiaci [30].

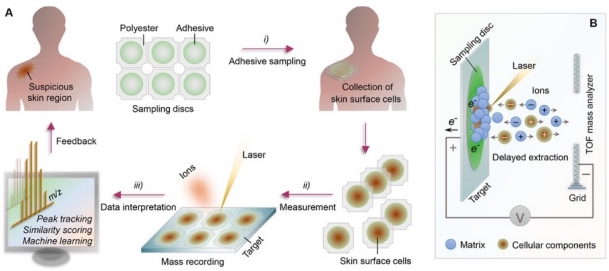

Figura 3.1: (A)Rappresentazione schematica della metodologia usata per identificazione cancro alla pelle. (B) Rappresentazione della spettrometria di massa (MALDI-TOF). [30]

Ad esempio Phillips *et al.* in [32], hanno utilizzato un algoritmo basato su IA per per l'identificazione di melanoma maligno da immagini di lesioni cutanee, mentre Zhu *et al.* hanno sviluppato una metodologia chimica per ottenere un monitoraggio della pelle rapido e non invasivo [33]: attraverso un campionamento adesivo vengono prelevate piccole quantità di pelle che saranno poi analizzate usando una macchina chiamata spettrometro di massa MALDI-TOF. I risultati vengono poi analizzati usando l'algoritmo di intelligenza artificiale per interpretarli rapidamente e correttamente. Il procedimento è illustrato nella Figura 3.1.

Un altro esempio di applicazione, lo possiamo trovare in [34], dove Alshareef *et al.* realizzano un modello per il monitoraggio dello stress.
Sono stati sviluppati diversi approcci per il monitoraggio dello stress che si basano su segnali biologici, tuttavia questi modelli tendono ad essere altamente personalizzati per persone specifiche e non si adattano bene a nuovi pazienti.
Questo significa che tali modelli funzionano bene quando monitorano persone per le quali sono già stati addestrati, ma tendono ad adattarsi troppo alle loro caratteristiche, come la loro fisiologia e il modo in cui reagiscono allo stress, e quindi non funzionano bene quando monitorano persone non precedentemente note al sistema.
L'articolo propone una soluzione a questo problema adottando un approccio di validazione *Leave-One-Subject-Out (LOSO)*. Questo metodo cerca di creare un modello che sia abbastanza generale da rilevare lo stress anche in individui non inclusi nel set di addestramento, migliorando la sua capacità di riconoscere lo stress in nuovi pazienti. In particolare il modello utilizza diversi sensori, come accelerometri, elettrocardiografi, termometri, per raccogliere dati fisiologici. I dati raccolti formano una sequenza di misurazioni nel tempo che devono essere analizzate dal modello per capire se la persona sta vivendo una condizione di stress.
Viene poi utilizzata una rete neurale per identificare relazioni tra i dati nelle sequenze temporali.
Viene utilizzato un metodo di validazione LOSO, il che significa che il modello viene addestra-

to su dati di tutti i soggetti tranne uno, e poi testato sull'individuo escluso, così da garantire che il modello possa generalizzare su pazienti mai visti prima.
Dopo aver processato i vari dati, il modello produce un *output* costituito da una classificazione binaria, che indica se la persona sta vivendo stress o meno. Tale modello superato quelli tradizionali ottenendo una precisione del 96%.

Un ulteriore esempio di utilizzo è il modello sviluppato da Khan *et al.* in [35] per il rilevamento di tumori celebrali.
Tradizionalmente i metodi utilizzati per rilevare tumori celebrali sono la biopsia e la valutazione delle Immagini a Risonanza Magnetica (MRI), i quali, però, possono essere soggetti a errori umani.
Pertanto, lo studio, esamina l'utilizzo del modello *Partial Tree* (PART) per classificare i tumori celebrali in base ai loro gradi (I-IV), confrontandolo con altri metodi utilizzati, tra cui CART, *Random forest* e *Random Tree*.
In particolare, il modello PART è un algoritmo di apprendimento supervisionato, che quindi impara a fare previsioni sulla base di dati etichettati, che combina le caratteristiche di due tecniche di apprendimento automatico:

- **C4.5:** è un algoritmo di costruzione di alberi decisionali

- **Ripper:** è un metodo che crea una serie di regole per arrivare alla classificazione.

Il modello PART parte dalle immagini MRI del cervello, per ricavarne caratteristiche importanti, come 'quanto è grande il tumore?' o 'in che zona si trova'.
Attraverso Ripper verrano create delle regole, come 'se il tumore è più grande di 2cm è probabile che sia maligno', queste regole verranno poi applicate attraverso PART a tutte le immagini. Se l'immagine rispetta una certa regola, il modello le assegna una determinata classe, come 'benigno' o 'maligno'.
Dopo aver applicato una regola, PART elimina i casi già classificati e continua con altre regole per classificare tutte le immagini.
La struttura del modello adottato è rappresentata dalla Figura 3.2. Tale modello è risultato più preciso di altri precedentemente utilizzati (oltre il 95%), ha un costo computazionale inferiore ed è resistente all'*overfitting*, ovvero la tendenza di adattarsi troppo bene ai dati di apprendimento e poco a quelli nuovi, grazie alla sua capacità di generare regole localmente.

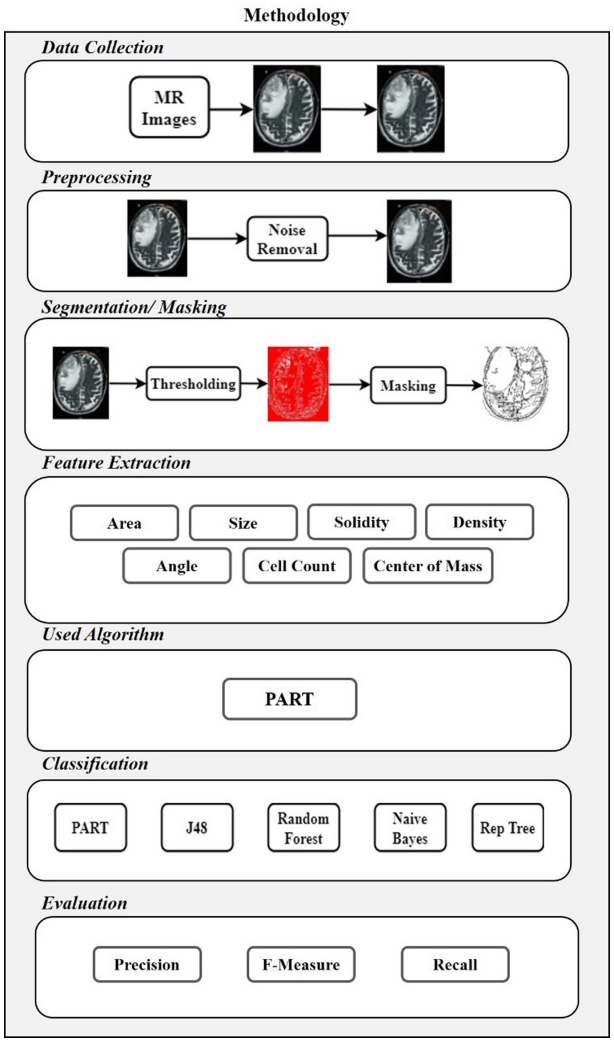

Figura 3.2: Metodologia proposta in [35]

3.3.2 Utilizzo della blockchain nei dispositivi IoMT

La tecnologia *blockchain*, descritta per la prima volta da Satoshi Nakamoto [36], consente di registrare e verificare transazioni o dati in modo sicuro, trasparente e immutabile.
È essenzialmente un registro digitale distribuito che viene mantenuto e aggiornato da una rete di nodi *peer-to-peer* anziché da un'unica entità centrale.
Le varie transazioni vengono registrate come un "blocco" di dati, e ogni blocco è crittograficamente collegato a quello che lo precede, in modo da creare una catena cronologica irreversibile: la *blockchain*, come raffigurato in Figura 3.3.
L'obiettivo di Nakamoto era proprio garantire trasparenza, sicurezza e tracciabilità delle transazioni senza la necessità di un'autorità centrale, e proprio per questo utilizza il concetto di *hash* [37].
L'hash è una stringa di lunghezza fissa che accompagna ogni blocco, qualsiasi modifica ai dati di un blocco altererebbe anche l'hash di quel blocco e di tutti i blocchi successivi, rendendo

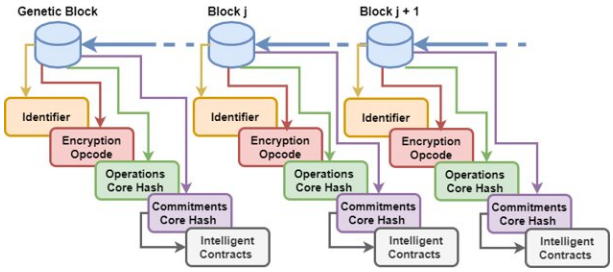

Figura 3.3: Architettura della blockchain [25].

praticamente impossibile che si modifichino transazioni senza essere rilevati.
Infine, per aggiungere nuovi blocchi alla catena, la maggior parte dei nodi nella rete deve concordare sulla validità delle transazioni stesse, questo avviene tramite specifici meccanismi di consenso, tra cui :

- *proof of work*: in questo metodo i nodi competono per risolvere problemi matematici complessi, il primo che riesce a trovare la soluzione aggiunge il nuovo blocco alla catena e viene ricompensato. I nodi non vincenti che hanno partecipato al consenso dovranno, invece, accertare che la soluzione trovata sia corretta.

