Università degli Studi di Padova

Dipartimento di Diritto pubblico, internazionale e comunitario

Dipartimento di Ingegneria dell'Informazione

Corso di Laurea in Diritto e Tecnologia

Sicurezza e safety in ambienti industriali basati su IoT

Relatrice:
Dott.ssa Sara Baldoni

Candidato:
Francesco Tommasin
Matricola: 2045901

Anno Accademico 2023-2024

Sommario

Questo elaborato tratta le problematiche e le opportunità in ambito di sicurezza e safety derivate dall'applicazione di sistemi basati su Internet of Things (IoT) in contesti industriali. In questi scenari, la sicurezza sia informatica sia fisica deve essere presa in considerazione in quanto un funzionamento diverso da quello previsto, seppur lieve, può essere causa di danni economici e d'immagine per le aziende ma soprattutto può essere dannoso per la salute delle persone coinvolte. L'obiettivo di questo studio è dunque di comprendere il funzionamento dell'Industrial Internet of Things e di analizzare i metodi più adatti e funzionali per la sua implementazione con estremo riguardo per la sicurezza e la safety. In ambito di sicurezza, verranno trattate le misure preventive da mettere in atto contro eventuali attacchi informatici e per la salvaguardia dei dati e dei processi, analizzando gli approcci attualmente esistenti in letteratura. Per quanto riguarda la safety, verranno valutati i possibili rischi e come essi possono essere previsti e gestiti grazie all'impiego di sistemi di IoT in modo da garantire la continuità operativa e la salvaguardia dei sistemi e dei lavoratori.

Indice

Sommario **III**

Elenco delle figure **VII**

Elenco delle tabelle **VIII**

1 Introduzione **1**

2 Internet of Things **3**

2.1 La nascita e diffusione dell'IoT 3

2.2 I componenti dell'IoT 4

2.2.1 Sensori 4

2.2.2 Acquisizione dati 5

2.2.3 Attuatori 5

2.2.4 Unità di elaborazione 6

2.3 Modelli di comunicazione 6

2.3.1 Device-to-Device 6

2.3.2 Device-to-Cloud 7

2.3.3 Device-to-Gateway 7

2.3.4 Back-End Data Sharing 8

2.4 Ambiti applicativi 9

2.4.1 Domotica 9

2.4.2 Smart City 10

2.4.3 Smart Healthcare 11

3 Industrial IoT **13**

3.1 Cos'è l'IIoT 13

3.2 Architettura dell'Industrial IoT 14

3.3 Analisi di ambienti applicativi 18
3.3.1 Industria manifatturiera 18
3.3.2 Industria energetica 19
3.3.3 Industria chimica 20

4 Sicurezza **23**
4.1 Principi fondamentali 23
4.1.1 Riservatezza 23
4.1.2 Integrità 25
4.1.3 Disponibilità 27
4.2 Problemi di sicurezza nell'IIoT 27
4.2.1 DDoS e framework di mitigazione 28
4.2.2 Phishing 32
4.2.3 Attacco alla supply chain 34

5 Safety **37**
5.1 Standard di safety 37
5.1.1 ISO 31000 - Risk management 38
5.1.2 IEC 61508 41
5.2 Studio di *framework* e sistemi di *safety* industriali 42
5.2.1 *Public Safety Framework* per IIoT 42
5.2.2 *Safety* nell'industria mineraria 44
5.2.3 Sistema di risposta alla emergenze nelle aree di produzione . . . 45

6 Conclusioni **49**

Acronimi **51**

Bibliografia **54**

Elenco delle figure

2.1 Modello Device-to-Device 7
2.2 Modello Device-to-Cloud 7
2.3 Modello Device-to-Gateway 8
2.4 Modello Back-End Data Sharing 9

3.1 Architettura dell'Industrial IoT [39] 15

4.1 Architettura del MLDMF [45] 29
4.2 Test di efficacia del MLDMF [45] 31

5.1 Framework di gestione del rischio [10] 39
5.2 Processo di gestione del rischio [10] 40
5.3 Public Safety Framework [30] 43
5.4 Rilevamento dati tramite G-Link-200 [26] 46
5.5 Processo di analisi dati con CNN [26] 47
5.6 Accuratezza del modello CNN [26] 47

Elenco delle tabelle

4.1 Comparazione algoritmi 24

5.1 Probabilità di fallimento della funzione in un sistema a bassa domanda . 41

5.2 Probabilità di fallimento della funzione in un sistema ad alta domanda o continuo 42

5.3 Condizioni di allerta. 45

Capitolo 1

Introduzione

L'evoluzione tecnologica degli ultimi decenni ha fornito innumerevoli possibilità in diversi ambiti, sia della vita quotidiana che del lavoro. Tuttavia, quando i vantaggi sono così innovativi e desiderabili, è facile distogliere l'attenzione dai pericoli e gli aspetti più pratici e a primo impatto trascurabili dei nuovi strumenti.

L'*Internet of Things* è una rete interconnessa di dispositivi che svolgono diverse funzioni, dall'acquisizione di dati, alla rilevazione di cambiamenti nell'ambiente o modifiche attive a quest'ultimo. L'utilizzo di questi strumenti si è diffuso ormai anche nell'industria con l'*Industrial Internet of Things*.

I casi di incidente dovuti ad errori umani sono nella maggior parte delle istanze causati da una valutazione del rischio non adatta, ma essa non è sempre conseguenza di una mancanza di attenzione o di una attribuzione dell'importanza minore di quanto richiesto, bensì di un'insufficiente formazione riguardo ad argomenti che necessitano di un continuo studio per via della loro natura in costante mutamento.

Il metodo migliore per poter prevedere in misura accettabile i rischi e i vantaggi dell'Internet of Things (IoT) è, prima di tutto, comprenderne il funzionamento e la struttura, ed è la fase preliminare di questo studio: individuare le caratteristiche che lo rendono così diffuso e richiesto ormai da tutti, in modo da poterlo adoperare con la consapevolezza delle difficoltà di sviluppo e utilizzo e l'individuazione di strumenti per renderlo efficace ed efficiente.

Il secondo capitolo di questa tesi è dunque un'introduzione al mondo dell'IoT, senza soffermarsi su specifici ambiti a lungo, ma studiandone la struttura e funzionamento da un punto di vista tecnico.

Nel terzo capitolo la focalizzazione è incentrata sull'Industrial Internet of Things

(IIoT), cioè quella branca dell'IoT dell'industria ormai diffusa in quasi tutti i settori, da quello agricolo a quello militare, minerario e molti altri.

Dopo aver capito come opera e qual è la sua struttura operativa, nel quarto capitolo si entra nel punto fondamentale dell'elaborato, cioè la sicurezza: data la diffusione dell'IoT in ambito industriale, sia privato che pubblico, i dati raccolti sono innumerevoli, e come essi anche i pericoli di furto o corruzione delle informazioni. Non è possibile pensare di sfruttare tecnologie di massa senza implementare metodi di sicurezza per la salvaguardia della *privacy* e del *business*.

La sezione finale è incentrata sulla safety in relazione all'IIoT: se ci si trova in realtà industriali la sicurezza non riguarda solo l'impresa, ma anche chi opera al suo interno, ovvero i lavoratori, che devono essere costantemente protetti sotto ogni aspetto, e loro per primi devono conoscere le tecnologie con cui operano quotidianamente.

