(lezione 1)

TELEMEDICINA→ tele (distanza spaziale e temporale) e medicina (curare);
è il trasferimento di informazioni mediche tramite vie di comunicazione elettroniche per migliorare lo stato di salute del paziente, connettendo paziente e medico e facilitando la comunicazione tra medici.
-provider centric: 1° e 2° fase dagli anni 60' (dal 2000 scambio di documneti)
-patient centric: 3° fase (attuale), ora il paziente si attiva per migliorare la propria salute

e-health → telemedicina → m-health

TELEMEDICINA IN ITALIA→ modalità di erogazione di servizi sanitari tramite ICT in situazioni in cui paziente e clinico non si trovano nella stessa località; trasmissione sicura di info e dati di carattere medico (testi, suoni, immagini, video, altri dati monodimensionali) necessari per prevenzione, diagnosi, trattamento e controllo; non sostituisce la prestazione sanitaria ma la integra per potenziare efficacia e efficienza.
-Caratterizzato da: tipologia paziente, ambito (telecardiologia, teleneurologia...), finalità (monitoraggio, prevenzione...), relazione (B2B, B2C, B2B2C); copertura territoriale, luogo di fruizione, luogo di erogazione, comunità a cui è rivolto il servizio, modalità temporale (in tempo reale o differita) e durata, rischio clinico, professionisti coinvolti presso il luogo di fruizione e di erogazione, parametri monitorati, tariffario.
-Attori coinvolti: utenti (fruiscono del servizio), centro erogatore (struttura SSN pubblica o privata o operatori SSN), centro servizi (struttura che gestisce la manutenzione del sistema informativo utilizzato dal centro erogatore)
-la televisita non può essere usata come visita di diagnostica ma come visita di controllo per patologie accertate, prescritta attraverso ricetta e prenotata tramite CUP
-il referto viene caricato sul fascicolo sanitario elettronico con firma digitale del medico
-teleconsulto e teleconsulenza coinvolgono prettamente figure di tipo clinico che discutono del quadro clinico del paziente o sulle modalità di assistenza; la teleassistenza coinvolge invece anche il paziente
CONSENSO INFORMATO→il paziente deve essere informato di: in cosa consiste la prestazione, vantaggi e rischi; gestione di dati personali e clinici; professionisti coinvolti; chi sono il data controller e il data protector officer, secondo GDPR, come contattarli e quali sono i suoi diritti sui dati

REQUISITI→ rete internet, portale web, pc-smartphone-tablet, login semplice per i pazienti, compatibilità con GDPR, certificazione come dispositivo medico
il centro erogatore deve indicare un direttore sanitario e un responsabile della parte tecnologica (manutenzione e gestione) e in assenza di pc-smartphone-tablet disponibilità di asl, farmacie o studi medici

PNRR (piano nazionale ripresa e resilienza)

OBBIETTIVI→ -generare un fascicolo sanitario elettronico valido a livello nazionale (DL 27 gennaio 2022)
Missione 6 salute: generare PNT (piattaforma nazionale telemedicina) con un unico deposito dati EDS (ecosistema dati sanitari) scritti secondo lo standard FHIR per essere usati a scopo di ricerca
nuovo FSE 2.0→ fronteggiare invecchiamento demografico, ridurre divario territoriale all'accesso alle cure, fornire ai cittadini informazioni sanitarie corrette e gestire meglio le emergenze sanitarie; dovrà contenere dati identificativi, referti, diagnosi e profilo sanitario, cartelle cliniche, prescrizioni, vaccinazioni, dossier farmaceuitico e dati generati dai pazienti (tenuti separati perché non certificati)
FHIR→ (Fast Healthcare Interoperability Resources) è uno standard sviluppato da HL7 (Health Level Seven International) per facilitare lo scambio elettronico di dati sanitari in modo rapido, sicuro e interoperabile, superando le complessità tradizionali dell'integrazione tra diversi sistemi software.