- *proof of stake*: in questo sistema, i validatori vengono scelti in base alla quantità di beni digitali che possiedono e mettono in "stake" come garanzia. Chi viene scelto verifica il blocco e riceve una ricompensa.

Quindi, dati i suoi numerosi lati positivi, la *blockchain* può essere utilizzata anche in ambito sanitario per gestire e proteggere i dati sensibili dei pazienti, migliorando l'efficienza e l'affidabilità del sistema.

Tuttavia, l'integrazione della blockchain nell'IoMT presenta alcune sfide:

- Privacy: sebbene la *blockchain* offra una sicurezza intrinseca grazie alla sua struttura decentralizzata e immutabile, la gestione di grandi volumi di dati medici sensibili richiede soluzioni avanzate per garantire la privacy dei pazienti. La sfida è trovare un equilibrio tra proteggere la riservatezza e garantire l'integrità e verificabilità dei dati.

- Scalabilità: i dispositivi IoMT generano un'enorme quantità di dati, questo può generare problemi di scalabilità nella *blockchain*, poiché ogni transazione deve essere verificata e registrata da tutti i nodi della rete: questo può causare ritardi e intasamenti del sistema.

- Interoperabilità: i dispositivi IoMT provengono spesso da produttori diversi e utilizzano protocolli differenti. Integrare questi dispositivi in una blockchain unificata richiederebbe standard internazionali e l'interoperabilità tra le varie tecnologie.

Alcuni studi propongono possibili soluzioni a riguardo. Lakhan *et al.* sviluppano un modello chiamato *"Blockchain-Enabled Cost-Efficient Scheduling"* [38], che utilizza la *blockchain* per migliorare la pianificazione delle attività nell'IoMT. Questo modello si concentra sulla riduzione dei costi e della latenza, garantendo, al contempo, un'elevata sicurezza. BECSAF utilizza anche *smart contract* per garantire che i dati dei pazienti siano gestiti in modo sicuro ed efficiente. Le simulazioni effettuate dimostrano che questo approccio riduce significativamente i rischi di sicurezza, la latenza e i costi, rendendolo una soluzione promettente per l'integrazione della blockchain nell'IoMT.

Abbas *et al.*, invece, hanno sviluppato un modello chiamato "Blockchain-assisted Secure Data Management Framework (BSDMF)" [39], un sistema che utilizza la *blockchain* per la gestione sicura dei dati sanitari.
Questo modello si concentra sulla protezione dei dati durante il loro trasferimento e la loro gestione. BSDMF include meccanismi di crittografia e valutazione della fiducia tra i nodi della rete per garantire che solo gli utenti autorizzati possano accedere ai dati. I risultati sperimentali indicano che BSDMF raggiunge un alto livello di precisione e affidabilità, con tempi di risposta e latenza ridotti.

Un esempio di utilizzo in ambito sanitario lo possiamo trovare in [40]. Si tratta di un modello dove viene sfruttata la tecnologia *blockchain* per il monitoraggio dei pazienti. In particolare, i pazienti usano dei dispositivi medici indossabili, che monitorano costantemente i loro segnali vitali, e inviano i dati a un dipositivo chiamato Sensor Data Provider (SDP). Viene utilizzato il Patient-Centric Agent (PCA), il quale è un software che gestisce i dati raccolti da SDP, e classifica i dati in base alla loro rilevanza e può decidere di comprimere o archiviare tali dati.
Quando i dati sono considerati sensibili (ad esempio, rilevazioni anomale di segni vitali), il PCA decide di memorizzarli nella *blockchain*, questo perchè i dati aggiunti alla *blockchain* non possono essere modificati o cancellati. A differenza di altre *blockchain* pubbliche, il PCA seleziona i *miner*, quindi coloro che valideranno i nuovi blocchi, per ridurre il consumo energetico e migliorare le prestazioni. La struttura del modello adottato è rappresentata nella Figura 3.4.

Dato che i dispositivi medici indossabili hanno limitate risorse energetiche, Uddin *et al.* si sono concentrati sullo sviluppo di tecniche di crittografia e autenticazione leggere, adatte alla comunicazione tra i dispositivi IoMT e il SDP, nonché tra il SDP e il PCA.
La crittografia asimmetrica tradizionale è infatti troppo pesante per questi dispositivi: al suo posto, viene preferita la crittografia simmetrica, che richiede meno risorse computazionali ed energetiche, migliorando allo stesso tempo la sicurezza grazie all'uso di tecniche di crittografia

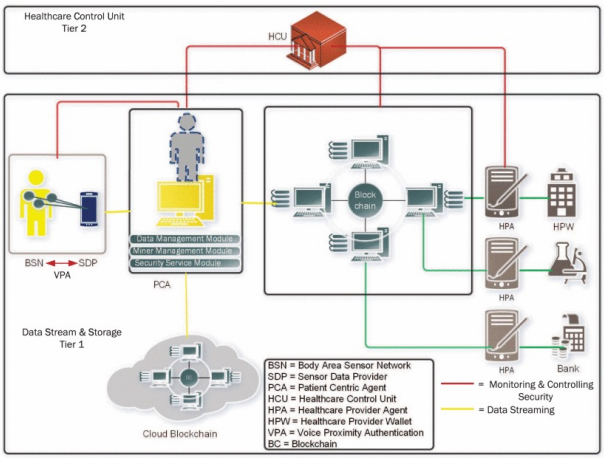

Figura 3.4: Architettura del modello [40]

come l'Keyed-Hash Message Authentication Code (HMAC), che combina un algoritmo di hash con una chiave segreta per creare un codice di autenticazione.
Inoltre, poiché i dispositivi IoMT generano un'enorme quantità di dati, è stato necessario implementare una pre-elaborazione dei dati prima che siano inviati alla *blockchain*.
I vantaggi di questa soluzione sono molteplici, innanzitutto viene garantita l'integrità dei dati, che una volta registrati non possono essere modificati senza autorizzazione, riduce i costi di comunicazione e il consumo energetico e non ha necessità di collaborare con terze parti.

Tuttavia, nonostante le numerose potenzialità di queste tecnologie, rimane essenziale la necessità di bilanciare l'innovazione tecnologica con la sicurezza e la privacy dei pazienti.
Le sfide legate alla scalabilità, all'interoperabilità e alla sicurezza devono essere affrontate con soluzioni innovative, ma anche con un approccio etico che metta al centro il benessere dei pazienti: solo in questo modo sarà possibile realizzare appieno il potenziale dell'IoMT, creando un ecosistema sanitario avanzato, sicuro e in grado di migliorare la qualità della vita dei pazienti senza compromettere i loro diritti fondamentali.
La strada da percorrere richiede quindi un equilibrio attento tra progresso tecnologico e tutela dei valori umani, per un futuro in cui la tecnologia e la sanità possano coesistere in modo armonioso e sostenibile.