Capitolo 2

Internet of Things

2.1 La nascita e diffusione dell'IoT

"*Internet of Things*" è un termine coniato da Kevin Ashton nella sua presentazione a Procter & Gamble nel 1999, in cui proponeva di sfruttare la tecnologia Radio Frequency IDentification (RFID) nella catena di approvvigionamento P&G [4]. Come lui stesso ha ipotizzato, se i computer avessero informazioni su ogni cosa assimilando dati autonomamente, la società ne beneficerebbe enormemente [4]. Senza entrare nel merito di discussioni filosofiche sull'effettivo funzionamento di un'utopica società sorretta dalla tecnologia senza l'intervento umano, è innegabile l'utilità di calcolatori che alleggeriscono il carico lavorativo assicurando un grado di precisione quasi perfetto.

L'idea alla base dell'IoT è quindi la diffusione di dispositivi in ogni ambito possibile, in modo da raccogliere dati per controllare lo stato delle cose e avere il più possibile sotto controllo ogni situazione, per essere poi in grado di elaborare e condividere tali dati così da agire direttamente sull'ambiente tramite gli attuatori. Ma quali sono i fattori che maggiormente hanno consentito la sua evoluzione? I principali sono [32]:

- *La nascita degli indirizzi IP*: grazie all'Internet Protocol Address (IP) è possibile la comunicazione fra dispositivi creando una rete che consente ai vari strumenti di essere collegati e fornire le informazioni o compiere le azioni desiderate.

- *Ubiquitous Computing*: una rete pervasiva di dispositivi che portano a termine il loro scopo preciso, senza la necessità che l'uomo sia a conoscenza del loro funzionamento o addirittura della loro presenza.

- *Il progresso tecnologico*: un fattore scontato ma che merita particolare attenzione, soprattutto per l'evoluzione nella dimensione della tecnologia, infatti i dispositivi dell'IoT devono possibilmente essere di dimensioni ridotte e necessariamente non invasivi, e questa possibilità è data dalla miniaturizzazione dei processori e i componenti.

2.2 I componenti dell'IoT

I componenti principali dell'IoT sono i sensori, gli attuatori, e gli elaboratori che forniscono capacità computazionale, essi devono poter comunicare tra loro in modo da raccogliere ed utilizzare dati efficientemente.

2.2.1 Sensori

I sensori hanno il compito di rilevare cambiamenti esterni, interagendo con l'ambiente ma senza compiere azioni che lo modificano, si limitano a raccogliere informazioni che vengono utilizzate successivamente. Fondamentale è l'attenzione che deve essere posta sui dati rilevati dai sensori, essi non devono essere corrotti da fattori esterni, come eccessivo rumore nel segnale o perdita di dati.

Esistono numerosi tipi di sensori, fra essi notiamo:

- *Sensori di temperatura*: possono operare come dei veri e propri termometri digitali che osservano la temperatura dell'ambiente in cui sono posti, segnalando opportunamente quando viene superato un certo limite di rischio. Un esempio pratico è un sensore che misura la temperatura dell'acqua in un sistema di irrigazione automatizzato per garantire una crescita ottimale delle piante [38].

- *Sensori di prossimità*: rilevano la distanza di oggetti nell'area operativa tramite radiazioni elettromagnetiche, la loro applicazione è in ambito di sicurezza e efficienza, come il conteggio di merce, sensori di parcheggio eccetera.

- *Sensori di movimento*: percepiscono il movimento di un'entità (oggetto o persona) nell'area designata inviando di conseguenza un segnale. Sono utilizzati ampiamente nella sicurezza per evitare intrusioni o furti.

2.2.2 Acquisizione dati

Il processo di acquisizione dati da parte dei sensori si basa sulla conversione di un segnale fisico in un segnale digitale comprensibile ed utilizzabile dalla macchina. Le fasi di questo processo sono le seguenti:

1. *Segnale*: distinguiamo i sensori attivi, i quali devono per primi inviare un segnale per effettuare la misurazione, in questo modo non sono sempre in ricezione; e passivi, che sono sempre in ascolto. I sensori misurano un segnale fisico che viene convertito in elettrico.

2. *Campionamento*: il processo di campionamento consiste nel convertire un segnale continuo nel tempo in un segnale discreto, rilevandone il valore dell'ampiezza ad intervalli determinati. In questa fase è bene decidere la frequenza alla quale si deve effettuare il campionamento basandosi sulla natura del segnale, se esso varia rapidamente la frequenza dovrà essere più elevata, altrimenti è sufficiente una frequenza inferiore.

3. *Quantizzazione*: dopo aver campionato il segnale nel tempo, esso deve essere quantizzato, ovvero il valore continuo della misurazione viene mappato in un alfabeto finito risultando, alla fine di tutto il processo, in una stringa di bit utilizzabili dal computer.

2.2.3 Attuatori

Gli attuatori, a differenza dei sensori, non hanno il compito di misurare fattori ambientali, bensì di agire in base ad essi, attuando cambiamenti o operazioni che altrimenti non avverrebbero. Una volta che i sensori raccolgono i dati, essi vengono inviati all'unità di elaborazione che a sua volta attiva gli attuatori inviandogli un segnale; mentre da una parte i sensori hanno il compito di ricevere segnali dall'esterno, gli attuatori compiono azioni che manipolano l'ambiente trasformando i segnali ricevuti in comportamenti.

Alcuni tipi di attuatori sono [25]:

- *Elettrici*: trasformano segnali elettrici in operazioni meccaniche, ad esempio il movimento di una macchina elettrica.

- *Idraulici*: composti da cilindri o fluidi, sfruttano l'elevata energia generata dalla pressione, questo movimento genera un output lineare, rotazionale o oscillatorio.

- *Pneumatici*: producono un movimento rotatorio o lineare utlizzando gas come l'aria compressa che tramite la pressione fornisce grandi quantità di energia con poco sforzo.

- *Termici*: non sfruttano l'elettricità, bensì la temperatura, che innesca un processo basato su elevati sbalzi termici.

2.2.4 Unità di elaborazione

Le unità di elaborazione all'interno del sistema IoT svolgono il ruolo di intermediari: i dati raccolti dai sensori vengono inviati ai computer ed elaborati da essi, hanno il compito di interpretare le informazioni ricevute per utilizzarle poi nel modo più opportuno. Nel momento in cui determinate azioni devono essere eseguite, gli elaboratori comunicano con i dispositivi designati, come gli attuatori.

2.3 Modelli di comunicazione

Una volta compreso da cosa è costituito l'Internet of Things, è bene studiare come questi dispositivi comunicano fra loro, per questo scopo sono stati definiti quattro modelli di comunicazione dall'Internet Architecture Board (IAB) nel 2015 (RFC 7452) [41]. Il framework delineato in questo documento ha lo scopo di fornire una guida nella progettazione delle reti di comunicazione degli smart object.

2.3.1 Device-to-Device

In questo modello (Figura 2.1) si hanno due dispositivi che comunicano fra di loro senza il bisogno di intermediari, l'esempio utilizzato nel documento [41] è un interruttore che deve interagire con una lampadina, entrambi sviluppati da diversi produttori. Per raggiungere lo scopo, essendo i fabbricanti differenti, essi devono accordarsi preventivamente sui protocolli da adottare in fase di sviluppo, in modo da rendere successivamente comunicanti i dispositivi, ad esempio: quali tecnologie utilizzare a livello fisico (ad esempio Bluetooth, ZigBee [13]), quali protocolli adottare a livello di trasporto (ad esempio User Datagram Protocol (UDP), Transmission Control Protocol (TCP)) e di applicazione, e quali misure di sicurezza adottare.

