La Sicurezza nel Mondo IoT: Analisi Approfondita di Vulnerabilità, Attacchi e Strategie di Mitigazione

Abstract:
Il presente rapporto offre un'analisi approfondita della centralità della sicurezza all'interno del crescente ecosistema dell'Internet delle Cose (IoT). Esamina le cause fondamentali delle vulnerabilità nei prodotti IoT commerciali, analizza casi di studio significativi di attacchi reali e classifica sistematicamente le debolezze di sicurezza attraverso i vari strati architetturali dell'IoT. Un'esplorazione dettagliata dei protocolli IoT più diffusi (ZigBee, BLE, LoRaWAN) mette in evidenza i loro specifici meccanismi di sicurezza, le vulnerabilità intrinseche e i vettori di attacco documentati. Il rapporto va oltre l'esposizione tecnica per discutere le ampie implicazioni dei fallimenti della sicurezza IoT, che comprendono la sicurezza fisica, la resilienza delle infrastrutture critiche e le ripercussioni economiche. Successivamente, delinea un approccio sfaccettato alla mitigazione, esaminando il panorama normativo in evoluzione e promuovendo robuste pratiche ottimali sia per i produttori che per gli utenti finali. Infine, il rapporto identifica le tendenze emergenti, come l'impatto del 5G, dell'edge computing, dell'intelligenza artificiale e della blockchain, sul futuro della sicurezza IoT, offrendo raccomandazioni lungimiranti per la ricerca, lo sviluppo e un'adozione responsabile.

1. Introduzione: L'Internet of Things e la Centralità della Sicurezza

L'Internet delle Cose (IoT) rappresenta una trasformazione paradigmatica, con decine di miliardi di dispositivi connessi a Internet, che convertono oggetti fisici in entità "intelligenti".[1] Questa integrazione pervasiva si estende a diversi settori, tra cui le città intelligenti, le case intelligenti, l'assistenza sanitaria e la sorveglianza, modificando radicalmente la vita quotidiana e le operazioni industriali.[1] La rapida crescita dei dispositivi IoT è destinata a proseguire, con stime che prevedono 18,8 miliardi di dispositivi connessi entro la fine del 2024, e un'ulteriore espansione in nuove aree e compiti automatizzati.[2]

La natura intrinseca dei servizi IoT spesso richiede la rivelazione intenzionale di informazioni personali e private in cambio di funzionalità avanzate e personalizzate.[1] Questo rende la sicurezza e la privacy non solo caratteristiche desiderabili, ma requisiti fondamentali per la progettazione e l'implementazione delle tecnologie e dei servizi IoT.[1] La proliferazione della connettività, pur offrendo una comodità e un'efficienza senza precedenti, introduce anche una vasta gamma di rischi nuovi ed emergenti, che vanno dalle violazioni della privacy dei dati al dirottamento dei dispositivi e agli attacchi di denial-of-service.[3] Le conseguenze di una sicurezza IoT inadeguata sono gravi e multidimensionali, estendendosi oltre le tradizionali violazioni dei dati per includere potenziali violazioni della privacy individuale, malfunzionamenti critici dei dispositivi medici, furto di dati finanziari e persino danni fisici.[4] Questi rischi sottolineano la necessità critica di robuste misure di cybersecurity lungo l'intero ciclo

di vita dell'IoT.[3]

La vasta scala e la notevole diversità dei dispositivi IoT, unita alla loro integrazione in domini critici, amplificano intrinsecamente la superficie di attacco e la complessità della messa in sicurezza dell'intero ecosistema. Con miliardi di dispositivi connessi, ognuno con le proprie specificità hardware, software e protocollari, si crea un ambiente eterogeneo che rende estremamente difficile l'applicazione di un approccio di sicurezza unificato. Quando questi dispositivi eterogenei sono interconnessi e integrati in infrastrutture vitali, come quelle delle città intelligenti o dei sistemi sanitari, una vulnerabilità in un singolo tipo di dispositivo può innescare effetti a cascata sull'intero sistema, potenzialmente portando a interruzioni diffuse, come osservato con la botnet Mirai.[1] La "densità pervasiva" di questi dispositivi implica che i fallimenti della sicurezza possono avere un impatto diretto sull'ambiente fisico.[5] Questo sposta la sfida della sicurezza da sistemi isolati a ecosistemi complessi e interconnessi, dove il fallimento di un singolo componente può avere conseguenze sproporzionatamente ampie.

2. Fattori Scatenanti delle Vulnerabilità nei Prodotti IoT Commerciali

Una sfida significativa nel panorama IoT è la realtà diffusa che molti prodotti IoT commerciali sono forniti con meccanismi di sicurezza inadeguati, incompleti o mal progettati.[1] Questa situazione è spesso radicata nell'origine dei produttori. Molti di essi provengono dal mercato dei sensori e attuatori a basso costo, tipicamente impiegati nell'automazione domestica, nel controllo dell'illuminazione o nella videosorveglianza.[1] Questi dispositivi erano originariamente concepiti per operare in sistemi isolati, dove la sicurezza non rappresentava una preoccupazione o una minaccia primaria.[1] La carenza di una solida esperienza in cybersecurity tra questi produttori, unita alla forte pressione per ridurre i costi e i tempi di immissione sul mercato, ha spesso condotto alla commercializzazione di prodotti IoT in cui la sicurezza è trascurata o considerata un ripensamento.[6]

Un fattore umano critico che contribuisce alle vulnerabilità è la frequente mancanza di educazione degli utenti in merito alle pratiche di sicurezza di base.[1] Questa scarsa consapevolezza si traduce spesso nel mancato rispetto da parte degli utenti anche delle procedure più elementari per proteggere i propri dispositivi, come la modifica delle password preinstallate di fabbrica.[1] L'uso di password predefinite o deboli rappresenta una "opportunità a portata di mano" per l'accesso non autorizzato.[8]

La combinazione di pressioni economiche (basso costo, rapido time-to-market) e una

storica carenza di esperienza in cybersecurity tra i produttori di hardware tradizionali genera un "debito di sicurezza" sistemico all'interno dell'ecosistema IoT. Ciò si manifesta non solo come difetti individuali, ma come una filosofia di progettazione e un modello di business che accettano implicitamente un livello di sicurezza inferiore. I dispositivi originariamente pensati per ambienti isolati vengono ora esposti alla rete globale, ereditando le loro carenze di sicurezza iniziali. Questo porta a una vasta base installata di dispositivi intrinsecamente vulnerabili. Il problema è ulteriormente aggravato dalla scarsa formazione degli utenti in materia di sicurezza, che spesso non riescono a implementare misure di protezione basilari, come la modifica delle password predefinite, anche quando queste sono disponibili. Questa situazione crea una vulnerabilità a più livelli: prodotti intrinsecamente insicuri vengono distribuiti e utilizzati da utenti non informati, dando vita a un ambiente altamente sfruttabile. Questo "debito di sicurezza" implica che, anche con futuri miglioramenti, l'eredità dei dispositivi insicuri persisterà per anni, ponendo rischi continui.

3. Casi Studio di Attacchi Noti: Lezioni dal Campo

L'analisi di attacchi reali fornisce una chiara comprensione delle vulnerabilità sfruttate e delle loro conseguenze nel mondo IoT.