Capitolo 4

La necessità di proteggere la privacy nei sistemi IoMT

4.1 Introduzione alla privacy nei dispositivi IoMT

La sicurezza dei dispositivi è essenziale per proteggerli da potenziali attacchi informatici, ma non è sufficiente per garantire una protezione assoluta dei dati.
Le tecniche fin qui analizzate, come la crittografia a chiave simmetrica, asimmetrica e i sistemi senza chiave, sono fondamentali per garantire la sicurezza delle comunicazioni e proteggere i dati da accessi non autorizzati. Tuttavia, la protezione dei dati va oltre la sicurezza tecnica e riguarda anche come questi vengono raccolti, trattati, e conservati. È fondamentale adottare una gestione responsabile delle informazioni, che garantisca trasparenza nei confronti degli utenti e rispetti i loro diritti.
Gli utenti dei dispositivi IoMT devono essere informati in modo chiaro su quali dati vengono raccolti, per quale scopo e per quanto tempo saranno conservati.
Solo attraverso una combinazione di sicurezza tecnica e un'adeguata gestione della privacy è possibile garantire una protezione efficace dei dati

4.1.1 Tipi di dati sensibili nei dispositivi IoMT

Nei sistemi IoMT, come detto in precedenza, vengono scambiati una vasta quantità di dati altamente sensibili, tra questi dati troviamo:

- **Informazioni Personali Identificabili (PII):** le informazioni personali identificabili sono quelle informazioni che possono essere utilizzate per identificare direttamente l'individuo (come nome, cognome, data di nascita), o che possono essere utilizzate insieme

ad altre informazioni per identificare un individuo. [41]
Questi dati vengono associati ai dati clinici e biometrici per fornire una visione completa della storia del paziente, ma la loro protezione è essenziale per evitare furti di identità.

- **Dati biometrici:** nel considerare i dati biometrici in questo contesto, è possibile fare una distinzione:
  - **Dati biometrici come identificatori**: in questo contesto, i dati biometrici sono usati per identificare in modo univoco una persona. Ad esempio, un dispositivo medico potrebbe richiedere l'impronta digitale di un paziente per autorizzare l'accesso ai suoi dati sanitari.
  - **Dati biometrici per monitoraggio della salute:** in questo caso ci si riferisce a dati raccolti, spesso in tempo reale, e utilizzati per monitorare le condizioni di salute del paziente o per il rilevamento precoce di potenziali anomalie. Ad esempio il battito cardiaco, la pressione sanguigna, i livelli di glucosio nel sangue, e altri segnali vitali.
- **Dati relativi alla diagnosi e al trattamento:** rientrano in questa categoria le informazioni relative alle diagnosi mediche e alle terapie prescritte.
- **Dati di localizzazione:** i dispositivi IoMT possono anche raccogliere dati di localizzazione per monitorare la posizione dei pazienti, ed eventualmente inviare supporto.

4.2 Normative e Regolamenti sulla Privacy

Per assicurare un elevato livello di sicurezza ai pazienti, le normative e regolamenti giocano un ruolo fondamentale. Esistono varie normative a riguardo che si possono applicare, anche se non ne è stata creata una *ad hoc* per i dispositivi IoMT, nel paragrafo successivo verranno indicate le principali.

4.2.1 Normative internazionali

4.2.1.1 Il Regolamento generale sulla protezione dei dati

Il GDPR, enrato in vigore nel 2018, è il regolamento più rilevante a livello europeo per la protezione dei dati personali e può essere applicato anche al settore sanitario e ai dispositivi IoMT [42]. Questo regolamento si applica a qualsiasi entità che tratti dati personali di cittadini

dell'Unione Europea, indipendentemente dalla sede geografica del titolare del trattamento. Di particolare rilevanza sono:

- **l'articolo 5**, che stabilisce i principi fondamentali nel trattamento dei dati, tra cui la minimizzazione dei dati (devono essere raccolti solo i dati strettamente necessari per le finalità dichiarate) e la limitazione delle finalità (i dati devono essere raccolti per scopi specifici e legittimi e non devono essere ulteriormente trattati in modo incompatibile con tali scopi).

- **l'articolo 6**, il quale stabilisce le basi legali che rendono legittimo il trattamento dei dati personali: prima di trattare i dati personali di un individuo, l'entità responsabile (il titolare del trattamento) deve assicurarsi che esista una base giuridica valida per tale trattamento.
  Il consenso dell'interessato è una delle basi giuridiche più utilizzate, tale consenso deve essere:

  - libero: il consenso non deve essere obbligato o forzato.
  - esplicito: il consenso deve essere dato chiaramente e senza ambiguità.
  - informato: l'interessato deve essere pienamente informato su come verranno trattati i suoi dati.
  - revocabile: il consenso può essere revocato in qualsiasi momento senza penalità per l'interessato.

  Altre basi legali previste dall'articolo 6 sono:

  - l'esecuzione di un contratto: il trattamento dei dati è lecito se necessario per l'esecuzione di un contratto di cui l'interessato è parte.
  - l'obbligo legale: il trattamento è lecito se necessario per adempiere a un obbligo legale al quale è soggetto il titolare del trattamento, ad esempio un ospedale, potrebbe dover trattare dati personali per la comunicazione di determinate malattie contagiose alle autorità sanitarie.
  - interessi vitali dell'interessato o di un'altra persona: il trattamento dei dati personali è consentito quando è necessario per proteggere gli interessi vitali dell'interessato o di un'altra persona, questo è particolarmente rilevante in caso di emergenze o quando il paziente non è cosciente.

- esercizio di pubblici poteri: questa base legale si applica quando il trattamento è necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di poteri pubblici di cui è investito il titolare del trattamento, ad esempio la raccolta di dati sanitari per monitorare un'epidemia.
- legittimo interesse del titolare del trattamento: il trattamento è lecito se è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a meno che tali interessi non siano superati dagli interessi o dai diritti e dalle libertà fondamentali dell'interessato.

- **l'articolo 9**, il quale riguarda il trattamento delle categorie particolari di dati, chiamati comunemente sensibili. In particolare stabilisce come il trattamento di dati sanitari sia vietato, salvo specifiche eccezioni, come il consenso dell'interessato o la tutela degli interessi vitali.

- **l'articolo 25**, stabilisce i principi di privacy *by design* e privacy *by default*: secondo il principio di privacy *by design* i dispositivi IoMT devono essere progettati, fin dal principio, con apposite misure di sicurezza per proteggere i dati personali durante tutte le fasi del loro ciclo di vita. Privacy *by default* significa, invece, che il trattamento dei dati personali deve essere limitato al minimo necessario.

- **l'articolo 32**, impone l'obbligo di adottare misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato come la cifratura dei dati.

- **gli articoli 44-50**, stabiliscono che i dati sanitari non debbano essere trasferiti in Paesi terzi, salvo eccezioni.

4.2.1.2 Health insurance portability and accountability act (HIPAA)

La normativa HIPAA viene applicata negli Stati Uniti ed è utilizzata proprio per la protezione dei dati sanitari [43]. Tra gli articoli più rilevanti possiamo trovare:

- **Privacy rule** (45 CFR Part 160 e 164, Subpart E): questa è una sezione centrale della normativa, dove si stabiliscono per esempio le condizioni in cui i dati sanitari possano essere utilizzati o divulgati, si stabilisce la necessità del consenso da parte del paziente per l'utilizzo dei dati, viene poi descritto come i dati sanitari possano essere de-identificati, per rendere i pazienti non identificabili.

- **Security rule** (45 CFR Part 160 e 164, Subpart C): questa sezione stabilisce gli standard di sicurezza per proteggere i dati sanitari. In particolare, si evidenzia come l'entità devono garantire la riservatezza, l'integrità e la disponibilità dei dati; vengono definite misure tecniche, come la cifratura e la gestione degli accessi, per garantire la protezione.
- **Breach notification rule**: questa regola impone alle entità di comunicare eventuali violazioni dei dati ai pazienti, entro un determinato periodo di tempo

4.2.1.3 Direttiva (UE) 2022/2555

Sebbene la direttiva Network and Information Security Directive (NIS 2) sia focalizzata sulla sicurezza delle reti e dei sistemi informatici, è rilevante per l'IoMT in quanto riconosce le infrastrutture sanitarie come settore critico, andando quindi ad imporre rigorosi obblighi da rispettare, ad esempio: le infrastrutture devono avere delle misure di gestione del rischio, hanno l'obbligo di notificare tempestivamente gli incidenti di sicurezza, devono garantire che i loro sistemi siano resilienti ed effettuare delle valutazioni periodiche sulla sicurezza delle reti. Inoltre la NIS 2 introduce una serie di sanzioni per le organizzazioni che non rispettano tali obblighi. [44]

4.2.2 Standard di sicurezza internazionali

Gli standard sono dei documenti tecnici che definiscono dei requisiti che determinati prodotti o servizi devono soddisfare, o descrivono il modo in cui una determinata attività dovrebbe svolgersi con l'obiettivo di garantire qualità, sicurezza o interoperabilità, senza però imporre obblighi vincolanti. Può anche essere una guida che fornisce informazioni generali su un argomento o un glossario che definisce il vocabolario impiegato in un settore.
In generale gli standard non sono vincolanti, tuttavia, l'interoperabilità e la compatibilità possono rendere uno standard *de facto* vincolante, poiché il mancato rispetto di alcuni standard ampiamente adottati può rendere difficile l'interoperabilità [45].