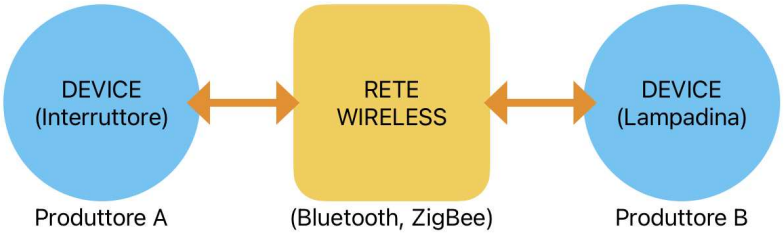

Figura 2.1: Modello Device-to-Device

2.3.2 Device-to-Cloud

Nella comunicazione Device-to-Cloud (Figura 2.2), i dispositivi, come i sensori, che raccolgono dati, li inviano successivamente ad un Application Service Provider (ASP), solitamente è il *provider* stesso che produce i dispositivi, limitando i problemi di interoperabilità. Per garantire una comunicazione ottimale vengono in ogni caso adottati gli standard già presenti come Constrained Application Protocol (CoAP), IP, UDP. I problemi che possono sorgere riguardano l'inoperabilità del dispositivo nel caso in cui la rete del provider divenisse inutilizzabile, o l'*hardware* obsoleto in seguito ad aggiornamenti o cambiamenti del *software*. Per garantire longevità al prodotto la compagnia può fornire la possibilità di modificare il sistema operativo del dispositivo, oppure l'utilizzatore, se consentito, può cambiare il servizio *cloud* a cui fare affidamento.

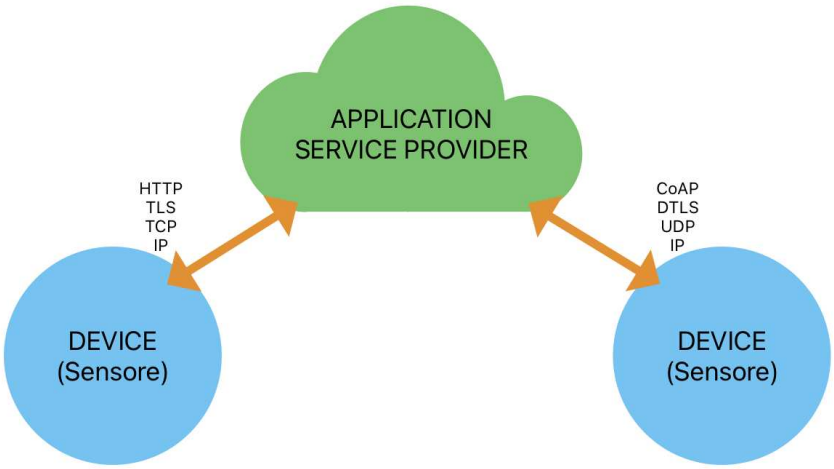

Figura 2.2: Modello Device-to-Cloud

2.3.3 Device-to-Gateway

Analogo al modello Device-to-Cloud, nel modello Device-to-Gateway (Figura 2.3) i dati vengono ugualmente inviati ad un *cloud*, tuttavia, data la natura degli *smart object* uti-

lizzati in questi ambienti, e la mancanza di una connessione diretta da loro al *cloud*, c'è la necessità di porre un *gateway* intermedio che permetta il collegamento. Un vantaggio della presenza del *gateway* è nella sicurezza e interoperabilità, dato che può fare da tramite nel caso in cui il servizio *cloud* non sia fornito dallo stesso produttore del dispositivo. I *fitness tracker* sono un esempio di *smart object* che sfrutta questo modello di comunicazione, non essendo solitamente dotati di una connessione autonoma al *cloud*, si appoggiano ad altri dispositivi come lo smartphone che assumono il ruolo di *gateway*.

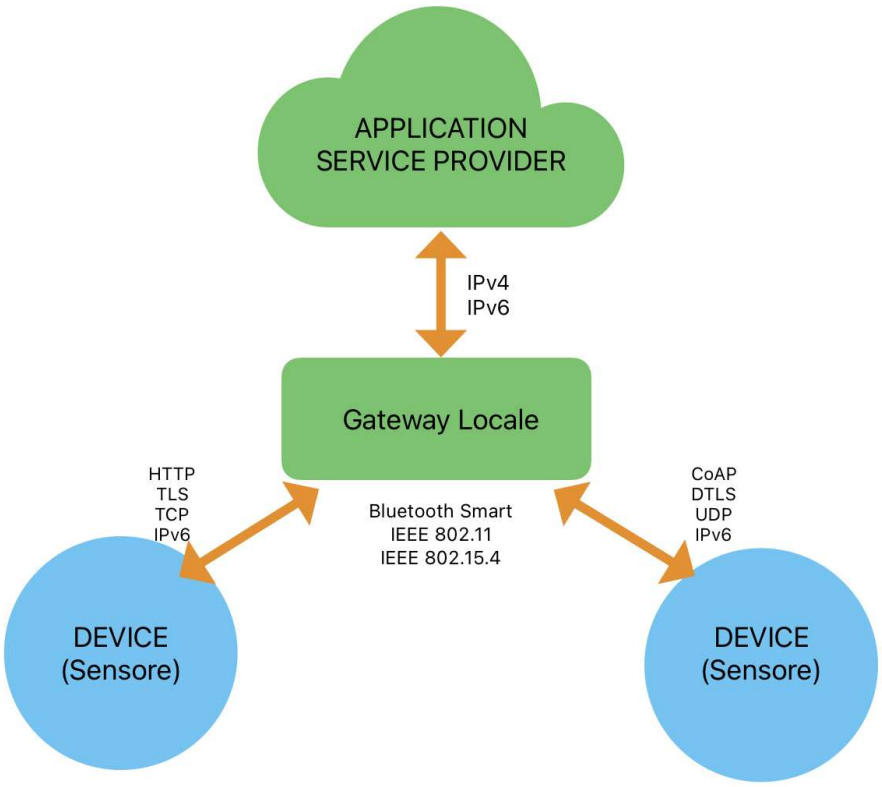

Figura 2.3: Modello Device-to-Gateway

2.3.4 Back-End Data Sharing

Il modello Device-to-Cloud causa isolamento, data la forzata comunicazione e condivisione di dati con il servizio *cloud* del produttore. Nel caso in cui l'utilizzatore del dispositivo volesse condividere i dati salvandoli su diverse reti si sfrutta il Back-End Data Sharing (Figura 2.4), che consente di esportare i dati da altri *cloud* di *provider* differenti. Rimane comunque indispensabile l'utlizzo di standard e protocolli comuni, altrimenti la comunicazione non è possibile.