3.1. L'Attacco Mirai Botnet (Agosto 2016)

L'attacco Mirai Botnet è stato un massiccio attacco Distributed Denial of Service (DDoS) lanciato contro Dyn, un importante fornitore di infrastrutture DNS (Domain Name System).[1] Il meccanismo di sfruttamento ha coinvolto dispositivi IoT come telecamere e DVR, identificati tramite scansioni internet per dispositivi vulnerabili con porte aperte, impostazioni di fabbrica predefinite e nomi utente e password preinstallati.[1] I dispositivi infetti si univano alla botnet Mirai, controllata da un server centrale di comando e controllo, per inondare i bersagli con traffico.[1] L'impatto è stato devastante: i dispositivi IoT compromessi hanno generato 1,2 terabit al secondo di traffico, causando interruzioni diffuse per siti web importanti come Twitter, Reddit, Netflix e Airbnb in Nord America ed Europa, classificandosi come uno dei più grandi attacchi DDoS di tutti i tempi.[1]

3.2. Vulnerabilità nei Dispositivi Medici Connessi (2017)

Nel 2017, un gruppo di ricerca ha identificato gravi falle di sicurezza in pacemaker e defibrillatori prodotti da St. Jude Medical, principalmente a causa di una mancanza di autenticazione.[1] Questa vulnerabilità avrebbe potuto consentire a un attaccante di accedere ai dispositivi impiantati nel corpo umano, permettendo l'estrazione di dati e la possibilità di sovraccaricare i dispositivi con messaggi per esaurirne più

rapidamente la batteria.[1] La FDA ha confermato queste vulnerabilità di cybersecurity.[1] Simili problemi di sicurezza sono stati riscontrati nel monitor cardiaco per neonati Owlet, dove l'intera interfaccia Wi-Fi non era autenticata.[1] In questo caso, un attaccante avrebbe potuto disconnettere completamente il Wi-Fi, interrompendo gli avvisi critici che monitorano il battito cardiaco di un bambino.[1]

3.3. L'Hack delle Jeep Cherokees (2016)

Nel 2016, i ricercatori di cybersecurity Charlie Miller e Chris Valasek hanno scoperto e sfruttato una vulnerabilità di sicurezza replicabile nelle Jeep Cherokees, che ha avuto un impatto su 1,4 milioni di veicoli e ha portato a un richiamo del prodotto.[1] Il loro meccanismo di sfruttamento ha coinvolto la scansione della rete Sprint per trovare veicoli esposti online, consentendo loro di connettersi alla piattaforma di connettività in-veicolo Uconnect. Una vulnerabilità di esecuzione di codice remoto ha permesso loro di eseguire comandi arbitrari.[1] Da Uconnect, sono riusciti a penetrare nella rete interna del veicolo, il bus CAN (Controller Area Network), che controlla le funzioni critiche del veicolo. Questo ha permesso loro di inviare messaggi alle Electronic Control Units (ECU) che controllano lo sterzo, la frenata, la trasmissione e la velocità, dimostrando un controllo fisico remoto sul veicolo.[1]

Questi casi di studio illustrano una progressione significativa nei fallimenti della sicurezza IoT: dalla vasta interruzione di servizi (Mirai) a minacce dirette alla vita umana (dispositivi medici) e al controllo di sistemi fisici (Jeep). Questa progressione evidenzia che le violazioni della sicurezza IoT non sono confinate al solo regno digitale, ma hanno conseguenze tangibili, gravi e crescenti nel mondo reale, distinguendole dalle tradizionali preoccupazioni di sicurezza IT. La gravità dell'impatto aumenta notevolmente tra gli esempi, passando da interruzioni di servizio a scenari che implicano direttamente danni fisici o perdita di vite. Questo sposta la discussione sulla sicurezza oltre la riservatezza, l'integrità e la disponibilità dei dati (la triade CIA) per includere la sicurezza e il benessere umano. L'integrazione crescente dell'IoT in domini critici per la sicurezza (sanità, trasporti, controllo industriale) significa che i fallimenti della cybersecurity hanno ora implicazioni dirette sulla sicurezza. Ciò rende necessaria una rivalutazione dei modelli di rischio, dei quadri normativi e delle pratiche ingegneristiche per dare priorità alla "sicurezza by design" con una forte enfasi sulla sicurezza fisica, piuttosto che trattare la sicurezza come un aspetto secondario. Il concetto di "Internet delle Minacce" [6] diventa una realtà lampante quando la sicurezza fisica è in gioco.

La tabella seguente riassume gli attacchi IoT noti e le vulnerabilità sfruttate, fornendo una panoramica comparativa chiara delle metodologie di attacco e dei loro obiettivi.

Tabella 1: Riepilogo Attacchi IoT Noti e Vulnerabilità Sfruttate

Nome dell'Attacco	Anno/Periodo	Dispositivi IoT Coinvolti	Vulnerabilità Sfruttate	Impatto Principale	Fonte
Mirai Botnet	Agosto 2016	Telecamere, DVR	Porte aperte, impostazioni di fabbrica predefinite, credenziali preinstallate	Attacco DDoS massivo, interruzione servizi internet	[1]
Pacemaker/Defibrillatore St. Jude Medical	2017	Pacemaker, defibrillatori	Mancanza di autenticazione	Estrazione dati, esaurimento batteria, rischio per la vita	[1]
Owlet (sensore neonati)	2017	Sensore cardiaco per neonati	Interfaccia Wi-Fi non autenticata	Disconnessione Wi-Fi, interruzione allarmi critici	[1]
Jeep Cherokees hack	2016	Veicoli (1.4 milioni)	Vulnerabilità di esecuzione di codice remoto (Uconnect)	Controllo remoto di sterzo, freni, trasmissione, velocità	[1]

4. Classificazione Dettagliata delle Vulnerabilità nell'Architettura IoT

L'architettura IoT può essere suddivisa in strati, ognuno dei quali presenta specifiche vulnerabilità che possono essere sfruttate dagli attaccanti.

4.1. Thing Layer (Strato degli Oggetti)

Questo strato comprende i dispositivi IoT fisici, come sensori e attuatori. Le vulnerabilità a questo livello sono diverse e possono compromettere l'integrità e la disponibilità dei dati e dei dispositivi stessi.

Una minaccia comune è la Cattura del Nodo (Node Capturing), in cui un attaccante può fisicamente rubare o sostituire un nodo legittimo con uno malevolo, introducendo così un dispositivo compromesso nella rete.1 Un'altra vulnerabilità significativa è l'Iniezione di Codice Malevolo (Malicious Code Injection). Gli attaccanti possono iniettare codice dannoso nella memoria del nodo. Questo è particolarmente critico poiché gli aggiornamenti firmware e software sono spesso eseguiti "over-the-air" (OTA). Se il processo OTA non è crittografato, un attaccante può intercettare la comunicazione e iniettare firmware malevolo, compromettendo l'integrità e la funzionalità del dispositivo.1
Gli **Attacchi di Iniezione di Dati Falsi (False Data Injection Attack)** si verificano quando un nodo malevolo viene utilizzato per iniettare dati errati nel sistema IoT, portando a risultati falsi e a potenziali malfunzionamenti delle applicazioni IoT che si basano su letture accurate dei sensori.[1] Inoltre, i nodi IoT sono frequentemente distribuiti in ambienti aperti, rendendoli suscettibili all'**Intercettazione e Interferenza (Eavesdropping and Interference)**. Gli attaccanti possono intercettare e catturare i dati durante la trasmissione o l'autenticazione, compromettendo la riservatezza dei dati.[1] Infine, gli **Attacchi di Privazione del Sonno (Sleep Deprivation Attacks)** mirano a esaurire la batteria dei dispositivi IoT a bassa potenza, costringendoli a rimanere attivi. Questo porta a un denial of service (DoS) da parte di quei nodi, rendendoli inutilizzabili.[1]

4.2. Network Layer (Strato di Rete)

Questo strato gestisce la comunicazione tra i dispositivi IoT e l'infrastruttura internet più ampia. Gli **Attacchi DoS/DDoS (Denial of Service/Distributed Denial of Service)** sono un rischio preponderante, in cui gli attaccanti inondano i server target con richieste indesiderate, rendendoli incapaci di fornire servizi agli utenti legittimi.[1] Le applicazioni IoT sono estremamente suscettibili agli attacchi DDoS distribuiti se un attaccante riesce a controllare numerosi dispositivi IoT, formando efficacemente una botnet, come dimostrato dall'attacco Mirai.[1]

Gli **Attacchi di Routing (Routing Attacks)** sono un'altra categoria di minacce, in cui nodi malevoli tentano di reindirizzare i percorsi di trasferimento dei dati.[1] L'**Attacco Sinkhole** ne è un esempio: un avversario pubblicizza un percorso di routing apparentemente migliore per attirare i nodi a instradare il traffico attraverso il nodo compromesso. L'attaccante può quindi eliminare o modificare i pacchetti di dati prima di inoltrarli, rendendo difficile il rilevamento.[1] Questo è un attacco comune nelle reti di sensori wireless.[1] Un altro tipo è l'**Attacco Wormhole**, in cui un attaccante stabilisce una connessione fuori banda (wormhole) tra un nodo compromesso e un dispositivo, aggirando i protocolli di sicurezza standard.[1]

4.3. Middleware e Gateway Layers

Questi strati fungono da ponte tra i dispositivi IoT e le applicazioni, gestendo la traduzione dei protocolli e l'elaborazione dei dati. L'**Attacco Man-in-the-Middle (MitM)** è una minaccia significativa, in particolare per protocolli come MQTT, che utilizzano un modello di comunicazione publish-subscribe. Se un attaccante controlla il broker MQTT, può diventare un MitM, ottenendo il controllo completo su tutte le comunicazioni senza che i client ne siano a conoscenza.[1]

