Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Informatica per il Management

Guardiani Digitali: L'impatto dell'AI sulla Sicurezza dei Dispositivi IoT

Relatore:
Chiar.mo Prof.
Jocelyne Elias

Presentata da:
Jonathan Ted Benson
Cerullo Uyi

Sessione III
Anno Accademico 2022/23

A mia mamma, Svetlana,
a cui devo ogni mio successo.

Indice

Introduzione

L'Internet delle Cose (IoT) è una delle rivoluzioni digitali più significative del nostro tempo. Attraverso l'interconnessione di dispositivi fisici con il mondo digitale, l'IoT promette di trasformare radicalmente la nostra vita quotidiana, migliorando l'efficienza, l'accessibilità e la comodità in molteplici settori, tra cui la casa intelligente, la salute, l'industria e la mobilità. Tuttavia, mentre l'IoT continua a espandersi in modo esponenziale, sorgono sfide di sicurezza senza precedenti.
La sicurezza nell'IoT diventa una priorità critica, poiché un crescente numero di dispositivi connessi si traduce in una superficie di attacco più ampia e più complessa. Minacce quali l'accesso non autorizzato, il furto di dati, il controllo malevolo dei dispositivi e gli attacchi DDoS (Distributed Denial of Service) si diffondono. Le soluzioni tradizionali di sicurezza cibernetica spesso si scontrano con limiti significativi quando applicate all'IoT.
È in questo contesto che l'Intelligenza Artificiale (AI) emerge come una risorsa fondamentale nella protezione dei dispositivi IoT. L'AI offre un approccio innovativo e dinamico alla sicurezza, consentendo di rilevare e mitigare minacce in tempo reale, adattarsi a schemi di attacco in evoluzione e migliorare continuamente la protezione. Questa tesi si propone di esplorare in profondità il ruolo dell'AI nella sicurezza dei dispositivi IoT, analizzando le sfide, le opportunità e le implicazioni etiche legate a questa convergenza tra tecnologie avanzate.
Negli ultimi anni, abbiamo assistito a una crescente adozione di soluzioni di AI per migliorare la sicurezza degli oggetti connessi. Tuttavia, molti interrogativi rimangono aperti. Come possono le tecnologie di AI contribuire a rilevare minacce e mitigare vulnerabilità nei dispositivi IoT? Quali sono gli aspetti etici e le questioni legate alla privacy che derivano dall'uso dell'AI nell'ambito della sicurezza IoT? Quali sono i casi di studio concreti che dimostrano l'efficacia di questa convergenza tecnologica?
Questo lavoro ha l'obiettivo di rispondere a queste domande attraverso un'analisi approfondita e una revisione della letteratura esistente, esaminando le applicazioni dell'AI nella sicurezza IoT e valutando i risultati ottenuti. Inoltre, esploreremo le

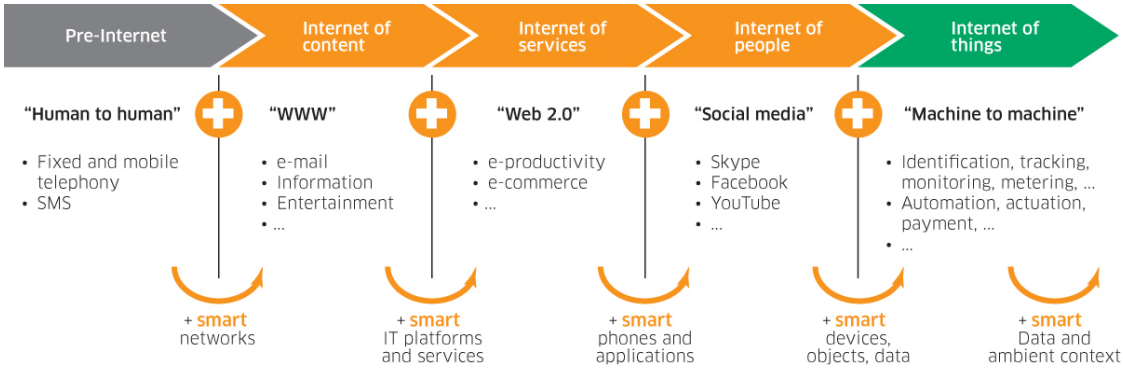

Figura 1: Evoluzione dell'Internet delle Cose (IoT). [1]

implicazioni etiche e normative di questa nuova frontiera della sicurezza cibernetica.

Alla luce di queste considerazioni, questa tesi sostiene che l'Intelligenza Artificiale rappresenti un pilastro essenziale per garantire un futuro sicuro e affidabile per l'Internet delle Cose. La sua capacità di apprendere, adattarsi e rispondere dinamicamente alle minacce rappresenta un baluardo cruciale nella protezione dei dispositivi IoT e delle reti a cui sono collegati. Con questa premessa, ci immergeremo nell'esplorazione dell'AI come guardiano digitale per il mondo sempre più connesso dell'IoT.

Capitolo 1

Fondamenti dell'Internet delle Cose (IoT)

1.1 Definizione e concetti chiave dell'IoT

Internet delle Cose (IoT) è un concetto tecnologico che si riferisce a una rete di dispositivi fisici, apparecchi e altri oggetti incorporati con sensori, software e tecnologie, che sono in grado di raccogliere e scambiare dati con altri dispositivi e sistemi attraverso Internet o altre reti di comunicazione. "Internet of Things" (IoT) è una visione affascinante di un mondo in cui gli oggetti che ci circondano, dai termostati alle automobili, diventano "intelligenti" grazie alla connessione a Internet. Ciò significa che questi oggetti non solo esistono fisicamente, ma possono anche comunicare tra loro e con noi, e persino prendere decisioni basate sui dati che raccolgono dall'ambiente circostante.

Questi dispositivi, noti come "dispositivi IoT", sono dotati di sensori che agiscono come gli occhi e le orecchie del sistema. Possono misurare temperature, umidità, pressione, movimento e una vasta gamma di altre grandezze. Ma la loro vera intelligenza emerge dalla loro capacità di comunicare attraverso reti di connessione, come Wi-Fi, 4G o 5G, o protocolli a bassa potenza come LoRaWAN. Questa comunicazione bidirezionale o unidirezionale consente loro di condividere dati con diversi sistemi di gestione.

Tutti questi dati raccolti da oggetti IoT possono essere processati internamente, in locale, oppure finire in uno spazio predefinito chiamato "cloud". È qui che i dati vengono elaborati e analizzati per estrarre informazioni significative. Si può pensare ad un termostato intelligente che raccoglie dati sulla temperatura interna ed esterna della casa e li invia al cloud, dove un algoritmo di apprendimento automatico determina il momento migliore per accendere o spegnere il riscaldamento,

risparmiando energia.
Questo enorme flusso di dati generato dagli oggetti IoT è noto come "big data". Per affrontarlo, sono necessari strumenti avanzati di analisi dei dati che possono identificare modelli, tendenze e anomalie. L'apprendimento automatico è uno di questi strumenti, consentendo ai sistemi IoT di adattarsi e migliorare nel tempo.
Le applicazioni dell'IoT sono diffuse in vari settori, tra cui:
- Sanità (eHealth): L'IoT è fondamentale per il monitoraggio remoto dei pazienti, la gestione delle cure mediche e la raccolta di dati sanitari. Dispositivi come monitor cardiaci portatili, sensori di glucosio elettronici e dispositivi di monitoraggio del sonno rientrano in questa categoria.
- Casa Intelligente (Smart Home): L'IoT è ampiamente utilizzato per migliorare l'automazione domestica, inclusi dispositivi come telecamere di sicurezza, luci connesse, elettrodomestici intelligenti e sistemi di gestione dell'energia.
- Industria (Industria 4.0): Nell'industria, l'IoT è utilizzato per l'automazione avanzata, il monitoraggio degli asset, la manutenzione predittiva e la gestione della catena di approvvigionamento. Sensori e dispositivi IoT sono ampiamente utilizzati in ambienti industriali.
- Agricoltura (Smart Farming): L'IoT è adottato per migliorare l'agricoltura, consentendo ai coltivatori di monitorare le condizioni dei campi, l'irrigazione, il bestiame e l'uso delle risorse in tempo reale.
Questi sono solo alcuni esempi dei numerosi settori in cui l'IoT sta rivoluzionando il modo in cui operiamo e viviamo.

1.2 Evoluzione e crescita dell'IoT

Secondo una ricerca dell'Osservatorio Internet of Things della School of management del Politecnico di Milano, nel 2022 il mercato italiano dell'Internet of Things ha superato gli 8 miliardi di euro, conseguendo un +13% rispetto all'anno precedente, nonostante i problemi legati alla carenza di semiconduttori e di materie prime, oltre all'instabilità economica e politica della guerra in Ucraina.
"Prosegue la crescita del mercato dell'Internet of Things, sia in termini di valore che di maturità dell'offerta – afferma Giulio Salvadori, Direttore dell'Osservatorio IoT –. Cresce la consapevolezza di aziende, pubbliche amministrazioni e consumatori, sempre più interessati a gestire da remoto asset e dispositivi smart, attivando servizi e funzionalità avanzate, mentre si accende la competizione con nuovi player globali. Nel contempo, aumentano le aspettative per il futuro, anche grazie ai grandi investimenti previsti dal PNRR e ai frequenti rincari dell'energia, che spingono

aziende e consumatori a porre maggiore attenzione ai consumi, sfruttando anche le tecnologie smart" [2].
Sempre dallo studio dell'Osservatorio IoT risulta che tra i diversi ambiti, la fetta più grande del mercato sia rappresentata dalle Smart Car, con un fatturato da 1,4 miliardi di euro, pari al 17% del totale. Al secondo posto, le applicazioni IoT nel mondo utility (Smart Metering e Smart Asset Management) con 1,37 miliardi di euro, in crescita ma ormai prossime alla saturazione: nel 2022 sono stati installati altri 1,1 milioni di contatori gas connessi in utenze domestiche (84% del parco complessivo) e 1,7 milioni di smart meter elettrici di seconda generazione (64% del totale). Seguono poi Smart Building (1,3 miliardi), Smart City (830 milioni), Smart Factory (780 milioni), Smart Home (770 milioni), Smart Logistics (715 milioni) e Smart Agriculture (540 milioni). Gli ambiti che stanno crescendo di più all'interno del mercato IoT, però, in particolare sono Smart Agriculture (+32%), Smart Factory (+22%) e Smart Building (+19%) [2].
Il mercato IoT italiano ha fatto tanti passi in avanti rispetto a un decennio fa, in cui era difficile rinvenire ambiti di applicazioni concrete e una reale maturità del paradigma tecnologico. Oggi invece è indubbio che alcuni ambiti dell'IoT siano maturi e tecnologicamente avanzati. L'Internet delle cose si farà sempre più forte grazie ad alcuni grandi alleati, il primo dei quali è il 5G, che nel prossimo futuro potrebbe abilitare servizi davvero innovativi basati sulla localizzazione. Inoltre, si sta affermando una progressiva tendenza alla semplificazione dell'aspetto connettività: da questo punto di vista le tecnologie Low Power Wide Area (LPWA) in banda non-licenziata sono sempre più adottate. "Il 2021 è stato un anno rilevante per le tecnologie LoRaWAN e SigFox – ha spiegato Antonio Capone, Responsabile scientifico dell'Osservatorio Internet of Things -. LoRaWAN è stato formalmente riconosciuto come standard dall'International Telecommunication Union (ITU-T), il principale ente di standardizzazione delle tecnologie di comunicazione, mentre SigFox ha lavorato per consolidare la sua presenza sul mercato e sul dispiegamento di nuove reti."
Ogni settore presenta sfide e opportunità uniche per l'applicazione dell'IoT, che vanno dalla migliore gestione delle risorse alla creazione di nuovi servizi e soluzioni innovative. Tuttavia, per realizzare appieno questo potenziale, è essenziale affrontare le sfide legate alla sicurezza e garantire che questi oggetti intelligenti siano veramente sicuri e affidabili.