4.2.2.1 ISO/IEC 27701:2019

Gli standard ISO sono elaborati da membri volontari che partecipano ai lavori di un'organizzazione di standardizzazione (*Formal Standardization Organization*), essi hanno il diritto di presentare proposte di standard che saranno poi valutate da comitati competenti [45]. Questo standard fornisce una guida per l'implementazione di un sistema di gestione della privacy (Privacy Information Management System) in linea con le normative come il GDPR.

4.2.2.2 ISO/IEC 29100

Si tratta di un ulteriore standard ISO che fornisce un quadro di riferimento per la gestione della privacy. Questo standard si sovrappone in alcuni punti al GDPR, sebbene non sia una guida alla sua applicazione. In particolare, questo standard definisce i principi fondamentali della privacy, come la limitazione della raccolta dei dati, l'uso limitato dei dati personali e la sicurezza dei dati, e stabilisce le pratiche e le procedure necessarie per proteggere i dati personali [41].

4.3 Possibili soluzioni

Nell'articolo di Hireche *et al.* [6] vengono descritti alcuni modelli per assicurare la protezione della privacy nei dispositivi IoMT.
In particolare, Cano e Cañavate-Sanchez [46] sviluppano un modello basato sull'utilizzo di un Algoritmo di Firma Digitale a Curva Ellittica (ECDSA) integrato al concetto di doppia firma. La doppia firma è un meccanismo che consente di collegare due insiemi di informazioni in modo che ciascuno rimanga nascosto a una delle parti coinvolte, garantendo allo stesso tempo autenticità e integrità. Questo concetto è nato nel contesto dell'*e-commerce*, dove si desidera mantenere segrete alcune informazioni a specifiche entità.
In questo contesto specifico la doppia firma serve affinchè il cloud possa verificare se i dati provengono da un dispositivo IoMT autentico senza rivelare l'identità di quest'ultimo.

L'ECDSA è un algoritmo di crittografia asimmetrica che utilizza le curve ellittiche per generare una firma digitale. L'ECDSA si basa sulle curve ellittiche perché queste consentono di raggiungere un elevato livello di sicurezza con chiavi più corte rispetto ad altri algoritmi, consentendo così di ridurre il costo computazionale ed energetico. In particolare, il mittente usa la propria chiave privata per generare una firma, da inviare assieme al messaggio. Il destinatario usa la chiave pubblica del mittente per verificare che la firma corrisponda all'*hash* del messaggio ricevuto.
Nel modello elaborato da Cano e Cañavate-Sanchez, i dispositivi IoMT raccolgono i dati sanitari e calcolano il corrispettivo *hash*, viene poi calcolato anche un *hash* dell'identificativo del dispositivo IoMT, che garantisce l'autenticità dell'origine dei dati. Successivamente i due *hash* vengono concatenati, vengono poi firmati con la chiave privata del dispositivo, qui viene utilizzato l'algoritmo ECDSA che sfrutta le curve ellittiche per creare una doppia firma.
Il dispositivo IoMT invia poi i dati firmati al dispositivo di *edge computing*, il quale userà la

chiave pubblica del dispositivo per verificare che i dati non siano stati alterati e provengano proprio da quel dispositivo. L'*edge computing* non ha accesso ai dati sanitari crittografati, quindi non può leggere il contenuto dei dati raccolti, garantendo la privacy dei dati, li potrà però inoltrare al *cloud*.

Il *cloud* riceve i dati crittografati dal dispositivo di *edge computing* e li decifra con la sua chiave privata, verificando che i dati non siano stati manomessi. Sebbene il *cloud* possa accedere ai dati sanitari, l'identità del dispositivo IoMT che li ha inviati rimane anonima, garantendo la protezione dell'identità.

I vantaggi del modello sono diversi, tra cui: la privacy dei dati che non sono accessibili ai dipositivi di *edge computing* e l'identità del dispositivo rimane nascosta al *cloud*. Inoltre grazie all'uso della firma digitale, sia il *cloud* che i dispositivi di *edge computing* possono verificare che i dati provengano da un dispositivo IoMT autentico e che non siano stati alterati.

Un altro esempio è quello proposto da Ahamad e Pathan [47], i quali hanno sviluppato un modello chiamato Security and Privacy-aware Mobile Healthcare Framework (SPMHF), progettato per garantire sicurezza e privacy dei dati, e allo stesso tempo conformità con l'HIPAA. Tale modello è rappresentato in Figura 4.1.

Come si può vedere in figura, innanzitutto i dati sanitari vengono raccolti ogni minuto attraverso sensori, sia IMDs che IoWD, vengono poi trasmessi allo *smartphone* del paziente tramite Bluetooth. I dati vengono poi cifrati utilizzando una chiave simmetrica condivisa tra l'app sanitaria del sensore e l'app sanitaria del telefono del paziente. L'app sanitaria sullo *smartphone* del paziente decifra il messaggio ricevuto dal sensore. Una volta decifrato, il messaggio viene inoltrato in modo sicuro al *Trusted Platform Module (TPM)* dell'ospedale, che è un hardware dedicato alla sicurezza, tramite il *cloud*. Qui vengono verificati i dati. Se i valori raccolti dai sensori sono nei limiti normali, l'ospedale aggiorna semplicemente il *database*. In caso di valori anomali, invece, viene inviato un avviso al medico e ai familiari del paziente. Se necessario, può anche inviare un'ambulanza al luogo in cui si trova il paziente. In questo modo, si garantisce un intervento rapido in situazioni di emergenza.

I dati vengono cifrati usando delle chiavi simmetriche. Queste chiavi sono condivise tra l'applicazione sanitaria del sensore e l'applicazione sanitaria dello *smartphone* del paziente. Per garantire più sicurezza, le chiavi vengono rigenerate ad ogni sessione di comunicazione utilizzando algoritmi di *hashing*.

Il sistema, inoltre, sfrutta la White Box Cryptography (WBC) per garantire che le chiavi crittografiche siano conservate in modo sicuro all'interno dell'app sanitaria. La WBC è particolarmente importante perché protegge le chiavi anche se un attaccante ha pieno accesso al

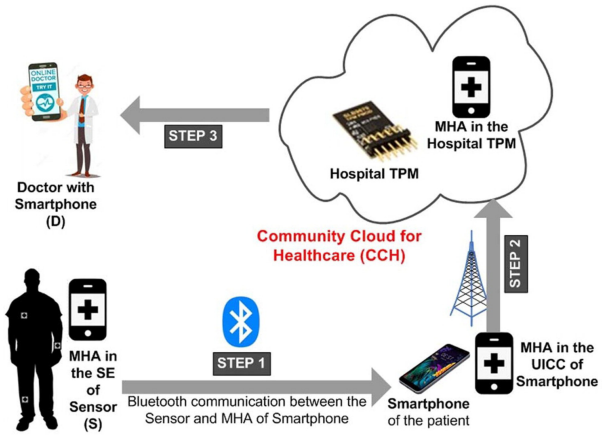

Figura 4.1: Security and Privacy-aware Mobile Healthcare Framework (SPMHF) [47]

dispositivo. Questa tecnica consente di mantenere le chiavi nascoste e sicure all'interno dell'applicazione, garantendo che non vengano esposte, anche in ambienti non sicuri (come lo *smartphone* dell'utente).

4.4 Prospettive future

In un contesto in cui i dispositivi IoMT sono sempre più diffusi e integrati nella vita quotidiana, è cruciale aumentare la consapevolezza degli utenti sui rischi legati alla gestione e alla protezione dei propri dati personali.