Un'altra problematica riguarda le **Questioni di Crittografia End-to-End (End-to-End Encryption Issues)**. Sebbene la crittografia end-to-end sia fondamentale per la riservatezza dei dati, i gateway spesso devono decifrare e poi ricifrare i messaggi per la traduzione dei protocolli. Durante questo processo, i dati diventano temporaneamente esposti e suscettibili a violazioni.[1]

L'architettura a strati dell'IoT, pur offrendo modularità, crea superfici di attacco distinte a ogni livello. Una vulnerabilità sfruttata a un livello inferiore, come lo Strato degli Oggetti, può spesso fungere da abilitatore o punto di partenza per attacchi più gravi a livelli superiori, come lo Strato di Rete o il Middleware. Ad esempio, se un attaccante inietta codice malevolo in un dispositivo IoT [1], quel dispositivo compromesso può essere poi utilizzato per attacchi di iniezione di dati falsi o, più criticamente, diventare parte di una botnet per attacchi DoS/DDoS a livello di rete.[1] Allo stesso modo, un attacco sinkhole riuscito a livello di rete [1] si basa sulla compromissione di un nodo a livello di oggetto. Le problematiche relative alla crittografia end-to-end a livello di Middleware/Gateway [1] sorgono perché il gateway, agendo come traduttore, deve temporaneamente esporre i dati, creando un punto di vulnerabilità critico anche se il dispositivo stesso è sicuro. Questa interconnessione implica che la messa in sicurezza dell'IoT non può basarsi su misure di sicurezza isolate per ogni strato. È essenziale una strategia olistica di "difesa in profondità", in cui i controlli di sicurezza a un livello sono progettati per prevenire o mitigare attacchi che potrebbero originare o propagarsi attraverso vulnerabilità in altri strati. L'anello più debole della catena può compromettere l'intero sistema, sottolineando la necessità di una sicurezza robusta su tutti i componenti architetturali.

La tabella seguente offre una categorizzazione sistematica delle vulnerabilità identificate per ciascun strato dell'architettura IoT.

Tabella 2: Vulnerabilità per Strato dell'Architettura IoT

Strato Architetturale	Tipo di Vulnerabilità/At	Descrizione	Esempi (se	Fonte

IoT	tacco	Breve	applicabile)	
Thing Layer	Node Capturing	Sostituzione di un nodo legittimo con uno malevolo.		[1]
	Malicious Code Injection	Iniezione di codice malevolo nella memoria del nodo, spesso tramite aggiornamenti OTA non crittografati.	Iniezione firmware malevolo	[1]
	False Data Injection Attack	Iniezione di dati errati nel sistema IoT tramite un nodo malevolo.	Letture sensore inaccurate	[1]
	Eavesdropping and Interference	Intercettazione e cattura di dati durante trasmissione/autenticazione in ambienti aperti.		[1]
	Sleep Deprivation Attacks	Esaurimento della batteria di dispositivi a bassa potenza, causando DoS.		[1]
Network Layer	DoS/DDoS Attacks	Inondazione di server target con richieste per interrompere i servizi.	Mirai Botnet Attack	[1]
	Routing Attacks	Reindirizzamento dei percorsi di	Sinkhole Attack, Wormhole	[1]

		trasferimento dati tramite nodi malevoli.	Attack	
Middleware and Gateway Layers	Man-in-the-Middle Attack	Controllo del broker MQTT per intercettare tutte le comunicazioni.	Attacco al broker MQTT	[1]
	End-to-End Encryption Issues	Esposizione temporanea dei dati durante decrittografia/ricrittografia per traduzione protocolli.	Dati vulnerabili al gateway	[1]

5. Analisi Approfondita dei Protocolli IoT Popolari e delle Loro Debolezze di Sicurezza

La sicurezza dei dispositivi IoT dipende in gran parte dai protocolli di comunicazione utilizzati. Un'analisi dettagliata di ZigBee, Bluetooth Low Energy (BLE) e LoRaWAN rivela le loro specifiche misure di sicurezza, ma anche le vulnerabilità intrinseche e i vettori di attacco documentati.

5.1. ZigBee

Misure di Sicurezza:
ZigBee utilizza i livelli PHY e MAC dello standard IEEE 802.15.4.1 Il livello di rete (NWK) fornisce funzionalità di routing, sicurezza e configurazione dei dispositivi.1 Un coordinatore di rete funge da Trust Center, responsabile dell'autenticazione dei dispositivi che richiedono di unirsi alla rete, dell'accettazione o del rifiuto delle richieste di adesione, del mantenimento e della distribuzione delle chiavi di rete, e dell'abilitazione della sicurezza end-to-end.1 ZigBee impiega due chiavi crittografiche a 128 bit: una chiave di collegamento (link key) per le comunicazioni unicast e una chiave di rete (network key) per le comunicazioni broadcast, condivisa all'interno della rete. I fornitori possono anche fornire chiavi master specifiche per il dispositivo.1 I metodi di acquisizione delle chiavi includono la preinstallazione, il trasporto della chiave (solitamente dal Trust Center) e lo stabilimento della chiave utilizzando la crittografia asimmetrica (ad esempio, Elliptic Curve Diffie-Hellman).1
Vulnerabilità e Attacchi Specifici:
Nonostante le funzionalità di sicurezza, le chiavi di collegamento o di rete vengono spesso inviate non crittografate via etere durante il trasporto della chiave.1 Questo rende possibile un Attacco di Sniffing della Chiave di Rete ZigBee. Un attaccante può utilizzare un dongle USB

Texas Instruments CC2531 con il software SmartRF Protocol Packet Sniffer per catturare e analizzare questi dati, acquisendo così la chiave di rete.1 Questa vulnerabilità evidenzia un difetto critico di implementazione in cui chiavi sicure vengono trasmesse in modo insicuro.
Un altro attacco comune è l'**Attacco Sinkhole**, molto diffuso nelle reti di sensori wireless.[1] Un nodo compromesso diffonde false informazioni sulle sue capacità di routing, fingendo di avere un percorso ottimale verso la Base Station.[1] Gli altri nodi reindirizzano quindi il loro traffico attraverso questo nodo malevolo, consentendo all'attaccante di eliminare o modificare i pacchetti di dati, rendendo difficile il rilevamento.[1] Un esempio pratico di attacco Sinkhole è stato dimostrato in una rete mesh ZigBee: un tablet Android compromesso, agendo come nodo legittimo, può essere hackerato tramite malware (ad esempio, un Trojan) per modificare i parametri di potenza di trasmissione del suo SoC ZigBee.[1] Aumentando la sua qualità di collegamento percepita (che nelle reti mesh è spesso legata alla potenza di trasmissione), il dispositivo malevolo può diventare un percorso di routing attraente, eseguendo efficacemente un attacco sinkhole e intercettando/modificando il traffico.[1]

5.2. Bluetooth Low Energy (BLE)

Misure di Sicurezza:
BLE opera nella banda ISM a 2,4 GHz senza licenza, utilizzando 40 canali.1 Il livello MAC è diviso in pubblicità (3 canali) e trasferimento dati (37 canali).1 I dati vengono inviati a raffiche per risparmiare energia, consentendo ai periferici di rimanere in modalità sleep.1 Gli indirizzi MAC BLE sono nascosti, con indirizzi casuali che cambiano frequentemente. Esistono tre tipi: indirizzo statico casuale (per ciclo di accensione), indirizzo privato risolvibile (RPA, generato con una chiave di risoluzione dell'identità per dispositivi fidati) e indirizzo privato non risolvibile (anonimato completo).1 La crittografia e l'autenticazione si basano su AES con chiavi a 128 bit. La chiave di collegamento simmetrica viene generata durante una procedura di pairing che include lo scambio di funzionalità (non crittografato), lo stabilimento della chiave (chiave temporanea, chiave a breve termine), la distribuzione della chiave (chiavi a lungo termine) e il bonding (memorizzazione delle chiavi di collegamento comuni).1 I metodi di pairing includono "Just Works" (TK=0, nessuna sicurezza), "Numeric Comparison" (richiede display, conferma utente) e "Passkey" (input utente, valori di commitment, maggiore sicurezza).1
Vulnerabilità e Attacchi Specifici:
Un esempio lampante di vulnerabilità è lo Sniffing del Traffico di Rete, come dimostrato da un caso di studio sui fitness tracker.1 La vulnerabilità risiede nella frequenza dei pacchetti di advertising BLE e nella scarsa gestione degli indirizzi.1 I fitness tracker pubblicizzano continuamente la loro presenza, soprattutto quando non sono connessi a uno smartphone.1 Il problema è che la maggior parte dei tracker utilizza indirizzi statici o indirizzi privati risolvibili che non cambiano, nemmeno dopo una scarica completa della batteria.1 Questo li rende altamente vulnerabili al tracciamento mentre gli utenti si muovono in luoghi pubblici.1 La quantità di traffico dati BLE è correlata all'intensità del movimento dell'utente, consentendo a