Capitolo 2

Sicurezza nell'Internet delle Cose (IoT)

2.1 Minacce e vulnerabilità comuni nell'IoT

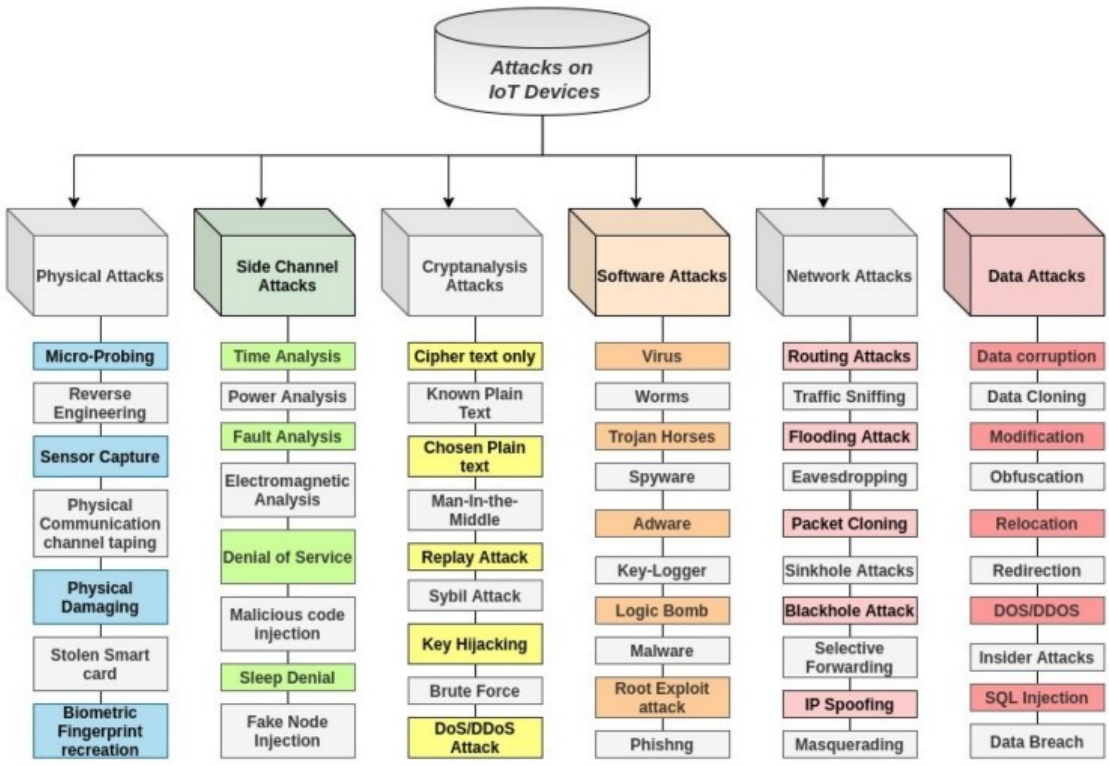

Figura 2.1: Tassonomia attacchi IoT. [3]

Con l'espansione dell'IoT, sorgono preoccupazioni legate alla sicurezza. La protezione dei dati, la prevenzione degli accessi non autorizzati e la difesa contro gli attacchi informatici sono questioni fondamentali e diventano un aspetto cruciale nella progettazione e nell'implementazione di sistemi IoT. Le architetture di rete utilizzate da questi dispositivi supportano diversi protocolli per comunicare tra loro. Tuttavia, a seconda del tipo di connessione e delle caratteristiche dei dispositivi, nascono problemi di sicurezza e vulnerabilità a numerosi tipi di attacco, che sfruttano le vulnerabilità del sistema.

2.1.1 Physical Attacks

Gli attacchi fisici sono associati ai dispositivi hardware nella rete che influiscono sulle funzionalità fisiche del sistema.
1) *Micro-Probing*: è un tipo di attacco invasivo che richiede la manipolazione fisica dei semiconduttori, tramite l'uso di strumenti specializzati, per accedere fisicamente ai componenti interni di un dispositivo, come microcontroller, microprocessori, o altri chip, al fine di estrarre dati e informazioni sensibili;
2) *Reverse Engineering*: prevede la riscrittura e manipolazione degli algoritmi o dell'intero codice utilizzati dal dispositivo al fine di rivelare informazioni sensibili;
3) *Sensor Capture*: l'attaccante acquisisce accesso ai sensori del dispositivo per compromettere la rete, rimuovere nodi dalla rete e ridistribuirne di nuovi malevoli.
4) *Physical Communication Channel Tapping*: l'attaccante utilizza i tap di rete per estrarre segnali dal canale, senza interrompere la connessione. Il disagio può essere causato dalla deviazione del traffico;
5) *Physical Damaging*: questo tipo di attacco ha lo scopo di manomettere i sensori del dispositivo. Questi sensori vengono spesso lasciati incustoditi operare in ambienti esterni e ciò rappresenta una notevole vulnerabilità;
6) *Stolen Smart Card*: quando una smart card viene perduta, l'attaccante può facilmente risalire alla password applicando tecniche di password cracking offline;
7) *Biometric Fingerprint Recreation*: l'attaccante acquisisce accesso al sistema ed entra in possesso del modello biometrico presente sul dispositivo, manipolando i dati registrati e inserendone di falsi per garantirsi l'ammissione.

2.1.2 Side Channel Attacks

Gli attacchi side-channel (attacchi a canali secondari) sono associati a exploit di sicurezza che hanno lo scopo di raccogliere informazioni accessorie derivanti dal-

l'esecuzione di un programma, da cui è possibile misurare e sfruttare gli effetti indiretti del sistema invece che prendere di mira direttamente il programma.
1) *Time Analysis*: l'attacco side-channel di questo tipo avviene quando un'attaccante osserva il tempo di esecuzione impiegato dalle operazioni di crittografia del sistema. Questo permetta all'aggressore di ottenere informazioni sulle chiavi segrete, dati sensibili e altre variabili;
2) *Power Analysis*: le proprietà fisiche del dispositivo vengono studiare dagli attaccanti per calcolarne la potenza e i livelli di consumo energetico. Questa metodologia è governata da diverse leggi fisiche, fluttuazioni di tensione, proprietà dei semiconduttori del dispositivo e molti altri fattori;
3) *Fault Analysis*: gli aggressori effettuano questo attacco introducendo errori nell'implementazione delle operazioni di crittografia per ricavare informazioni sullo stato interno. Ad esempio, inducendo il processore ad alta tensione o stato di alta temperatura, che si traduce in un output falso, consentendo all'aggressore di dedurre istruzioni del processore e del suo comportamento interno;
4) *Electromagnetic Analysis*: l'obiettivo che sta dietro all'analisi elettromagnetica è quello di catturare le chiavi crittografiche utilizzate nelle funzioni di crittografia. I segnali elettromagnetici emessi dal dispositivo vengono catturati ed analizzati per portare questo tipo di attacco;
5) *Denial of Service*: l'attacco side-channel DoS avviene a causa di diversi parametri che vengono considerati per misurare le prestazioni nella crittoanalisi. L'attacco temporale tende a rallentare il processo provocando un allagamento della rete, con segnali che ne provocano lo spegnimento;
6) *Malicious Code Injection*: la fuga di informazioni dai canali laterali consente ad un utente malintenzionato di recuperare dati e segreti, quindi, eseguire codice malevolo senza i dovuti privilegi, oppure sfruttare vulnerabilità del sistema per eseguire codice malevolo da remoto;
7) *Sleep Denial*: questo attacco colpisce ogni sensore della rete ponendo forzatamente i nodi in modalità sleep, influenzando le prestazioni della rete;
8) *Fake Node Injection*: l'aggressore aggiunge un falso nodo nella rete in cui intende iniettare codice dannoso, tentando di consumare l'energia degli altri sensori tenendoli occupati, il che a sua volta fa collassare l'intera rete. Il falso nodo inoltre funge da man-in-the-middle per raccogliere segreti e informazioni.

2.1.3 Cryptanalysis Attacks

Gli attaccanti utilizzano diverse tecniche per violare i sistemi crittografici delle reti. L'attacco tramite crittoanalisi è una tecnica in cui viene effettuato uno studio approfondito delle modalità di crittografia di un sistema, al fine di determinarne i punti deboli. Gli attaccanti si basano sulla natura dell'algoritmo e sulle caratteristiche generali del plaintext (testo in chiaro).
1) *Cipher Text Only*: questo modello di attacco viene utilizzato dall'aggressore quando questi ha accesso ai soli testi cifrati e non a quelli in chiaro, seppur avendo qualche conoscenza della linguaggio utilizzato o della distribuzione statistica dei caratteri nel testo in chiaro;
2) *Known Plain Text (KPA)*: Il KPA si verifica quando il crittoanalista ha accesso sia al testo in chiaro che al testo cifrato. Questo modello di attacco viene utilizzato per rilevare le chiavi segrete utilizzate per la crittografia e i codici;
3) *Chosen Plain Text (CPA)*: Il CPA generalmente presuppone che l'aggressore sia in grado di generare il testo cifrato per qualsiasi testo semplice arbitrario, con conseguente riduzione di sicurezza del crittosistema. In questo modello, l'avversario interagisce con la macchina di crittografia per rilevare la chiave crittografica;
4) *Man-In-The-Middle (MITM)*: il modello è associato all'intercettazione attiva e all'intercomunicazione tra entità che credono di comunicare direttamente tra loro. L'aggressore agisce come una terza parte tra le entità, senza essere notato, stabilendo una connessione individuale con la vittima e controllando l'intera comunicazione. L'attaccante intercetta i messaggi e ne inserisce di nuovi per aggirare l'autenticazione reciproca tra le due parti;
5) *Replay Attack*: si tratta di un tipo di attacco passivo, eseguito ritardando la trasmissione dei dati in modo doloso e fraudolento. L'attacco viene eseguito intercettando i dati e ritrasmettendoli dopo aver apportato modifiche;
6) *Sybil Attack*: l'attaccante tenta di controllare la rete creando numerose false identità. Nella rete di sensori, un falso nodo con vera identità comunica con gli altri nodi vicini e distribuisce identità multiple non lecite. Le false identità degradano e compromettono l'affidabilità del sistema, l'integrità dei dati e la sicurezza;
7) *Key Hijacking*: nel key hijacking, o session hijacking, viene eseguito un tentativo di dirottamento della sessione o delle chiavi segrete al fine di ottenere l'accesso non autorizzato ai dispositivi in una rete. Questa tecnica viene utilizzata per fornire accesso ad un server remoto ad un utente sconosciuto;
8) *Brute Force*: le tecniche di "hit and trial" sono comuni nel tentativo di indovinare le password, eseguendo numerosi tentativi al fine di trovare la combinazione corretta;

9) *DoS/DDoS*: questo attacco viene performato attraverso le collisioni di hash, sfruttando il caso pessimo di ricerca a runtime delle hash tables. Il sistema consuma buona parte del suo tempo e risorse per la ricerca piuttosto che per eseguire compiti importanti e tasks.