(lezione 2)
Ha l'obbiettivo di rafforzare e unificare la protezione dei dati personali e regola il trattamento di questi ultimi da parte di aziende e organizzazioni
GDPR→ regolamento europeo sulla gestione dei dati (25 maggio 2018)
Attori coinvolti→ data owner (proprietario dei dati); data controller (titolare del trattamento-azienda che chiede i dati); data processor (chi processa i dati); third party (persona autorizzata a processare i dati); DPO (responsabile protezione dati) (avvocato che assicura il rispetto del GDPR all'interno dell'azienda); DPA (garante privacy, responsabile nazionale privacy).
Parliamo di dati personali, dati genetici, biometrici e riguardanti la salute che vengono raccolti, memorizzati, collezionati, visionati, estratti, rimossi o distrutti.
L'obbiettivo è la protezione dell'utente da 'data breach' (perdita, distruzione, alterazione, accessi non autorizzati).
Diritti del data owner: accesso ai dati, eliminazione i dati, leggibilità dei dati, notifica di breach, collezione di dati strettamente necessari, dvee essere consapevole dei dati collezionati, i dati non possono essere riutilizzati e devono essere cancellati o anonimizzati alla fine del ciclo.

PRIVACY→ by default: massima protezione adottabile; by design: vengono implementate tecniche e misure ai primi stadi del design (pseudonimizzazione-nome e cognome non sono associati direttamente ai dati ma tramite un codice paziente, ci sarà una look up table che conterrà le relazioni tra nome e codice paziente) (anonimizzazione- come prima ma senza look up table-non nomi solo codici)

COMPLIANCE BY DESIGN→pianificare il corretto sistema dall'inizio (differente dal compliance by detection- risovi i problemi quando si verificano)
misure di sicurezza (ISO 27000,WP 202 per applicazioni mobili)→corretta scelta di modelli

per l'immagazzinamento dati, ricordare all'utente di cambiare password, usare identificatori temporanei
RIASSUNTO rischi principali→distruzione, alterazione o uso inappropriato dei dati e accesso non autorizzato

Un app di telemedicina può essere sviluppata dopo l'ok di un comitato etico (MDD); la direttiva definisce come dispositivo medico qualunque software, usato solo o in combinazione con altri dm atto a diagnosi, prevenzione, monitoraggio o prognosi di malattie
Li classifica tipicamente in classe I, classe IIA se da esso dipende la vita del paziente; di solito ha la stessa classe del dispositivo medico cui è collegato (anche IIB)

L'esperienza utente è importantissima, sarà l'utilizzatore finale e tutto deve essere congruo alle sue richieste, accessibile e intuitivo per qualsiasi classe di pazienti.
Alle spalle è indispensabile un team multidisciplinare che include diverse figure di tipo clinico ma anche ingegneri, avvocati, esperti di etica e il governo. Il paziente stesso deve essere attivamente coinvolto nel processo di design valutando i prototipi man mano

(lezione 3)

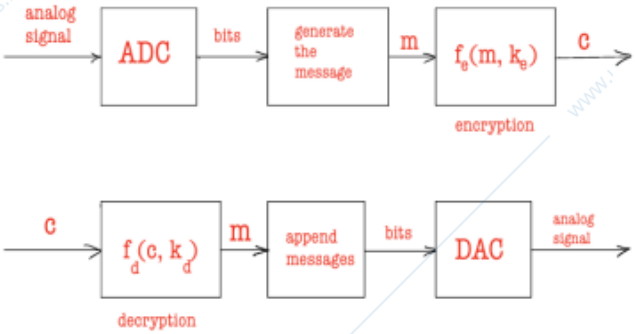
SICUREZZA E PRIVACY

Termini tecnici: malware-software maligno designato a danneggiare un dispositivo, ransomware-software che cifra i dati in un computer (viene poi chiesto un riscatto per ottenere chiave di cifratura), virus-software che infette pc a catena, worm-virus che fa crollare la connessione a internet, backdoor, trojan horse-un software apparentemente innocente, spyware-software che ruba info all'utente, spoofing-persona/programma fine di essere un'altra persona/programma per trarre dei vantaggi, man-in-the-middle-D si mette tra A e B, denial of service-sovraccarico del trafico che fa crashare il sito.
*alta mortalità a causa di data breach-oltre 2000 persone ogni anno*

AGID ha fatto una lista di possibili accorgimenti per evitare ciò: lista dispositivi che posso accedere al servizio e login temporanei, molteplici fattori di autorizzazione, diversi backup dei dati su diversi dispositivi, dati immagazzinati criptati

