La Cybersicurezza nelle reti e nei sistemi per l'*e-Health*

Potenzialità e sfide delle tecnologie emergenti

PhD. Samuela Persia
Funzionario
Certificazione e Vigilanza

Roma, 17/05/2023

TECNOLOGIE EMERGENTI PER e-Health

RETI DI TELECOMUNICAZIONE AD ELEVATE PRESTAZIONI (5G/6G)

ALGORITMI DI SUPPORTO ALLE DECISIONI (AI)

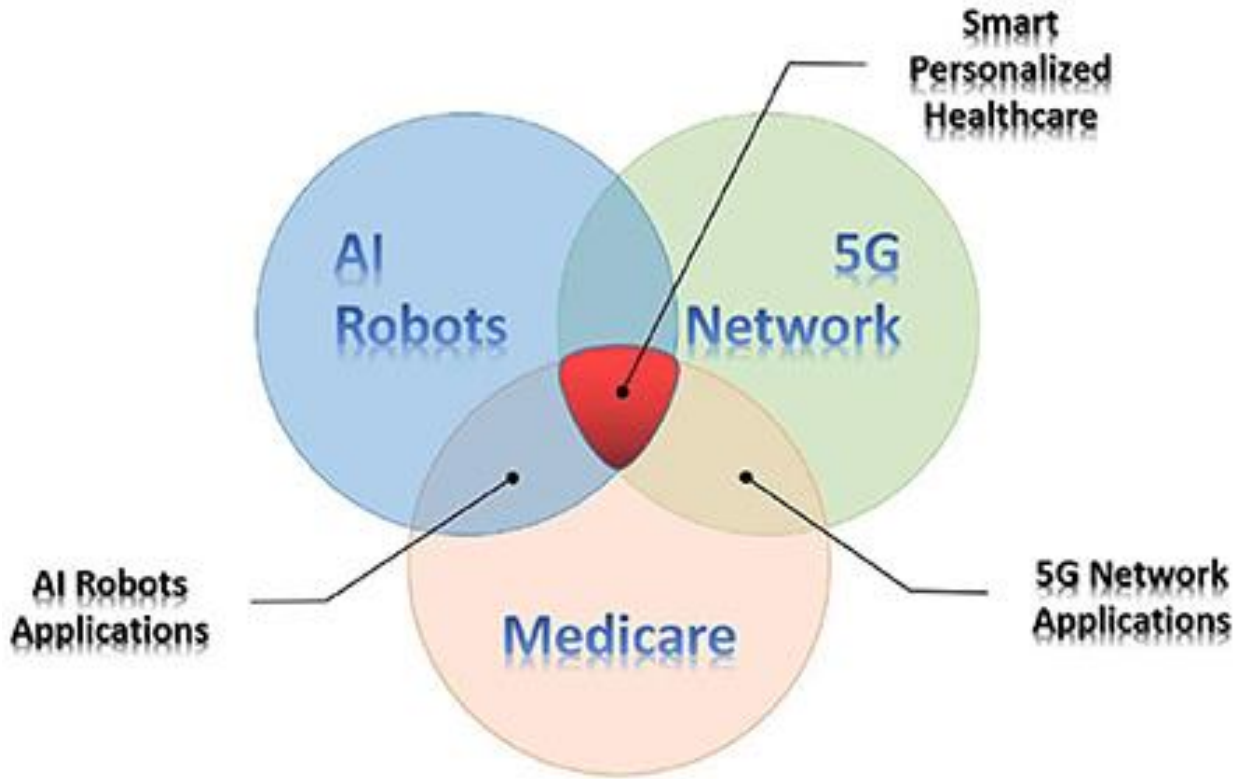
DISPOSTIVI ETEROGENEI CONNESSI (IoT)

CAPACITÀ DI ELABORAZIONE IN TEMPO REALE (EDGE COMPUTING)

La combinazione delle tecnologie emergenti permette di realizzare applicazioni di healthcare avanzate