2.1.4 Software Attacks

I dispositivi non sono solo il bersaglio finale degli hacker ma rappresentano anche un punto di accesso al sistema generale, in cui eseguire codice senza privilegi e avviare attività che ostacolano il normale funzionamento del sistema.
1) *Virus*: è un programma o parte di codice che si attacca a un codice legittimo per essere eseguito. Il programma virus non viene eseguito finché non si trova nelle condizioni più vantaggiose per essere portato a termine. Un virus ha effetti dannosi sul software del sistema causati dalla corruzione dei dati con cui entra in contatto;
2) *Worms*: per eseguire questo attacco, gli aggressori si avvalgono di un software autonomo che si propaga senza alcun intervento umano o di altro software. Il dispositivo viene preso di mira sfruttando le sue vulnerabilità, avvalendosi anche dei suoi servizi di trasporto per spostarsi attraverso più dispositivi;
3) *Trojan*: generalmente sotto forma di programma legittimo, viene eseguito sfruttando l'interazione con l'utente. L'aggressore induce l'utente a caricare ed eseguire un programma o download con conseguenti danni alla macchina ospite tramite il furto di dati, la corruzione dei file e la proliferazione di altri malware;
4) *Spyware*: questi software mirano a raccogliere informazioni critiche su un individuo o un'organizzazione, fingendo di essere entità legittima e inviando tali informazioni a elementi terzi, a insaputa dell'utente. Questa tecnica consente di accedere al dispositivo senza il consenso del consumatore;
5) *Adware*: si tratta di software che richiedono il click dell'utente, presenti sotto forma di annunci e pubblicità su pagine e siti web legittimi. Una volta cliccato sull'annuncio, una backdoor viene installata sul sistema per avere accesso a dati sensibili;
6) *Key-Logger*: le credenziali di accesso utente vengono spesso rubate da malintenzionati attraverso l'utilizzo di programmi che registrano le sequenze di tasti digitati sulla tastiera. Tutte le informazioni digitate possono essere recuperate e l'accesso alle password può avvenire tramite l'utilizzo di programmi di key-logging;
7) *Logic Bomb*: il software viene iniettato con un pezzo di codice dannoso che esegue il suo payload e funzionalità in risposta a determinate condizioni o eventi specifici;

8) *Malware*: gli aggressori cercano informazioni sul network al fine di trovare vulnerabilità per eseguire codice malevolo ed infettare il sistema. L'obiettivo è di rubare informazioni confidenziali, distruggere dati e disabilitare la rete.
9) *Root Exploit Attack*: prevede che un attaccante ottenga accesso al sistema con privilegi di amministratore per eseguire serie di comandi, sfruttando le vulnerabilità note e intaccare la rete e i dispositivi associati;
10) *Phishing*: l'utente viene ingannato da messaggi o email fraudolente che tentano di infiltrare software dannosi e recuperare informazioni riservate.

2.1.5 Network Attacks

I sensori, che rappresentano i nodi del sistema, sono collegati attraverso la rete per condividere dati e trasmettere informazioni. Gli attaccanti adottano diverse tecniche avanzate per accedere ad un sistema individuale o ad una rete organizzata. Questa varietà di attacchi e minacce deve essere presa in considerazione in maniera tempestiva nell'ambiente IoT, per poter costruire strategie di difesa efficienti.
1) *Routing Attacks*: vengono definite le vulnerabilità del sistema di routing che vengono sfruttate per eludere i processi di autenticazione. Lo spoofing del router, le modifiche alle tabelle di routing e il reindirizzamento dei pacchetti router sono esempi di questo metodo di attacco;
2) *Traffic Sniffing*: questa minaccia implica il monitoraggio continuo della rete da parte di un malintenzionato e l'acquisizione dei pacchetti trasferiti. Dall'analisi di questi è possibile recuperare informazioni ed ottenere indicazioni dettagliate sui dispositivi;
3) *Flooding Attack*: questa tecnica viene utilizzata per impedire alla rete di eseguire il suo normale funzionamento. La rete viene bombardata da un gran numero di pacchetti e comandi che esauriscono le risorse della rete e la sua capacità di elaborazione, rendendola essenzialmente fuori uso;
4) *Eavesdropping*: sorta di attacco di sniffing associato al recupero di informazioni trasferite tra i dispositivi, collegati tramite un canale non sicuro. Il furto di informazioni avviene principalmente a causa della mancanza di sicurezza del canale di comunicazione;
5) *Packet Cloning*: nell'attacco di clonazione dei pacchetti, un avversario può catturare un pacchetto dal traffico della rete ed estrarre informazioni. Dopodiché può riprogrammarlo per creare un clone del pacchetto catturato e immetterlo nella rete, facendolo passare come legittimo. La risposta del ricevente del pacchetto potrebbe rivelare segreti e altre informazioni sensibili;

6) *Sinkhole Attacks*: si tratta di un attacco di dirottamento in cui l'aggressore assume il controllo di una porzione della rete di dispositivi connessi, deviando il traffico da destinazioni legittime verso una destinazione controllata dall'aggressore. In sostanza, l'attacco sinkhole modifica la normale rotta di comunicazione dei dispositivi connessi;
7) *Blackhole Attack*: l'attacco del "buco nero" si verifica in una rete, inclusa una rete IoT, quando il traffico di dati viene dirottato e reindirizzato verso un nodo o entità controllata dall'attaccante, con l'obiettivo di rendere inaccessibili o distruggere i dati;
8) *Selective Forwarding*: in questo caso, un dispositivo malevolo all'interno di una rete di dispositivi IoT seleziona intenzionalmente quali pacchetti di dati inoltrare e quali ignorare e scartare. Ciò può essere dannoso poiché compromette la comunicazione affidabile tra i dispositivi nella rete IoT;
9) *IP Spoofing*: un attaccante invia pacchetti di dati da un indirizzo IP fittizio o manipolato per nascondere la sua vera identità o per impersonare un'altra entità nella rete;
10) *Masquerading*: l'aggressore si fa passare per un'entità o dispositivo legittimo all'interno di una rete. In contesto IoT, questo significa che un dispositivo malevolo si presenta in modo fraudolento come un dispositivo autorizzato e attendibile.

2.1.6 Data Attacks

I dispositivi IoT forniscono servizi convenienti alla quotidianità, ma spesso a discapito della sicurezza. Il compromesso tra sicurezza e convenienza ha creato una situazione di interesse per gli attaccanti, che si avvalgono di strumenti intelligenti e sistemi per acquisire conoscenze sulle vulnerabilità della rete e del sistema. A causa di queste vulnerabilità, i dati possono essere minacciati dai numerosi attacchi.
1) *Data Corruption*: situazione in cui le informazioni raccolte, elaborate e trasmesse da dispositivi IoT vengono danneggiate o alterate in qualche modo, influenzando la loro integrità e affidabilità;
2) *Data Cloning*: si riferisce all'atto di duplicare o replicare in modo fraudolento i dati provenienti da dispotivi IoT. Questo può avere conseguenze gravi, poiché i dati clonati possono essere utilizzati per ingannare i sistemi di monitoraggio o manipolare le decisioni automatizzate;
3) *Modification*: si tratta di un attacco attivo basato sull'intercettazione e la conseguente manipolazione dei dati;
4) Obfuscation: l'offuscamento non è un attacco diretto ma un facilitatore di at-

tacco, che fornisce dettagli, regole o tecniche per nascondere eventuali attacchi dall'IDS (Intrusive Detection System) o altre componenti di rilevamento;
5) *Relocation*: i dati vengono migrati da un sistema di storage all'altro, di modo che l'attaccante possa effettuare sniffing costante delle informazioni trasferite;
6) *Redirection*: il reindirizzamento è una vulnerabilità che consente ad un aggressore di indurre gli utenti di un'applicazione a seguire un collegamento che porta a un sito o a una fonte esterna non attendibile;
7) *DoS/DDoS*: l'intenzione di un aggressore di eseguire un attacco DoS consiste nel disturbare in maniera massiccia il regolare funzionamento di una rete o di un sistema;
8) *Insider Attack*: questo tipo di attacco malevolo viene eseguito da una persona considerata "insider", ovvero autorizzata ad accedere al sistema. L'attacco è semplificato dal fatto che l'operante conosce l'infrastruttura del sistema;
9) *SQL Injection*: modalità di attacco alla sicurezza web che mira alle vulnerabilità di una rete per iniettare query dannose e ottenere accesso non autorizzato al database;
10) *Data Breach*: l'intenzione è di recuperare informazioni private e/o riservate che potrebbero derivare da furto, perdita di unità di archiviazione, hardware o altro. Una violazione dei dati può anche essere involontaria e può verificarsi a causa della corruzione accidentale dei supporti di memorizzazione, con conseguente fuga di dati.

2.2 Approcci tradizionali alla sicurezza IoT e limitazioni

Gli approcci tradizionali alla sicurezza dei dispositivi IoT si basano su principi consolidati di sicurezza informatica, ma affrontano sfide uniche dovute alla natura distribuita e alla diversità dei dispositivi IoT.
Innanzitutto, la crittografia è un elemento chiave negli approcci tradizionali. L'uso di algoritmi crittografici (a chiave simmetrica, a chiave pubblica e ibridi) protegge i dati durante la trasmissione, impedendo a potenziali attaccanti di intercettare e comprendere informazioni sensibili. Inoltre, la crittografia può essere utilizzata per proteggere l'accesso ai dispositivi, garantendo che solo utenti autorizzati possano interagire con essi.
L'autenticazione è un altro pilastro fondamentale. Richiedere credenziali valide o utilizzare meccanismi di autenticazione a due fattori aiuta a garantire che solo

persone o dispositivi autorizzati possano accedere ai dati o controllare i dispositivi IoT. L'autenticazione è particolarmente importante nei contesti in cui la sicurezza è essenziale, ad esempio nel settore sanitario o nell'industria.
Il monitoraggio continuo del traffico di rete è un aspetto importante degli approcci tradizionali alla sicurezza IoT. Identificare e rispondere prontamente a comportamenti anomali o a tentativi di accesso non autorizzato è cruciale per mitigare le minacce. Le soluzioni di monitoraggio possono rilevare pattern di traffico sospetti o comportamenti che possono indicare un attacco in corso.
L'implementazione di patch e aggiornamenti regolari è un'altra pratica comune. Gli sviluppatori rilasciano regolarmente aggiornamenti di sicurezza per affrontare nuove vulnerabilità e minacce. Mantenere i dispositivi IoT aggiornati riduce la probabilità di sfruttare falle di sicurezza note.
L'isolamento dei dispositivi è spesso implementato per limitare l'impatto di una potenziale violazione. Se un dispositivo viene compromesso, l'isolamento può impedire la propagazione dell'attacco all'intera rete.
Inoltre, l'educazione degli utenti e degli sviluppatori è un componente fondamentale. Gli utenti devono essere consapevoli delle pratiche di sicurezza e delle potenziali minacce, mentre gli sviluppatori devono essere formati per progettare sistemi resilienti e sicuri fin dall'inizio.
Gli approcci tradizionali alla sicurezza IoT incorporano principi consolidati di crittografia, autenticazione, monitoraggio del traffico e aggiornamenti regolari. La diversità e la complessità degli ambienti IoT richiedono una progettazione attenta e soluzioni adattate alle specifiche sfide del settore, ma questi presentano tuttavia numerosi limiti:

- Diversità degli Standard di Sicurezza: non esiste un singolo standard di sicurezza universalmente accettato per dispositivi IoT. La mancanza di omogeneità negli standard di sicurezza comporta una mancanza di coerenza nelle pratiche di sicurezza adottate da vari produttori.