Valutare il RISCHIO di ogni possibile evento (probabilità del rischio * costo danni in euro) e prendere adeguate contromisure→deve essere trovato un equilibrio perché sistemi iper sicuri possono rendere il sistema inutilizzabile a cause di sequenze complesse di operazioni

Non è raccomandato utilizzare la crittografia standard dei sistemi di trasmissioni utilizzati→ è consigliato usare crittografia end-to-end (dati crittografati quando vengono generati e solo la destinazione finale è autorizzata a decrittografarli




CRITTOGRAFIA→ testo convertito in una sequenza di numeri o di bit (le immagini sono già sequenze di bit); i segnali vengono convertiti da analogici a digitali generando sequenze di bit→i messaggi sono piccole porzioni di bit e sono gli input dell'algoritmo di crittografia→"c" è il testo criptato che si scambiano A e B
La sicurezza dipende dalle chiavi Ke e Kc

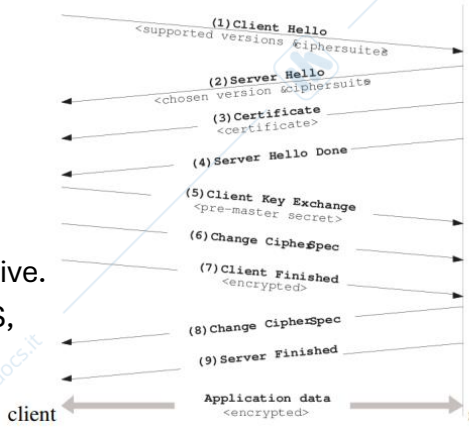
CRITTOGRAFIA SIMMETRICA (CHIAVE PRIVATA)
Ke=Kd=K le chiavi sono le stesse, è assunto che siano conosciute sia da A che da B
esempio→ Hai un **messaggio** mmm di N bit. Hai una **chiave** K lunga anch'essa N bit. Per **cifrare** il messaggio, calcoli c=m⊕Kc , cioè fai lo **XOR bit a bit** tra messaggio e chiave. Il risultato è la **parola cifrata** c. Il destinatario, per **decifrare**, prende la parola cifrata c e applica di nuovo **XOR** con la **stessa chiave** K. Ottiene così c⊕K=m, cioè ricostruisce il messaggio originale.
DES→ il messaggio di N bit viene spezzato in blocchi di M bit; ciascun blocco passa attraverso una tabella di sostituzione (look-up table) che ne trasforma i bit, quindi i blocchi riassemblati sono ulteriormente "mescolati" da una permutazione. Questo processo si ripete per P cicli e, a ogni ciclo, si fa l'XOR dei dati con una chiave segreta K. Per decifrare, il destinatario ripete le stesse operazioni all'inverso, usando la stessa chiave e le stesse tabelle.
PROBLEMA→ A e B devono condividere la **stessa chiave** e quindi devono trovare un modo sicuro per scambiarla. Se non esiste un canale protetto per trasferire la chiave, la sicurezza rischia di essere compromessa.

CRITTOGRAFIA ASIMMETRICA
si basa su due chiavi: una pubblica, nota a tutti, e una segreta, conosciuta solo dal proprietario. Questo approccio consente di cifrare i messaggi in modo che solo il destinatario, con la sua chiave segreta, possa decifrarli. Tuttavia, una limitazione fondamentale è che non si può essere certi dell'identità del mittente, lasciando spazio a potenziali attacchi come il "man-in-the-middle".
FIRMA DIGITALE→applicazione della crittografia asimmetrica che garantisce l'autenticità di un documento. Il mittente utilizza la sua chiave segreta per firmare l'hash del documento, e chiunque può verificare l'autenticità utilizzando la chiave pubblica del mittente. Questo sistema assicura che il documento non sia stato alterato e proviene effettivamente dal mittente.
CRITTOGRAFIA ASIMMETRICA BIDIREZIONALE→ consente alle due parti (es. Alice e Bob) di scambiarsi messaggi in modo sicuro e autenticato. Entrambe utilizzano le proprie chiavi segrete e pubbliche per cifrare e decifrare i messaggi, garantendo riservatezza delle comunicazioni e l'identità dei mittenti. Base per le comunicazioni sicure in molte applicazioni moderne.
RSA→utilizzato per scambio sicuro di chiavi; PROCEDURA→generazione coppia chiavi usando *p* e *q* (num primi), calcolo n=p*q, crea una chiave pubblica *e* e una privata *d*, cifratura (c=m^e*mod n) e decifratura (m=c^d*mod n)

