DAL SENSORE AL CLOUD: SFRUTTARE EDGE, FOG COMPUTING E MONITORAGGIO DEI DATI PER UNA DIGITALIZZAZIONE INDUSTRIALE SICURA ED ECONOMICAMENTE SOSTENIBILE

Filippo Genuario, Giuseppe Santoro, Michele Giliberti

* INVEST & ENGINEERING s.r.l., Viale Paolo Borsellino e Giovanni Falcone, 17, 70125 Bari BA
info@progettoacross.com

SOMMARIO

Nell'era della digitalizzazione, l'adozione delle tecnologie IoT (*Internet of Things*) e delle infrastrutture *cloud* è divenuta cruciale per le aziende. L'*Edge Computing*, una tecnologia emergente che si colloca tra i sensori e il *cloud*, offre soluzioni innovative per la gestione e l'elaborazione dei dati in prossimità della loro origine. Questo articolo esplora come l'*Edge Computing* e il monitoraggio dei dati possano migliorare i processi aziendali, riducendo la latenza, migliorando la sicurezza e ottimizzando le risorse. Viene qui messa in evidenza l'importanza di un approccio consapevole e sostenibile nei processi di digitalizzazione industriale, con un focus particolare sulle sfide legate alla sicurezza delle reti e alla protezione dei dati. Inoltre, vengono qui confrontate diverse tecniche di *machine learning* e *deep learning* per la sicurezza delle reti, evidenziando benefici e limitazioni di ciascuna di esse. Poi, vengono presentati gli impatti economici e i vantaggi attesi dall'implementazione della tecnologia IoT in ambito industriale, delineando un quadro completo delle sfide future.

1. INTRODUZIONE

Il termine "*Internet of Things*" (IoT) è stato coniato nel 1999 e si riferisce alla capacità degli oggetti quotidiani di connettersi a Internet, comunicare e interagire con altri dispositivi e utenti. L'IoT ha il potenziale di rivoluzionare vari settori industriali, migliorando l'efficienza operativa e riducendo i costi attraverso l'automazione e l'analisi dei dati raccolti dai sensori.

Il ***Cloud Computing*** (CC), definito come la fornitura di risorse scalabili e virtualizzate come servizi su Internet, ha già trasformato significativamente il settore IT [1], [2]. Tuttavia, l'invio di grandi volumi di dati non elaborati al cloud può risultare inefficiente a causa della latenza e dei costi di banda. L'***Edge Computing*** (EC) risponde a queste sfide elaborando i dati vicino alla fonte, riducendo così la latenza e migliorando l'efficienza complessiva del sistema. Il CC offre vari servizi, tra cui *Infrastructure-as-a-Service* (IaaS), *Platform-as-a-Service* (PaaS) e *Software-as-a-Service* (SaaS). Questi servizi consentono alle aziende di utilizzare risorse IT senza dover investire in costose infrastrutture fisiche. Il *cloud* facilita anche l'interconnessione di dispositivi IoT, che possono essere utilizzati per monitorare e controllare processi industriali in tempo reale [3]. L'architettura IoT comprende vari livelli, tra cui sensori e attuatori, connettività, capacità di elaborazione, archiviazione e analisi dei dati. Il ***Fog Computing*** (FC), un'estensione dell'EC, funge da ponte tra i dispositivi IoT e il *cloud*, elaborando i dati a livello locale prima di inviarli al *cloud*. Questo approccio riduce il carico di dati sul *cloud*, migliora la latenza e consente una risposta più rapida ai dati critici.

Il monitoraggio continuo dei dati è fondamentale per garantire l'affidabilità e la sicurezza delle operazioni industriali. I dati raccolti dai sensori possono essere utilizzati per ottimizzare i processi, prevedere guasti e ridurre i tempi di inattività. Inoltre, un monitoraggio efficace dei dati consente di prendere decisioni informate basate su analisi approfondite, migliorando così la produttività e l'efficienza operativa . Lo scopo di questo articolo è esplorare come l'Ee il monitoraggio dei dati possano migliorare i processi aziendali, riducendo la latenza, migliorando la sicurezza e ottimizzando le risorse. Si evidenzia inoltre l'importanza di un approccio consapevole e sostenibile nei processi di digitalizzazione industriale, affrontando le sfide legate alla sicurezza delle reti e alla protezione dei dati. Il documento propone un confronto di diverse tecniche di *machine learning* e *deep learning* per la sicurezza delle reti oltre a presentare gli impatti economici attesi dalla tecnologia IoT in ambito industriale.

2. METODOLOGIA PER L'ACQUISIZIONE E L'ELABORAZIONE DEI DATI MEDIANTE FC ED EC

La differenza fondamentale tra il FC e il CC è che il *cloud* è un sistema centralizzato, mentre il FC è un'architettura distribuita decentralizzata. Il FC funge da punto di connessione tra i dispositivi e i server remoti. Definisce quali informazioni saranno inviate al client e quali dovrebbero essere elaborate localmente. In questo senso, il FC agisce come un *gateway* intelligente, scaricando il carico sul *cloud* e consentendo una conservazione, elaborazione e analisi più efficiente dei dati [4]. I nodi wireless dominano la comunicazione nell'IoT. A causa delle restrizioni delle risorse nel livello di perce-