Tenendo conto della tipologia di dati, particolarmente sensibili, è essenziale che gli utenti siano consapevoli e abbiano il controllo di come i loro dati vengano utilizzati.

Le aziende e le istituzioni sanitarie giocano un ruolo fondamentale nel promuovere questa consapevolezza: devono fornire informazioni chiare e accessibili riguardo ai diritti degli utenti, spiegare loro come vengono trattati i dati e garantire che siano disponibili strumenti per gestire e limitare l'accesso alle informazioni personali.

Migliorare le misure di protezione della privacy non solo garantirà il rispetto dei diritti individuali, ma favorirà anche una maggiore adozione di queste tecnologie, che potranno portare a un sistema sanitario più efficiente, personalizzato e sicuro.

Solo attraverso una collaborazione attiva tra utenti, aziende e legislatore sarà possibile creare un ambiente più sicuro, in cui ogni individuo possa prendere decisioni informate e consapevoli.

In definitiva, la sfida principale consiste nel garantire che la protezione della privacy non sia percepita come un ostacolo all'innovazione, ma piuttosto come una componente essenziale per il suo successo a lungo termine.

Capitolo 5

Analisi di un *framework* di sicurezza

5.1 Introduzione

Come visto finora, il crescente utilizzo dell'IoMT ha offerto nuove opportunità per migliorare il trattamento dei pazienti, rivoluzionando così il settore sanitario. Tuttavia, questa interconnessione dei dispositivi medici può far nascere significative sfide di sicurezza.
In questo capitolo verrà analizzato un *framework* di sicurezza per l'IoMT, che è stato proposto da Alzahrani *et al.* in [48] per affrontare queste sfide.
Questo *framework* combina due metodologie di analisi decisionale multi-criterio: il Fuzzy Analytic Hierachy Process (FUZZY AHP) e il Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), al fine di selezionare e valutare le migliori soluzioni per la sicurezza dei dispositivi IoMT. Il *framework* è rappresentato in Figura 5.1.

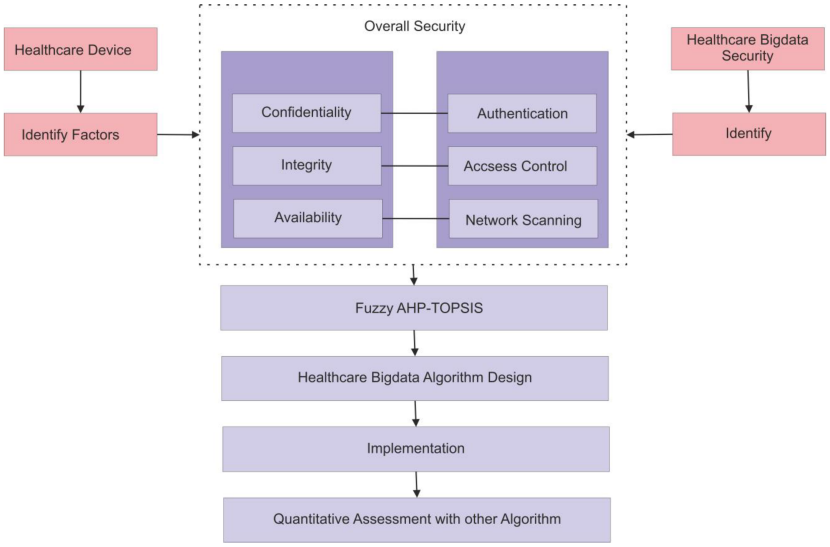

Figura 5.1: Struttura del framework [48].

5.2 Tipologie di attacco e vettori di attacco

Nel presente *framework* vengono evidenziati quali possono essere le varie superfici di attacco, ossia i punti vulnerabili attraverso cui gli attaccanti possono penetrare nel sistema:

- **Superficie di attacco umana:** si riferisce a minacce interne, come attacchi di *phishing* e manipolazioni psicologiche, come il *social engineering*, la maggior parte delle volte effettuati da personale interno con autorizzazioni elevate, che può accedere ai sistemi in modo non autorizzato, intenzionalmente o accidentalmente.

- **Superficie di attacco dei protocolli di comunicazione:** le vulnerabilità dei protocolli di comunicazione possono essere sfruttate per attacchi come, *man in the middle*, *DDoS* o *spoofing*.

- **Superficie di attacco fisica:** include attacchi che richiedono l'accesso fisico ai dispositivi, come l'utilizzo di chiavette USB infette. Gli attacchi *side-channel* (attacchi collaterali) possono sfruttare i consumi energetici o altre caratteristiche del dispositivo per ricavare informazioni sensibili.

- **Superficie di attacco aggregata:** si tratta di attacchi che sfruttano combinazioni di vulnerabilità, quindi a livello di persone, di reti e sistemi, per attacchi più complessi.

Tra i vettori di attacco, quindi le diverse modalità attraverso cui gli aggressori possono penetrare nel sistema, nel *framework* troviamo:

- **Archiviazione di dati nel *cloud*:** i dati sanitari vegono spesso archiviati nel *cloud*, e, se manca un'adeguata autenticazione, crittografia o controlli di accesso, gli *hacker* potrebbero accedere a tali dati più facilmente.

- **Connessione del *gateway* al *cloud*:** i dispositivi medici spesso si collegano al *cloud* tramite i *gateway*, ossia dispositivi intermedi. Se i *gateway* non sono adeguatamente protetti, possono diventare un punto d'accesso per gli attacchi che compromettono i dati in transito tra i dispositivi e il *cloud*.

- ***Software* e *hardware* vulnerabili:** i dispositivi IoMT potrebbero avere vulnerabilità nel loro *software*, come una mancanza di aggiornamenti di sicurezza, o utilizzare *hardware* compromessi. Gli attaccanti possono sfruttare queste debolezze per introdurre *malware* nel dispositivo.

- **Protocollo di comunicazione:** i dispositivi IoMT utilizzano protocolli di comunicazione *wireless*, come Wi-FI o Bluetooth, che potrebbero essere obsoleti o configurati in modo errato, facilitando la suscebilità del sistema ad attacchi quali *man in the middle*, *spoofing* o *denial of service*.

- **Connettività delle applicazioni:** le applicazioni utilizzate per monitorare o gestire i dispositivi IoMT spesso si connettono ai dispositivi tramite Wi-Fi o altre reti. Se queste applicazioni non hanno sufficienti controlli di sicurezza (come crittografia o autenticazione), potrebbero essere un altro vettore di attacco.

5.3 Fattori di sicurezza

Il *framework* si basa su tre principali fattori di sicurezza, che devono essere presi in considerazione per garantire la protezione e l'affidabilità dei dispositivi: riservatezza, disponibilità e integrità, definiti nella Sezione 3.

Dopo aver identificato questi attributi di sicurezza, il *framework* spiega come i sistemi di sicurezza debbano essere progettati per mitigare i danni o, in alcuni casi, eliminarli completamente. A tal fine, si implementano diversi meccanismi di difesa che affrontano sia gli attacchi diretti sia quelli indiretti. Gli attacchi diretti sono quelli che mirano esplicitamente a violare una vulnerabilità del sistema, come tentativi di accesso non autorizzato. Gli attacchi indiretti, invece, sfruttano vulnerabilità esterne o terze parti per compromettere la sicurezza, ad esempio attacchi di *phishing*.
Uno degli strumenti centrali in questo contesto è il monitoraggio delle reti. Il monitoraggio costante delle reti IoMT permette di rilevare attività anomale, traffico sospetto o accessi non autorizzati, fornendo un quadro in tempo reale dello stato di sicurezza della rete. Grazie a tecniche avanzate di analisi del traffico e rilevamento delle intrusioni il sistema può individuare *pattern* che indicano tentativi di violazione delle reti.
Inoltre, l'uso di certificati digitali diventa essenziale per garantire che solo i dispositivi e gli utenti autorizzati possano accedere alle informazioni, mentre l'uso della crittografia è fondamentale sia per proteggere i dati in transito sia quelli archiviati.

Un altro aspetto importante trattato è la capacità di rilevamento degli attacchi: il sistema di sicurezza deve essere in grado di monitorare e rilevare eventuali tentativi di attacco, definirne il tipo e l'origine.