un attaccante di inferire l'attività (ad esempio, seduto, che cammina, che corre).1 Inoltre, i dati BLE mostrano schemi diversi per le diverse andature degli utenti, consentendo l'identificazione delle persone da un piccolo gruppo di utenti.1
Un altro attacco critico è l'**Attacco KNOB (Key Negotiation of BLE)**. Questo attacco sfrutta gli scambi di funzionalità non crittografati durante la procedura di pairing.[1] Un attaccante Man-in-the-Middle (MitM) può degradare l'entropia di qualsiasi chiave a lungo termine (LTK) e chiave di sessione BLE a soli 7 byte.[1] Questa bassa entropia consente all'attaccante di forzare la chiave con attacchi a forza bruta.[1] Una volta che l'attaccante conosce la chiave di sessione, può decifrare tutto il testo cifrato scambiato tra le parti legittime e iniettare testo cifrato valido nella sessione, annullando tutte le garanzie di sicurezza.[1] Questo attacco è conforme allo standard, remoto e furtivo, e colpisce varie versioni e dispositivi Bluetooth.[13]

5.3. LoRaWAN

Misure di Sicurezza:
LoRaWAN utilizza AES-CTR come schema di crittografia.1 La chiave AppSKey è impiegata per la crittografia end-to-end.1 Il contatore per AES-CTR è il contatore del frame nel frame MAC di LoRa, piuttosto che un vero nonce crittografico.1
Vulnerabilità e Attacchi Specifici:
La vulnerabilità critica di LoRaWAN risiede nell'Eavesdropping LoRa. Il difetto principale è l'uso del contatore del frame come contatore per AES-CTR. Questo contatore viene resettato a 0 dopo ogni sessione di trasmissione, portando al riutilizzo dello stesso keystream più volte.1 Quando lo stesso keystream viene utilizzato, l'operazione XOR di due testi cifrati crittografati con quel flusso è uguale all'operazione XOR dei loro corrispondenti testi in chiaro.1 Sebbene ciò non riveli direttamente il testo in chiaro, un attaccante che conosce o può indovinare parte di un testo in chiaro (ad esempio, "temperatura: " da un sensore) può utilizzare tecniche come il "crib-dragging" per dedurre parti dei messaggi originali.1 Questo compromette la riservatezza dei dati trasmessi.15
Un tema ricorrente tra ZigBee, BLE e LoRaWAN è che anche i protocolli con caratteristiche di sicurezza teoricamente solide possono essere resi vulnerabili a causa di scelte di implementazione pratiche, compromessi di progettazione (ad esempio, risparmio energetico vs. privacy) o errori crittografici fondamentali. Ciò sottolinea che la "sicurezza by design" deve estendersi oltre la specifica teorica del protocollo fino alla distribuzione pratica e al comportamento dell'utente. Ad esempio, per ZigBee, la vulnerabilità risiede nel *trasporto* della chiave, non nella sua forza, indicando un difetto di implementazione. Per BLE, la problematica è un compromesso: il pairing "Just Works" privilegia la facilità d'uso rispetto alla sicurezza, e i produttori/utenti spesso disabilitano o ignorano le funzionalità di privacy (indirizzi randomizzati) per comodità, portando a fughe di dati. L'attacco KNOB sfrutta un difetto nella *negoziazione* dei parametri di sicurezza, consentendo un downgrade

prima che venga applicata una crittografia robusta. Per LoRaWAN, si tratta di una grave errata applicazione crittografica: il riutilizzo di un contatore come nonce in AES-CTR, una vulnerabilità nota nelle cifrature a flusso. Questo significa che l'algoritmo è forte, ma la sua *applicazione* è difettosa. Questo schema, osservato in diversi protocolli, suggerisce che per ottenere una sicurezza IoT robusta sono necessari non solo algoritmi crittografici forti, ma anche pratiche di implementazione sicure, un'attenta considerazione dei compromessi tra usabilità e sicurezza, l'adesione alle migliori pratiche crittografiche (ad esempio, nonce unici) e, potenzialmente, l'applicazione normativa per colmare queste lacune tra la sicurezza teorica e la realtà pratica. Il problema spesso non è *quale* sicurezza è disponibile, ma *come* viene applicata e *se* viene utilizzata correttamente.

La seguente tabella offre un confronto dettagliato delle misure di sicurezza, delle vulnerabilità e degli attacchi specifici per ciascuno dei protocolli IoT esaminati.

Tabella 3: Confronto Sicurezza e Attacchi nei Protocolli IoT (ZigBee, BLE, LoRaWAN)

Protocollo	Misure di Sicurezza Chiave	Vulnerabilità Specifica	Meccanismo dell'Attacco	Esempio/Caso Studio	Fonte
ZigBee	IEEE 802.15.4 PHY/MAC, NWK (routing, sicurezza), Trust Center (autenticazione, gestione chiavi), Chiavi a 128 bit (link, network, master), Acquisizione chiavi (preinstallazione, trasporto, stabilimento	Network Key Sniffing Attack	Chiavi inviate non crittografate via etere; cattura con dongle USB e software sniffer.	Texas Instruments CC2531 USB dongle, SmartRF Protocol Packet Sniffer	[1]

	con ECC)				
		Sinkhole Attack	Nodo compromesso pubblicizza percorso migliore; reindirizzamento traffico, modifica/eliminazione dati.	Tablet Android compromesso in rete mesh ZigBee	[1]
BLE	2.4 GHz ISM, 40 canali, MAC layer (advertising/data transfer), Burst data per risparmio energia, Indirizzi MAC nascosti (Random Static, RPA, Non-resolvable Private), AES-128 bit per crittografia/autenticazione, Pairing (Feature exchange, Key establishment, Key distribution, Bonding), Metodi di Pairing ("Just Works", Numeric Comparison,	Network Traffic Sniffing (Privacy Leakage)	Pacchetti di advertising frequenti, scarsa gestione indirizzi (statici/non mutevoli); tracciamento utente, inferenza attività/identità.	Fitness Tracker (es. Fitbit)	[1]

	Passkey)				
		KNOB Attack	Sfruttamento scambi di funzionalità non crittografati durante il pairing; downgrade entropia chiave a 7 byte; attacco MitM.	Attacco MitM per degradare chiavi LTK/sessione BLE	[1]
LoRaWAN	AES-CTR per crittografia, AppSKey per crittografia end-to-end, Contatore del frame MAC come contatore AES-CTR.	Eavesdropping LoRa (Key Stream Reuse)	Contatore del frame resettato a 0 dopo ogni sessione; riutilizzo dello stesso keystream; XOR di testi cifrati rivela XOR di testi in chiaro.	"Crib-dragging" per dedurre messaggi da sensori di temperatura	[1]

6. Implicazioni e Conseguenze a Lungo Termine delle Vulnerabilità IoT

Le vulnerabilità nell'IoT hanno implicazioni di vasta portata che trascendono le tradizionali violazioni dei dati, configurandosi come una minaccia per la sicurezza fisica, la stabilità delle infrastrutture critiche e l'economia globale.