zione, molti protocolli wireless sono ottimizzati per utilizzare meno energia per il funzionamento, comunicazioni limitate o una gamma di copertura estesa. Attualmente, l'industria fornisce una molteplicità di metodi diversi. Lo strato *Fog* è idealmente posizionato per integrare questi numerosi protocolli wireless e semplificare la sua interazione con lo strato *cloud*. Ciò aiuta nella gestione delle sottoreti di sensori e attuatori, fornendo sicurezza, instradando le comunicazioni tra i dispositivi e migliorando l'affidabilità del sistema. Inoltre, identificando e comprendendo il formato di rappresentazione, questo strato fornisce l'interoperabilità di vari protocolli. Lo strato *Fog* consente di rendere visibili e accessibili tramite Internet dispositivi non basati su IP [5]. Il FC è un promettente paradigma che fornisce servizi di calcolo all'*edge* della rete, consentendo nuovi servizi e applicazioni per il futuro di Internet. Rispetto ad altri paradigmi, come i *cloudlet*, il *Mobile Cloud Computing* (MCC) e il *Mobile Edge Computing* (MEC), il FC ha una posizione di collocazione migliore in quanto è implementato più vicino ai nodi IoT. Inoltre, supporta l'estensione dei servizi basati su *cloud*, contribuendo così a fornire servizi efficienti, con una significativa minimizzazione della latenza. Tuttavia, l'esistenza del FC non sostituisce il servizio *cloud*, piuttosto, lo migliora. Considerando il concetto di EC e CC, molteplici paradigmi informatici sono già stati utilizzati nella tecnologia informatica.

Nel campo della tecnologia informatica sono stati creati diversi paradigmi informatici prendendo in considerazione i concetti di *edge* e *cloud computing*. *Mobile Edge Computing* (MEC) e *Mobile Cloud Computing* (MCC) sono esempi di sviluppi prospettici nell'ambito del cloud e dell'edge computing (si veda la Figura 1). MEC è ampiamente considerato un abilitatore critico per lo sviluppo attuale delle stazioni base cellulari. Allo stesso tempo, MCC offre le risorse di elaborazione necessarie per agevolare l'esecuzione remota di applicazioni mobili scaricate più vicino agli utenti finali. Il FC, come MEC e MCC, può anche abilitare il calcolo all'*edge*. Oltre alla rete *edge*, il FC può estendersi alla rete centrale. Per essere più specifici, i componenti di rete *edge* e *core* possono essere impiegati come infrastruttura di elaborazione nel FC. La figura 1, presenta un'immagine comparativa che fornisce una rapida panoramica delle differenze e delle funzioni dei paradigmi citati [6].

3. IMPLEMENTAZIONE DI UN SISTEMA DI ACQUISIZIONE IOT

L'implementazione di un sistema IoT efficace richiede una metodologia ben strutturata per l'acquisizione e l'elaborazione dei dati. Ogni fase del processo, dalla selezione dei sensori fino alla visualizzazione e utilizzo dei dati, gioca un ruolo fondamentale nel garantire l'affidabilità, la sicurezza e l'efficacia del sistema complessivo. Di seguito sono riportati i passaggi critici coinvolti in questa metodologia, evidenziando l'importanza di ogni fase e fornendo linee guida pratiche per ottimizzare il processo.

- **Selezione dei sensori**. La selezione dei sensori è un passo cruciale per garantire l'acquisizione di dati accurati e affidabili. È importante considerare le specifiche tecniche dei sensori, come la gamma di misura, la precisione, la frequenza di campionamento e la sensibilità. Inoltre, i sensori devono essere adatti all'ambiente operativo e supportare modalità di comunicazione compatibili con il sistema .
- ***Pre-processing* dei dati**. Il *pre-processing* dei dati comprende vari passaggi, tra cui la pulizia dei dati, la gestione dei valori mancanti, la trasformazione delle variabili e la normalizzazione delle caratteristiche. Questo processo è essenziale per garantire che i dati siano pronti per l'analisi e l'elaborazione successiva. L'obiettivo è ridurre il rumore e migliorare la qualità dei dati, facilitando così una migliore interpretazione e utilizzo .
- **Trasmissione dei dati al *cloud***. Una volta preprocessati, i dati possono essere trasmessi al *cloud* per l'archiviazione e l'analisi. È importante utilizzare protocolli di comunicazione ottimizzati per garantire una trasmissione sicura ed efficiente. Alcuni dei protocolli comuni includono MQTT, CoAP e HTTP, ciascuno con vantaggi specifici a seconda delle esigenze dell'applicazione [7].
- **Archiviazione e sicurezza dei dati**. L'archiviazione sicura dei dati è essenziale per proteggere le informazioni sensibili e garantire la conformità alle normative. Il *cloiud* offre soluzioni scalabili per l'archiviazione dei dati, ma è fondamentale implementare misure di

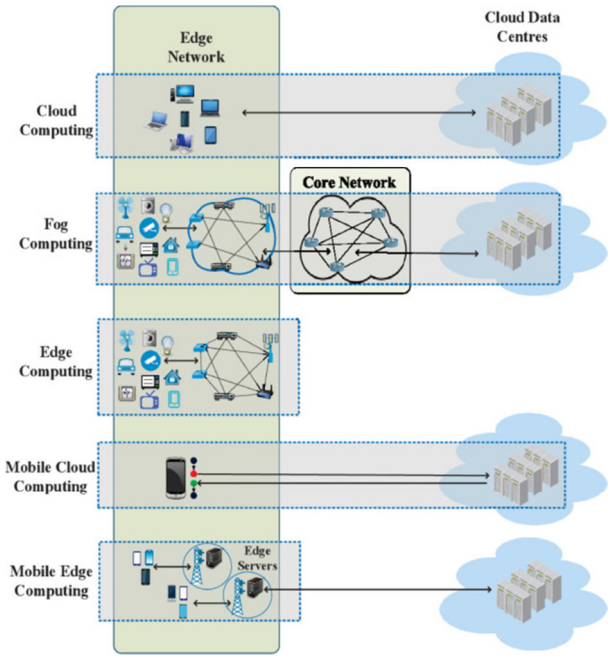

Figura 1. Il dominio del cloud, fog, edge, mobile cloud e del mobile edge computing [6]

sicurezza adeguate, come l'autenticazione e l'autorizzazione, la crittografia dei dati e la gestione delle chiavi.