Combinazione delle tecnologie per servizi healthcare personalizzati

- Combinando la **rete di comunicazione come il 5G** con **piattaforme sanitarie cloud, intelligenza artificiale, IoT, interazione uomo-computer pervasiva e deep learning** è possibile realizzare servizi medici all'avanguardia in grado di migliorare l'efficacia medica complessiva, ***Smart Personalized Healthcare***
- Come risultato si definiranno **futuri modelli medici**, in grado di ottenere avanzate soluzioni in ambito sanitario non ottenibili considerando l'impiego di una sola delle tecnologie emergenti



La digitalizzazione del settore sanitario *se da un lato offre* ***soluzioni innovative*** *ad elevate prestazioni dall'altro pone sfide sul* ***mantenimento della sicurezza*** *e sul* ***preservare*** *il settore sanitario da un sempre più crescente aumento di minacce cyber*

Cybersicurezza nell'Healthcare

Impatto applicazioni e-Health

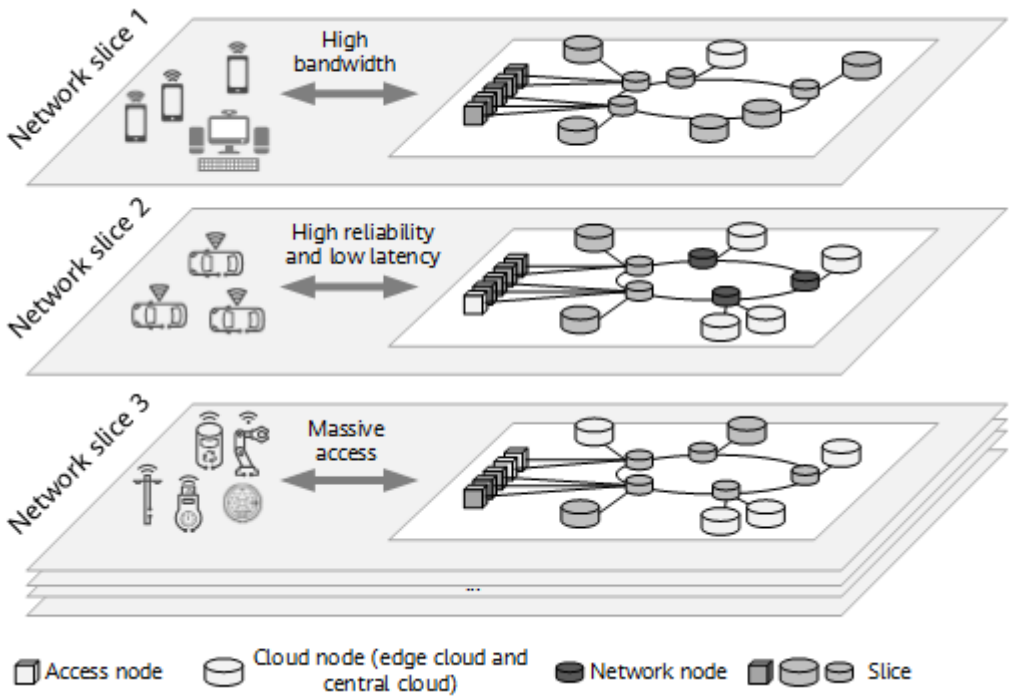
L'impatto nell'adozione delle applicazioni healthcare dipenderà fortemente da quanto sarà percepita la fiducia in tali soluzioni in termini di sicurezza e salvaguardia delle informazioni

- La ***fiducia*** nelle applicazioni in ambito sanitario dipendono da fattori quali:
  - **resilienza** della rete di telecomunicazione che assicuri le prestazioni necessarie per lo specifico servizio
  - **garanzia** di implementazione di **misure di cybersicurezza** nei dispositivi che trasmettono dati sensibili
  - **scrutinio tecnologico delle apparecchiature** e componenti di cui si avvalgono i servizi di e-health