AUTENTICAZIONE→garantire che le parti coinvolte in una comunicazione siano realmente chi dichiarano di essere.
ASIMMETRICA→(coppia di chiavi (pubblica e privata) fornita da un'autorità di certificazione) A invia un messaggio cifrato con la propria chiave privata, B lo decifra con la chiave pubblica associata, se il messaggio è leggibile, si conferma l'identità del mittente.
SIMMETRICA→(condividono una chiave segreta comune) A invia un "nonce" (numero casuale) a B come sfida, B utilizza la chiave segreta per cifrare il nonce e lo invia ad A, A decifra il messaggio ricevuto e verifica che corrisponda al nonce inviato.
AUT. A 2 FATTORI→secondo livello di verifica (OTP, dati biometrici)

GESTIONE PASSWORD→se archiviate in chiaro sono vulnerabili: SOLUZIONI→ hash (trasformano la pwd in un valore univoco di lunghezza fissa), hash con salt (un valore 'salt' viene aggiunto alla pwd prima di calcolare l'hash) (solo utenti autorizzati possono accedere ai file con queste info)
*la funzione hash non è invertibile, non è crittografia*
-WebAuthn consente di autenticarsi senza pwd tramite app autenticatrice per smartphone →aiuta a prevenire il phishing- attacco informatico progettata per ingannare le persone e indurle a fornire informazioni sensibili come credenziali di accesso, numeri di carte di credito o dati personali.
*Nei sistemi di telemedicina, è essenziale garantire che solo utenti autorizzati possano accedere ai dati sensibili dei pazienti*

INTEGRITA'→capacità di garantire che le informazioni non siano state modificate, né intenzionalmente né per errore, durante il loro utilizzo, trasmissione o archiviazione
*Le funzioni di hash generano un'impronta digitale unica di un messaggio o di un dato, qualsiasi modifica, anche minima, al messaggio viene rilevata*
Backup→è essenziale avere copie di backup dei dati per ripristinare la versione originale, devono essere regolari, archiviati in più posizioni e verificati per garantire la loro correttezza.
-La crittografia simmetrica combinata con hash permette di verificare l'integrità, se il messaggio generato e quello calcolato corrispondono, B sa che m non è stato alterato e che proviene da A
-Crittografia asimmetrica: -firma digitale, -digital signature
-HTTP/HTTPS →garantisce l'integrità dei dati trasmessa tramite il web (oltre a autenticazione e sicurezza)
→HTTPS è un protocollo sicuro che si basa su protocolli ssl o tsl
SSL handshake→Il server invia un certificato digitale contenente la sua chiave pubblica, il client verifica il certificato e genera una chiave temporanea (pre-master secret), la chiave viene condivisa e usata per la crittografia simmetrica delle comunicazioni successive.
!!!La TLM non si può basare solo sulla sicurezza garantita da HTTPS, è necessario un sistema di cifratura specifico!!!




Tutto questo avviene prima di effettuare il login; username e password verranno comunicati già cifrati

PROTEZIONE DATI

I dati possono trovarsi in tre stati principali: a riposo (archiviati), in uso (attivi, in fase di modifica o elaborazione), in transito (trasferiti tra dispositivi)→la crittografia vari a seconda dello stato dei dati, ma è particolarmente importante gestire i dati a riposo per mitigare rischio di furto

Slz1→CRITTOGRAFIA DEL DATABASE: il database viene crittografato con chiave Kdb, ogni utente ha una propria chiave Ku che protegge Kdb crittografandola. Quando un utente accede al database deve prima decifrare Kdb con la propria chiave.