- Limitazioni di Risorse: molti dispositivi IoT operano con risorse limitate, come potenza di elaborazione, memoria e capacità della batteria. Queste limitazioni possono rendere difficile l'implementazione di misure di sicurezza avanzate senza compromettere le prestazioni e la durata della batteria.

- Mancanza di Aggiornamenti Regolari: alcuni dispositivi IoT, specialmente quelli che operano in ambienti critici o in settori in cui la sostituzione frequente dei dispositivi è difficile, potrebbero non ricevere aggiornamenti regolari di sicurezza. Ciò li rende vulnerabili a nuove minacce.

- Problemi di Identità e Autenticazione: la gestione delle identità e delle credenziali nei dispositivi IoT è piuttosto complessa, ma alcuni dispositivi potrebbero disporre di implementazioni deboli di autenticazione, rendendoli suscettibili ad attacchi di impersonificazione e accessi non autorizzati.

- Scarse Pratiche di Sviluppo Sicuro: a causa di vincoli di tempo e risorse, alcuni sviluppatori potrebbero non adottare pratiche di sviluppo sicuro quando creano software per dispositivi IoT. Questo può portare all'introduzione di vulnerabilità nel codice, facilitando gli attacchi.

- Interconnessione e Interoperabilità: L'interconnessione di dispositivi e sistemi eterogenei crea nuove opportunità per gli attacchi. La mancanza di standard chiari per l'interoperabilità introduce rischi di sicurezza quando i dispositivi devono comunicare tra loro.

- Problemi di Privacy: la raccolta e la trasmissione di grandi quantità di dati da parte dei dispositivi IoT solleva numerose preoccupazioni sulla privacy. Le pratiche di sicurezza potrebbero rivelarsi non essere sufficienti a garantire la protezione dei dati personali.

- Rischi Fisici: a differenza di molti dispositivi tradizionali, gli IoT spesso operano in ambienti fisicamente accessibili. Ciò aumenta il rischio di manipolazioni fisiche e accesso non autorizzato ai dispositivi.

Affrontare questi limiti richiede un approccio più completo e specifico per gli ambienti IoT. È in questo contesto che l'utilizzo dell'Intelligenza Artificiale (AI) nella sicurezza degli IoT offre un approccio innovativo per affrontare le sfide e limitazioni dei tradizionali metodi di sicurezza. L'AI può portare benefici significativi, soprattutto considerando la complessità e la diversità degli ambienti IoT.

Capitolo 3

Applicazione dell'Intelligenza Artificiale nella Sicurezza IoT

3.1 Ruolo critico dell'AI nella sicurezza IoT

Integrare l'AI nella sicurezza degli IoT non solo migliora la capacità di rilevare e rispondere agli attacchi, ma consente anche una gestione più intelligente e dinamica della sicurezza in un ecosistema IoT in rapida evoluzione. Con la graduale crescita delle applicazioni di rete intelligenti e grazie allo sviluppo di sensori ibridi controllati dalle più recenti schede programmabili, l'Internet delle Cose può generare una enorme quantità di dati.
La mole di dati generati dalla rete su larga scala viene archiviata su supporti di grande capacità di archiviazione, server privati e spesso servizi cloud. I dati archiviati comprendono dati non elaborati – grezzi – che potrebbero produrre risultati innovativi dal punto di vista delle previsioni. Tuttavia, i dispositivi IoT, i nodi gateway, i server proxy e persino i server dotati di elevata capacità computazionale non sempre sono in grado di elaborare tale quantità di dati.
In questo contesto l'Intelligenza Artificiale arriva in soccorso, apportando algoritmi ibridi innovativi, basati su alberi decisionali e approcci statistici, in grado di consumare tali dati e fornire capacità di apprendimento in tempo reale alla rete IoT operativa. L'inclusione dell'AI nella rete non solo migliora la capacità di elaborazione della stessa, ma fornisce anche supporto all'infrastruttura del database. La Figura 3.1 rappresenta una rete IoT integrata ad un database cloud basato sull'AI per la gestione dei dati, l'apprendimento e il miglioramento dei feedback. Più gli algoritmi apprendono e imparano a fornire riscontri, più saranno precise e attendibili le correzioni apportate ai dati. Questo si traduce in risultati più accurati, ottenuti dal complesso assemblaggio di elementi e tecnologie eterogenee.

L'idea di base nell'utilizzo del Machine Learning (ML) e dell'AI è quella di rendere automatico il sistema di apprendimento attraverso esperienza.

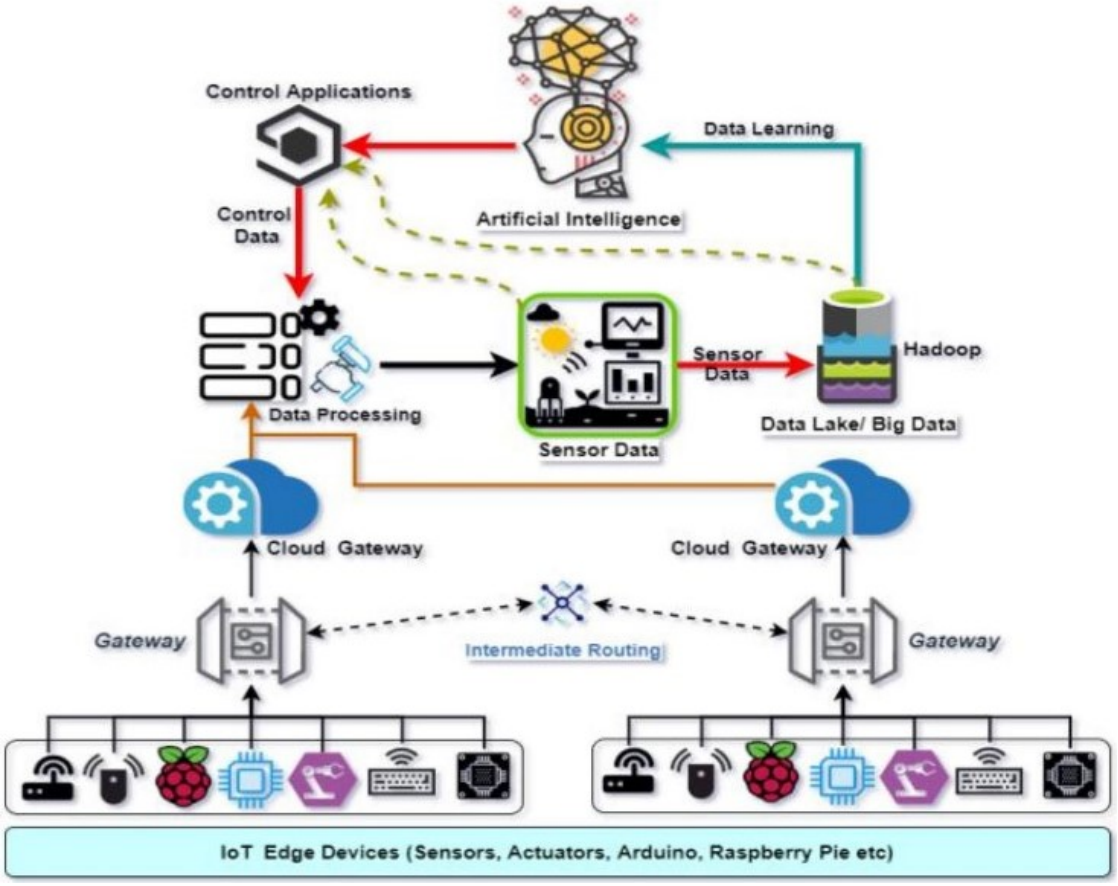

Figura 3.1: Rete IoT e database cloud. [3]

I modelli basati sull'AI sono rappresentati da procedure iterative, con fasi differenti di collezione dei dati da parte dei dispositivi e di allenamento dei modelli utilizzando i "classificatori". Le varie fasi della Figura 3.2 rappresentano la catena di operazioni messe in atto dagli algoritmi di AI per il processo di apprendimento, allenamento e testing dei dati e feedback ottenuti:
- *Data Collection*: i dispositivi interconnessi comunicano attraverso la rete producendo dati che vengono archiviati in grandi spazi di memoria o storage cloud per garantirne l'integrità. I dati di formato eterogeneo attendono di essere processati;
- *Data Pre-processing*: i dati grezzi raccolti sono generalmente incompleti o non comprensibili immediatamente. Il processo di pre-processing li rende quindi leggibili ed interpretabili;
- *Sampling*: in AI il dataset ottenuto viene successivamente diviso in training set e testing set, di modo che il modello apprenda dai dati di training, mentre i test vengono applicati sui dati di testing;
- *AI-based Classification*: il modello è progettato sulla base del dataset, degli inte-

ressi degli analisti, e risultato atteso dal data trends. L'esistenza di diversi modelli basati sull'intelligenza artificiale facilitano il compito di analizzare i dati e applicare il modello adatto. I diversi algoritmi reagiscono e vengono addestrati in base allo specifico problema di classificazione;
- *Final Model*: I samples prelevati dai dati di training vengono usati per effettuare la predizione del valore target. Il valore della predizione viene salvato per essere successivamente valutato;
- *Evaluating Model*: la performance del modello viene valutata sulla base del testing effettuato e su definiti parametri di accuratezza, precisione e punteggio F1 ottenuto (precision + recall, metrica utilizzata per valutare l'accuratezza del modello di classificazione). Le componenti principali dell'F1 score sono:

1. Precision (Precisione): Misura la proporzione di istanze positive identificate correttamente rispetto a tutte le istanze identificate come positive. Si calcola come:

$$\text{Precision} = [(\text{True Positive})/(\text{True Positive}+\text{False Positive})]$$

2. Recall (Recupero o Sensibilità): Misura la proporzione di istanze positive identificate correttamente rispetto al totale delle istanze positive effettive. Si calcola come:

$$\text{Recall} = [(\text{True Positive})/(\text{True Positive}+\text{False Negatives})]$$

L'F1 score è quindi definito come la media armonica tra precision e recall ed è calcolato con la formula

$$\text{F1} = 2 \times [(\text{Precision} \times \text{Recall})/(\text{Precision}+\text{Recall})]$$

L'F1 score varia da 0 a 1, dove 1 rappresenta il miglior risultato possibile, indicando una perfetta precisione e recall. È particolarmente utile quando ci sono classi sbilanciate o quando entrambi precision e recall sono importanti per la valutazione delle prestazioni del modello.

3.2 Algoritmi di prevenzione delle intrusioni basati sull'AI

Gli algoritmi di prevenzione delle intrusioni basati sull'Intelligenza Artificiale nel campo IoT sono progettati per rilevare e mitigare potenziali minacce alla sicurezza.