Resilienza delle reti nelle applicazioni di Healthcare

Resilienza delle Reti di telecomunicazioni

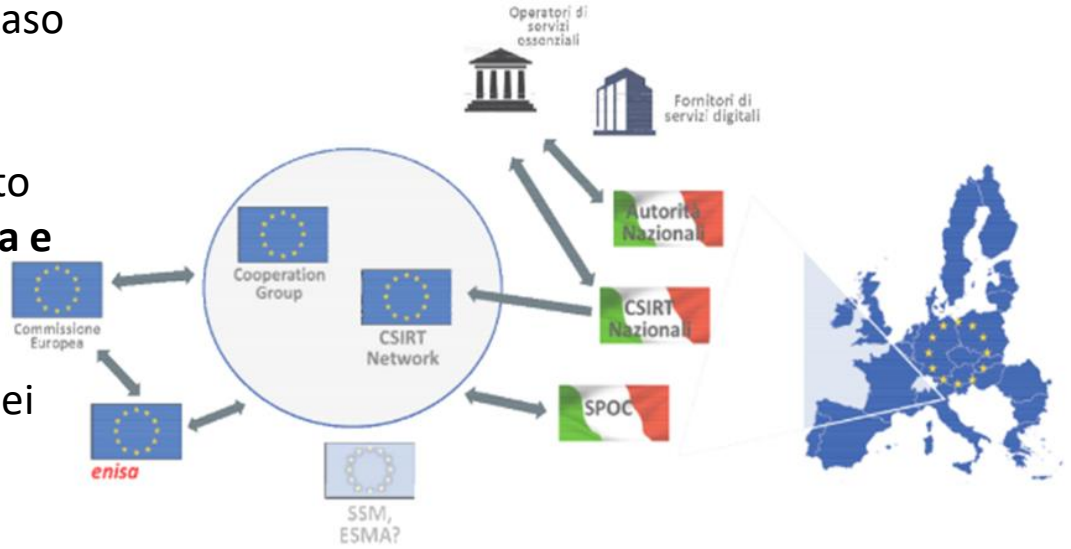
- **Le reti ad elevate prestazioni** di comunicazione ad elevata capacità trasmissiva, latenza e resilienza quali il 5G/6G si basano su un'alta **flessibilità** grazie alla quale sono in grado di fornire requisiti di rete molto differenti in base alle richieste delle specifiche applicazioni
- Ciò è possibile grazie al **concetto di virtualizzazione** della rete, e non più ad un concetto «monolitico» delle reti che ha caratterizzato le reti di precedente generazione, per il quale è possibile realizzare ***Network Slicing*** in grado di soddisfare specifiche esigenze di affidabilità e resilienza per soddisfare gli **SLA** (***Service Level Agreement***) delle specifiche applicazioni
- La rete 5G è la prima rete «***Secure by Design***» per cui vengono implementate funzionalità di sicurezza da parte dall'ente standardizzatore delle reti 3GPP (***3rd Generation Partnership Project***) come ad esempio nel documento **ETSI TS 33.117** e nelle specifiche tecniche dedicate



Cybersicurezza nell'healthcare: applicazione direttive Europee

DIRETTIVA NIS

- La Direttiva NIS è stata adottata dalla UE nel luglio 2016 e rappresenta uno dei primi tentativi di migliorare il livello di difesa delle infrastrutture critiche degli Stati membri. **In Italia è stata recepita con il D.Lgs. n. 65/2018**. I principali punti della NIS sono:
  - ***Istituire un gruppo di cooperazione*** al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati, composto da rappresentanti degli Stati Membri, della Commissione e dell'ENISA;
  - **Creare una rete di gruppi di intervento** per la sicurezza informatica in caso di incidente (***rete CSIRT***)
  - ***Identificare i settori di servizi da considerarsi essenziali*** per il mantenimento di attività sociali ed economiche fondamentali dello stato
  - Operatori di servizi essenziali **devono implementare misure di sicurezza e notificare senza ritardo all'autorità competente gli incidenti** aventi un impatto rilevante sulla continuità dei servizi essenziali prestati
  - ***Adottare una strategia nazionale in materia di sicurezza*** della rete e dei sistemi informativi, e a definirne gli obiettivi e le opportune misure strategiche e regolamentari