Slz2→CRITTOGRAFIA VIA SERVER: l'utente invia la richiesta di accesso ai dati al server che conosce la chiave d'accesso al database e restituisce i dati. Le comunicazioni avvengono in modo sicuro con protocolli specifici del servizio di TLM (misure di sicurezza elevate per proteggere il software)

!!!I dati sul pc del medico devono essere cifrati (BitLocker, VeraCrupt) (importante spegnere il pc perché, se acceso le chiavi sono in memoria e possono essere rubate)!!!

(lezione 4)

TELECOMUNICAZIONI

Un sistema di telecomunicazione è un sistema che permette di trasferire info da un luogo a un altro o da un tempo a uno successivo→sistema ideale sarebbe wireless, veloce, efficiente dal punto di vista energetico, sicuro e globale, ma nella pratica occorrono compromessi. Questo richiede bilanciamenti tra le risorse disponibili, la complessità dei sistemi e le esigenze specifiche delle applicazioni.

TEORIA DEI SEGNALI→Un segnale è una rappresentazione fisica che varia nel tempo e può essere descritto attraverso parametri quali ampiezza, frequenza e fase. La trasformata di Fourier e lo spettro di potenza sono strumenti essenziali per analizzare segnali nei domini del tempo e della frequenza.

Processi casuali→il destinatario non conosce a priori le info trasmesse

MEZZI DI TRASMISSIONE→segnali vengono trasmessi principalmente attraverso canali elettrici, che includono cavi di rame (economici, ma soggetti a interferenze e maggiore attenuazione), cavi coassiali (capacità di banda superiore rispetto ai cavi intrecciati) e fibre ottiche (trasmissione ad alta velocità e basse perdite, ideali per lunghe distanze), oppure attraverso il vuoto utilizzando onde elettromagnetiche.

*La scelta del mezzo è strettamente legata alle esigenze (banda, distanza, costi)*

INFORMAZIONE TRAMITE I MEZZI DI TRASMISSIONE→la comunicazione tramite fili fisici (come nei telefoni fissi) era limitata dalla necessità di connessioni dirette tra utenti. Con l'aumentare del numero di utenti, è stato necessario sviluppare tecniche come la **modulazione** e il **multiplexing**→DSB, AM, FM e PM, permettono di spostare il segnale vocale su frequenze diverse per adattarlo al mezzo di trasmissione. Inoltre, il multiplexing in frequenza consente la trasmissione simultanea di più segnali su un singolo canale, rendendo possibile la gestione di un gran numero di utenti.

IMPEDIMENTI ALLA TRASMISSIONE→Non esistono canali ideali che trasmettano il segnale dal modulatore alla destinazione senza alterazioni.
principali problemi dei canali sono:
-Attenuazione: riduce la potenza del segnale durante la trasmissione, ma può essere compensata con ripetitori o amplificatori.
-Distorsioni: derivano sia da comportamenti non lineari (amplificatori) che da riflessioni (echi), ma possono essere mitigate con equalizzatori.
-Interferenze: nei cavi, causano effetti di cross-talk (effetto magnetico tra cavi); nei sistemi wireless, possono includere segnali indesiderati o intenzionali (jammers).
-Rumore: inevitabile in ogni sistema, richiede filtri per minimizzarlo, pur senza eliminarlo completamente.

STRUTTURA DI UN SISTEMA DI TRASMISSIONE→componenti chiave necessari per trasferire segnali da una sorgente a un ricevitore:
-Sorgente: genera un segnale fisico, che viene convertito in segnale elettrico da un trasduttore.
-Trasmettitore: il segnale viene modulato per adattarsi alla banda del canale, amplificato per compensare le perdite e trasmesso attraverso il canale (cavi, fibre ottiche o atmosfera).
-Ricevitore: elabora il segnale ricevuto, amplificandolo, filtrandolo e demodulandolo per recuperare il segnale originale e attraverso un trasduttore converte il segnale elettrico in una forma percepibile dall'utente (es acustico).