Dalla Violazione della Privacy al Dirottamento di Infrastrutture Critiche

Le vulnerabilità IoT si estendono oltre le violazioni dei dati, comprendendo significative preoccupazioni per la privacy a causa della raccolta e trasmissione di vaste quantità di dati sensibili.[1] Le conseguenze possono includere il dirottamento dei dispositivi, dove gli attaccanti prendono il controllo delle funzioni dei dispositivi per lanciare ulteriori attacchi o interrompere le operazioni.[3] Botnet su larga scala formate da dispositivi IoT compromessi possono sopraffare e disabilitare infrastrutture critiche e servizi online, come dimostrato dall'attacco Mirai.[1] L'integrazione dell'IoT negli edifici

intelligenti, ad esempio, ha portato a casi in cui attori malevoli sfruttano i dispositivi per disabilitare i controller, reclutare dispositivi di controllo degli accessi fisici in botnet o ottenere l'accesso iniziale alle reti aziendali.[16] Per l'IoT industriale (IIoT) e la tecnologia operativa (OT), le vulnerabilità nei data historian o nell'archiviazione remota dei dati OT possono espandere la superficie di attacco delle reti critiche.[16]

Rischi nella Supply Chain

La compromissione della catena di approvvigionamento dei dispositivi IoT può introdurre codice o componenti malevoli, lasciando i dispositivi vulnerabili agli attacchi anche prima che raggiungano l'utente finale.[3] Le complesse catene di approvvigionamento che coinvolgono decine o centinaia di componenti provenienti da diversi fornitori rendono la garanzia e la documentazione della sicurezza di ogni componente un'impresa enorme.[17]

Impatto Economico

Le conseguenze finanziarie del mancato rispetto dei requisiti normativi sono severe, con multe che possono raggiungere fino a 15 milioni di euro o il 2,5% del fatturato annuo mondiale, a seconda di quale sia maggiore, nell'ambito di quadri normativi come l'EU Cyber Resilience Act.[17] I prodotti non conformi possono affrontare restrizioni di accesso al mercato, vietandone la vendita nei mercati regolamentati, come evidenziato dal PSTI Act del Regno Unito.[17] Oltre alle multe, i richiami di prodotti dovuti a preoccupazioni di cybersecurity, come il richiamo da parte della FDA di quasi 500.000 pacemaker nel 2017, possono costare ai produttori milioni in spese di richiamo.[17]

Le implicazioni delle vulnerabilità IoT spostano fondamentalmente la cybersecurity da una preoccupazione puramente digitale a una "cyber-fisica", dove gli exploit digitali possono tradursi direttamente in danni fisici, interruzioni delle infrastrutture critiche e costi economici e sociali significativi. Questa interconnessione amplifica il potenziale di fallimenti diffusi e a cascata in vari settori. L'aspetto unico dell'IoT è la sua interfaccia diretta con il mondo fisico. A differenza delle tradizionali violazioni IT che potrebbero portare a perdita di dati o frodi finanziarie, le violazioni IoT possono causare la perdita di vite umane, l'arresto di infrastrutture critiche (ad esempio, reti elettriche, trasporti) e danni ambientali su larga scala. L'attacco Mirai ha dimostrato come dispositivi apparentemente innocui (telecamere, DVR) possano essere trasformati in armi per abbattere importanti servizi internet, evidenziando l'effetto di amplificazione della scala. Il rischio della catena di approvvigionamento [3] significa che le vulnerabilità possono essere incorporate alla fonte, rendendole più difficili da rilevare e mitigare in seguito, aumentando il rischio sistemico. Questo "nesso

cyber-fisico" implica che la valutazione del rischio per l'IoT deve incorporare i principi di ingegneria della sicurezza accanto alla cybersecurity tradizionale. Le crescenti sanzioni finanziarie e regolamentari [17] riflettono un crescente riconoscimento sociale di questi rischi amplificati, spingendo a una maggiore responsabilità da parte dei produttori. L'aumento del punteggio medio di rischio dei dispositivi [16] indica un panorama di minacce in escalation che colpisce tutti i settori, sottolineando che queste implicazioni non sono teoriche ma presenti e in peggioramento.

7. Strategie di Mitigazione e Best Practices per un Ecosistema IoT Sicuro

La mitigazione delle vulnerabilità IoT richiede un approccio coordinato che coinvolga sia i produttori che gli utenti e le organizzazioni.

7.1. Responsabilità dei Produttori e Panorama Normativo

L'imperativo della "Security by Design" è sempre più riconosciuto, con i regolatori che promuovono l'integrazione delle funzionalità di sicurezza nei dispositivi IoT fin dalla fase di progettazione, piuttosto che trattare la sicurezza come un ripensamento.[6] Ciò include pratiche di sviluppo sicure, una robusta autenticazione dei dispositivi e un design hardware sicuro.[18] I produttori sono tenuti a implementare processi di gestione delle vulnerabilità e a fornire supporto e aggiornamenti di sicurezza continui per l'intero ciclo di vita del prodotto.[2] Questo comprende politiche chiare per gli aggiornamenti del firmware e patch regolari.[8]

Il panorama normativo sta evolvendo rapidamente per affrontare queste sfide. L'**EU Cyber Resilience Act (CRA)**, la cui piena attuazione è prevista entro il 2027, introduce requisiti di sicurezza obbligatori per i prodotti con elementi digitali, ponendo l'accento sulla sicurezza by design, la gestione delle vulnerabilità e una documentazione completa. La non conformità può comportare multe fino a 15 milioni di euro o il 2,5% del fatturato annuo mondiale.[17] Il **UK Product Security and Telecommunications Infrastructure (PSTI) Act (2022)** vieta le password predefinite, richiede trasparenza sul supporto agli aggiornamenti di sicurezza e impone politiche di divulgazione delle vulnerabilità per i prodotti IoT di consumo, con restrizioni di accesso al mercato per i dispositivi non conformi.[17] Negli Stati Uniti, il **NIST IoT Cybersecurity Framework**, sebbene non sia una regolamentazione in sé, guida i requisiti normativi, come il US Cyber Trust Mark. L'U.S. IoT Cybersecurity Improvement Act del 2020 impone al NIST di creare standard minimi di sicurezza IoT per i dispositivi del governo federale, concentrandosi sullo sviluppo sicuro, la gestione delle identità, il patching e la gestione della configurazione.[17] Infine, la **FDA**

Cybersecurity Requirements (Healthcare IoT) ha rafforzato le aspettative di cybersecurity per i dispositivi medici attraverso la guida per la presentazione pre-mercato e i requisiti di gestione della sicurezza post-mercato, come dimostrato dal richiamo dei pacemaker del 2017.[7]

Le sfide di conformità per i produttori sono significative. Il **tracciamento e la messa in sicurezza dei componenti di terze parti** sono complessi a causa delle intricate catene di approvvigionamento, dove un singolo dispositivo può incorporare numerosi componenti di diversi fornitori.[17] I **requisiti SBOM (Software Bill of Materials)**, inventari completi dei componenti software, stanno diventando un'aspettativa normativa ma sono difficili da creare e mantenere manualmente.[17] Inoltre, le **valutazioni continue della sicurezza** sono sempre più richieste dai quadri normativi per l'intero ciclo di vita del prodotto, il che rappresenta un onere operativo significativo per i produttori con risorse limitate.[17] La **gestione del rischio della catena di approvvigionamento** impone ai produttori la responsabilità della sicurezza lungo tutta la loro supply chain, richiedendo processi formali di valutazione dei fornitori e requisiti contrattuali di sicurezza.[17]

Il panorama normativo globale sta subendo una trasformazione significativa, passando da linee guida volontarie a requisiti obbligatori che attribuiscono esplicitamente ai produttori la responsabilità della "sicurezza by design" e della gestione continua delle vulnerabilità per l'intero ciclo di vita del prodotto. Questo rappresenta un cambiamento cruciale dalla correzione reattiva alla sicurezza proattiva e integrata. Le sanzioni finanziarie e le restrizioni di accesso al mercato [17] forniscono forti incentivi alla conformità. Tuttavia, le sfide identificate per i produttori, come il tracciamento dei componenti di terze parti, i requisiti SBOM e le valutazioni continue, rivelano le difficoltà pratiche. Molti produttori, specialmente quelli di dispositivi IoT a basso costo [1], non dispongono dell'esperienza o delle risorse per soddisfare questi requisiti stringenti. Questa spinta normativa sta forzando un cambiamento fondamentale nelle pratiche di produzione, potenzialmente portando a un aumento dei costi per i consumatori o a un consolidamento nel mercato IoT, poiché i produttori più piccoli e meno sicuri faticano a conformarsi. Sottolinea anche un potenziale collo di bottiglia nella catena di approvvigionamento, dove la sicurezza dei singoli componenti di diversi fornitori diventa di primaria importanza. La mancanza di standard universali [7] complica ulteriormente questo aspetto, suggerendo la necessità di una maggiore armonizzazione internazionale per evitare sforzi di conformità frammentati.

La seguente tabella offre una panoramica strutturata delle principali regolamentazioni

e framework che influenzano la sicurezza IoT.