4. VISUALIZZAZIONE E UTILIZZO DEI DATI

L'adozione di tecnologie emergenti come l'intelligenza artificiale, il *machine learning*, l'*Edge* AI, la visualizzazione avanzata dei dati, la *blockchain* e i *digital twin* sta trasformando il panorama della visualizzazione e dell'utilizzo dei dati IoT. Queste tecnologie offrono nuove opportunità per migliorare l'efficienza operativa, la sicurezza e la competitività delle aziende. È essenziale per le imprese rimanere aggiornate su queste innovazioni e considerare come possono essere integrate nelle loro strategie di digitalizzazione per massimizzare i benefici. Nel contesto dell'implementazione dell'IoT, sono disponibili strumenti e servizi che consentono di sfruttare al meglio i dati raccolti, migliorando l'accessibilità, la comprensione e l'utilizzo delle informazioni rilevanti. Questi componenti rivestono un ruolo fondamentale e contribuiscono a fornire decisioni immediate e informate agli utenti. In questo contesto, l'approccio include la creazione di *dashboard* personalizzate, l'uso di API RESTful e la configurazione di sistemi di notifica in tempo reale. Per quanto riguarda le *dashboard* personalizzate, strumenti come *Grafana* e *Kibana* si distinguono. *Grafana*, una piattaforma open-source, permette di creare *dashboard* interattive con la visualizzazione in tempo reale di dati provenienti dai sensori IoT, offrendo vari formati tra cui grafici a barre, grafici a dispersione e pannelli personalizzati. È altamente personalizzabile e consente di aggiungere avvisi e notifiche. *Kibana*, parte di *Elasticsearch*, è spesso utilizzato per l'analisi dei dati di log, ma può anche essere esteso per la visualizzazione di dati IoT. Per quanto riguarda i servizi di visualizzazione *cloud*, Amazon QuickSight di AWS e Microsoft Power BI offrono la creazione di *dashboard* interattive e report basati sui dati IoT archiviati in servizi *cloud* come Amazon S3, Amazon Redshift o Amazon RDS. Questi strumenti si integrano perfettamente con i servizi *cloud* dei rispettivi provider, offrendo funzionalità avanzate per la visualizzazione dei dati. L'esposizione dei dati tramite API RESTful è un passo cruciale. Fornendo un'API RESTful, si permette l'accesso programmatico ai dati IoT archiviati nel *cloud*, consentendo agli sviluppatori di creare applicazioni personalizzate che utilizzano e visualizzano i dati in modo dinamico. L'implementazione della sicurezza API è altrettanto importante, con l'autenticazione e l'autorizzazione che proteggono l'accesso ai dati tramite l'API. Questo può essere realizzato mediante servizi di gestione delle identità come AWS Cognito o Azure Active Directory. Per personalizzare ulteriormente le *dashboard*, strumenti come Grafana consentono l'uso di *script* e *query* personalizzate per manipolare i dati prima della visualizzazione, come il calcolo di medie mobili o l'aggregazione di dati in modi specifici. È anche possibile creare pannelli personalizzati per visualizzare dati in modi unici, integrando mappe, grafici geografici, grafici a bolle o persino visualizzazioni 3D per rappresentare dati complessi in modo intuitivo. Un aspetto essenziale è garantire l'accesso sicuro alle API. Ciò può essere raggiunto tramite protocolli di autenticazione sicura come OAuth e la gestione dei *token*. Servizi come AWS Cognito o Auth0 semplificano la gestione delle credenziali e dei token, assicurando un ambiente sicuro. Passando alla gestione delle notifiche e degli allarmi, Amazon SNS e Firebase Cloud Messaging emergono come opzioni rilevanti. Questi sistemi di notifica in tempo reale consentono di inviare avvisi a utenti, applicazioni o dispositivi in risposta a eventi critici rilevati dai dati IoT. La configurazione degli allarmi è fondamentale per monitorare i dati in tempo reale. Impostare regole basate su soglie o *pattern* di dati consente di ricevere avvisi quando i dati superano determinati limiti critici. L'integrazione con servizi di notifica garantisce che utenti o personale responsabile siano tempestivamente informati in caso di problemi. Un altro aspetto chiave è il registro degli eventi, che tiene traccia di tutti gli eventi rilevanti nei dati IoT, compresi dati di sensori, notifiche e allarmi. Questo registro è utile per scopi di audit e analisi post evento. Per monitorare le prestazioni, è possibile implementare il monitoraggio delle prestazioni del sistema con strumenti come Prometheus per il monitoraggio avanzato. Analizzando la frequenza delle notifiche e gli eventi critici, è possibile migliorare l'efficacia del sistema di notifiche, anche attraverso l'apprendimento automatico per identificare modelli e tendenze. Infine, l'integrazione con sistemi di *ticketing* come JIRA o ServiceNow facilita la gestione delle operazioni IT, tracciando azioni correttive e monitorando le prestazioni nel tempo. L'invio di notifiche su più canali, come e-mail, SMS o chat aziendale, garantisce che gli utenti ricevano avvisi in diversi contesti, migliorando la reattività complessiva. Un ulteriore passo avanti nella visualizzazione e utilizzo dei dati è rappresentato dall'adozione di tecnologie emergenti come l'IA e il ML, che stanno rivoluzionando il modo in cui i dati IoT vengono analizzati e utilizzati. Queste tecnologie consentono di trasformare grandi volumi di dati non strutturati in informazioni utili e *actionable insights*. Ad esempio, gli algoritmi di ML possono essere utilizzati per rilevare anomalie nei dati in tempo reale, prevedere guasti ai macchinari e ottimizzare i processi produttivi. L'implementazione di modelli di ML nei sistemi IoT permette di automatizzare l'analisi dei dati, riducendo il tempo necessario per prendere decisioni critiche. Tecnologie come le reti neurali profonde (*deep learning*) possono essere utilizzate per riconoscere *pattern* complessi nei dati, fornendo previsioni accurate che possono aiutare a migliorare l'efficienza operativa e ridurre i