SISTEMI DIGITALI
Teorema di campionamento → rappresentare segnali analogici come sequenze discrete di campioni, successivamente quantizzati e codificati in bit
ANALOGICO VS DIGITALE→i sistemi digitali superano quelli analogici in termini di qualità del segnale (nonostante la possibilità di errori dovuti al rumore possono ridurre significativamente la probabilità di errore attraverso tecniche di progettazione avanzate), robustezza, sicurezza e flessibilità, rendendoli la scelta predominante nelle moderne telecomunicazioni.
MULTIPLEXING→consente di combinare più segnali su un unico canale (tecniche: FDM-divide lo spettro in sottobande ognuna associata a un segnale, TDM-divide il tempo in slot per gestire segnali digitali, CDM-codici unici per trasmettere simultaneamente nello stesso spettro)
ACCESSO MULTIPLO→condivisione di un canale di trasmissione comune tra più utenti (tecniche: FDMA-sottobande, TDMA-slot temporali, CDMA-codici unici)
ALLOCAZIONE DELLE FREQUENZE→garantisce che diversi servizi e applicazioni possano operare senza interferenze reciproche (telecomunicazioni, TV, radio, GPS, WiFi e comunicazioni satellitari)

(lezione 5)

RETI DI COMUNICAZIONE→vengono utilizzate per trasferire informazioni da un punto a un altro; includono: -terminali (telefoni, stampanti), -collegamenti (canali di comunicazione) (diretti (point-to-point), centralizzati con nodi periferici (point-to-multi-point), distribuiti (broadcast, tv, gps)), -nodi (instradano le informazioni)
Le reti utilizzano **canali fisici** (costituiscono il collegamento fisico) e **canali logici** (separano il flusso dei dati secondo il tipo di informazione trasmessa)
TOPOLOGIE DI RETE (strutture di interconnessione tra i nodi):
-a Stella: ogni nodo è connesso a uno centrale (hub)→se l'hub si guasta tutta la rete smette di funzionare (Bluetooth e sensori per telemedicina)
-a Bus: i nodi condividono un singolo cavo→pro-(semplice e usata in vecchie versioni ethernet), contro-(guasto al bus interrompe la rete)
-ad Anello: ogni nodo è connesso a due nodi adiacenti→ se si guasta un nodo salta la linea (non più utilizzato)
-a Maglia: nodi interconnessi in modo parziale o totale → tolleranza a guasti grazie ai percorsi multipli tra i nodi ma elevata complessità e costi
-ad Albero: struttura gerarchica, ogni nodo è collegato a nodi inferiori tramite ramificazioni→isola una parte della rete in caso di guasto
Svolgono operazioni essenziali per garantire la comunicazione. La **segnalazione** permette di instaurare, controllare e chiudere le connessioni, mentre la **commutazione** avviene secondo due approcci: il **circuit switching** e il **packet switching**. La **trasmissione** si occupa del trasferimento dei dati, mentre la **gestione** cura manutenzione, monitoraggio e supporto agli utenti.
Nel **Circuit Switching**, viene stabilito un percorso fisso tra sorgente e destinazione, dedicato esclusivamente agli utenti fino alla fine della comunicazione (comunicazioni interattive e sensibili ai ritardi: telefonate, videoconferenze).
Nel **Packet Switching**, i dati sono suddivisi in pacchetti indipendenti, ciascuno con un'intestazione per l'instradamento (trasferimento dati: internet), efficiente e flessibile perché la rete è utilizzata solo quando serve.
PROTOCOLLI DI RETE→architettura a livelli (modello **OSI** a 7 livelli è lo standard universale):
-**Fisico**: garantisce la trasmissione fisica dei segnali;-**Link**: gestisce errori nella trasmissione e controlla l'accesso;-**Rete**: si occupa dell'instradamento dei pacchetti;-**Trasporto**: ritrasmette i pacchetti mancanti o errati;-**Sessione**: coordina e gestisce le sessioni;-**Prestazione**: traduce i dati;-**Applicazione**: Interfaccia con l'utente
Meccanismi: incapsulamento (ogni livello aggiunge un'intestazione ai dati ricevuti dal livello superiore) e decapsulamento (ogni livello riceve i dati, rimuove l'intestazione e li invia al livello superiore).
*L'architettura a strati permette di separare le funzionalità della rete in blocchi gestibili, favorendo l'interoperabilità tra diversi sistemi e protocolli. Il modello OSI offre una base teorica, ma Internet utilizza spesso una semplificazione pratica basata su soli 4 livelli (modello TCP/IP).*