Tabella 4: Panoramica delle Regolamentazioni Chiave sulla Sicurezza IoT

Regolamentazione/Framework	Regione/Paese	Anno di Entrata in Vigore/Proposta	Obiettivi Principali	Requisiti Chiave per i Produttori	Conseguenze della Non-Conformità	Fonte
EU Cyber Resilience Act (CRA)	Unione Europea	Proposto 2022, atteso 2027	Alto livello comune di cybersecurity per prodotti digitali	Sicurezza by design, gestione vulnerabilità, documentazione completa, aggiornamenti software	Multe fino a €15M o 2.5% fatturato annuo mondiale	[17]
UK Product Security and Telecommunications Infrastructure (PSTI) Act	Regno Unito	2022	Migliorare sicurezza prodotti IoT di consumo	Divieto password predefinite, trasparenza aggiornamenti, politiche divulgazione vulnerabilità	Restrizioni accesso al mercato UK	[17]
NIST IoT Cybersecurity Framework (US)	Stati Uniti	2020 (IoT Cybersecurity Improvement Act)	Guida per requisiti sicurezza IoT (es. US Cyber Trust Mark)	Sviluppo sicuro, gestione identità, patching, gestione configuraz	Agenzie federali non possono acquistare dispositivi non	[17]

				ione	conformi	
FDA Cybersecurity Requirements (Healthcare IoT)	Stati Uniti	Continuo (rafforzato)	Rafforzare aspettative cybersecurity per dispositivi medici	Guida pre-mercato, gestione sicurezza post-mercato	Richiami di prodotti (es. pacemaker 2017)	[7]

7.2. Best Practices per Utenti e Organizzazioni

Oltre alle responsabilità dei produttori, gli utenti e le organizzazioni giocano un ruolo cruciale nella protezione degli ecosistemi IoT.

La **configurazione sicura e la gestione delle credenziali** sono fondamentali. Le password predefinite devono essere cambiate immediatamente.[1] È imperativo implementare password forti e uniche e aggiornarle regolarmente.[8] Laddove possibile, è consigliabile utilizzare l'autenticazione a più fattori (MFA), preferibilmente con token hardware o app di autenticazione.[8] È inoltre essenziale implementare una robusta autenticazione dei dispositivi per garantire che solo i dispositivi autorizzati accedano alla rete.[18]

La **segmentazione della rete** è una pratica chiave: isolare i dispositivi IoT dalle reti IT principali previene violazioni a livello di sistema [2], limitando il raggio d'azione di una potenziale compromissione.[3] Per quanto riguarda la **crittografia**, tutti i dati in transito e a riposo devono essere crittografati utilizzando protocolli di crittografia robusti come TLS 1.3 o superiore.[2] È fondamentale garantire la crittografia end-to-end per proteggere le informazioni sensibili [2] e rinnovare regolarmente chiavi e certificati di crittografia.[8]

Gli **aggiornamenti regolari** sono vitali. Le vulnerabilità di sicurezza devono essere affrontate prontamente e gli aggiornamenti rilasciati senza indugio.[7] È consigliabile automatizzare la gestione del firmware, tracciare le versioni e stabilire un programma di aggiornamento routinario.[8] Gli aggiornamenti regolari correggono le vulnerabilità di sicurezza e migliorano la resilienza dei dispositivi.[18] Va notato che molti dispositivi IoT più economici spesso non ricevono aggiornamenti di sicurezza robusti, lasciando le vulnerabilità non patchate.[22]

Il **monitoraggio e la risposta agli incidenti** sono componenti essenziali. I dispositivi IoT devono essere monitorati per attività sospette utilizzando strumenti di sicurezza come i sistemi di rilevamento delle intrusioni.[3] L'implementazione di funzionalità

anti-manomissione (tamper-evident) è cruciale per rilevare e rispondere a interferenze fisiche.[18] È inoltre necessario sviluppare piani completi di risposta agli incidenti.[8]

La **minimizzazione dei dati e il consenso informato** sono principi etici e di sicurezza. La raccolta e la conservazione dei dati personali dovrebbero essere limitate a quanto strettamente necessario per la funzione del dispositivo.[1] È fondamentale garantire la trasparenza nelle pratiche di raccolta dei dati e ottenere un consenso significativo dagli utenti.[7]

Infine, l'**educazione degli utenti** è un pilastro. È necessario istruire dipendenti e consumatori sui rischi IoT e sulle pratiche sicure, inclusa l'identificazione degli attacchi di phishing e l'uso di password robuste.[3] Dare agli utenti gli strumenti per gestire le proprie impostazioni di privacy li responsabilizza a prendere decisioni informate sui dati che sono disposti a condividere.[18]

Nonostante la complessità della sicurezza IoT, molte vulnerabilità diffuse e attacchi riusciti continuano a derivare dalla mancata implementazione di pratiche fondamentali di igiene cibernetica, in particolare per quanto riguarda le credenziali predefinite, gli aggiornamenti regolari e la segmentazione della rete. Questo sottolinea il ruolo critico, spesso sottovalutato, dell'educazione degli utenti e delle politiche organizzative nella mitigazione dei rischi IoT. La ricorrenza di questi problemi "di base" in diverse fonti, anche nel contesto di minacce IoT avanzate, suggerisce che il problema non riguarda sempre exploit sofisticati "zero-day", ma piuttosto la diffusa negligenza dei controlli di sicurezza fondamentali. Questo rappresenta un vettore di vulnerabilità significativo perché è facilmente sfruttabile su larga scala (ad esempio, Mirai). I "vincoli di risorse" di molti dispositivi IoT [22] li rendono anche più vulnerabili ad attacchi semplici come il DoS se mancano le protezioni di base. Una sicurezza IoT efficace richiede un duplice approccio: soluzioni tecniche avanzate per minacce complesse e l'adozione diffusa di un'igiene cibernetica di base. Ciò impone un onere significativo sull'educazione degli utenti e sulla chiara comunicazione delle pratiche sulla privacy [18], oltre che sui produttori per abilitare e imporre queste pratiche attraverso impostazioni predefinite sicure e interfacce user-friendly. Senza affrontare questi fattori umani e operativi fondamentali, anche le tecnologie di sicurezza più avanzate potrebbero rivelarsi insufficienti.

La seguente tabella riassume le migliori pratiche per la sicurezza IoT, delineando il ruolo di utenti e produttori.

Tabella 5: Best Practices per la Sicurezza IoT: Ruolo di Utenti e Produttori

Area di Best Practice	Descrizione della Best Practice	Responsabilità Principale	Beneficio per la Sicurezza	Fonte
Gestione Credenziali	Cambiare password predefinite; usare password forti e uniche; MFA; autenticazione robusta dei dispositivi.	Utente/Organizzazione, Produttore	Prevenire accessi non autorizzati; rafforzare l'autenticazione.	1
Rete	Segmentazione della rete per isolare i dispositivi IoT dalle reti IT principali.	Organizzazione	Limitare la diffusione di violazioni; contenere i danni.	2
Crittografia	Crittografare tutti i dati in transito e a riposo (es. TLS 1.3+); crittografia end-to-end; rinnovo chiavi.	Produttore, Organizzazione	Proteggere la riservatezza dei dati; prevenire intercettazioni.	2
Aggiornamenti	Aggiornamenti regolari di firmware e software; gestione automatizzata; politiche chiare di patching.	Produttore, Utente/Organizzazione	Correggere vulnerabilità note; migliorare la resilienza del dispositivo.	7
Monitoraggio e Risposta	Monitoraggio attività sospette;	Organizzazione	Rilevare e rispondere	3

	sistemi di rilevamento intrusioni; funzionalità anti-manomissione; piani di risposta agli incidenti.		rapidamente alle minacce; mitigare i danni.	
Dati e Privacy	Minimizzazione della raccolta dati; trasparenza; consenso informato; gestione impostazioni privacy.	Produttore, Utente/Organizzazione	Proteggere la privacy degli utenti; ridurre il rischio di esposizione dati.	[1]
Educazione Utenti	Campagne di sensibilizzazione; formazione su rischi e pratiche sicure; strumenti per gestione privacy.	Organizzazione	Migliorare la consapevolezza e il comportamento di sicurezza degli utenti.	[3]

8. Tendenze Emergenti e Prospettive Future nella Sicurezza IoT (2023-2025)

Il futuro della sicurezza IoT è intrinsecamente legato all'evoluzione delle tecnologie abilitanti e all'emergere di nuovi paradigmi architetturali.