Il settore sanitario è ritenuto un settore che fornisce servizi essenziali e quindi rientra nell'ambito di applicazione della Direttiva NIS -> **operatori di servizi essenziali** sono tenuti ad adottare le misure tecniche e organizzative per limitare il rischio nel settore dell'healthcare

DIRETTIVA NIS II

- Il **14 dicembre 2022** è stata definitivamente approvata la Direttiva n. 2555/2022, NIS-II, che abroga la direttiva precedente la NIS. Le principali novità sono:
  - ***estensione*** della NIS ad altri soggetti ***tra cui i soggetti operanti nel settore della produzione di dispositivi medici***
  - ***Identificazione degli operatori di servizi essenziali soggetti alla Direttiva*** non più demandato agli Stati Membri , in quanto sarà la Direttiva stessa a definirli in modo tale da applicare criteri uniformi
  - resta l'obbligo di adottare misure tecniche ed organizzative adeguate alla gestione dei rischi, ma viene ***aggiunta una lista di misure specifiche come ad esempio la certificazione ai sensi CSA (Cyber Security Act)***
  - ***resta l'obbligo di notifica degli incidenti con impatto rilevante, ma viene regolamentato con maggiori dettagli (es notifica effettuata entro 24 ore)***
  - ***le sanzioni*** per le violazioni degli obblighi della Direttiva vengono fissate dai singoli stati, tuttavia, la Direttiva NIS 2 stabilisce delle soglie di incremento ossia pari ad un massimo di almeno 10 milioni di euro o fino al 2% del fatturato totale annuo mondiale dell'impresa interessata

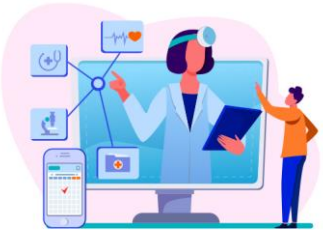
Il recepimento della NIS-II comporterà in futuro l'inclusione delle valutazioni di dispositivi medicali nelle attività di cybersicurezza nazionale

DIRETTIVA RED

- La direttiva sulle apparecchiature radio della Commissione europea **(CE) 2014/53/UE (RED)** istituisce un quadro normativo per le apparecchiature radio, stabilendo i **requisiti essenziali per la sicurezza e la salute, la compatibilità elettromagnetica (EMC) e l'efficienza dello spettro radio**.
- La **nuova direttiva include** ora l'articolo 3, paragrafo 3, allo scopo di definire i requisiti dei dispositivi in **relazione alla cybersecurity**.
- Il regolamento è volto a incrementare la cybersecurity, la protezione dei dati personali e la protezione dalle frodi per i dispositivi wireless applicabili disponibili sul mercato dell'UE. Il regolamento diventerà obbligatorio il **1° agosto 2024**, offrendo ai fabbricanti di dispositivi un periodo di transizione di 30 mesi per conformarsi ai requisiti di cybersecurity di cui all'articolo 3, paragrafo 3.
- Alcuni esempi di dispostivi includono:

  - ***dispositivi connessi***
  - ***apparecchiature radio per la cura dei bambini***
  - ***apparecchiature radio destinate ad essere indossate***

In tale ambito rientrano le apparecchiature per applicazioni sanitarie



Con l'applicazione della ***direttiva RED*** si introdurranno requisiti di cybesicurezza in tutte le apparecchiature connesse e quindi anche per apparecchiature e sistemi per servizi sanitari

ACN per cybersicurezza nell’healthcare

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

Il Servizio Certificazione e Vigilanza

CENTRO DI VALUTAZIONE E CERTIFICAZIONE NAZIONALE (CVCN)

QUALIFICAZIONE DEI SERVIZI CLOUD

ORGANISMO ISPETTIVO E DI VIGILANZA

NATIONAL CYBERSECURITY CERTIFICATION AUTHORITY (NCCA)

Possibilità di certificazione, su base volontaria, di dispositivi e-Health (Common Criteria)

ORGANISMO DI CERTIFICAZIONE DELLA SICUREZZA INFORMATICA (OCSI)

CENTRO DI VALUTAZIONE E CERTIFICAZIONE NAZIONALE (CVCN)