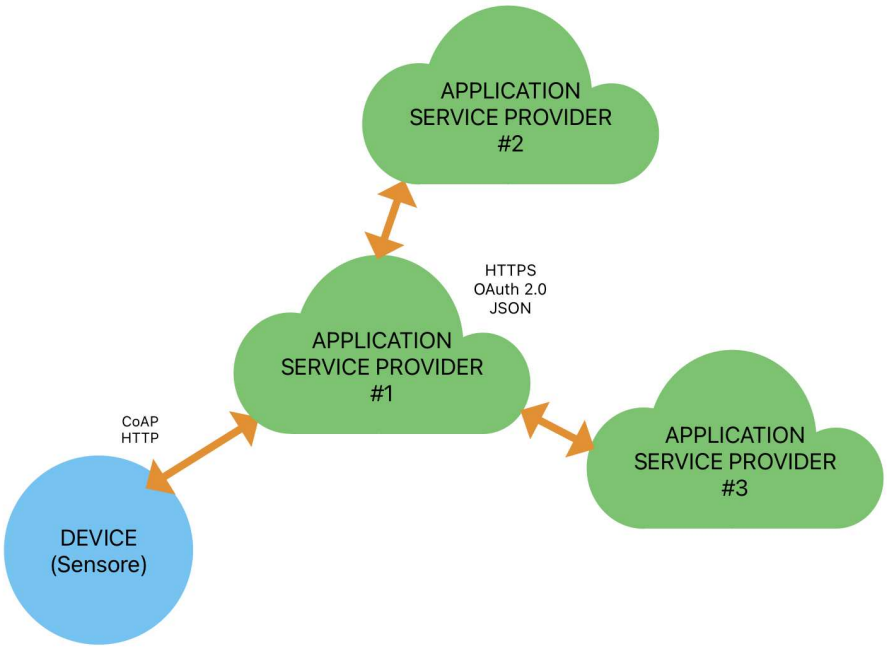

Figura 2.4: Modello Back-End Data Sharing

2.4 Ambiti applicativi

Le applicazioni dell'IoT sono varie, e nonostante il loro funzionamento alla base sia simile, i processi di implementazione e la conseguente evoluzione derivata dalla differenza dell'ambiente in cui ci si trova sono molto importanti: un dispositivo con lo stesso scopo come un sensore termico può variare molto nel suo utilizzo se adoperato in ambito domotico o industriale, nonostante il principio fondamentale sia sempre il rilevamento della temperatura.

2.4.1 Domotica

La domotica studia l'applicazione dell'IoT nelle case, che diventano "*smart home*". Una *smart home* è dotata di sensori che rilevano determinate azioni o comportamenti e, raccogliendo i dati, consentono agli attuatori di compiere a loro volta altre azioni programmate, ad esempio: l'accensione delle luci quando si entra in casa, il regolamento automatico del clima interno basato sulla temperatura rilevata, serrature intelligenti o telecamere che trasmettono in tempo reale la situazione.

Le categorie applicative della domotica maggiormente diffuse che si possono individuare sono tre [9]:

- *Smart home* che pongono attenzione sulla salute dei residenti controllando le loro azioni e il loro stato, sia per gli anziani, che per i bambini, a seconda della loro

progettazione.

- La seconda tipologia ha come obiettivo la sicurezza della casa, controllandola continuamente tramite sistemi di rilevamento e di allarme e informando il proprietario in caso di violazione.

- Un'ultima categoria applicativa individuabile riguarda l'intrattenimento, per migliorare l'esperienza abitativa tramite dispositivi audio multi stanza o dispositivi di riproduzione video interattivi accessibili senza il contatto diretto (tramite riconoscimento vocale).

2.4.2 Smart City

La cosiddetta "città intelligente" è un progetto difficile da realizzare, ma al contempo vantaggioso per tutti gli abitanti: una città connessa e comunicante può essere più sicura e vivibile. L'infrastruttura di una *smart city* coinvolge innumerevoli sensori posti in tutta la città che raccolgono continuamente dati, i quali vengono poi inviati a server centralizzati incaricati di analizzarli e condividerli dove necessario. Oltre a quello economico e politico-decisionale, uno dei problemi maggiori dello sviluppo di una città intelligente è, come studiato precedentemente, l'interoperabilià: essendo i dispositivi innumerevoli e di produzione differente, renderli tutti comunicanti fra loro è complesso. Un importante ed esaustivo studio sulle potenzialità e problematiche di questa branca dell'IoT è stato svolto sulla città di Padova [50].

Esempi di funzionalità di città intelligenti sono:

- *Qualità dell'aria*: monitorare l'inquinamento tramite dispositivi in modo da salvaguardare la salute non solo delle persone, ma anche della flora e della fauna della città.

- *Gestione del traffico*: adottando un sistema intelligente di controllo del traffico tramite GPS o telecamere si può ridurre lo smog e aumentare la sicurezza stradale.

- *Illuminazione intelligente*: basandosi sul periodo dell'anno, il clima e le condizioni atmosferiche, è possibile programmare l'accensione e spegnimento dei sistemi di illuminazione della città riducendo il consumo e i costi.

2.4.3 Smart Healthcare

L'assistenza sanitaria intelligente è un ambito applicativo dell'Internet of Things che richiede particolare attenzione trattandosi della salute delle persone. Può essere tanto efficace quanto rischioso se non vengono effettuati controlli costanti e anche preventivi.

I vantaggi della Smart Healthcare possono essere:

- *Efficacia*: l'utilizzo di dispositivi tecnologici consente un monitoraggio continuo che non sarebbe altrimenti possibile per un operatore umano.
- *Efficienza*: il costo di determinati macchinari intelligenti può essere elevato a primo impatto, ma rendono necessarie meno risorse umane diminuendo i costi nel tempo.
- *Assistenza remota*: limitando il bisogno di intervento umano, un paziente può essere trattato anche dalla propria abitazione, monitorando i segnali inviati dai dispositivi, garantendo più spazio negli ospedali per pazienti più a rischio e permettendo alle persone di essere curate in un ambiente familiare.

Capitolo 3

Industrial IoT

3.1 Cos'è l'IIoT

Uno degli ambiti maggiormente influenzati dall'avvento dell'Internet of Things è sicuramente quello industriale. Da sempre uno degli obiettivi principali dell'industria è di automatizzare i processi senza il bisogno dell'intervento umano, e le nuove tecnologie disponibili rendono possibile, almeno in parte, questo processo. Nascono quindi le "fabbriche intelligenti" che operano autonomamente e più efficientemente rispetto al passato, sia da un punto di vista di output di produzione, che di riduzione dei costi.

L'utilizzo di macchinari di precisione garantisce una qualità superiore del prodotto e un'efficienza molto più elevata. Implementare i nuovi dispositivi, come sensori (Sezione 2.2.1) ed attuatori (Sezione 2.2.3)insieme al cloud computing e l'intelligenza artificiale, è l'idea alla base dell'Industria 4.0 [21]. Si tratta di una rivoluzione industriale ormai non più ipotetica ma diffusa ovunque. Nel 2018 nell'International Journal of production economics è stato pubblicato un articolo che analizza il potenziale impatto industriale dell'industria 4.0 che, dopo gli ultimi anni, è diventato innegabile [8].

Le caratteristiche di questa rivoluzione risiedono non solo nell'automazione dei processi e l'interconnesione della fabbrica, ma anche nei "Big Data" [34], ossia enormi quantità di dati (raccolti nel caso dell'IoT dai sensori) che individualmente possono non possedere molto valore, ma che se analizzati nel complesso sono inestimabili. Tramite questi dati è possibile individuare *pattern* per prevedere l'andamento del mercato e le preferenze del consumatore. Gli ambienti applicativi dell'IIoT non sono solo fabbriche per la produzione, ma anche altri come l'ambito minerario, agricolo, dei trasporti e dell'energia. Per poterli analizzare c'è la necessità di individuare prima un framework comune

dell'IIoT, come mostrato in Sezione 3.2.

3.2 Architettura dell'Industrial IoT

Un'architettura stabilisce i protocolli e i dispositivi con l'obiettivo di uniformare le reti con determinati standard per renderle comprensibili e interagenti con l'esterno. I dispositivi sono già stati affrontati (Sezione2.2), così come i modelli di comunicazione (Sezione2.3). Conoscere già queste componenti aiuta a comprendere meglio le motivazioni dietro alla scelta di una particolare architettura, quella proposta in [39] è a tre strati, ed è quella analizzata in questo elaborato (Figura 3.1):

- *EDGE (Fisico)*: in questa parte della rete sono collocati i dispositivi come sensori, attuatori e computer che comunicano fra loro in reti locali e indipendenti, a loro volta queste reti comunicano con l'esterno attraverso dei gateway.