costi. L'*Edge AI*, una forma di intelligenza artificiale che viene eseguita direttamente sui dispositivi *edge* piuttosto che nel *cloud*, consente di elaborare i dati localmente, riducendo la latenza e migliorando la reattività del sistema. Questo approccio è particolarmente utile in applicazioni che richiedono una risposta in tempo reale, come la manutenzione predittiva, il controllo di qualità e la sicurezza industriale. L'integrazione dell'AI nell'EC consente di eseguire analisi sofisticate e prendere decisioni rapide senza la necessità di inviare grandi volumi di dati al cloud, migliorando l'efficienza operativa e riducendo i costi di banda, aumentando la sicurezza dei dati. Le tecnologie di visualizzazione avanzata stanno migliorando la capacità delle aziende di interpretare i dati IoT. Strumenti come la realtà aumentata (AR) e la realtà virtuale (VR) stanno emergendo come potenti mezzi per visualizzare dati complessi in modo intuitivo. Ad esempio, i tecnici possono utilizzare dispositivi AR per visualizzare dati di sensori sovrapposti agli oggetti fisici, facilitando la diagnosi dei problemi e la manutenzione. Inoltre, le piattaforme di visualizzazione dei dati stanno diventando sempre più sofisticate, offrendo funzionalità come la visualizzazione 3D e le *dashboard* interattive, permettendo di esplorare i dati da diverse prospettive, identificando facilmente tendenze e anomalie. É da evidenziare, inoltre, il concetto di "*digital twin*" che sta guadagnando popolarità come strumento per migliorare l'efficienza operativa e la gestione delle risorse. Un *digital twin* è una replica digitale di un *asset* fisico, come una macchina o un impianto, che simula il comportamento e le condizioni operative reali. Utilizzando i dati raccolti dai sensori IoT, il *digital twin* può fornire una visione dettagliata e in tempo reale delle operazioni, permettendo di ottimizzare i processi e prevedere problemi prima che si verifichino. L'integrazione dei *digital twin* con le tecnologie di AI e ML consente di simulare scenari complessi e testare strategie operative senza rischi, migliorando la capacità decisionale e riducendo i tempi di inattività.

5. MONITORAGGIO, MANUTENZIONE, AGGIORNAMENTI E OTTIMIZZAZIONI

La gestione efficace di un sistema IoT richiede un monitoraggio costante, registrazione dettagliata e manutenzione proattiva. Questi aspetti sono essenziali per garantire la stabilità e l'efficacia del sistema IoT nel tempo. Amazon CloudWatch è uno strumento fondamentale che rientra nel servizio di monitoraggio e osservabilità di AWS. Permette di raccogliere metriche, individuare anomalie e impostare allarmi per il tuo sistema IoT, monitorando parametri come la latenza dei dati e l'utilizzo delle risorse. Inoltre, Prometheus, un sistema *open source*, è utile per il monitoraggio delle applicazioni e dei servizi. Un possibile impiego è quello di raccogliere e memorizzare metriche dai dispositivi IoT e visualizzarle tramite *Grafana*, un'applicazione *open source* per la creazione di *dashboard* personalizzate. Configurare gli allarmi è essenziale. Ad esempio, si può impostare un allarme per ricevere notifiche in tempo reale quando la temperatura supera una soglia critica. Per garantire che le notifiche raggiungano le persone o i team responsabili in modo tempestivo, possono essere impiegati sfruttare servizi come Amazon SNS. Nei sistemi IoT è importante anche la registrazione dettagliata per catturare eventi importanti e errori nel sistema. È possibile configurare registrazioni dettagliate per registrare dati di sensori, attività degli utenti e informazioni sullo stato del sistema. Questi log possono essere archiviati in modo sicuro e resiliente utilizzando servizi di archiviazione come Amazon S3 o Azure Blob Storage e analizzare i lof con strumenti del tipo *Elasticsearch*, *Logstash*, *Kibana* o servizi di analisi dei *log cloud*. Per quanto riguarda la manutenzione proattiva, essa comprende aggiornamenti regolari del *firmware*, *rollback* pianificati in caso di problemi, pianificazione della sostituzione di sensori difettosi o batterie scariche, ottimizzazione delle risorse *cloud* e configurazione di *auto-scaling* per adattare automaticamente le risorse alle esigenze. La calibrazione periodica dei sensori è importante per garantire la precisione delle misurazioni. Inoltre, il monitoraggio della rete è cruciale per rilevare problemi di connettività e prestazioni. L'analisi delle prestazioni dei dispositivi IoT è necessaria per identificare segni precoci di malfunzionamenti o deterioramento così come lo sono la pianificazione del ripristino di emergenza e la documentazione accurata delle attività di manutenzione sono pratiche fondamentali.