8.1. L'Impatto di 5G e Edge Computing

La proliferazione delle reti **5G** è una tendenza chiave, offrendo velocità più elevate, latenza inferiore e maggiore capacità.[2] Questo abilita l'elaborazione e la comunicazione dei dati in tempo reale per miliardi di dispositivi connessi, accelerando l'espansione dell'IoT in aree come le città intelligenti, le soluzioni sanitarie avanzate e i veicoli autonomi.[23] La network slicing 5G consente sezioni di rete dedicate e personalizzate per esigenze specifiche, migliorando l'efficienza in vari settori.[2]

L'**Edge Computing** sta diventando sempre più importante, portando l'elaborazione dei dati più vicino alla fonte (il dispositivo IoT), riducendo le latenze e risparmiando

larghezza di banda di rete.[2] Questo è cruciale per azioni in tempo reale nell'automotive e nell'automazione industriale.[23] L'edge computing migliora anche la privacy e la sicurezza dei dati mantenendo le informazioni sensibili localmente, riducendo i rischi associati all'elaborazione basata su cloud e favorendo la conformità normativa.[2]

8.2. Il Ruolo dell'Intelligenza Artificiale (AI) nella Sicurezza IoT

La combinazione di AI e IoT (AIoT) sta rendendo i dispositivi più intelligenti e veloci, consentendo loro di elaborare vaste quantità di dati istantaneamente all'edge senza una dipendenza costante dall'infrastruttura cloud.[2] Le applicazioni IoT basate sull'AI consentono un processo decisionale più intelligente, una manutenzione predittiva e il rilevamento delle anomalie in tempo reale.[2] Le telecamere intelligenti dotate di AI possono analizzare i feed video per rilevare proattivamente attività insolite o minacce alla sicurezza.[25] L'AI può anche analizzare il traffico di rete per identificare potenziali minacce.[24] L'AI contribuisce a semplificare la gestione della rete, ottimizzare l'allocazione delle risorse e adattare dinamicamente le misure di sicurezza in base ai dati in tempo reale e alle informazioni contestuali.[25] Tuttavia, l'integrazione dell'AI con l'IoT presenta sfide legate al volume di dati e alla necessità di proteggere gli algoritmi AI stessi dagli attacchi.[24]

8.3. Blockchain per la Sicurezza IoT

La tecnologia **Blockchain** può migliorare la sicurezza fornendo registrazioni decentralizzate e a prova di manomissione, archiviate su registri distribuiti, garantendo l'integrità e la sicurezza dei dati.[23] Può risolvere problemi di scalabilità, affidabilità e privacy autenticando, standardizzando e proteggendo l'adozione dei dati da parte dei dispositivi.[27] La blockchain consente ai sensori di trasferire dati senza la necessità di una terza parte fiduciaria, riducendo i singoli punti di fallimento e migliorando la privacy.[27] Offre un ecosistema resiliente implementando algoritmi crittografici per una maggiore privacy, garantendo robustezza e stabilità delle risorse, e consentendo ai partecipanti di visualizzare i blocchi (ma non il contenuto effettivo della transazione, protetto da chiavi private).[27]

La convergenza di 5G ed Edge Computing con l'IoT sta fondamentalmente rimodellando l'architettura IoT, consentendo un'elaborazione altamente distribuita e in tempo reale e riducendo la dipendenza dalle infrastrutture cloud centralizzate. Questo spostamento, pur migliorando l'efficienza e la privacy, distribuisce anche la superficie di attacco più ampiamente verso l'edge, rendendo necessari nuovi paradigmi di sicurezza incentrati sull'intelligenza a livello di dispositivo, sulla fiducia decentralizzata e sul rilevamento adattivo delle minacce basato sull'AI. La transizione verso l'edge modifica radicalmente il luogo in cui i dati vengono elaborati e dove devono essere

applicati i controlli di sicurezza. I modelli di sicurezza perimetrale tradizionali, progettati per i data center centralizzati, diventano meno efficaci. Il vantaggio dell'edge computing di "mantenere le informazioni sensibili localmente" [23] è un beneficio per la privacy, ma significa anche che le responsabilità di sicurezza sono spostate su dispositivi edge potenzialmente meno sicuri e con risorse limitate. Ciò crea una superficie di attacco più distribuita. Questa evoluzione architetturale richiede un cambiamento nel pensiero sulla sicurezza, passando da una difesa centralizzata a un paradigma di sicurezza distribuita. L'AI [2] diventa cruciale per il rilevamento delle anomalie in tempo reale e l'applicazione di politiche adattive all'edge. La Blockchain [23] offre una potenziale soluzione per la fiducia decentralizzata e l'integrità dei dati in questo ambiente altamente distribuito, affrontando problemi di scalabilità e singoli punti di fallimento. Tuttavia, la messa in sicurezza dei modelli AI stessi e la gestione del sovraccarico computazionale della blockchain sui dispositivi edge diventano nuove sfide.

9. Conclusioni e Raccomandazioni Future

La sicurezza è un fattore centrale e non negoziabile nel mondo dell'Internet delle Cose, la cui pervasività e integrazione in settori critici amplificano esponenzialmente la superficie di attacco e la complessità della protezione. I prodotti IoT commerciali sono spesso afflitti da un "debito di sicurezza" sistemico, derivante dalla pressione sui costi, dalla mancanza di esperienza dei produttori e dalla scarsa consapevolezza degli utenti. Ciò ha portato a minacce che vanno dal massiccio denial-of-service, come l'attacco Mirai, a rischi diretti per la vita umana, come dimostrato dalle vulnerabilità nei dispositivi medici e nel controllo dei veicoli. L'architettura a strati dell'IoT introduce molteplici superfici di attacco, e le debolezze specifiche dei protocolli, spesso legate a implementazioni imperfette o compromessi di progettazione, possono compromettere l'intero sistema. Il panorama normativo sta evolvendo verso un approccio più proattivo, imponendo la "sicurezza by design" e la gestione del ciclo di vita del prodotto, ma ciò pone sfide significative per i produttori. Parallelamente, la persistenza di attacchi basati su carenze igieniche cibernetiche di base sottolinea l'importanza cruciale dell'educazione degli utenti. In sintesi, la sicurezza IoT è una responsabilità condivisa che richiede sforzi concertati da parte di produttori, regolatori e utenti.

Nonostante i progressi, permangono sfide significative. L'eredità di miliardi di dispositivi insicuri già distribuiti e la difficoltà di applicare patch a unità sparse rappresentano un ostacolo persistente. Esiste una tensione intrinseca tra l'usabilità, l'efficienza dei costi e la robustezza della sicurezza, che spesso porta a compromessi. La complessità di mettere in sicurezza dispositivi eterogenei provenienti da catene di approvvigionamento diverse rimane una sfida ingegneristica e gestionale. Infine, la

necessità di una continua educazione degli utenti e l'adattamento a minacce in continua evoluzione richiedono un impegno costante.

Per affrontare queste sfide e costruire un ecosistema IoT più resiliente, si propongono le seguenti raccomandazioni future:

Ricerca e Sviluppo:

- **Sicurezza per Dispositivi con Risorse Limitate:** Concentrare la ricerca su principi di sicurezza by design ottimizzati per dispositivi con vincoli di risorse, garantendo protezione senza compromettere l'efficienza.
- **Soluzioni di Sicurezza basate su AI:** Sviluppare soluzioni di sicurezza avanzate basate sull'intelligenza artificiale per il rilevamento delle minacce in tempo reale e la risposta automatizzata all'edge, assicurando al contempo la sicurezza dei modelli AI stessi.
- **Applicazioni Blockchain per IoT:** Esplorare e perfezionare le applicazioni della blockchain per la fiducia decentralizzata, la gestione delle identità e l'integrità della catena di approvvigionamento nell'IoT.
- **Crittografia Resistente ai Computer Quantistici:** Indagare soluzioni crittografiche resistenti ai computer quantistici per garantire la sicurezza a lungo termine dell'IoT di fronte alle future capacità computazionali.

Regolamentazione e Standardizzazione:

- **Armonizzazione Internazionale:** Promuovere l'armonizzazione internazionale delle normative e degli standard di sicurezza IoT per ridurre la frammentazione e facilitare la conformità globale.
- **Adozione Obbligatoria di SBOM:** Incoraggiare l'adozione obbligatoria di Software Bill of Materials (SBOM) e di robusti quadri di divulgazione delle vulnerabilità in tutto il settore.
- **Linee Guida per la Risposta agli Incidenti Cyber-Fisici:** Sviluppare linee guida chiare e specifiche per la risposta agli incidenti che coinvolgono sistemi cyber-fisici, data la loro capacità di causare danni nel mondo reale.