- *PLATFORM (Rete)*: è lo strato intermedio che fa da collegamento, la rete in questa fase è più ampia rispetto alle reti locali iniziali; il suo compito è di garantire la trasmissione dei dati in modo sicuro e senza perdite.

- *ENTERPRISE (Applicazione)*: l'ultimo strato funziona analogamente allo strato di applicazione nell'architettura base IoT [3] in cui vengono forniti i servizi tramite interfacce accessibili agli utenti, i dati raccolti dai dispositivi iniziali e trasmessi allo strato applicativo sono elaborati ed analizzati tramite software per adempiere allo scopo prefissato.

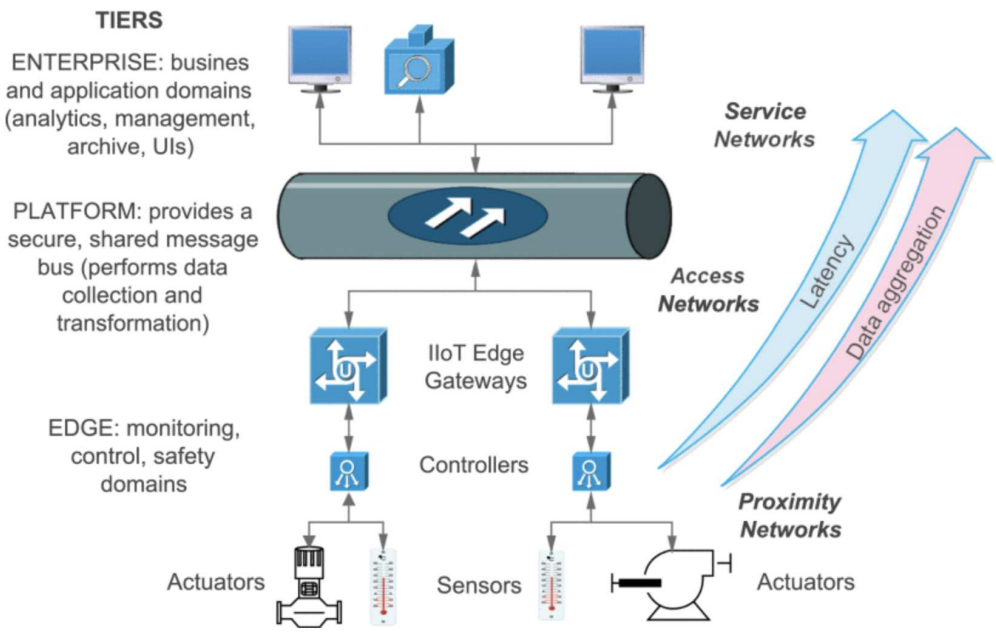

Figura 3.1: Architettura dell'Industrial IoT [39]

Per implementare quest'architettura in ambito industriale possono essere sfruttate le tecnologie sviluppate negli ultimi anni[24]:

- *Edge/Fog Computing* [28]: in ambito industriale, soprattutto quando si opera in reti molto grandi con un numero elevato di dispositivi, il *cloud computing* può risultare non adatto. La capacità del *cloud* di rispondere e operare in modo efficace è compromessa dalla quantità di informazioni ricevute e trasmesse e dalla distanza che i dati devono percorrere per raggiungere il *cloud* remoto. La soluzione a questo problema è l'*edge computing* che consiste in un'architettura di calcolo distribuito in cui i dati vengono prima elaborati ai margini della rete per poi essere indirizzati al *cloud* centrale. In questo modo i dati raccolti dai dispositivi devono percorre distanze minori, riducendo la latenza così da avere un tempo di risposta ottimale. Inoltre elaborando i dati localmente, e non interamente sfruttando il *cloud*, si risparmia larghezza di banda, gestendo perciò meglio le risorse e aumentando la scalabilità e la sicurezza. La differenza principale fra il *cloud computing* e l'*edge computing* è quindi la presenza di *server* distribuiti più vicini ai punti di raccolta dati che riducono la latenza e il carico di ogni singolo *server*, è una soluzione ottimale per industrie che coprono molto spazio o che, anche in spazi ridotti, hanno troppi dispositivi per un solo *data center*.

- *Blockchain* [17]: la tecnologia Blockchain si basa su nodi distribuiti e decentralizzati (*Distributed Ledger Technology*), e il suo obiettivo principale è di garantire

sicurezza e affidabilità. Ogni utente della rete rappresenta un nodo ed è in possesso del registro condiviso da tutti contenente le transazioni effettuate nella rete, visibili a tutti e modificabili solo con il consenso degli altri utenti. Ciò rende quasi impossibile alterare un dato al fine di commettere, ad esempio, reato di frode, perchè andrebbe modificato contemporaneamente in tutta la rete e la modifica dovrebbe essere concordata. Le transazioni vengono trasmesse su blocchi che si legano al precedente come una catena tramite hash per crittografare le informazioni. L'hash è una funzione che trasforma dati di qualsiasi dimensione in una stringa di lunghezza fissa e univoca. In questo modo ogni blocco ha un suo identificativo, a sua volta il blocco successivo ha un suo hash che contiene anche l'hash del blocco precedente, legando così i due. Il significato di decentralizzazione della blockchain è la mancanza di controllo da parte di un singolo individuo o istituzione, coloro che validano le transazioni sono gli stessi nodi e i meccanismi per il consenso rendono possibile questo processo (Proof of Work (PoW) [12], Proof of Stake (PoS) [35]).

- *Machine Learning (ML)*: è un ramo dell'Intelligenza Artificiale (IA) basato sui modelli di apprendimento. Tramite algoritmi appositi è possibile creare delle IA che imparano dai dati accumulati, così da poter dare risposte e prendere decisioni grazie ad esperienze pregresse. Per sviluppare un modello di ML funzionante è necessario l'algoritmo fondamentale, che è lo "scheletro" dell'intelligenza, ne definisce il sistema e opera su una funzione obiettivo, essa misura l'effettiva accuratezza della risposta ottenuta da parte del modello rispetto a quella attesa, fornendo un'indicazione della sua precisione e livello di intelligenza. Anche i dati sono estremamente importanti, più sono e migliore sarà il rendimento, in ambiti in cui si lavora con *Big Data* [34] si ha una efficacia molto più elevata; in ambienti industriali fra le applicazioni possibili rientrano la rilevazione predittiva delle minacce e degli errori, la manutenzione predittiva e la sicurezza. I problemi che possono nascere dall'utilizzo di ML riguardano ad esempio la trasparenza dei processi, dato che gli algoritmi sono estremamente complessi risulta difficile fornire una spegazione adeguata sul loro funzionamento, incorrendo in problemi di natura legale che rischiano di limitare o interrompere i processi industriali.