Ottimizzare i costi e gestire gli aggiornamenti in modo efficiente sono altrettanto cruciali per garantire la sostenibilità del sistema IoT. Ciò include la gestione delle versioni del software e del *firmware*, il *testing* degli aggiornamenti, la pianificazione dei *rollback*, l'automazione degli aggiornamenti, la strategia *canary deployment*, la definizione della frequenza degli aggiornamenti e il monitoraggio dei costi operativi. Inoltre, è importante considerare l'implementazione di servizi *serverless*, l'ottimizzazione del traffico IoT e la programmazione dei picchi di utilizzo per ridurre i costi operativi complessivi. Questa versione dettagliata del protocollo di sviluppo dovrebbe fornire una guida completa per l'implementazione di un sistema di acquisizione, *pre-processing* e invio dei dati di campo dal FC al *cloud*, con una particolare attenzione ai dettagli operativi e tecnici. Adattate ogni fase in base alle esigenze specifiche e alle complessità del progetto assicura lo sviluppo di sistemi *sensor-to-cloud* semplici ed efficienti.

6. SICUREZZA E CONFORMITÀ NELLE INFRASTRUTTURE IOT

Nel campo dell'informatica, l'implementazione della sicurezza riveste un ruolo di fondamentale importanza. Esistono diverse misure e strategie mirate a garantire la protezione dei dati e la conformità alle normative vigenti. La sicurezza informatica è particolarmente critica nei sistemi IoT, dove la protezione dei dati e delle reti è essenziale [8].

La crittografia è centrale per la sicurezza dei dati nell'IoT. Per garantire che i dati non possano essere intercettati o alterati durante la trasmissione tra il dispositivo di FC e il *cloud*, viene utilizzato il Protocollo Transport Layer Security (TLS). È essenziale configurare correttamente i certificati SSL/TLS per i dispositivi FC e i *server cloud*. Servizi come Let's Encrypt rendono più accessibili certificati SSL/TLS gratuiti e automatizzati. Per la crittografia dei dati archiviati nel *cloud*, la maggior parte dei servizi cloud offre opzioni per la crittografia dei dati utilizzando chiavi gestite dal servizio stesso. È cruciale implementare una gestione delle chiavi robusta, utilizzando servizi dedicati come AWS Key Management Service (KMS) o Azure Key Vault, per proteggere le chiavi di crittografia. La rotazione regolare dei certificati SSL/TLS contribuisce a limitare i danni in caso di compromissione di un certificato. Nei dispositivi IoT, i certificati autofirmati possono essere utilizzati per la crittografia *end-to-end*, ma è importante gestirli attentamente e distribuirli in modo sicuro. La gestione delle chiavi comprende l'implementazione di un sistema di controllo degli accessi basato su ruoli (RBAC). Questo sistema definisce chi ha accesso ai dati e alle risorse, assegnando i permessi minimi necessari a ciascun utente o servizio. La rotazione periodica delle chiavi di crittografia è fondamentale per ridurre il rischio associato alla compromissione delle chiavi a lungo termine. Consentire agli utenti autorizzati di gestire le proprie chiavi di crittografia in modo sicuro, inclusa la rotazione o la revoca quando necessario, è una pratica di sicurezza essenziale. L'uso di *hardware security modules* (HSM) per conservare e gestire le chiavi di crittografia in un ambiente altamente sicuro e resistente agli attacchi è altamente raccomandato. L'automazione della rotazione delle chiavi di crittografia riduce notevolmente il rischio e il coinvolgimento umano nell'operazione. Implementare un sistema di monitoraggio delle attività delle chiavi aiuta a rilevare l'uso delle chiavi e comportamenti anomali.

La conformità alle normative è un ulteriore aspetto cruciale per le aziende dell'ambito IoT. Ad esempio, nell'Unione Europea, il Regolamento Generale sulla Protezione dei Dati (GDPR) richiede che le aziende limitino la raccolta e l'elaborazione dei dati personali solo quando necessario e ottengano il consenso degli utenti. La conformità al GDPR implica anche garantire il diritto degli utenti di accedere ai propri dati, correggerli e richiederne la cancellazione. Per garantire la conformità al Regolamento Generale sulla Protezione dei Dati (GDPR), le aziende devono adottare diverse misure di sicurezza. Una di queste è l'implementazione della crittografia *end-to-end*, che protegge i dati personali sia durante la trasmissione che durante l'archiviazione, impedendo così l'accesso non autorizzato. Un'altra misura importante è l'uso di tecniche di pseudonimizzazione, che riducono i rischi associati ai dati personali, rendendo le informazioni meno identificabili senza dati aggiuntivi. Inoltre, le aziende devono ottenere il consenso esplicito degli utenti prima di raccogliere e trattare i loro dati personali, assicurandosi che gli utenti siano pienamente consapevoli di come i loro dati verranno utilizzati. Infine, è fondamentale garantire agli utenti il diritto all'oblio, permettendo loro di richiedere la cancellazione dei propri dati quando non sono più necessari per le finalità per le quali erano stati raccolti. Queste misure non solo aiutano a rispettare il GDPR, ma aumentano anche la fiducia degli utenti nella gestione dei loro dati personali.

L'*auditing* delle attività, infine, è cruciale per tenere traccia di chi accede ai dati, quando e cosa fa con essi. Pianificare audit regolari della sicurezza e delle politiche è necessario per garantire che le misure di sicurezza siano adeguate e che la conformità normativa sia mantenuta. La documentazione delle politiche di sicurezza, incluse le procedure di accesso e le misure di sicurezza implementate, è essenziale affinché tutto il personale coinvolto sia a conoscenza di tali politiche. La conservazione dei dati deve essere regolamentata da politiche chiare che rispettino i requisiti normativi. Il principio di "*Privacy by Design*" implica l'integrazione di misure di sicurezza e protezione dei dati fin dall'inizio dello sviluppo del sistema IoT così come i test di penetrazione regolari aiutano a identificare e risolvere le vulnerabilità di sicurezza.