Adozione Consapevole:

- **Campagne di Sensibilizzazione Pubblica:** Implementare continue campagne di sensibilizzazione pubblica per educare gli utenti sulle pratiche di sicurezza IoT di base e sulle loro responsabilità.
- **Framework di Valutazione del Rischio IoT:** Incoraggiare le organizzazioni ad adottare framework completi di valutazione del rischio IoT e a integrare la sicurezza IoT nelle loro strategie di cybersecurity più ampie.

- **Selezione dei Fornitori:** Dare priorità alla selezione dei fornitori basata su un comprovato impegno alla sicurezza by design e al supporto continuo post-vendita.

Queste raccomandazioni mirano a creare un futuro in cui l'IoT possa realizzare il suo pieno potenziale di innovazione e connettività, garantendo al contempo la sicurezza e la privacy degli individui e la resilienza delle infrastrutture critiche.

Bibliografia

- Antonioli, Daniele, Nils Ole Tippenhauer, and Kasper Rasmussen. "Key negotiation downgrade attacks on bluetooth and bluetooth low energy." *ACM Transactions on Privacy and Security (TOPS)* 23.3 (2020): 1-28. [1]
- Coppolino, Luigi, et al. "My smart home is under attack." *2015 IEEE 18th International Conference on Computational Science and Engineering*. IEEE, 2015. [1]
- Das, Aveek K., et al. "Uncovering privacy leakage in BLE network traffic of wearable fitness trackers." *Proceedings of the 17th international workshop on mobile computing systems and applications*. 2016. [1]
- Meneghello, Francesca, et al. "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices." *IEEE Internet of Things Journal* 6.5 (2019): 8182-8201. [1]
- Vidgren, Niko, et al. "Security threats in ZigBee-enabled systems: Vulnerability evaluation, practical experiments, countermeasures, and lessons learned." *2013 46th Hawaii International Conference on System Systems*. IEEE, 2013. [1]
- Yang, Xueying, et al. "Security vulnerabilities in LoRaWAN." *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, 2018. [1]

Bibliografia

1. 8_Security.pdf
2. 2025 IoT Trends: Innovations, Industry Growth & Future Outlook | POND IoT, accesso eseguito il giorno maggio 24, 2025, https://www.pondiot.com/blog/iot-trends-in-2025-what-is-next
3. What are IoT Risks? - Bitsight, accesso eseguito il giorno maggio 24, 2025, https://www.bitsight.com/glossary/iot-risks
4. My Smart Home is Under Attack | Request PDF - ResearchGate, accesso eseguito il giorno maggio 24, 2025, https://www.researchgate.net/publication/304287806_My_Smart_Home_is_Under_Attack
5. (PDF) Security Vulnerabilities in LoRaWAN - ResearchGate, accesso eseguito il giorno maggio 24, 2025,

https://www.researchgate.net/publication/325423212_Security_Vulnerabilities_in_LoRaWAN
6. Internet of Threats? A survey of practical security vulnerabilities in real IoT devices - Michele Polese, accesso eseguito il giorno maggio 24, 2025, https://polese.io/assets/pdf/2019_menegheelo_iot.pdf
7. Internet of Things (IoT): Security, privacy, consumer protections - Counsel Stack Learn, accesso eseguito il giorno maggio 24, 2025, https://blog.counselstack.com/internet-of-things-iot-security-privacy-consumer-protections/
8. Top 10 IoT Security Risks and How to Mitigate Them - SentinelOne, accesso eseguito il giorno maggio 24, 2025, https://www.sentinelone.com/cybersecurity-101/data-and-ai/iot-security-risks/
9. Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned | Request PDF - ResearchGate, accesso eseguito il giorno maggio 24, 2025, https://www.researchgate.net/publication/261457783_Security_Threats_in_ZigBee-Enabled_Systems_Vulnerability_Evaluation_Practical_Experiments_Countermeasures_and_Lessons_Learned
10. Performance Analysis of Spatial Distribution and Channel Quality Adaptive Protocol with DDOS Attacks In VANET - International Journal of Computer Applications | IJCA, accesso eseguito il giorno maggio 24, 2025, https://www.ijcaonline.org/archives/volume182/number38/30312-2019918376/
11. Your Signal, Their Data: An Empirical Privacy Analysis of Wireless-scanning SDKs in Android - arXiv, accesso eseguito il giorno maggio 24, 2025, https://arxiv.org/html/2503.15238v1
12. Uncovering Privacy Leakage in BLE Network Traffic of Wearable Fitness Trackers - Parth Pathak, accesso eseguito il giorno maggio 24, 2025, http://phpathak.com/files/hotmobile-fitness.pdf
13. Key Negotiation Downgrade Attacks on Bluetooth and Bluetooth Low Energy - Infoscience, accesso eseguito il giorno maggio 24, 2025, https://infoscience.epfl.ch/entities/publication/bbcd6705-2b92-491c-beb4-b550ffea7c98
14. Key Negotiation Downgrade Attacks on Bluetooth and Bluetooth Low Energy - OUCI, accesso eseguito il giorno maggio 24, 2025, https://ouci.dntb.gov.ua/works/lRAzY6P4/
15. Analysis of Lorawan Protocol and Attacks Against Lorawan-Based IoT Devices, accesso eseguito il giorno maggio 24, 2025, https://www.researchgate.net/publication/382245445_Analysis_of_Lorawan_Protocol_and_Attacks_Against_Lorawan-Based_IoT_Devices
16. Forescout's 2025 report reveals surge in device vulnerabilities across IT, IoT, OT, and IoMT, accesso eseguito il giorno maggio 24, 2025, https://industrialcyber.co/reports/forescouts-2025-report-reveals-surge-in-device-vulnerabilities-across-it-iot-ot-and-iomt/
17. How IoT Security Challenges Impact Regulatory Compliance - Finite State, accesso eseguito il giorno maggio 24, 2025,

https://finitestate.io/blog/iot-compliance-regulations-security-challenges
18. IoT Device Security Best Practices: Safeguarding Connected Systems - Neumetric, accesso eseguito il giorno maggio 24, 2025, https://www.neumetric.com/iot-device-security-best-practices/
19. The US Government Creates IoT Security Standards - Nozomi Networks, accesso eseguito il giorno maggio 24, 2025, https://www.nozominetworks.com/blog/the-u-s-government-is-creating-security-standards-for-iot-devices
20. IoT Cybersecurity: EU, US and UK Regulations (2024) - Thales, accesso eseguito il giorno maggio 24, 2025, https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/iot-regulations
21. IoT Security Regulations: A Compliance Checklist – Part 1 | Tripwire, accesso eseguito il giorno maggio 24, 2025, https://www.tripwire.com/state-of-security/iot-security-regulations-compliance-checklist-part-1
22. IoT Security Challenges (Most Critical Risk of 2025) - StationX, accesso eseguito il giorno maggio 24, 2025, https://www.stationx.net/iot-security-challenges/
23. 10 Emerging Technology Trends in IoT: Exploring the Future - Mapsted, accesso eseguito il giorno maggio 24, 2025, https://mapsted.com/blog/technology-trends-in-iot
24. Artificial Intelligence in IoT: Enhancing Connectivity and Efficiency - Device Authority, accesso eseguito il giorno maggio 24, 2025, https://deviceauthority.com/artificial-intelligence-in-iot-enhancing-connectivity-and-efficiency/
25. AI and IoT: Everything You Need to Know | The Meraki Blog, accesso eseguito il giorno maggio 24, 2025, https://meraki.cisco.com/blog/2024/09/ai-and-iot-everything-you-need-to-know/
26. What is IoT with Blockchain? - IBM, accesso eseguito il giorno maggio 24, 2025, https://www.ibm.com/think/topics/blockchain-iot
27. Blockchain and IoT Security: everything you need to know - Chakray, accesso eseguito il giorno maggio 24, 2025, https://chakray.com/blockchain-iot-security/
28. 18th IEEE International Conference on Computational Science and Engineering (CSE-2015), Porto, Portugal, 20-23 October 2015, accesso eseguito il giorno maggio 24, 2025, https://fe.up.pt/specs/events/cse2015/CSE2015-Program.htm
29. A Survey and Analysis of Recent IoT Device Vulnerabilities - ResearchGate, accesso eseguito il giorno maggio 24, 2025, https://www.researchgate.net/publication/379300512_A_Survey_and_Analysis_of_Recent_IoT_Device_Vulnerabilities