5.4 Metodo integrato FUZZY AHP-TOPSIS

Il *framework* utilizza il metodo integrato FUZZY AHP - TOPSIS per selezionare le strategie di sicurezza più appropiate per i dispositivi IoMT, tenendo conto di criteri e alternative multiple.

L'AHP è un metodo utilizzato per prendere decisioni complesse in cui si devono valutare diverse alternative in base a più criteri. L'idea principale è scomporre il problema in una gerarchia di obiettivi, criteri e sottocriteri per poi valutare e confrontare le alternative.

Il metodo FUZZY AHP, migliora il metodo tradizionale AHP introducendo la logica *fuzzy*, che consente di gestire l'incertezza e l'imprecisione. Nel contesto informatico ci possono essere, infatti, numerose incertezze, ad esempio non è sempre possibile valutare con precisione quale sia il rischio di una specifica vulnerabilità o l'efficacia di una determinata misura di sicurezza. Il metodo FUZZY AHP prevede inanzittutto di scomporre il problema decisionale in una struttura gerarchica a diversi livelli, come mostrato in Figura 5.2, ad esempio:

- **obiettivo:** trovare la migliore strategia di sicurezza
- **criteri:** i principali fattori che devono essere considerati per valutare la sicurezza del sistema. In Figura 5.2 sono rappresentati da:
  - livello di compromissione (T1)
  - integrità, disponibilità e riservatezza (T2)
  - tipologia di attacco (T3)
  - origine dell'attacco (T4)
  - livello dell'attacco (T5)
- **alternative:** le soluzioni da valutare e confrontare. In Figura 5.2, le alternative sono rappresentate dai nodi A1, A2, A3, A4, A5, e A6.

Successivamente si procede a valutare i criteri e le alternative a coppie rispetto all'obiettivo. Nel metodo FUZZY AHP si utilizzano numeri *fuzzy*, ovvero una triade di numeri che rappresenta una stima minima, media e massima.

Dopo aver fatto tutti i confronti tra i criteri, bisogna calcolare i pesi relativi di ciascun criterio. Questo step permette di capire quanto ciascun criterio pesa nell'influenzare la decisione finale. Anche in questo caso i pesi sono espressi come numeri *fuzzy*. Successivamente i pesi vanno trasformati in numeri reali, solitamente trovando la media dei valori *fuzzy*. Poi si moltiplicano i pesi ottenuti per ogni alternativa con i pesi dei criteri corrispondenti e si sommano i

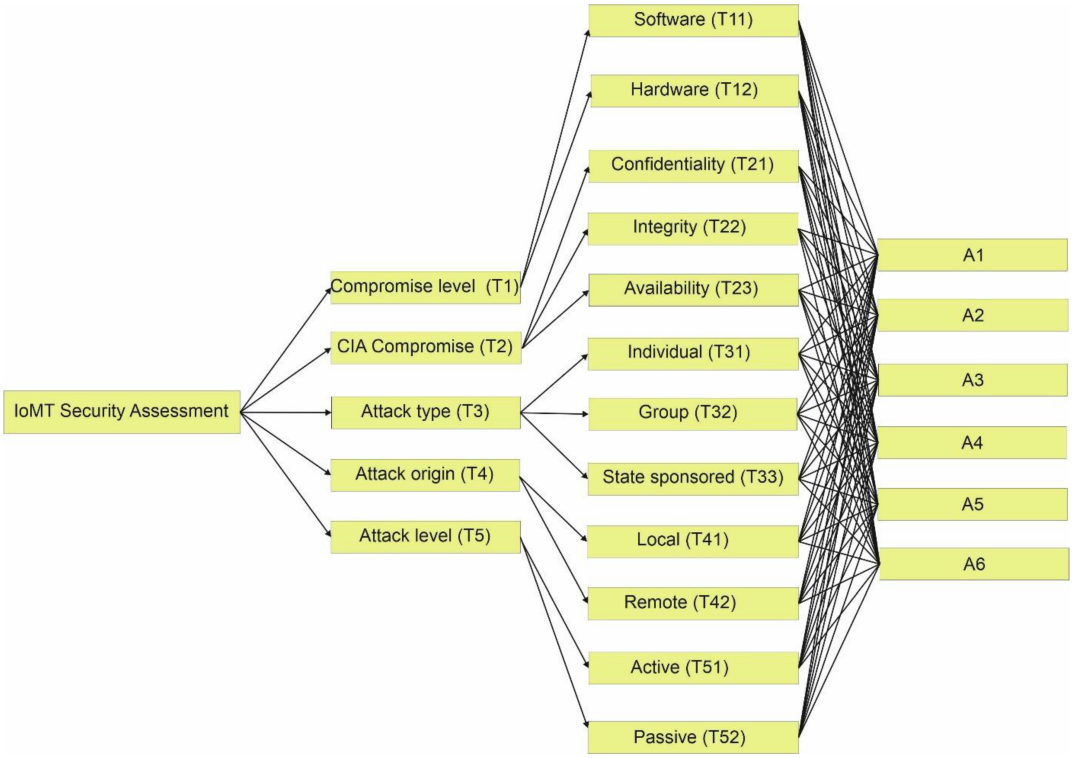

Figura 5.2: Struttura gerarchica per la valutazione delle alternative [48].

risultati per ottenere un punteggio complessivo per ciascuna alternativa. Dopo aver calcolato i punteggi per tutte le alternative, quella con il punteggio più alto sarà la soluzione preferita rispetto all'obiettivo iniziale.

Dopo aver determinato i pesi dei criteri con FUZZY AHP, entra in gioco il metodo TOPSIS. Questo metodo è utilizzato per classificare e selezionare le alternative migliori, cercando quella che più si avvicina alla "soluzione ideale", cioè la combinazione perfetta di tutti e tre i criteri. Ogni alternativa viene valutata per ciascun criterio. Questa valutazione può essere data in modo numerico, creando una matrice decisionale. Fatto questo bisogna identificare due scenari:

- **soluzione ideale positiva:** rappresenta lo scenario migliore per ciascun criterio
- **soluzione ideale negativa:** rappresenta lo scenario peggiore per ciascun criterio

Ogni alternativa viene valutata in funzione di quanto è vicina alla soluzione ideale positiva e quanto è lontana dalla soluzione negativa, utilizzando la distanza euclidea, consentendo così di identificare la misura di sicurezza che bilancia meglio tutti i fattori di rischio e beneficio. Si calcola poi il punteggio relativo C_i con la seguente formula:

$$C_i = \frac{D_i^-}{D_i^+ + D_i^-}, \tag{5.1}$$

dove D_i^- è la distanza dalla soluzione negativa mentre D_i^+ è la distanza dalla soluzione ideale positiva. Il risultato sarà compreso tra 0 e 1:

- più C_i è vicino a 1, migliore è l'alternativa
- più C_i è vicino a 0, peggiore è l'alternativa

L'alternativa con il punteggio più alto è quella che si avvicina di più alla soluzione ideale e che si distanzia di più da quella negativa.

5.5 Risultati

Nel *framework* sono state analizzate diverse alternative di sicurezza per i dispositivi IoMT. I dati utilizzati per l'analisi sono stati ottenuti tramite questionari somministrati a 85 esperti di sicurezza, provenienti sia dal settore accademico sia da quello industriale. Gli esperti hanno fornito le loro valutazioni sui vari aspetti della sicurezza dei dispositivi IoMT, aiutando così a stabilire un confronto tra le diverse alternative di sicurezza. I criteri di valutazione includevano la capacità delle soluzioni di proteggere la riservatezza dei dati, mantenere l'integrità delle informazioni, garantire la disponibilità dei sistemi, il tipo, l'origine e il livello di attacco, come raffigurato in Figura 5.2.

Ogni alternativa è stata valutata rispetto ai criteri utilizzando i pesi calcolati attraverso il metodo FUZZY AHP, per poi utilizzare il metodo TOPSIS per calcolare la distanza euclidea rispetto alla soluzione ideale positiva e negativa. I punteggi relativi delle sei alternative sono rappresentati dal diagramma in Figura 5.3:

La soluzione 'A2' ha ottenuto il punteggio più alto, quindi, tra le alternative analizzate, è risultata quella che meglio risponde ai criteri di sicurezza stabiliti. Questo la rende la scelta preferibile per garantire la protezione dei dispositivi IoMT.
Al contrario, l'alternativa 'A6' ha ottenuto il punteggio di sicurezza più basso, risultando particolarmente vulnerabile.