SUCA

SCIMPANZE

NON SONO

LECCESE

FASCISTONE

SEI tu

INTERNET

Originariamente progettata per collegare computer, Internet è ora una rete globale che collega anche dispositivi IoT, con il 5G come elemento abilitante fondamentale. I dispositivi finali, chiamati host, si dividono in client (ad esempio laptop e smartphone) e server (che archiviano dati e applicazioni). Google, per esempio, gestisce enormi data center, cruciali per il funzionamento del Web.
Gli ISP, come TIM e Vodafone in Italia, offrono accesso a Internet tramite diverse tecnologie (ADSL, LTE, Wi-Fi), mentre in alcune regioni rurali degli Stati Uniti si fa uso di ISP satellitari. Internet differisce dal WWW, che è solo una delle applicazioni che utilizza l'infrastruttura della rete. La sua funzione principale è il trasferimento di dati, che avviene suddividendo le informazioni in pacchetti e utilizzando router per instradarli.
I protocolli fondamentali per Internet sono TCP/IP. TCP garantisce una comunicazione affidabile, mentre IP si occupa dell'indirizzamento e dell'instradamento dei pacchetti. La rete funziona grazie a una varietà di collegamenti fisici (come fibre ottiche e connessioni wireless) e router, che utilizzano tabelle di routing per determinare il percorso dei pacchetti. La velocità e l'efficienza del trasferimento dipendono dal numero di router attraversati e dal traffico presente nelle code dei router.
PROTOCOLLI INTERNET
Il livello di rete utilizza il protocollo IP per trasferire datagrammi tra host.
Il livello di trasporto garantisce l'affidabilità con TCP o la velocità con UDP, bilanciando larghezza di banda, ritardi e trasferimento affidabile.
Nel livello applicativo, sono introdotte tecnologie chiave come DNS e HTTP, oltre all'importanza crescente dell'IoT, che integra dispositivi intelligenti in settori come la sanità e l'automazione domestica.
La privacy e la sicurezza sono sfide critiche, affrontate tramite IPv6 e standard di comunicazione a bassa potenza come 6LoWPAN.

RETI MOBILI
Dall'1G agli anni '80 al 5G odierno, la complessità tecnologica è aumentata, riducendo le dimensioni delle celle per migliorare la capacità e l'efficienza. Il 5G introduce velocità elevate (fino a 10 Gbit/s), latenze ridotte (4-6 ms) e supporto per miliardi di dispositivi grazie a tecnologie come **Multi-access Edge Computing (MEC)**, che elabora i dati vicino all'utente migliorando la privacy.
Le reti 5G trovano applicazione nella **telemedicina**, con strumenti innovativi come consultazioni virtuali in alta definizione, ambulanze connesse che trasmettono dati in tempo reale e chirurgia robotica remota resa possibile dalla bassissima latenza. Inoltre, tecnologie come la realtà aumentata e virtuale migliorano la formazione medica e la pianificazione degli interventi.
Nonostante i progressi, restano sfide legate alla copertura in aree remote e alla qualità della connessione. Soluzioni satellitari come **Starlink** forniscono accesso Internet in zone isolate, supportando applicazioni critiche come la telemedicina. Tuttavia, la stabilità della rete e la

riduzione dei guasti sono prioritarie, poiché interruzioni potrebbero compromettere servizi vitali.

POSIZIONAMENTO
Il GPS, sistema militare statunitense, e Galileo, sistema civile europeo, forniscono informazioni di posizionamento basate sulla misurazione dei ritardi di propagazione dei segnali trasmessi da satelliti sincronizzati. Questi sistemi sono fondamentali per molte tecnologie, incluse le reti mobili.
In telemedicina, i sistemi di posizionamento trovano applicazioni in test medici come il **6-Minute Walking Test**, utilizzato per monitorare malattie neurologiche. L'uso di sistemi di posizionamento indoor (IPS) migliora la raccolta dei dati, permettendo di misurare la velocità istantanea e non solo la distanza percorsa. Tuttavia, i segnali GPS sono poco efficaci indoor a causa delle attenuazioni, e per questo si ricorre a punti di accesso Wi-Fi.