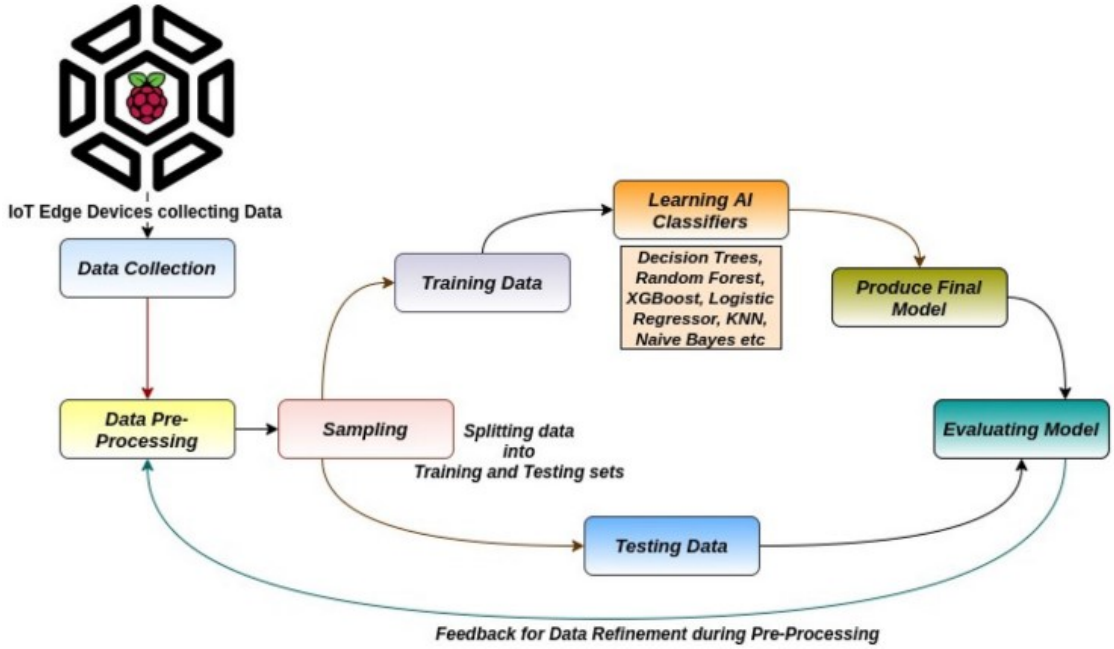

Figura 3.2: Processo di dati IoT basato su AI. [3]

Questi algoritmi utilizzano tecniche di apprendimento automatico e analisi avanzate per identificare comportamenti anomali o attacchi in corso. Tramite l'analisi del comportamento gli algoritmi di AI possono apprendere il normale comportamento dei dispositivi IoT e delle reti. In questo modo, quando si verificano deviazioni significative da questo comportamento, gli algoritmi possono rilevare tali anomalie, indicando potenziali attacchi o violazioni. A differenza delle firme di minacce tradizionali, gli algoritmi di AI possono rilevare nuove minacce senza la necessità di aggiornamenti frequenti delle definizioni. Ciò li rende particolarmente efficaci nel rilevare attacchi innovativi che potrebbero sfuggire ai metodi di rilevamento convenzionali.

Gli algoritmi di AI possono adattarsi dinamicamente a nuovi contesti e ambienti senza richiedere configurazioni manuali estese. Questa adattabilità e apprendimento continuo consente agli algoritmi di migliorare nel tempo, affrontando nuove minacce man mano che emergono. Ciò fornisce una difesa robusta contro gli attacchi in continua evoluzione. Inoltre, gli algoritmi di AI possono comprendere il contesto operativo dei dispositivi IoT. Questa comprensione del contesto riduce la probabilità di falsi positivi, consentendo una migliore distinzione tra attività normali e attività sospette.

Alcuni sistemi di prevenzione delle intrusioni basati sull'AI sono in grado di attivare risposte automatiche agli eventi sospetti, come l'isolamento di dispositivi compromessi o la restrizione dell'accesso. Ciò contribuisce a fornire una risposta

automatica e a limitare i danni prima che si diffondano.
L'AI eccelle nell'analisi di grandi quantità di dati, caratteristica fondamentale nell'ambito IoT dove la mole di informazioni generata dai dispositivi è considerevole. Gli algoritmi possono identificare pattern significativi all'interno di questo flusso di dati.

3.2.1 Reti Neurali (Autoencoder)

L'implementazione di reti neurali - modelli ispirati al funzionamento del cervello umano con strati di neuroni artificiali - in un dispositivo IoT per la sicurezza segue una logica tecnica specifica. I principi di base della logica implementativa delle reti neurali in questo contesto sono:

- **Rilevamento Anomalie**

  Obiettivo: Rilevare comportamenti anomali o attività sospette nei dati generati dai dispositivi IoT.
  Implementazione:

  - Utilizzo di reti neurali per il rilevamento delle anomalie, ad esempio, autoencoder o reti neurali ricorrenti.
  - Addestramento del modello con dati normali per imparare il comportamento normale.
  - Durante il funzionamento, il modello confronta costantemente nuovi dati con il comportamento appreso e segnala le deviazioni significative.

- **Classificazione delle Minacce**

  Obiettivo: Classificare le attività in categorie come "normale", "sospetto" o "minaccioso".
  Implementazione:

  - Utilizzo di reti neurali per la classificazione, come reti neurali convoluzionali (CNN) o reti neurali ricorrenti (RNN).
  - Addestramento del modello con dati etichettati per diverse categorie di attività.
  - Il modello assegna automaticamente nuovi dati a una categoria specifica basandosi sull'addestramento.

- **Analisi del Comportamento**

  Obiettivo: Analizzare il comportamento dei dispositivi IoT per identificare pattern significativi o inconsueti.
  Implementazione:

- Utilizzo di reti neurali per l'analisi del comportamento, ad esempio, Recurrent Neural Network (RNN) o Long Short-Term Memory (LSTM).
- Addestramento del modello con sequenze storiche di dati per catturare le dinamiche temporali.
- Il modello può prevedere il comportamento futuro o identificare anomalie basate su deviazioni dalle sequenze attese.

- **Apprendimento Continuo**

  Obiettivo: Consentire al sistema di adattarsi dinamicamente ai nuovi pattern di minacce e cambiamenti nell'ambiente.
  Implementazione:

  - Utilizzo di reti neurali con capacità di apprendimento continuo.
  - Il modello si aggiorna regolarmente con nuovi dati senza richiedere un completo riaddestramento.
  - L'adattamento continuo consente di mantenere una protezione efficace contro minacce in evoluzione.

- **Implementazione Edge**

  Obiettivo: Eseguire l'elaborazione dei dati direttamente sul dispositivo IoT (edge computing) per ridurre la latenza e migliorare la privacy.
  Implementazione:

  - Utilizzo di modelli di reti neurali ottimizzati per l'esecuzione su dispositivi con risorse limitate.
  - Riduzione della dipendenza da connessioni di rete, consentendo risposte più rapide e il trattamento locale dei dati sensibili.

- **Risposta Automatica**

  Obiettivo: Attivare risposte automatiche in risposta a comportamenti identificati come minacciosi.
  Implementazione:

  - Integrare reti neurali con sistemi di risposta automatica.
  - Configurare il sistema per attivare azioni di mitigazione, come l'isolamento del dispositivo o l'allarme, in risposta a segnalazioni di minacce.

- **Gestione delle Risorse**

  Obiettivo: Ottimizzare l'uso delle risorse del dispositivo IoT durante l'esecuzione di algoritmi di reti neurali.
  Implementazione:

- Scegliere o progettare reti neurali che siano efficienti in termini di risorse.
- Adottare tecniche di pruning o quantizzazione dei modelli per ridurre la dimensione e il carico computazionale.

L'implementazione pratica di queste logiche varia a seconda dei dettagli specifici dell'applicazione e delle caratteristiche del dispositivo IoT in questione, comprese le limitazioni di risorse. È importante bilanciare l'efficacia del modello con la capacità computazionale disponibile.

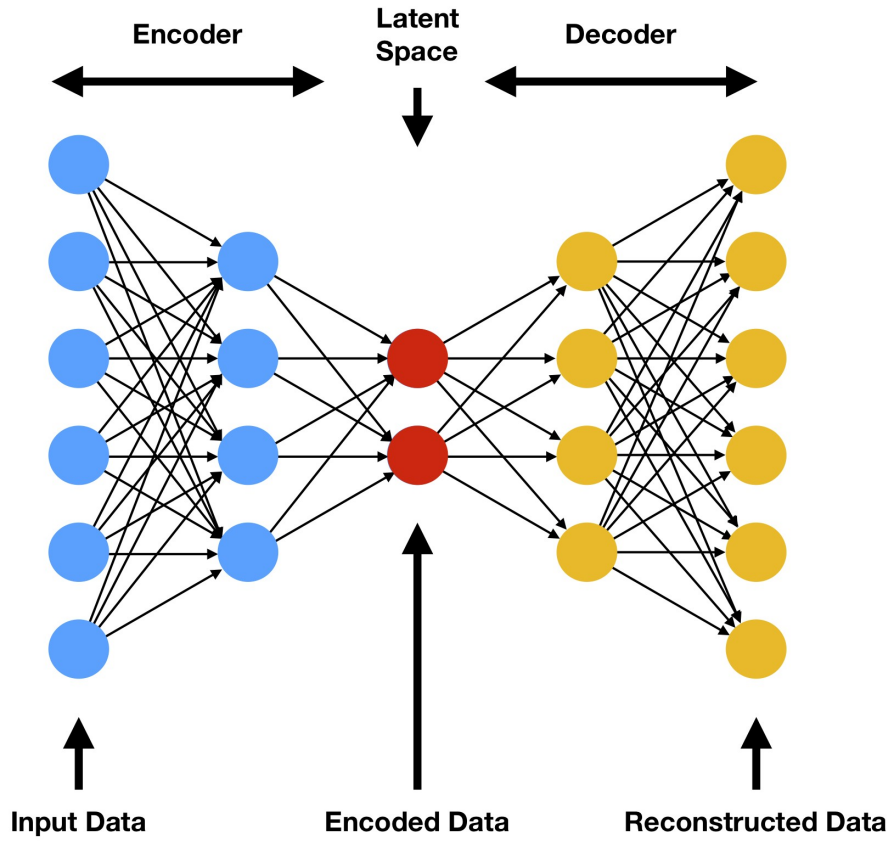

Figura 3.3: Autoencoder – Processo di codifica e decodifica dei dati presi in esame.

Autoencoder è una tipologia di rete neurale utilizzata nell'ambito dell'apprendimento automatico, e più precisamente nell'ambito della riduzione della dimensionalità e del riconoscimento delle caratteristiche. La sua struttura è composta da due parti principali, rappresentate in Figura 3.3: un encoder, che converte l'input in una rappresentazione più compatta chiamata "codice latente", e un decoder, che ricostruisce l'input originale da questo codice latente. L'obiettivo dell'autoencoder è di apprendere una rappresentazione efficiente dell'input in modo che il processo di codifica e decodifica generi una ricostruzione il più fedele possibile all'input originale.

Struttura di un Autoencoder:

1. Encoder:

   • La prima metà dell'autoencoder, l'encoder, comprime l'input in una rappresentazione più compatta.
   • Utilizza strati di neuroni per ridurre gradualmente la dimensione dell'input, condensandolo in un "codice latente" che rappresenta le caratteristiche principali.

2. Decoder:

   • La seconda metà, il decoder, ricostruisce l'input originale a partire dal codice latente.
   • Utilizza strati speculativi rispetto all'encoder per espandere progressivamente il codice latente nella forma dell'input originale.

3. Funzione di Costo:

   • L'obiettivo è minimizzare la differenza tra l'input originale e la sua ricostruzione.
   • Una comune funzione di costo è la Mean Squared Error (MSE), che misura la discrepanza media tra i valori reali e quelli previsti.

Utilizzi Principali:

1. Riduzione della Dimensionalità:

   • Gli autoencoder sono utilizzati per ridurre la dimensionalità dei dati, estraendo le caratteristiche più importanti.
   • Ad esempio, in imaging, possono essere utilizzati per la compressione delle immagini conservando le caratteristiche rilevanti.

2. Eliminazione del Rumore:

   • Possono essere addestrati per eliminare il rumore dai dati di input durante il processo di ricostruzione.
   • Utile per la gestione di dati affetti da disturbi o errori.