- *5G*: il 5G è il nuovo modello di reti mobili che garantisce una velocità di connesione maggiore e una latenza ridotta, supportando al contempo molti più dispositivi connessi, adattandosi alle necessità dell'IoT. Introduce anche il *network slicing*

[11], che consiste nel suddividere virtualmente una stessa rete ottenendo così più reti gestibili in modo diverso, ottimale in ambito aziendale (ad esempio per suddividere i reparti di una fabbrica che devono operare in modo indipendente). Delle categorie di utilizzo di rete 5G attualmente definite [19] sono l'eMBB (per reti con richiesta di velocità di connessione elevata ma banda ridotta per via del numero di dispositivi), URLLC (utilizzata per servizi che richiedono un tempo di risposta il più basso possibile come la sicurezza pubblica, il *disaster recovery* o l'assistenza sanitaria), e Massive IoT (reti con elevato numero di dispositivi a basso costo e basso dispendio di energia ma con la necessità di ampia copertura).

- *Software-Defined Networking (SDN)*: è un approccio di gestione della rete dinamico in modo da controllare il traffico e i processi in tempo reale e renderla più efficiente. Si basa sulla separazione del livello di controllo delle rete dal livello dei dati. Potendo programmare la rete tramite software essa diventa molto più flessibile e quindi si adatta meglio alla situazione che, in ambito industriale, può cambiare anche improvvisamente a causa di imprevisti, diventa perciò anche più sicura. La gestione centralizzata della rete consente anche la sua modifica immediata in caso di espansione migliorandone la scalabilità e permettendo la creazione di processi automatizzati. L'architettura suggerita per l'SDN è costituita da tre strati [44], cioè infrastruttura (costituito da dispositivi come router e switch che rilevano e comunicano lo stato della rete allo strato successivo e instradano i pacchetti ricevuti secondo le regole impostate), controllo (definisce le funzioni di instradamento e comunicazione con il livello di infrastruttura e le Application Programming Interface (API) per comunicare con il livello di applicazione), e applicazione (per l'accesso e gestione della rete da parte dell'utente tramite interfaccia).

- *Wireless Sensor Networks (WSN)* [49]: si tratta di reti costituite da numerosi sensori che raccolgono dati di vario tipo (temperatura, pressione, inquinamento, livello dell'acqua) in una determinata area. Il principio fondamentale di queste reti è la comunicazione wireless dei dispositivi sia tra di loro che con un sistema centrale di controllo (non sempre presente, dipende dall'architettura della rete). Come la maggior parte delle reti IIoT, la struttura deve consentire scalabilità e efficienza dei dispositivi, trattandosi in questo caso di sensori che coprono anche ampie aree, l'autonomia è un fattore importante, devono essere in grado di continuare

a funzionare per lunghi periodi e in condizioni avverse. Alcune implementazioni tipiche sono le *smart cities*, il monitoraggio ambientale e la sorveglianza.

3.3 Analisi di ambienti applicativi

Come già accennato in precedenza, l'IIoT può essere applicato in vari ambiti industriali, e una volta compresi i suoi principi operativi è possibile verificare in quali modi può migliorare l'ambiente di lavoro.

3.3.1 Industria manifatturiera

L'industria manifatturiera in seguito alla globalizzazione è diventata sempre più competitiva, il mercato si è aperto ad aziende di tutto il mondo e quindi ad una maggiore varietà dei prodotti. Questo obbliga i produttori non solo a migliorare la loro merce modificandola a seconda della richiesta in tempi rapidi, ma anche a fabbricare in grandi quantità velocemente per soddisfare la domanda. Per soddisfare queste necessità nasce il bisogno di sistemi realizzati appositamente per operare efficientemente in autonomia con una semplice supervisione da parte del personale.

Ci sono tre tecnologie principali sfruttate in questo ambiente [47]:

- *RFID* [42]: il principio alla base di questa tecnologia consiste nell'etichettare gli oggetti con dei particolari *tag* leggibili da dispositivi appositi con tecnologia RFID, così facendo i prodotti sono contrassegnati e facilmente riconducibili a delle informazioni salvate nei *database*. Può essere utilizzata nella gestione della catena di fornitura per tracciare gli oggetti in tutto il loro processo, i suoi vantaggi principali rispetto ai codici a barre sono la distanza di lettura maggiore, la possibilità di lettura simultanea di più merci anche senza il bisogno di contatto diretto e la quantità di dati immagazzinabili. Tutto questo migliora la gestione dei magazzini con una tracciabilità continua e accurata.

- *WSN*: si tratta delle Wireless Sensor Network analizzate in precedenza (Sezione 3.2), nell'industria manifatturiera possono anche essere utlizzate insieme alla tecnologia RFID che può rilevare e identificare gli oggetti, ma non il loro stato, come la sua temperatura o la composizione dei suoi materiali, aspetti che possono essere controllati tramite i sensori, che inviano successivamente le informazioni ottenu-

te al resto della rete, creando un sistema eterogeneo e che unisce tecnologie con funzioni diverse per rilevamenti più accurati.

- *Cloud Computing e Big Data*: negli scorsi anni sono stati proposti nuovi modelli denominati "Cloud Manufacturing (CMfg)" [40] che implementano il *Cloud Computing* [15] nell'ambiente manifatturiero, il quale riduce il bisogno fisico di risorse computazionali diminuendo costi iniziali e consumi dell'azienda. Il suo utilizzo aiuta a migliorare la gestione dei *Big Data* fondamentali per l'operatività dell'industria, e a ridurre i costi nel tempo che possono risultare elevati con il *Cloud Computing*, inoltre si dipende da terzi gestori del servizio, rischiando di compromettere la privacy, il fornitore del *cloud* deve essere affidabile.

Il ruolo principale dell'IoT nell'industria manifatturiera rimane comunque l'ottimizzazione dei processi, i quali sono molto dispendiosi di tempo e manodopera, per cui applicare macchinari che operano autonomamente sorretti da una catena di dispositivi che rendono tale possibilità realizzabile è l'obiettivo di tutti i centri di produzione moderni.

3.3.2 Industria energetica

Nell'ambiente dell'energia gli obiettivi principali degli ultimi anni sono l'utilizzo di fonti di energia rinnovabili in modo da ridurre i consumi e l'inquinamento, è un tema sempre più importante e spesso sottovalutato, ma l'utilizzo di strumenti intelligenti può contribuire nel raggiungere tale scopo. I vantaggi principali sono [16]:

- *Generazione di energia*: sfruttare dispositivi che misurano la quantità di energia richiesta aiuta nel comprendere quanta di essa è necessario produrre per soddisfare i clienti, riducendo i consumi e aumentando al contempo l'efficienza.

- *Smart Cities*: già trattate precedentemente (Sezione 2.4.2), le città intelligenti aiutano a migliorare il tenore di vita degli abitanti, e un sistema di gestione *smart* dell'energia tramite una rete di sensori che rilevano flussi e consumi monitorandone continuamente lo stato porta benefici anche alle industrie, sia dal punto di vista della sicurezza per il controllo dell'elettricità, che dal punto di vista dell'efficienza nei consumi. Anche il sistema dei trasporti ne beneficia, con la presenza di veicoli elettrici privati c'è il bisogno anche di stazioni di ricarica posizionate per la città e costantemente rifornite e monitorate, così come per i mezzi pubblici.

- *Energie rinnovabili*: come detto precedentemente, l'utilizzo di risorse rinnovabili è un aspetto fondamentale dell'industria energetica al giorno d'oggi, i dispositivi IoT possono supportare questo utilizzo in modo intelligente tramite la predizione dei consumi, il *load sharing* (per dividere il carico elettrico fra più generatori che operano in parallelo) e l'immagazzinamento delle risorse per ridurre gli sprechi.