AMBITO:

PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

APPLICAZIONE:

OBBLIGATORIA (LIMITATA AGLI ASSET NEL PERIMETRO)

VALUTAZIONE DI SICUREZZA DI ASSET NEL PERIMETRO

RILASCIA AUTORIZZAZIONI ALL'IMPIEGO NEL PERIMETRO CON EVENTUALI PRESCRIZIONI

LAP

ACCREDITA I LABORATORI DI PROVA (LAP)

CV

COLLABORA CON I CENTRI DI VALUTAZIONE DIFESA E INTERNO

ASSET OGGETTO DI VALUTAZIONE DEL CVCN

SOGGETTI APPARTENENTI AL PERIMETRO

ASSET NEL PERIMETRO E NELLE CATEGORIE DPCM 3 15/06/2021

- SCRUTINIO TECNOLOGICO DA PARTE DEL CVCN
- PRESCRIZIONI DI SICUREZZA
- NOTIFICA DEGLI INCIDENTI

ASSET NEL PERIMETRO (NON NELLE CATEGORIE DPCM 3)

- PRESCRIZIONI DI SICUREZZA
- NOTIFICA DEGLI INCIDENTI

ASSET FUORI DAL PERIMETRO

- NESSUN VINCOLO

POSSIBILI VALUTAZIONI FUTURE DEL CVCN IN AMBITO SANITARIO

SOGGETTI APPARTENENTI AL PERIMETRO

ASSET NEL PERIMETRO E NELLE CATEGORIE DPCM 3 15/06/2021

- SCRUTINIO TECNOLOGICO DA PARTE DEL CVCN
- PRESCRIZIONI DI SICUREZZA
- NOTIFICA DEGLI INCIDENTI

ASSET NEL PERIMETRO (NON NELLE CATEGORIE DPCM 3)

- PRESCRIZIONI DI SICUREZZA
- NOTIFICA DEGLI INCIDENTI

ASSET FUORI DAL PERIMETRO

- NESSUN VINCOLO

Affinché il CVCN possa analizzare dispositivi per e-Health occorrerà:

- includere il settore sanitario nel Perimetro (DPCM 131/2020);
- includere i sistemi di e-Health nel DPCM 3.

Il **CVCN** svolge, in tali casi, le attività necessarie alle valutazioni di sicurezza, tramite (art. 5 DPR 54/2021):

- **Test di corretta implementazione delle funzionalità di sicurezza**
- **Test di intrusione a supporto dell'analisi di vulnerabilità**

CONCLUSIONI

- Le nuove tecnologie portano con sé enormi opportunità nel settore dell'healthcare grazie alla possibilità di connettere diverse strutture sanitarie e dispositivi abilitando così potenziali **applicazioni innovative**
- Il crescente utilizzo di dispositivi mobili di IoT, AI e Edge computing porterà a progressi nel settore sanitario grazie ai quali i pazienti possono **ricevere diagnosi, e cure personalizzate da remoto attraverso la tecnologia digitale**.
- Per fare in modo che tutto questo diventi realtà, è necessario che le soluzioni vengano definite e realizzate con sistemi ***end-to-end affidabili***
- La sicurezza deve essere assicurata durante la connessione dei dispositivi alla rete e devono essere garantiti elevati livelli di **riservatezza, integrità e disponibilità delle informazioni e dei servizi**
- La **protezione delle informazioni private dei pazienti** deve essere garantita
- Le normative Europee, recepite a livello nazionale, mirano ad implementare tutte le misure necessarie affinché ci sia un **elevato livello di sicurezza di tutti i componenti** per la realizzazione di applicazioni sanitarie all'avanguardia
- Lo **scrutinio tecnologico di dispositivi di e-Health in ambito Perimetro (CVCN)** richiede interventi normativi

In questo processo si concorrerà a rimuovere barriere che ostacolino
la fiducia nella digitalizzazione del settore sanitario portando cosi a ***sostanziali progressi in cure mediche***
a vantaggio sia del paziente che l'operatore sanitario

Grazie

PhD. Samuela Persia
s.persia@acn.gov.it