Per quanto riguarda un'attività molto importante da consdiderare nell'ambito della sicurezza informatica dei dati è la pianificazione della risposta agli incidenti. Tale fase è essenziale e permette di definire chi è responsabile e di cosa durante una violazione della sicurezza. Mantenere aggiornati i componenti del sistema IoT con le ultime *patch* di sicurezza è fondamentale, e l'isolamento delle reti IoT dalle reti aziendali principali riduce il rischio di accesso non autorizzato. Infine, il test di sicurezza continuo e le valutazioni dell'impatto sulla *privacy* (PIA) garantiscono la costante sicurezza e conformità del sistema IoT. L'integrazione di tecniche di ML e DL nei sistemi di rilevamento delle intrusioni rappresenta un avanzamento significativo nella sicurezza delle reti IoT,

offrendo la possibilità di rilevare attacchi sconosciuti e adattarsi a nuovi tipi di minacce in tempo reale. Queste tecniche possono migliorare significativamente la capacità di monitorare, rilevare e rispondere a incidenti di sicurezza, contribuendo a garantire un ambiente sicuro e conforme per le infrastrutture IoT . Recentemente, anche grazie al progetto ACROSS [1] sviluppato dalla Invest & Engineering srl, sono state condotte ricerche approfondite sull'applicazione di tecniche di apprendimento automatico supervisionato per automatizzare il processo di rilevamento delle intrusioni nelle connessioni di rete. Questi approcci utilizzano meccanismi supervisionati, semi-supervisionati e non supervisionati per apprendere i *pattern* di varie attività normali e dannose in ampi corpus di eventi normali e di attacco a livello di rete e a livello di *host*. Le tecniche tradizionali di apprendimento automatico, come Decision Tree (DT), Random Forest (RF) e Support Vector Machine (SVM), sono state ampiamente utilizzate nel rilevamento delle intrusioni. Con lo sviluppo dell'apprendimento profondo, reti neurali convoluzionali (CNN), reti neurali ricorrenti (RNN) e *long short-term memory* (LSTM) stanno diventando popolari nel rilevamento delle intrusioni. Recenti studi hanno proposto modelli basati su DL per il rilevamento delle intrusioni, utilizzando una combinazione di CNN e LSTM per ottenere una rappresentazione accurata delle *feature* dei dati di traffico di rete IoT e classificarli ulteriormente. Questo approccio ibrido ha mostrato performance promettenti, con un'accuratezza elevata nel rilevamento delle intrusioni e nella classificazione degli attacchi . Inoltre, un altro approccio innovativo ha utilizzato *autoencoder* per apprendere una rappresentazione multicanale dei flussi di rete, combinando un approccio non supervisionato per la costruzione di *feature* multicanale con un approccio supervisionato che sfrutta le correlazioni di *feature cross-channel*. Questa metodologia ha dimostrato di essere efficace nel rilevamento delle intrusioni, migliorando la precisione e riducendo i falsi positivi .

La tabella 1 presenta un confronto tra diverse tecniche di ML e di DL utilizzate per il rilevamento delle intrusioni nelle reti, basato sui dati riportati nello studio del progetto ACROSS.

Questo confronto mette in evidenza sia i vantaggi sia gli svantaggi di ciascuna tecnica, permettendo di comprendere meglio le loro potenzialità e le loro limitazioni. La Random Forest emerge come una tecnica altamente accurata, raggiungendo un'accuratezza del 99.67% sul dataset KDD-99 Cup.

[1] Progetto cofinanziato con il Fondo Europeo di Sviluppo Regionale Puglia POR Puglia 2014 – 2020 – Progetto ACROSS - Codice: THA48Y5

Tabella 1. Confronto delle tecniche di *machine learning* e *deep learning* nei sistemi di rilevamento delle intrusioni.

Tecnica di ML/DL	Dataset	Accuratezza
Random Forest	KDD-99 Cup	99.67%
Naive Bayes	NSL-KDD	86.50%
Support Vector Machine (SVM)	UNSW-NB15	94.70%
Decision Tree (DT)	NSL-KDD	93%
K-Nearest Neighbors (KNN)	NSL-KDD	85.30%
Multi-Layer Perceptron (MLP)	NSL-KDD	84.76%
AdaBoost	NSL-KDD	99.30%
Convolutional Neural Network (CNN)	IoT-23	99.65%
Long Short-Term Memory (LSTM)	UNSW-NB15	82.78%
Recurrent Neural Network (RNN)	NSL-KDD	82.78%

Questo metodo è apprezzato per la sua facilità di interpretazione e la sua efficacia nel gestire *dataset* complessi, grazie alla combinazione di molteplici alberi decisionali. Tuttavia, il suo principale svantaggio risiede nel notevole tempo di calcolo richiesto per costruire e combinare gli alberi, specialmente con grandi *dataset*. Il Naive Bayes, applicato al *dataset* NSL-KDD, presenta un'accuratezza del 86.5%. È una tecnica semplice da implementare e particolarmente efficace con *dataset* piccoli o meno complessi. Tuttavia, questa semplicità si traduce in una scarsa accuratezza quando si affrontano dataset più complessi. La Support Vector Machine (SVM), utilizzata sul dataset UNSW-NB15, raggiunge un'accuratezza del 94.7%.