(lezione 7)

**BODY AREA NETWORKS (BAN)**→reti progettate per gestire sensori e attuatori sul corpo umano o al suo interno. Usa potenze di trasmissione molto basse per limitare l'assorbimento specifico nel corpo e prolungare la batteria
!non garantisce sicurezza, salute o protezione ambientale!
**SmartBAN**→ alternativa che si concentra su consumi ultra-bassi e complessità ridotta per applicazioni specifiche; ha una struttura a stella con un hub centrale (smartphone) connesso direttamente con max 16 nodi a max 1,5m di distanza; altamente efficiente con latenza max 10ms; i nodi inviano dati a velocità variabili in base alla tipologia di informazione trasmessa.
TDMA (time division multiple access) → gestisce il traffico tra i nodi e consente la condivisione dati assegnando intervalli temporali specifici ai nodi
D-Beacon→ un segnale periodico trasmesso dall'hub che sincronizza i nodi e stabilisce gli slot temporali disponibili per la trasmissione
C-Beacon→ segnali di configurazione che forniscono ai nodi i parametri necessari per la sincronizzazione e la trasmissione: una volta configurati, i nodi trasmettono i dati nei rispettivi slot assegnati, minimizzando il consumo energetico attraverso periodi di inattività tra le trasmissioni successive
Physical Layer→ r appresenta la base tecnologica per le comunicazioni all'interno della rete, definendo le frequenze, le modalità di modulazione e i codici di trasmissione utilizzati: utilizza una banda da 80Hz con 40 canali (3 per il controllo di rete e 37 per trasmettere i dati che operano contemporaneamente senza interferenza; Il processo di trasmissione coinvolge tre tipi di unità di dati. Il livello MAC fornisce un MPDU (MAC Protocol Data Unit), che viene codificato dallo strato fisico per generare un PSDU (Physical Layer Service Data Unit). Infine, per la trasmissione, il PSDU è ulteriormente confezionato in un PPDU (Physical Protocol Data Unit)
MAC (Medium Access Control)→ si occupa della gestione e del controllo dell'accesso ai canali di comunicazione; ha un ruolo fondamentale nel garantire che i nodi connessi alla rete

possano trasmettere e ricevere dati in modo ordinato, efficiente e senza conflitti. Attraverso protocolli come il D-Beacon per la sincronizzazione, lo Slotted Aloha per l'accesso al canale e le strategie di ritrasmissione e codifica, il livello MAC riesce a bilanciare affidabilità, prestazioni e consumo energetico.

MODELLI DI CANALE
-diretti (Line of Sight-LOS): il segnale viaggia senza ostacoli
-indiretti (Non Line of Sight-NLOS): il corpo o altri ostacoli possono attenuare o deviare il segnale
Grazie a simulazioni, i ricercatori hanno capito come migliorare la trasmissione anche in condizioni difficili, assicurando che i dati arrivino in modo affidabile e veloce.

TRASMISSIONE DATI→ Non si tratta solo di inviare informazioni come il battito cardiaco o la temperatura, ma anche di includere dettagli utili come la posizione del sensore, il livello di batteria o il livello di affidabilità della trasmissione.
Le **ontologie** servono a standardizzare queste informazioni, rendendo più facile la comunicazione tra i sensori e i sistemi di monitoraggio esterni. Sono state definite delle categorie per classificare i nodi (ad esempio, hub o sensore) e la loro posizione (sulla pelle, impiantati o esterni).

SWIMLANE SmartBAN→ Prima di tutto, l'hub configura i sensori e assegna loro uno slot temporale per trasmettere. Una volta configurati, i sensori raccolgono le informazioni (ad esempio, battito cardiaco o temperatura) e le inviano all'hub nel loro slot dedicato. L'hub, a sua volta, elabora i dati e li inoltra a sistemi esterni per l'analisi. Questo processo è molto organizzato: ogni nodo sa quando deve inviare i dati e quando deve restare inattivo per risparmiare energia.

SICUREZA→ si basa sull'uso di chiavi crittografiche per proteggere i dati durante la trasmissione. Ogni nodo e l'hub condividono una chiave principale e generano chiavi temporanee per crittografare le comunicazioni. Esistono tre livelli di sicurezza: non sicuro, autenticato e completamente crittografato. Tuttavia, il sistema deve essere semplice e poco dispendioso in termini di energia, perché i sensori hanno risorse limitate.