- *Utilizzo intelligente*: consiste, ad esempio all'interno di una fabbrica, nel monitorare tramite sensori i dispositivi ed il loro consumo di energia, così da poter allocare dinamicamente le risorse, se un dispositivo ha una determinata fascia oraria di utilizzo, è possibile non fornire energia ad esso durante quel periodo di tempo, dedicando più risorse a dispositivi a consumo più elevato. Grazie all'implementazione della rete IoT tutto ciò si può gestire da remoto.

3.3.3 Industria chimica

L'industria chimica è un settore ad alto rischio che richiede particolare attenzione per via delle condizioni e gli strumenti di lavoro, integrare i sistemi IoT aiuta ad aumentare la sicurezza operativa non solo in ambito informatico.

Lo sviluppo di sensori in grado di operare in condizioni ambientali estreme favorisce il lavoro con sostanze chimiche che per l'uomo possono risultare nocive. Poter effettuare esperimenti in un ambiente sterile senza l'intervento umano quindi non aumenta solo la sicurezza, ma anche l'efficacia dell'esperimento o misurazione stessa. Di conseguenza l'efficienza industriale incrementa e i benefici variano dalla riduzione dei costi a lungo termine e il miglioramento della qualità produttiva, al supporto innovativo, alimentato dalla sicurezza dell'ambiente e l'utilizzo di dispositivi che consentono di lavorare in modo preciso. Un ulteriore aspetto importante è la conformità normativa: trattandosi, come già detto, di un settore ad alto rischio, le norme sono molto stringenti e devono essere rispettate rigorosamente, grazie all'IoT è più facile soddisfare determinate richieste, data la facilità di monitoraggio e la possibilità di gestire gli strumenti da remoto e in massa per renderli operativi secondo le normative vigenti. Le emissioni chimiche devono essere controllate e contenute essendo sanzionabili e dannose, sono stati ideati a questo proposito dei framework di reti IoT composte da sensori che rilevano diversi gas presenti nell'aria per valutare il livello di inquinamento causato dall'impianto industriale. Il framework proposto e testato in [1] combina più tecnologie di comunicazione come

Zigbee [13] e LoRa [36] per mettere in comunicazione i nodi sensoriali che raccolgono i dati con l'Internet.

Un altro esempio effettivo di ambito applicativo nell'industria chimica sono le raffinerie [7] che necessitano di un controllo costante del livello chimico, esso viene effettuato da remoto tramite una rete di sensori perimetrali e se possibile anche interni per rilevamenti più accurati.

Capitolo 4

Sicurezza

4.1 Principi fondamentali

I principi fondamentali della sicurezza possono riassumersi con la triade Confidentiality Integrity Availability (CIA) [31], cioè con i concetti di riservatezza, integrità e disponibilità del dato. Essi devono essere rispettati per garantire un livello minimo di sicurezza. Si tratta in ogni caso di un modello concettuale che ha lo scopo di fornire una guida generale su come strutturare la sicurezza in modo efficace. All'interno di un'azienda, saper bilanciare questi fattori accresce l'efficienza grazie alla consapevolezza delle necessità, ad esempio se si lavora principalmente con dati sensibili dei clienti, dedicare maggiore attenzione alla loro protezione invece che ad altri aspetti meno rilevanti può fare la differenza.

4.1.1 Riservatezza

Il primo principio da trattare è la riservatezza, che consiste nel rendere i dati accessibili solo a chi ne ha l'autorizzazione e nella misura consentita. Il metodo più conosciuto per soddisfare questa necessità è la crittografia:

- *Chiave simmetrica* [2]: si tratta di un tipo di crittografia che utilizza una singola chiave sia in fase di cifratura che decifratura, è necessario dunque che mittente e destinatario la concordino preventivamente. In questo modo gli algoritmi a chiave simmetrica sono più rapidi, perchè richiedono solo la fase di cifratura del testo in chiaro (cioè il testo originale da proteggere) e di decifratura del testo criptato senza ulteriori operazioni intermedie, permettendo di operare su quantità di dati maggiori in minor tempo. Tuttavia la sicurezza di questo metodo risiede nella

protezione della chiave stessa, se la sua segretezza viene compromessa, i dati sono facilmente ottenibili da terzi. La fase di distribuzione delle chiavi perciò deve essere altamente confidenziale e univoca (non devono esistere chiavi uguali), questo aspetto però è molto dispendioso nel caso in cui si necessiti di un numero elevato di chiavi. I quattro principali algoritmi di cifratura a chiave simmetrica sono il Data Encryption Standard (DES) che è stato uno dei primi ad essere sviluppato, può cifrare testo in chiaro fino a 64 bit usando una chiave a 56 bit, opera su 16 *round*, cioè il testo in chiaro viene processato 16 volte in fase di cifratura oltre alla fase di permutazione iniziale e finale; il Triple DES (TDES) utilizza tre esecuzioni di DES con una lunghezza di 168 bit (56 * 3) in sequenza cifratura-decifratura-cifratura cambiando chiave (sempre a 56 bit) ad ogni fase; l'Advanced Encryption Standard (AES) è un algoritmo di cifratura a bit variabili, può operare con blocco da cifrare di 128 bit e chiave a 128 bit processando a 9 *round*, se entrambi sono di 192 bit 11 *round*, se invece sono 256 bit ci sono 13 *round*, questo lo rende molto flessibile; l'algoritmo Blowfish lavora su blocchi di 64 bit con una chiave variabile dai 32 ai 448 bit, il vantaggio di questo algoritmo è la complessità della chiave, grazie a questo fattore esso non è mai stato compromesso garantendo un'ottima sicurezza, tuttavia, data la possibilità di criptare blocchi di un massimo di 64 bit, il suo utilizzo negli ultimi anni è diminutito vista la necessità di lavorare su quantità di dati maggiori.

Tabella 4.1: Comparazione algoritmi

	Algoritmi a cifratura simmetrica			
	DES	TDES	AES	BLOWFISH
Dimensione blocco	64 bit	64 bit	128, 192, 256 bit	64 bit
Dimensione chiave	56 bit	168 bit	128, 192, 256 bit	32-448 bit
Round	16	48	9, 11, 13	16
Sviluppo	IBM 1975	IBM 1978	Joan Daeman 1998	Bruce Schneier 1998

- *Chiave asimmetrica* [48]: questo metodo di cifratura, detto anche a chiave pubblica, utilizza due chiavi, una privata e una pubblica. Ogni utente dispone di entrambe le chiavi univoche, quella privata è conosciuta solamente a lui, mentre quella pubblica è visibile a tutta la rete, tuttavia da essa non è possibile risalire alla prima. La cifratura a chiave asimmetrica viene utilizzata per garantire riservatezza (il mittente cifra il messaggio con la chiave pubblica del destinatario, il quale a sua volta lo decifra con la propria chiave privata) ma anche per l'autenticazione

(il mittente cifra il messaggio con la propria chiave privata e il destinatario lo decifra con la chiave pubblica della controparte, se il risultato è il messaggio inteso dal mittente, significa che è confermata l'identità). La complessità degli algoritmi è maggiore rispetto a quelli a chiave simmetrica, di conseguenza la sicurezza è maggiore, e non c'è bisogno di condividere le chiavi per comunicare, limitando il pericolo di compromissione delle trasmissioni. Fra gli algoritmi più utilizzati si notano Rivest-Shamir-Adleman (RSA) sviluppato nel 1977, utilizza una lunghezza variabile sia di chiave (solitamente almeno 2048 bit a seconda delle necessità) che di blocchi, viene utilizzato sia per la cifratura che per l'autenticazione e si basa sulla complessità computazionale della fattorizzazione dei numeri primi; l'algoritmo Diffie-Hellmann (1976) non viene utilizzato prettamente per la crittografia, bensì per la condivisione privata di chiavi su un canale non sicuro con l'obiettivo di stabilire una chiave segreta per comunicazioni successive; il Digital Signature Algorithm (DSA) (1991) ha applicazione principalmente nell'ambito delle firme digitali per verificare l'identità delle parti utilizzando il Secure Hash Algorithm (SHA), il mittente genera una firma digitale con la chiave privata, essa viene verificata poi dal ricevente con la chiave pubblica; l'Elliptical Curve Cryptography (ECC) (1985) sfrutta matematicamente le curve ellittiche per generare chiavi pubbliche più corte, utilizza la chiave pubblica per operazioni di autenticazione e di cifratura, e la chiave privata per verifica dell'identità e decrittazione,può essere implementato insieme agli algoritmi citati in precedenza per contribuire a ridurre il peso di calcolo aumentandone l'efficienza.