Questo metodo è noto per la sua buona accuratezza con dataset complessi, specialmente se vengono utilizzati *kernel* appropriati. Il principale svantaggio dell'SVM è la necessità di *tuning* dei parametri per ottenere le migliori prestazioni, un processo che può essere computazionalmente intensivo. Il Decision Tree (DT) mostra un'accuratezza del 93% sul dataset NSL-KDD. Questa tecnica è facile da interpretare e offre buone prestazioni su *dataset* piccoli. Tuttavia, tende a sovradattarsi facilmente, a meno che non vengano applicate tecniche di *pruning* per controllare l'*overfitting*. Il K-Nearest Neighbors (KNN), anch'esso applicato al *dataset* NSL-KDD, ha un'accuratezza del 85.3%. Questa tecnica è semplice da implementare ed efficace con *dataset* piccoli, ma le sue prestazioni scarseggiano con *dataset* complessi o con un grande numero di *feature*. Il Multi-Layer Perceptron (MLP) mostra un'accuratezza del 84.76% sul *dataset* NSL-KDD. È capace di apprendere *pattern* complessi grazie

alla sua struttura a strati multipli, ma richiede molte risorse computazionali per l'addestramento, specialmente con grandi *dataset*. L'AdaBoost, con un'accuratezza del 99.3% sul *dataset* NSL-KDD, migliora l'accuratezza combinando più modelli deboli per creare un classificatore forte. Tuttavia, come il Random Forest, richiede un notevole tempo di calcolo a causa dell'addestramento sequenziale dei modelli. Tra le tecniche di DL, la Convolutional Neural Network (CNN) applicata al *dataset* IoT-23 raggiunge un'accuratezza del 99.65%. Questo metodo è eccellente per l'elaborazione di dati spaziali, come immagini e dati sequenziali, ma richiede molte risorse computazionali per l'addestramento e l'inferenza. La Long Short-Term Memory (LSTM), utilizzata sul *dataset* UNSW-NB15, mostra un'accuratezza del 82.78%. Questa tecnica è particolarmente utile per l'elaborazione di dati sequenziali e temporali, ma anch'essa richiede molte risorse computazionali per l'addestramento. Infine, la Recurrent Neural Network (RNN), con un'accuratezza del 82.78% sul *dataset* NSL-KDD, è capace di apprendere *pattern* temporali, ma soffre di problemi di *vanishing gradient* e richiede molte risorse computazionali.

7. RITORNO ECONOMICO DEL MERCATO DELL'IOT

L'IoT - ossia sensori e attuatori collegati da reti a sistemi informatici - ha ricevuto un'enorme attenzione negli ultimi cinque anni. Un rapporto del McKinsey Global Institute [9] cerca di determinare esattamente come la tecnologia IoT possa creare un reale valore economico. Per avere una visione più ampia dei potenziali benefici e delle sfide dell'IoT nell'economia globale, sono stati analizzati oltre 150 casi d'uso, dalle persone i cui dispositivi monitorano salute e benessere ai produttori che utilizzano sensori per ottimizzare la manutenzione delle apparecchiature e proteggere la sicurezza di lavoratori. L'analisi di tipo *bottom-up* fatta dal McKinsey Global Institute per le applicazioni ha stimato che l'IoT abbia un impatto economico potenziale totale da 3,9 trilioni di $ a 11,1 trilioni di $ l'anno entro il 2025 (si veda la Figura 2). Alla fine, quel livello di valore, incluso il surplus del consumatore, sarebbe equivalente a circa l'11 percento dell'economia mondiale.

Raggiungere questo tipo di impatto richiederebbe l'esistenza di determinate condizioni, in particolare il superamento di ostacoli tecnici, organizzativi e normativi. In particolare, le aziende che utilizzano la tecnologia IoT dovranno svolgere un ruolo fondamentale nello sviluppo dei sistemi e dei processi idonei per massimizzarne il valore. Tra i risultati dello studio si evidenzia che:

- l'interoperabilità tra i sistemi IoT è fondamentale. Del potenziale valore economico che l'IoT consentirebbe di ottenere, l'interoperabilità è richiesta dal 40% al 60% in media per determinati scenari;
- attualmente, la maggior parte dei dati dell'IoT non è utilizzata. Ad esempio, su una piattaforma petrolifera con 30.000 sensori, è esaminato solo l'1% dei dati. Questo perché queste le informazioni sono utilizzate principalmente per rilevare e controllare le anomalie e non per l'ottimizzazione e la previsione, i J:₩FILMATIquali fornirebbero il massimo valore;
- le applicazioni *business-to-business* probabilmente acquisteranno più valore, quasi il 70%, rispetto agli usi *consumer*, sebbene le applicazioni *consumer*, come i *monitor fitness* e le auto a guida autonoma, attirino la maggiore attenzione e possano anche creare un valore significativo;
- l'IoT ha un grande potenziale nelle economie in via di sviluppo; tuttavia, si stima che avrà un maggiore impatto sul valore complessivo nelle economie avanzate a causa del più alto valore applicativo. Le economie in via di sviluppo potrebbero generare quasi il 40% del valore dell'IoT e quasi la metà in alcuni scenari;
- i clienti otterranno la maggior parte dei benefici. Si stima che gli utenti di IoT (aziende, altre organizzazioni e consumatori) possano acquisire il 90% del valore generato dalle applicazioni IoT. Ad esempio, nel 2025 il monitoraggio remoto potrebbe creare fino a 1,1 trilioni di dollari l'anno in termini di valore, migliorando la salute dei pazienti affetti da