3. Generazione di Dati:

   • Gli autoencoder possono essere utilizzati anche per generare nuovi dati simili a quelli di addestramento.
   • Sono alla base di molte tecniche di generazione di immagini, ad esempio.

4. Rilevamento delle Anomalie:

   • Quando addestrati su dati normali, gli autoencoder possono rivelare anomalie rilevando discrepanze significative tra l'input e la sua ricostruzione.

Gli autoencoder sono componenti chiave in diverse applicazioni di intelligenza artificiale, e la loro capacità di apprendere rappresentazioni efficienti li rende strumenti versatili in vari contesti, compreso il riconoscimento delle anomalie nelle applicazioni di sicurezza come nel contesto della cybersecurity.

3.2.2 Algoritmo Random Forest

L'algoritmo Random Forest è una tecnica di machine learning che opera sia in contesti di classificazione che di regressione [4]. È basato su un concetto noto come "ensemble learning", che consiste nell'addestrare più modelli (in questo caso alberi decisionali, come rappresentato in Figura 3.4) e combinare i loro risultati per ottenere una previsione più accurata e robusta rispetto a un singolo modello. Questo metodo riduce il rischio di overfitting [5] (caso in cui un modello statistico molto complesso si adatta ai dati osservati - il campione - perché ha un numero eccessivo di parametri rispetto al numero di osservazioni) e migliora la stabilità del modello complessivo.
Un Random Forest è composto da un insieme di alberi decisionali. Ogni albero è addestrato su un sottoinsieme casuale del set di addestramento. Il processo di addestramento di ogni albero coinvolge anche il sottocampionamento (sampling con sostituzione, o Bagging) degli esempi dal set di addestramento. Grazie al sottocampionamento e alla casualità di scelta delle caratteristiche, i singoli alberi nel Random Forest sono diversi.
Poiché ogni albero viene addestrato su un sottoinsieme di dati, è possibile valutare le performance del modello su dati che non sono stati utilizzati durante l'addestramento di ciascun albero. Questi dati sono noti come out-of-bag (OOB) e possono essere utilizzati per valutare l'errore del modello.

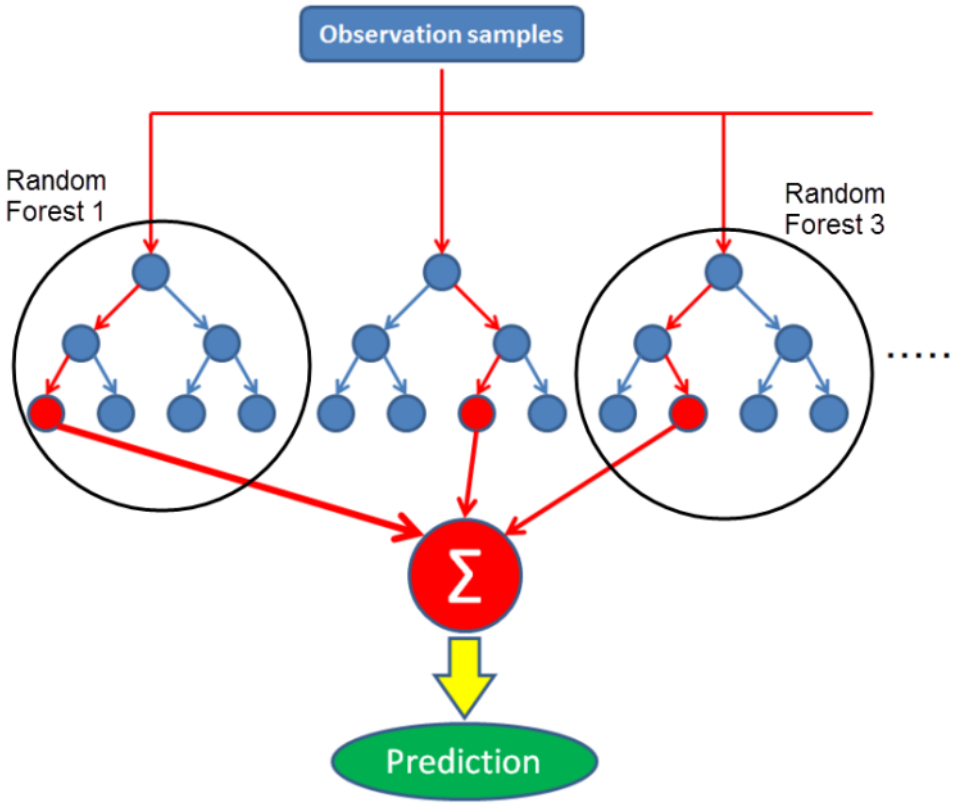

Figura 3.4: Random Forest – Utilizzo di numerosi alberi decisionali, addestrati separatamente per generare una previsione. Queste vengono successivamente aggregate per determinare la predizione finale.

L'algoritmo Random Forest, grazie alla sua versatilità e alla sua predisposizione ad operare con set di dati di grandi dimensioni e caratteristiche, si presenta come valido alleato per garantire la sicurezza dei dispositivi IoT. La sua abilità nel riconoscere modelli anomali nei dati è particolarmente preziosa: addestrato su dati rappresentativi di comportamenti normali, l'algoritmo è in grado di individuare deviazioni significative, indicando possibili minacce o attività non autorizzate. La capacità di rilevare in tempo reale e adattarsi a cambiamenti repentini nel contesto operativo è un aspetto cruciale. Nel panorama dinamico della sicurezza IoT, dove le condizioni possono variare rapidamente, Random Forest agisce come un "guardiano digitale" intelligente, fornendo un'analisi avanzata dei dati generati dai dispositivi IoT e rilevando in modo proattivo e in tempo reale potenziali minacce.

3.2.3 Support Vector Machines (SVM)

Il Support Vector Machine (SVM) è un algoritmo di apprendimento supervisionato utilizzato per problemi di classificazione e regressione. La sua idea di base è trovare un iperpiano ottimale che separi le diverse classi nel modo migliore possibile,

rappresentato in Figura 3.5.

Iperpiano → In uno spazio bidimensionale, un iperpiano è una linea che separa due classi. In spazi tridimensionali, diventa un piano.
Margine → Il margine è la distanza tra l'iperpiano e i punti più vicini delle due classi. SVM cerca di massimizzare questo margine, rendendo la separazione tra classi più robusta.
Support Vectors → I support vectors sono i punti dati che sono più vicini all'iperpiano e influenzano la sua posizione. Sono i punti critici per la definizione del margine.

La procedura di addestramento prevede che il modello riceva un insieme di dati di addestramento etichettati, con ogni esempio associato a una classe. Si seleziona un kernel che può essere lineare, polinomiale o gaussiano. Il kernel determina la trasformazione da uno spazio delle feature all'altro, rendendo il problema linearmente separabile. L'obiettivo è quello di costruire un iperpiano che massimizzi il margine: questo viene fatto risolvendo il problema di ottimizzazione vincolata. SVM risolve un problema di programmazione quadratica per determinare i pesi ottimali (coefficienti) per ciascuna feature e per trovare l'iperpiano di separazione ottimale. Se il problema non è linearmente separabile nello spazio originale delle feature, il kernel trick trasforma i dati in uno spazio di dimensione superiore, dove potrebbe essere possibile una separazione lineare. Dopo l'addestramento, per classificare un nuovo punto, viene valutato su quale lato dell'iperpiano cade.
L'applicazione del Support Vector Machine (SVM) per garantire e proteggere la sicurezza dei dispositivi IoT può essere effettuata in diversi modi:

1) *Rilevamento minacce* = SVM può essere addestrato per classificare il normale comportamento dei dispositivi IoT. Qualsiasi deviazione significativa da questo comportamento può essere considerata anomala e indicativa di un possibile attacco. Inoltre, SVM può essere utilizzato per identificare modelli di attività sospetti o inconsueti nei dati generati dai dispositivi IoT. Ad esempio, se un dispositivo inizia a inviare dati in modo anomalo o a interagire con altri dispositivi in modo insolito, SVM può rilevarlo.
2) *Controllo degli Accessi* = SVM può essere utilizzato per l'autenticazione degli utenti o dei dispositivi. Ad esempio, può essere addestrato per riconoscere i modelli di accesso regolari e identificare eventuali tentativi di accesso non autorizzato. Se un dispositivo IoT è programmato per comunicare solo con un set specifico di altri dispositivi, SVM può rilevare comunicazioni con dispositivi non

autorizzati.
3) *Sicurezza delle Reti* = SVM può essere implementato per il rilevamento di intrusioni di rete negli ambienti IoT. Può filtrare i pacchetti, analizzare il traffico di rete tra i dispositivi IoT e identificare schemi associati a tentativi di attacco.
4) *Analisi delle Vulnerabilità* = il modello può essere addestrato per rilevare pattern associati a exploit e attacchi noti. Può essere utilizzato come componente di un sistema di prevenzione delle intrusioni. SVM può monitorare le configurazioni dei dispositivi IoT e rilevare cambiamenti non autorizzati. Ad esempio, può rilevare se le impostazioni di sicurezza di un dispositivo sono state modificate senza autorizzazione.

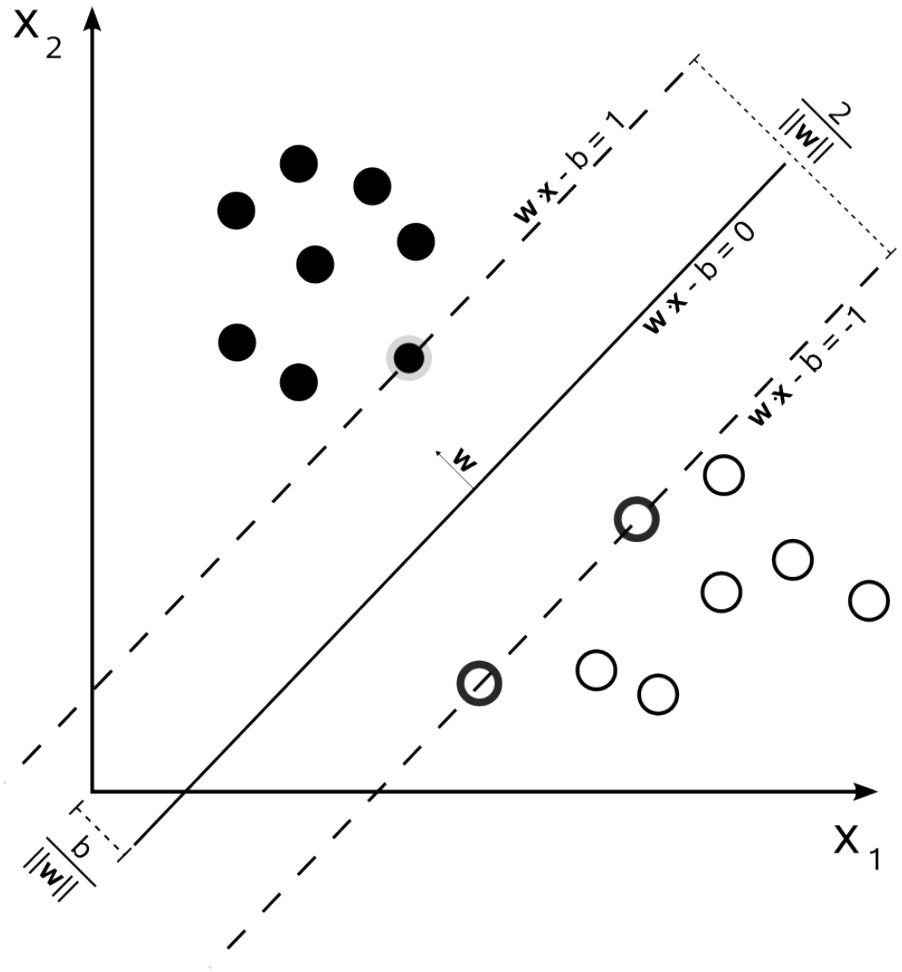

Figura 3.5: Support Vector Machines (SVM) – Esempio di separazione lineare usando le SVM. [6]

Capitolo 4

Case study: Darktrace

4.1 Cyber AI Loop

Darktrace è un'azienda all'avanguardia nel settore della sicurezza cibernetica, riconosciuta per la sua innovazione nell'applicazione dell'intelligenza artificiale (AI) per affrontare le minacce informatiche in modo proattivo e autonomo. Fondata nel 2013 a Cambridge [7], Darktrace si è affermata come una delle principali aziende specializzate nella difesa avanzata contro le minacce digitali, generando un fatturato di 415,5 milioni solo nel 2022.
Ciò che distingue Darktrace da altre soluzioni di sicurezza è la sua enfasi sulla "Cyber AI" o Intelligenza Artificiale Applicata alla Sicurezza Cibernetica. L'azienda adotta un approccio unico basato sull'apprendimento automatico e l'intelligenza artificiale per proteggere le reti e gli ambienti digitali. La sua piattaforma sfrutta algoritmi avanzati per comprendere il normale comportamento di una rete e rilevare in modo autonomo le anomalie che potrebbero indicare attività malevole.