5.6 Note conclusive

I dispositivi IoMT presentano vulnerabilità sia nelle fasi di progettazione che post - commercializzazione, che li espongono a minacce informatiche crescenti, tanto in numero, quanto in complessità.

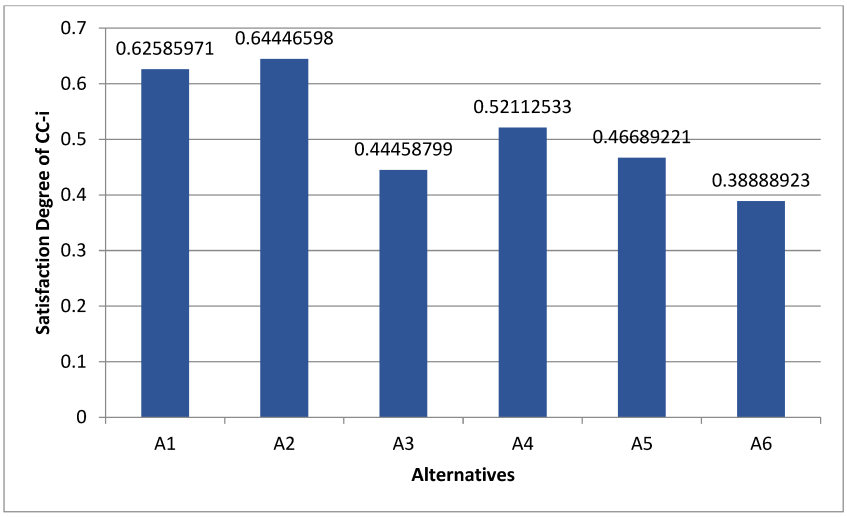

Figura 5.3: Grado di soddisfazione C_i delle alternative nel framework [48]

I dati sanitari generati da questi dispositivi sono altrettanto vulnerabili, essendo spesso inviati nel *cloud* per essere elaborati: qualsiasi modifica apportata ai dati durante il processo di elaborazione può avere conseguenze gravi, come mettere in pericolo la vita dei pazienti.

In questo capitolo è stato analizzato un *framework* di sicurezza, proposto da Alzahrani *et al.*, che integra le metodologie FUZZY AHP-TOPSIS, con lo scopo di selezionare le migliori strategie di sicurezza per i dispositivi IoMT. Nonostante l'efficacia del *framework* proposto, i ricercatori suggeriscono che altri approcci multi-criterio come ANP, ELECTRE, VIKOR e PROMETHEUS, potrebbero offrire ulteriori vantaggi per raffinare ulteriormente le valutazioni di sicurezza.

In definitiva, questo studio rappresenta una solida base per migliorare la protezione dei dispositivi IoMT e dei dati sensibili che essi trattano, ponendo le fondamenta per future ricerche e miglioramenti nei sistemi di sicurezza del settore sanitario.

Capitolo 6

Conclusioni

L'IoMT si sta rapidamente affermando come una tecnologia fondamentale per rivoluzionare il settore sanitario offrendo nuove opportunità per il monitoraggio, il trattamento e la gestione dei pazienti.

Tuttavia, come emerso dall'analisi condotta in questa Tesi, l'adozione di sistemi IoMT presenta delle questioni critiche in tema di sicurezza e protezione della *privacy*. La natura interconnessa ed eterogenea dei dispositivi medici, rende tali sistemi vulnerabili a una vasta gamma di minacce, dalle violazioni dei dati personali agli attacchi informatici sui dispositivi stessi.

Per affrontare queste problematiche, alcune delle soluzioni discusse sono: l'utilizzo della *blockchain*, dell'intelligenza artificiale e della crittografia. È importante però sottolineare che l'efficacia di tali soluzioni dipende anche dalla creazione di standard di sicurezza specifici per l'IoMT e dall'adozione di normative più stringenti in materia di protezione dati.

Guardando al futuro è chiaro che l'IoMT continuerà ad evolvere, portando con sé nuove opportunità e nuove sfide. L'intelligenza artificiale e la *blockchain*, in particolare, potranno svolgere un ruolo cruciale nel migliorare la sicurezza e la *privacy* dei sistemi sanitari, ottimizzando la gestione dei dati e prevenendo attacchi informatici. Sarà, però, fondamentale bilanciare l'innovazione tecnologica con la tutela dei diritti fondamentali dei pazienti, garantendo che il progresso non comprometta la sicurezza e la fiducia nelle nuove tecnologie.

In definitiva, l'IoMT ha le potenzialità per rivoluzionare il settore sanitario, ma la sua diffusione su larga scala richiederà un impegno continuo nel cercare possibili soluzioni sempre più sicure ed efficienti. Solo attraverso un approccio olistico, che coniughi innovazione tecnologica, regolamentazione e attenzione alla *privacy*, sarà possibile realizzare appieno le promesse di questa tecnologia emergente, creando un ecosistema sanitario più sicuro e sostenibile.

Acronimi

IoT Internet of Things

IoMT Internet of Medical Things

DDoS Distributed Denial of Service

IA Intelligenza Artificiale

ML Machine Learning

GDPR Regolamento generale sulla protezione dei dati

HIPAA Health insurance portability and accountability act

NIS 2 Network and Information Security Directive

LOSO Leave-One-Subject-Out

MRI Immagini a Risonanza Magnetica

PART *Partial Tree*

SDP Sensor Data Provider

PCA Patient-Centric Agent

HMAC Keyed-Hash Message Authentication Code

IMDs Dispositivi Medici Impiantabili

IoWD Dispositivi Indossabili

NFC Near-Field Communication

PAN Reti di Area Personale

ECG Elettrocardiografia

6LowPan Low Power Personal Area Network

RFID Radio Frequency Identification

BLE Bluetooth Low Energy

LoRaWAN Long Range Wide Area Network

IETF Internet Engineering Task Force

COAP Constrained application protocol

HTTP Hypertext Transfer Protocol

UDP User Datagram Protocol

TCP Transmission Control Protocol

MQTT Message Queue Telemetry Transport

IoTSF Iot Security Foundation

IIC Industrial Internet Consortium

DNS Domain Name System

ECDSA Algoritmo di Firma Digitale a Curva Ellittica

SPMHF Security and Privacy-aware Mobile Healthcare Framework

BSDMF Blockchain-assisted Secure Data Management Framework

WBC White Box Cryptography

PII Informazioni Personali Identificabili

TPM Trusted Platform Module

FUZZY AHP Fuzzy Analytic Hierachy Process

TOPSIS Technique for Order Preference by Similarity to Ideal Solution

Elenco delle figure

Bibliografia

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[2] K. Ashton *et al.*, "That 'internet of things' thing," *RFID journal*, vol. 22, no. 7, pp. 97–114, 2009.

[3] S. Tripathi, V. Makwana, M. Kumhar, H. Trivedi, J. Bhatia, S. Tanwar, and H. Shahinzadeh, "IoMT-Enabled Smart Healthcare: State-of-the-Art, Security and Future Directions," in *2023 14th International Conference on Information and Knowledge Technology (IKT)*, pp. 36–43, IEEE, 2023.

[4] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent advances in the internet-of-medical-things (IoMT) systems security," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8707–8718, 2020.

[5] M. A. Jabraeil Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, F. Norouzi, M. A. Jabraeil Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, and F. Norouzi, "IoT architecture," *Towards the Internet of Things: Architectures, Security, and Applications*, pp. 9–31, 2020.

[6] R. Hireche, H. Mansouri, and A.-S. K. Pathan, "Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 640–661, 2022.

[7] "IEEE Standard for Low-Rate Wireless Networks Corrigendum 1: Correction of Errors Preventing Backward Compatibility," *IEEE Std 802.15.4-2020/Cor 1-2022 (Corrigendum to IEEE Std 802.15.4-2020 as amended by IEEE Std 802.15.4z-2020, IEEE Std 802.15.4w-2020, IEEE Std 802.15.4y-2021, and IEEE Std 802.15.4aa-2022)*, pp. 1–22, 2023.

[8] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in IoMT communications: A survey," *Sensors*, vol. 20, no. 17, p. 4828, 2020.