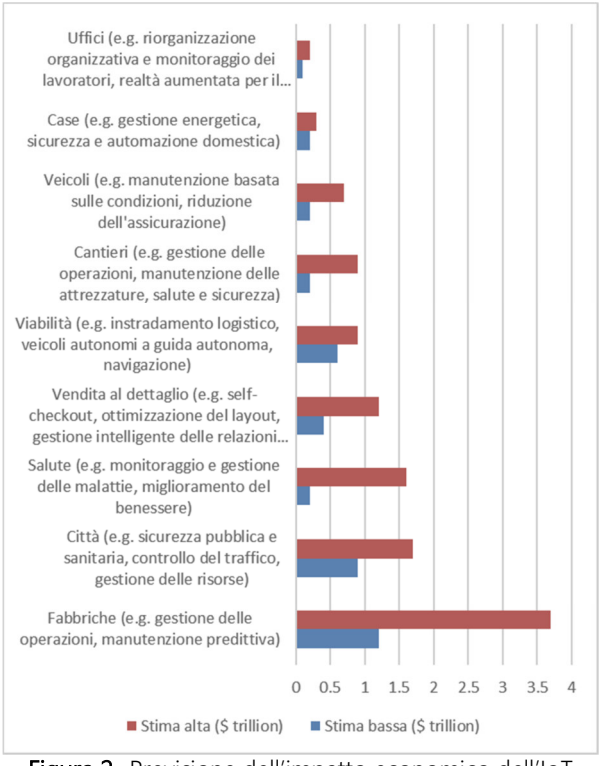

Figura 2. Previsione dell'impatto economico dell'IoT

malattie croniche;
- un'industria dinamica si sta evolvendo attorno alla tecnologia IoT. Come in altre ondate tecnologiche, sia gli incubatori che i nuovi *player* hanno opportunità. La digitalizzazione offusca le linee tra le società tecnologiche e altri tipi di imprese; i produttori di macchinari industriali, ad esempio, stanno creando nuovi modelli di business utilizzando i collegamenti e i dati IoT per offrire i propri prodotti come servizio.

8. CONCLUSIONI

L'EC e il monitoraggio dei dati sono elementi cruciali per migliorare i processi aziendali nell'era della digitalizzazione. La capacità di elaborare i dati vicino alla fonte riduce la latenza, migliora la sicurezza e ottimizza l'uso delle risorse. Adottare un approccio consapevole e sostenibile nella gestione dei dati e nell'implementazione delle tecnologie IoT può portare a significativi miglioramenti in termini di efficienza operativa e competitività. L'integrazione di tecnologie avanzate come il FC e il ML può ulteriormente potenziare le capacità delle aziende di analizzare e utilizzare i dati in modo efficace. In definitiva, un approccio consapevole e strategico alla digitalizzazione industriale è fondamentale per sfruttare appieno i benefici delle tecnologie IoT e *cloud*, migliorando la sostenibilità e l'efficienza dei processi aziendali. Tra i vantaggi dell'EC e del FC si possono annoverare:

- la riduzione della latenza, in quanto, elaborando i dati vicino alla fonte, si riduce significativamente la latenza rispetto all'invio dei dati al *cloud* per l'elaborazione. Questo è particolarmente importante per le applicazioni che richiedono risposte in tempo reale, come il controllo dei processi industriali e la gestione della sicurezza;
- il miglioramento della sicurezza grazie alla riduzione della necessità di trasmettere grandi volumi di dati su reti pubbliche. Inoltre, l'elaborazione locale consente di implementare misure di sicurezza specifiche per il contesto operativo, proteggendo meglio i dati sensibili;
- l'ottimizzazione delle risorse. Elaborando i dati localmente, le aziende possono ridurre il carico sui *server cloud* e ottimizzare l'uso delle risorse di rete. Questo non solo riduce i costi di banda, ma anche i tempi di risposta e il consumo energetico, contribuendo a un'operazione più sostenibile e efficiente;
- una soluzione scalabile e flessibile che può essere adattata alle esigenze specifiche delle diverse applicazioni industriali. L'implementazione di nodi *edge* consente una facile espansione e integrazione di nuovi dispositivi e sensori, supportando la crescita e l'evoluzione delle infrastrutture IoT .

BIBLIOGRAFIA

[1] B. Furht and A. Escalante, Eds., *Handbook of Cloud Computing*. Boston, MA: Springer US, 2010.

[2] B. Furht, "*Cloud Computing Fundamentals*," in Handbook of Cloud Computing, B. Furht and A. Escalante, Eds. Boston, MA: Springer US, 2010, pp. 3–19.

[3] S. Yangui, "*A Panorama of Cloud Platforms for IoT Applications Across Industries*," Sensors, vol. 20, no. 9, p. 2701, May 2020.

[4] F. Pisani, V. Martins Do Rosario, and E. Borin, "Fo*g vs. Cloud Computing: Should I Stay or Should I Go?*," Future Internet, vol. 11, no. 2, p. 34, Feb. 2019.

[5] A. M. Rahmani et al., *Smart e-Health Gate-way: Bringing Intelligence to Internet-of-Things Based Ubiquitous Healthcare Systems*. 2015.

[6] R. Mahmud, R. Kotagiri, and R. Buyya, "*Fog Computing: A Taxonomy, Survey and Future Directions*" in Internet of Everything, B. Di Martino, K.-C. Li, L. T. Yang, and A. Esposito, Eds. Singapore: Springer Singapore, 2018, pp. 103–130.

[7] D. Silva, L. I. Carvalho, J. Soares, and R. C. Sofia, "*A Performance Analysis of Internet of Things Networking Protocols: Evaluating MQTT, CoAP, OPC UA*" Appl. Sci., vol. 11, no. 11, p. 4879, May 2021.

[8] S. Srinivasa, J. M. Pedersen, and E. Vasilomanolakis, "*Open for hire: attack trends and misconfiguration pitfalls of IoT devices*" in Proceedings of the 21st ACM Internet Measurement Conference, Virtual Event, 2021, pp. 195–215.

[9] "mckinsey," *mckinsey*. [Online]. Available: https://www.mckinsey.com/.