Darktrace offre un prodotto innovativo sul mercato, il "Cyber AI Loop": si tratta di un sistema interconnesso di soluzioni di sicurezza informatica che opera in modo continuativo ed autonomo, al fine di rafforzare la sicurezza dei sistemi informatici.
Il Cyber AI Loop comprende quattro famiglie di prodotti basati sull'intelligenza artificiale: Darktrace PREVENT, Darktrace DETECT, Darktrace RESPOND e Darktrace HEAL, che funzionano nell'intera organizzazione sfruttando i dati interni ed esterni, contemporaneamente (Figura 4.1). Con ciascuna tecnologia che collabora e fornisce informazioni alle altre, la resilienza cibernetica viene notevolmente migliorata. Ogni componente del Cyber AI Loop è alimentato dal "Self-learning AI", tecnologia proprietaria Darktrace che impara a conoscere l'ambiente in cui

opera. Comprendendo la specifica organizzazione su misura, gli utenti vigenti e i dispositivi utilizzati, nonché le interazioni tra di essi, è in grado di costruire un senso evoluto di cosa è normale identificare in termini di comportamenti ed eventi, e di ciò che non lo è. Questo processo consente a Darktrace di far luce su minacce precedentemente sconosciute e imprevedibili.

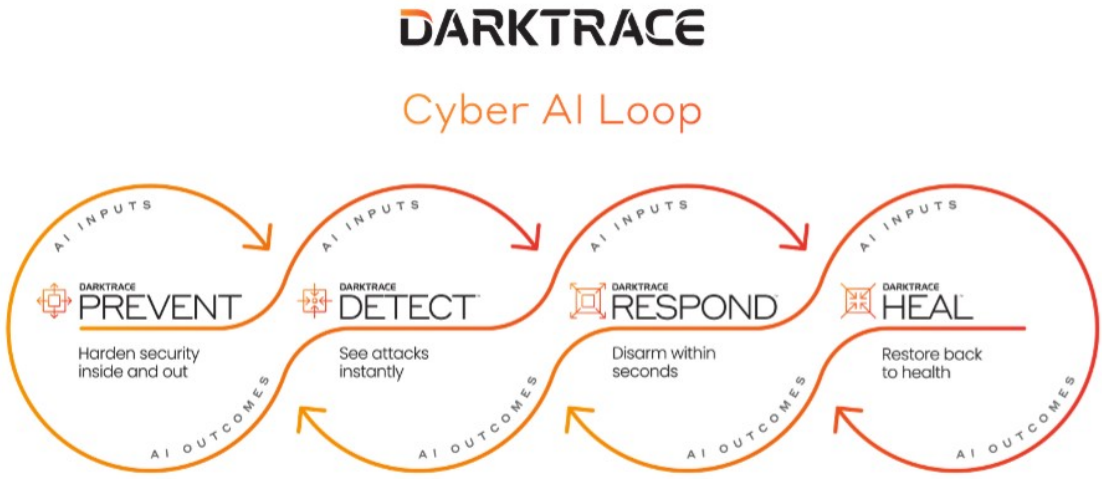

Figura 4.1: Il Cyber AI Loop di Darktrace

Il Cyber AI Loop di Darktrace è implementato grazie all'utilizzo dei Large Language Models (LLMs), termine che si riferisce a modelli linguistici avanzati e di dimensioni considerevoli, spesso alimentati da reti neurali profonde: questi modelli sono addestrati su enormi quantità di dati testuali per comprendere e generare il linguaggio umano in modo più sofisticato e contestualmente sensibile. Le caratteristiche che rendono così potenti i Large Language Models sono:
- capacità di memorizzare enormi quantità di parametri e informazioni durante l'addestramento;
- capacità di comprendere il contesto in cui operano in modo più profondo;
- capacità di essere adattati a una varietà di compiti senza la necessità di addestramento specifico per ciascun compito;
- capacità di applicazione in numerosi settori.
L'utilizzo di questa sofisticata tecnologia ha permesso a Darktrace di ottenere un forte vantaggio competitivo, premiato nel 2020 con il "Cyber Award's AI Product of the Year" e nel 2022 con "AI & Machine Learning Award" al Go:Tech Awards[7].

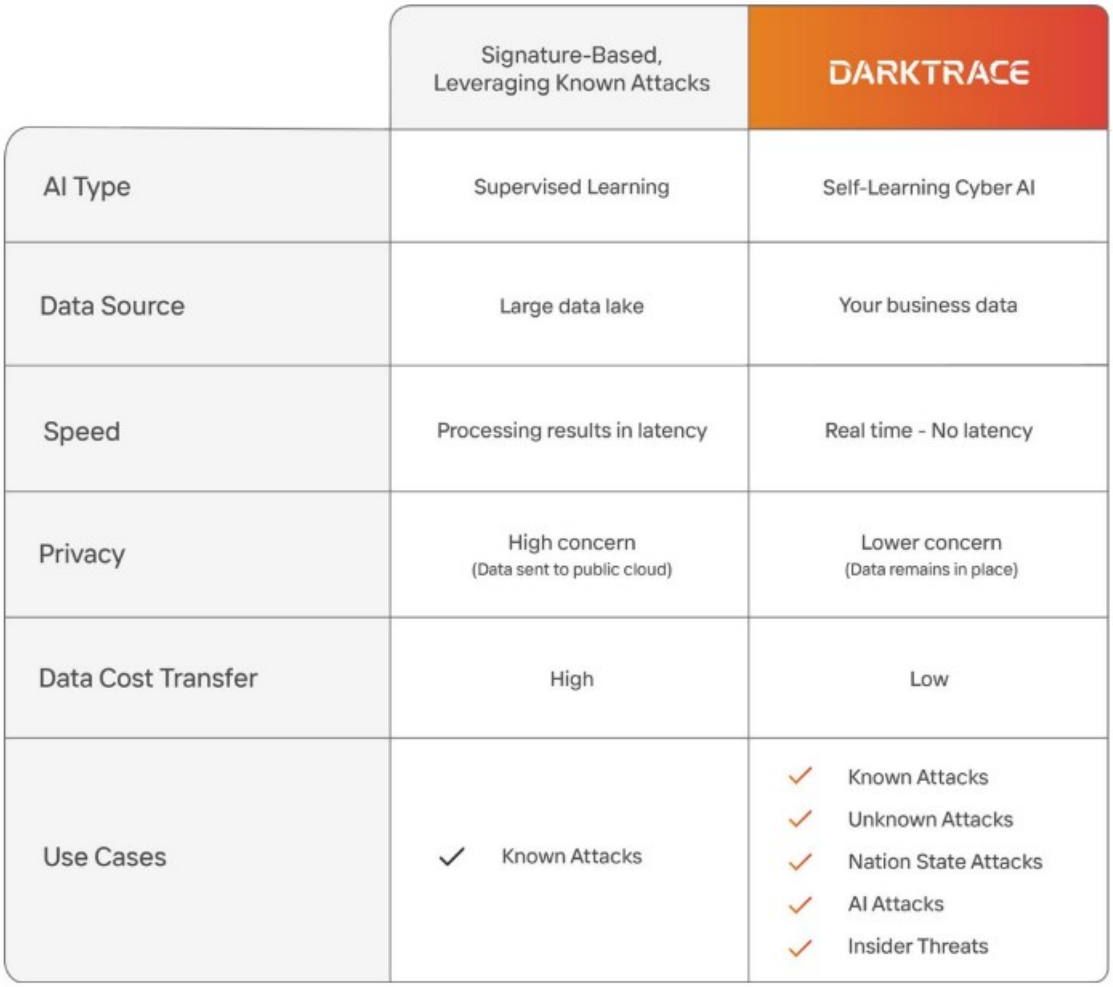

Figura 4.2: Comparazione tra il Cyber AI Loop offerto da Darktrace e i tradizionali strumenti di sicurezza.

La Figura 4.2 rappresenta i numerosi vantaggi derivanti dall'utilizzo del prodotto Cyber AI Loop rispetto all'utilizzo di tradizionali strumenti di sicurezza. Secondo un analisi di Darktrace, il Cyber AI Loop potrebbe ridurre i tempi di rilevamento di una potenziale minaccia del 95,83%, rispondere ad un eventuale attacco entro i primi 2,5 minuti e ridurre i tempi di triage del 90% [8].

Nel luglio del 2023 Darktrace si è resa protagonista nello sventare, per diversi clienti, una nuova minaccia informatica osservata per la prima volta nel marzo del 2023, conosciuta come Akira Ransomware. Si tratta di un attacco informatico della famiglia dei ransomware, tipo di malware che limita l'accesso del dispositivo che infetta e dei dati al suo interno, richiedendo un riscatto da pagare per rimuovere la limitazione. Grazie a Darktrace DETECT il SOC ha potuto osservare delle operazioni di ricognizione sospetta all'interno dei dispositivi, oltre a numerosi tentativi di movimento laterale. Lo strumento di analisi e investigazione autonoma di

Darktrace, il Cyber AI Analyst, è stato in grado di analizzare i molteplici eventi correlati all'attività di crittografia, e a fascicolarli in un unico report, l'AI Analyst Incident, presentando un riassunto dettagliato e completo dell'intero incidente dall'inizio della rilevazione di Darktrace. In combinazione con Darktrace RESPOND, il SOC ha potuto ripristinare poi il normale funzionamento dei dispositivi, gestendo e limitando i danni ricevuti.

Capitolo 5

Implicazioni Economiche e Giuridiche legate all'AIoT

5.1 Impatto nell'ambito economico

Gli investimenti nelle soluzioni di sicurezza IoT sono in costante aumento. Secondo alcune stime dell'International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), il mercato della sicurezza IoT è previsto raggiungere diversi miliardi di dollari nei prossimi anni (Figura 5.1). Questo include investimenti in tecnologie di rilevamento e risposta alle minacce basate sull'IA. Anche il tasso di crescita annuale composto (CAGR) per il mercato della sicurezza IoT è stato notevole, guidato dalla crescente consapevolezza delle minacce e dalla necessità di proteggere l'ecosistema IoT in espansione.