[9] E. Chiappini, S. Sollai, R. Longhi, L. Morandini, A. Laghi, C. E. Osio, M. Persiani, S. Lonati, R. Picchi, F. Bonsignori, *et al.*, "Performance of non-contact infrared thermometer for detecting febrile children in hospital and ambulatory settings," *Journal of clinical nursing*, vol. 20, no. 9-10, pp. 1311–1318, 2011.

[10] B. J. Saradha, G. Vijayshri, and T. Subha, "Intelligent traffic signal control system for ambulance using RFID and cloud," in *2017 2nd International Conference on Computing and Communications Technologies (ICCCT)*, pp. 90–96, IEEE, 2017.

[11] J. Bravo, R. Hervas, C. Fuentes, G. Chavira, and S. W. Nava, "Tagging for nursing care," in *2008 Second International Conference on Pervasive Computing Technologies for Healthcare*, pp. 305–307, IEEE, 2008.

[12] C. Polley, T. Jayarathna, U. Gunawardana, G. Naik, T. Hamilton, E. Andreozzi, P. Bifulco, D. Esposito, J. Centracchio, and G. Gargiulo, "Wearable bluetooth triage healthcare monitoring system," *Sensors*, vol. 21, no. 22, p. 7586, 2021.

[13] H. J. Lee, S. H. Lee, K.-S. Ha, H. C. Jang, W.-Y. Chung, J. Y. Kim, Y.-S. Chang, and D. H. Yoo, "Ubiquitous healthcare service using Zigbee and mobile phone for elderly patients," *International journal of medical informatics*, vol. 78, no. 3, pp. 193–198, 2009.

[14] L. Tian, S. Santi, A. Seferagić, J. Lan, and J. Famaey, "Wi-Fi HaLow for the Internet of Things: An up-to-date survey on IEEE 802.11 ah research," *Journal of Network and Computer Applications*, vol. 182, p. 103036, 2021.

[15] W. Jia, H. Peng, N. Ruan, Z. Tang, and W. Zhao, "WiFind: Driver fatigue detection with fine-grained Wi-Fi signal features," *IEEE Transactions on Big Data*, vol. 6, no. 2, pp. 269–282, 2018.

[16] H. Taleb, A. Nasser, G. Andrieux, N. Charara, and E. M. Cruz, "Energy consumption improvement of a healthcare monitoring system: application to LoRaWAN," *IEEE Sensors Journal*, vol. 22, no. 7, pp. 7288–7299, 2022.

[17] H. H. Alshammari, "The internet of things healthcare monitoring system based on MQTT protocol," *Alexandria Engineering Journal*, vol. 69, pp. 275–287, 2023.

[18] M. M. Islam, S. Nooruddin, F. Karray, and G. Muhammad, "Internet of things: Device capabilities, architectures, protocols, and smart applications in healthcare domain," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3611–3641, 2022.

[19] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, and S. R. Chaudhry, "IoT architecture challenges and issues: Lack of standardization," in *2016 Future technologies conference (FTC)*, pp. 731–738, IEEE, 2016.

[20] J. Saleem, M. Hammoudeh, U. Raza, B. Adebisi, and R. Ande, "IoT standardisation: Challenges, perspectives and solution," in *Proceedings of the 2nd international conference on future networks and distributed systems*, pp. 1–9, 2018.

[21] B. Bhushan, A. Kumar, A. K. Agarwal, A. Kumar, P. Bhattacharya, and A. Kumar, "Towards a secure and sustainable internet of medical things (iomt): Requirements, design challenges, security techniques, and future trends," *Sustainability*, vol. 15, no. 7, p. 6177, 2023.

[22] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 2018.

[23] Wikipedia, "Key escrow — wikipedia, l'enciclopedia libera," 2021. [Online; in data 10-settembre-2024].

[24] Wikipedia, "Funzione crittografica di hash — wikipedia, l'enciclopedia libera," 2024. [Online; in data 10-settembre-2024].

[25] M. S. Alkatheiri and A. S. Alghamdi, "Blockchain-assisted cybersecurity for the internet of medical things in the healthcare industry," *Electronics*, vol. 12, no. 8, p. 1801, 2023.

[26] S. Prabhakar, A. Ivanisov, and A. Jain, "Biometric recognition: Sensor characteristics and image quality," *IEEE Instrumentation & Measurement Magazine*, vol. 14, no. 3, pp. 10–16, 2011.

[27] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *2015 IEEE Symposium on Computers and Communication (ISCC)*, pp. 180–187, 2015.

[28] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 32–37, 2017.

[29] A. Mallik, "Man-in-the-middle-attack: Understanding in simple words," *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, vol. 2, no. 2, pp. 109–134, 2019.

[30] P. Manickam, S. Mariappan, S. Murugesan, S. Hansda, A. Kaushik, R. Shinde, and S. Thipperudraswamy, "Artificial Intelligence (AI) and Internet of Medical Things (IoMT) Assisted Biomedical Systems for Intelligent Healthcare.," *Biosensor*, 2022.

[31] W. McCulloch and W. Pitts, "A logical calculus of the ideas immanent in nervous activity.," *Bulletin of Mathematical Biophysics 5*, pp. 115–133, 1943.

[32] M. Phillips, H. Marsden, W. Jaffe, R. Matin, G. Wali, J. Greenhalgh, E. McGrath, R. James, E. Ladoyanni, A. Bewley, G. Argenziano, and I. Palamaras, "Assessment of Accuracy of an Artificial Intelligence Algorithm to Detect Melanoma in Images of Skin Lesions.," *JAMA Netw Open*, 2019.

[33] Y. Zhu, A. Lesch, X. Li, T.-E. Lin, N. Gasilova, M. Jović, H. M. Pick, P.-C. Ho, and H. H. Girault, "Rapid Noninvasive Skin Monitoring by Surface Mass Recording and Data Learning," *Jacs Au*, vol. 1, no. 5, pp. 598–611, 2021.

[34] M. S. Alshareef, B. Alturki, and M. Jaber, "A transformer-based model for effective and exportable iomt-based stress detection," in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, pp. 1158–1163, 2022.

[35] S. R. Khan, M. Sikandar, A. Almogren, I. U. Din, A. Guerrieri, and G. Fortino, "IoMT-based computational approach for detecting brain tumor," *Future Generation Computer Systems*, vol. 109, pp. 360–367, 2020.

[36] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Satoshi Nakamoto*, 2008.

[37] M. Di Pierro, "What Is the Blockchain?," *Computing in Science & Engineering*, vol. 19, no. 5, pp. 92–95, 2017.

[38] A. Lakhan, M. A. Mohammed, M. Elhoseny, M. D. Alshehri, and K. H. Abdulkareem, "Blockchain multi-objective optimization approach-enabled secure and cost-efficient scheduling for the Internet of Medical Things (IoMT) in fog-cloud system," *Soft Computing*, vol. 26, no. 13, pp. 6429–6442, 2022.

[39] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, "Blockchain-assisted secured data management framework for health information ana-

lysis based on Internet of Medical Things," *Personal and ubiquitous computing*, vol. 28, no. 1, pp. 59–72, 2024.

[40] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous Patient Monitoring With a Patient Centric Agent: A Block Architecture," *IEEE Access*, vol. 6, pp. 32700–32726, 2018.

[41] International Organization for Standardization, "ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework." https://www.iso.org/standard/45123.html, 2011. Accessed: 2024-08-30.

[42] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council."

[43] Centers for Medicare & Medicaid Services, "The Health Insurance Portability and Accountability Act of 1996 (HIPAA)," 1996.

[44] European Parliament and Council of the European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)." https://eur-lex.europa.eu/eli/dir/2022/2555, 2022.

[45] E. Lachaud, "ISO/IEC 27701 standard: Threats and opportunities for GDPR certification," *Eur. Data Prot. L. Rev.*, vol. 6, p. 194, 2020.

[46] M.-D. Cano and A. Cañavate-Sanchez, "Preserving data privacy in the internet of medical things using dual signature ECDSA," *Security and Communication Networks*, vol. 2020, no. 1, p. 4960964, 2020.

[47] S. S. Ahamad and A.-S. Khan Pathan, "A formally verified authentication protocol in secure framework for mobile healthcare during COVID-19-like pandemic," *Connection Science*, vol. 33, no. 3, pp. 532–554, 2021.

[48] F. A. Alzahrani, M. Ahmad, and M. T. J. Ansari, "Towards design and development of security assessment framework for internet of medical things," *Applied Sciences*, vol. 12, no. 16, p. 8148, 2022.