Market	Artificial Intelligence in Cybersecurity Market
Market size 2018	USD 9.8 Billion
Market size 2021	USD 14.9 Billion
Market size 2025	USD 36.6 Billion
Market size 2030	USD 133.8 Billion

Figura 5.1: Predizione del valore di mercato dell'Intelligenza Artificiale in Cybersecurity. [9]

L'implementazione di soluzioni di sicurezza IoT basate sull'AI ha contribuito alla creazione di nuovi posti di lavoro specializzati nel campo della sicurezza cibernetica e dell'AI. L'integrazione di AI nella sicurezza IoT ha dato luogo a nuovi modelli di business, come servizi avanzati di sicurezza gestita e consulenza specialistica.

Inoltre, secondo un sondaggio condotto da Forbes Advisor, il 64% delle aziende intervistate si aspetta che l'intelligenza artificiale contribuisca ad un generico aumento della produttività [10]. Il dato dimostra la crescente fiducia nel potenziale dell'AI come strumento in grado di trasformare i processi aziendali.
Tuttavia, questa rapida trasformazione porta con sé anche il timore, da parte dei lavoratori, di perdere il posto di lavoro: a seguito di un'indagine di Forbes Advisor il 77% degli intervistati ha espresso il timore che l'AI possa causare la perdita di posti di lavoro nel prossimo futuro, manifestando una forte preoccupazione circa il potenziale della tecnologia rispetto alle opportunità occupazionali [11]. Con l'evoluzione dell'AI, 400 milioni di lavoratori in tutto il mondo potrebbero essere sostituiti. Un rapporto McKinsey prevede che tra il 2016 e il 2030 i progressi dell'AI potrebbero produrre ripercussioni su circa il 15% della forza lavoro mondiale [12].
A compensare però le preoccupazioni legate alla possibile dispersione della forza lavoro, secondo una ricerca del World Economic Forum, l'AI dovrebbe creare circa 97 milioni di nuovi posti di lavoro. Si assisterà alla crescita della domanda di figure professionali in grado di offrire supporto nel campo dell'AI. Secondo il rapporto McKinsey, nel 2022 il 39% delle aziende ha dichiarato di aver assunto software engineer, mentre il 35% avrebbe assunto data engineer con mansioni connesse all'implementazione della tecnologia [12].
Per quanto riguarda le aziende, secondo una ricerca di Forbes Advisor il 64% dei proprietari di aziende ritiene che l'AI abbia il potenziale per migliorare le loro interazioni con i clienti, evidenziando una visione positiva del ruolo dell'AI nella valorizzazione del rapporto con i consumatori [10]. Il 43% delle aziende esprime la propria preoccupazione circa la dipendenza dalla tecnologia e un ulteriore 35% teme di non avere le competenze tecniche necessarie per utilizzare l'AI in modo efficace [10]. Da un'analisi condotta dall'Osservatorio Internet of Things della School of management del Politecnico di Milano sulla maturità delle grandi organizzazioni nel percorso di adozione dell'AI, emerge che il 34% delle grandi aziende si trova nell'era dell'implementazione, disponendo di risorse e competenze necessarie a sviluppare e portare in produzione le iniziative di AI [2].

5.2 Questioni legali, etiche e di privacy

L'integrazione massiccia di dispositivi IoT e l'uso crescente di soluzioni basate sull'AI per la sicurezza sollevano una serie di questioni legali, etiche e di privacy che richiedono attenta considerazione. Dal punto di vista legale, la raccolta, l'archivia-

zione e l'uso dei dati da parte dei dispositivi IoT devono conformarsi alle leggi sulla privacy esistenti. Ciò include il rispetto del Regolamento Generale sulla Protezione dei Dati (GDPR) in Europa e leggi correlate nelle altre giurisdizioni [13]. Le aziende devono garantire la trasparenza nella raccolta dei dati, ottenere consenso informato e adottare pratiche di sicurezza robuste per evitare le violazioni. Gli utenti devono essere pienamente informati su come i loro dati vengono raccolti, utilizzati e condivisi. È importante garantire un consenso chiaro e informato da parte degli utenti prima di raccogliere qualsiasi tipo di informazione. La trasparenza nelle pratiche di gestione dei dati contribuisce a costruire la fiducia degli utenti. L'etica nella gestione dei dati è un aspetto fondamentale. L'ingente raccolta di informazioni tramite dispositivi IoT può portare a profili estremamente dettagliati degli individui. Ciò solleva domande sull'accesso ai dati, sulla proprietà e sulla possibilità di utilizzare tali informazioni per scopi eticamente discutibili. È compito delle aziende quindi considerare le implicazioni etiche di come utilizzano e condividono i dati raccolti. In questo contesto "Privacy by Design" e "Privacy by Default" sono approcci essenziali quando si progettano e implementano dispositivi IoT e modelli basati sull'AI per garantire la massima protezione degli utenti. Questi principi dovrebbero essere integrati in tutte le fasi dello sviluppo e dell'implementazione, piuttosto che essere adottati come misure correttive a posteriori. Inoltre, i dispositivi e i modelli dovrebbero raccogliere e utilizzare solo i dati strettamente necessari per svolgere la loro funzione principale, evitando la raccolta e la conservazione di dati superflui.
Allo scopo di favorire la diffusione di pratiche comuni di sicurezza dei dispositivi IoT, il comitato tecnico per la cyber security (ETSI) ha rilasciato lo standard per la sicurezza informatica ETSI EN 303 645 (2020-04) da applicare al mercato IoT, con 13 regole per garantire la sicurezza nei dispositivi connessi, renderli conformi al GDPR e fornire linee guida per certificazioni future nel settore [14]:

- ☞ Non utilizzare "password universali", ovvero password ripetute per più account o canali contemporaneamente;
- ☞ Implementare un mezzo per gestire eventuali segnalazioni di vulnerabilità;
- ☞ Mantenere i software aggiornati nel tempo;
- ☞ Archiviare in modo sicuro eventuali parametri sensibili di sicurezza;
- ☞ Comunicare solamente attraverso canali sicuri;
- ☞ Minimizzare la superficie attaccabile e l'esposizione a minacce esterne;

- ☞ Garantire l'integrità del software;
- ☞ Rendere i sistemi resilienti alle interruzioni;
- ☞ Esaminare i dati di telemetria del sistema;
- ☞ Semplificare l'eliminazione dei dati utente da parte degli utenti;
- ☞ Semplificare le operazioni di installazione e manutenzione dei dispositivi;
- ☞ Convalidare i dati di input.

Implementare questi principi richiede un impegno significativo da parte degli sviluppatori, dei progettisti e delle organizzazioni coinvolte. Tuttavia, adottare un approccio proattivo alla privacy favorisce la produzione di dispositivi IoT e sistemi AI più affidabili, sicuri ed etici.

Conclusioni

Quello dell'AI è considerato uno degli sviluppi più promettenti nell'era dell'informazione, e la cybersecurity è probabilmente la disciplina che più potrebbe beneficiarne [15]. Nuovi algoritmi, tecniche, strumenti e imprese che offrono servizi basati sull'AI continuano ad affiorare sul mercato. Questi sistemi, comparati alle tradizionali soluzioni di cybersecurity, si presentano come più flessibili, adattabili e robusti, aiutando a migliorare le performance di sicurezza, l'autonomia e la protezione dei sistemi contro minacce cibernetiche sofisticate. Attualmente, le tecniche di Machine Learning sono probabilmente tra le più potenti e infleunti nel campo dell'AI.

Guardando al futuro, ci troviamo di fronte a una significativa trasformazione che va oltre l'Internet of Things (IoT), dirigendosi verso l'Internet of Everything (IoE). Questa evoluzione rappresenta un passo oltre la semplice connessione di dispositivi, coinvolgendo ogni aspetto delle nostre vite in un tessuto digitale interconnesso.
L'Internet of Everything (IoE) integra non solo oggetti fisici, ma anche dati, persone, processi e contesti in un'unica piattaforma digitale. Questa visione più ampia porta con sé nuove prospettive e possibilità, ma, al contempo, solleva sfide significative, in particolare in relazione alla sicurezza.
Con la crescente interconnessione tra ogni aspetto del nostro mondo, la superficie di attacco diventa più ampia e complessa. Un ecosistema IoE più esteso comporta la necessità di affrontare minacce che possono manifestarsi in modalità innovative e sofisticate.
L'evoluzione verso l'IoE richiede una revisione critica delle attuali strategie di sicurezza implementate. L'adozione di approcci avanzati basati sull'Intelligenza Artificiale (AI) diventa sempre più cruciale. Gli algoritmi di Machine Learning, addestrati per rilevare e mitigare minacce in tempo reale, possono diventare gli "occhi" digitali che sorvegliano continuamente questa vasta rete di interconnessioni.
Allo stesso tempo, l'approccio alla sicurezza dell'IoE richiederà una combinazione di tecniche avanzate, come la crittografia robusta, la gestione delle identità digitali

e la sicurezza della rete. La capacità di autenticare e autorizzare non solo i dispositivi fisici ma anche i dati in transito diventa un aspetto cruciale per garantire l'integrità dell'intero ecosistema.
Inoltre, l'IoE introduce nuove sfide etiche e legali. La raccolta massiccia di dati da ogni aspetto della nostra vita solleva questioni sulla privacy e la gestione etica di queste informazioni. Le normative e le leggi devono evolversi di pari passo per affrontare le complessità dell'IoE.
Mentre l'IoE offre una visione intrigante di un mondo interconnesso e intelligente, la sicurezza deve rimanere al centro di questa trasformazione.

Il presente studio ha fornito una panoramica approfondita sulle principali minacce legate all'ambiente degli IoT e sulle applicazioni dell'Intelligenza Artificiale alla sicurezza. Attraverso l'analisi degli algoritmi di AI e Machine Learning, abbiamo identificato soluzioni pratiche che possono essere implementate per mitigare le minacce emergenti. Tuttavia, mentre è possibile assistere ai progressi attuali, è essenziale considerare le sfide rimanenti e anticipare i futuri sviluppi.

La sicurezza degli IoT richiede un approccio collaborativo e continuo, coinvolgendo ricercatori, sviluppatori e responsabili delle politiche. Solo attraverso un impegno collettivo, unito a pratiche di sicurezza avanzate e riflessione etica continua, diventa possibile garantire un futuro digitale più sicuro e resiliente.

Bibliografia

[1] FutureSoftTech.com - "Evolution of internet of things"

[2] Osservatorio Internet of Things della School of management del Politecnico di Milano - "Internet of Things (IoT): il mercato cresce del +13%"

[3] "Complex and Intelligent Systems" (2022), Ankit Attkan, Virender Ranga

[4] Wikipedia - "Random Forest"

[5] Wikipedia - "Overfitting"

[6] Wikipedia – "Macchine a Vettore di Supporto"

[7] Wikipedia - "Darktrace"

[8] Darktrace - "Cyber security that learns you"

[9] IJARCCE - "The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review"

[10] Forbes Advisor – "How Businesses Are Using Artificial Intelligence In 2023"

[11] Forbes Advisor – "Over 75% Of Consumers Are Concerned About Misinformation From Artificial Intelligence"

[12] McKinsey & Company - "Economic potential of generative AI"

[13] REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

[14] ETSI EN 303 645 – "Cyber Security for Consumer Internet of Things: Baseline Requirements"

[15] "Artifical Intelligence In Cybersecurity", Nadine Wirkuttis and Hadas Klein