4.1.2 Integrità

L'integrità dei dati consiste nel garantire che essi rimangano intatti e non alterati da errori o modifiche non consentite, durante il loro intero ciclo di vita c'è il bisogno di mantenere la loro accuratezza e completezza. La accuratezza dei dati è l'esattezza di essi nel rappresentare le informazioni originali previste senza cambiamenti non voluti, la completezza è la presenza nell'insieme di tutti i dati senza perdite. All'interno di un'azienda, se l'integrità dei dati non è osservata, i processi produttivi e decisionali sono compromessi, come accennato più volte all'interno di questo elaborato, i dati sono la risorsa principale nell'industria moderna, e su di essi si basa il suo funzionamento, perciò fondare le decisioni su dati incorretti è estremamente pericoloso. Utilizzare dati errati

inoltre può comportare problemi legali, soprattutto in ambiti come quello sanitario o finanziario, dove si ha a che fare con la salute delle persone o il loro denaro, compromettere uno di questi aspetti a causa di informazioni sbagliate può essere legalmente perseguibile se il risultato è reato di frode o pericolo per il paziente. Un ulteriore aspetto fondamentale è la fiducia nell'azienda, se i dati stessi non sono affidabili e da ciò ne risente la sua credibilità, sorgono nuovamente problemi gravi.

Nel 2017 è stato proposto un framework per assicurare l'integrità dei dati sfruttando la Blockchain [23], in cui sono presenti quattro elementi principali: Data Owners Application (DOA) responsabile di generare e caricare i dati al Cloud Storage Service (CSS), il quale immagazzina i dati, Data Consumer Applications (DCAs) che sono i consumatori che hanno intenzione di accedere ai dati e la Blockchain. Gli obiettivi dello studio citato sono:

- la creazione di un servizio di gestione dei dati che garantisca integrità rimpiazzando i già esistenti servizi centralizzati con uno decentralizzato sfruttando la Blockchain. Il problema dei servizi centralizzati risiede nella fiducia nel fornitore terzo del *cloud*, sia da parte dei Data Owners (DOs) che dei Data Consumers (DCs);

- l'utilizzo di protocolli di verifica dell'integrità dei dati in un sistema decentralizzato che consenta sia ai DOs che ai DCs di interagire nello specifico coi dati senza affidarsi a terzi;

- dimostrare effettivamente la possibilità di implementare un sistema privato basato sulla Blockchain per lo scopo previsto.

Il servizio viene implementato tramite gli *smart contract* [51], cioè programmi autoeseguibili sulla Blockchain che vincolano in ugual modo entrambe le parti coinvolte, assicurando affidabilità. Questo li rende molto rapidi e imparziali, non necessitando di autorità che ne verifichino l'esecuzione.

L'effettivo trasferimento dei dati avviene dopo che tutti i nodi coinvolti nella trasmissione sono attivi sulla Blockchain (i DOs, i DCs, ed eventualmente il *cloud*) e il Peer to Peer File System (P2PFS) è stato inizializzato, ossia il software utilizzato per il trasferimento dei file. Tramite i protocolli di verifica di integrità (DOA to CSS-Y, DOA to CSS-N, DCAS to CSS-Y, DCAS to CSS-N) vengono controllati i dati nelle varie fasi della trasmissione e nei vari casi in cui ad accedere ai dati siano i DOs o i DCs.

4.1.3 Disponibilità

La disponibilità dei dati consiste nel garantire che i dati siano accessibili a tutti coloro che ne hanno l'autorizzazione quando ne hanno il bisogno, senza problemi o interruzioni. Per avere dati disponibili devono essere presenti dei fattori:

- *Sicurezza*: i dati devono essere protetti da attacchi che possono compromettere l'accesso da parte degli utenti.
- *Backup*: eseguire dei *backup* periodici consente di ripristinare i dati in caso di perdite o corruzione degli stessi.
- *Accesso continuativo*: avere un servizio che permette di accedere in ogni momento desiderato senza interruzione così di permettere di essere sempre operativi.

La disponibilità dei dati è minacciata, oltre che da pericoli come errori umani, disastri naturali o problemi di rete che impediscono l'accesso, anche da attacchi informatici come il Distributed Denial of Service (DDoS), in cui la rete viene sovraccaricata di traffico compromettendone il funzionamento e interrompendo i servizi, o come l'utilizzo di malware per infettare il sistema: i malware sono software maligni che danneggiano il sistema dall'interno dopo essersi infiltrati, fra essi si citano:

- *virus*: si attivano in seguito all'esecuzione di un file infetto da parte dell'utente,
- *worm*: si diffondono autonomamente senza il bisogno di esecuzione del file,
- *trojan*: all'apparenza un programma legittimo che dopo l'installazione può fornire accesso remoto da parte dell'*hacker* per impossessarsi dei dati
- *ransomware*: cifra da remoto i file nel computer, così da renderli inaccessibili al proprietario e richiedendo un riscatto per il rirpristino,
- *spyware*: raccoglie informazioni monitorando l'attività dell'utente senza il consenso, ottenendo informazioni private e sensibili.

.

4.2 Problemi di sicurezza nell'IIoT

Purtroppo quando si parla di sicurezza ci sono molti aspetti da valutare nelle reti IIoT, da quelli più generali come la triade CIA (Sezione 4.1) a quelli più pratici come la protezione

da attacchi esterni. Nelle successive sezioni verranno analizzate delle problematiche con soluzioni applicabili in ambito industriale.

4.2.1 DDoS e framework di mitigazione

Negli ultimi anni l'attenzione posta sugli attacchi DDoS è aumentata in parte a causa della *botnet* Mirai [20] (dal giapponese "futuro"). Essa è formata da quattro componenti operativi: il *bot*, cioè il dispositivo infettato dal malware il quale agisce in base al comando del *botmaster*; il *Command and Control server (CnC)* che fornisce un'interfaccia di controllo al *botmaster* per controllare il funzionamento della *botnet* (la rete di bot che compongono Mirai); il *loader* che aiuta la distribuzione degli eseguibili che diffondono il malware e infine il *report server* che fornisce un database con le informazioni sui dispositivi collegati alla *botnet*. Gli step con cui un attacco DDoS tramite Mirai viene effettuato sono descritti in [20]:

1. Tramite un attacco a forza bruta sui dispositivi della rete IoT si tenta di ottenere le credenziali di accesso.

2. Una volta ottenute le credenziali vengono inviate al *report server* le caratteristiche del dispositivo.

3. Il *botmaster* controlla lo stato della rete ed eventuali altri dispositivi attaccabili tramite il CnC.

4. Una volta deciso quali dispositivi vulnerabili della rete infettare, il *botmaster* invia il comando.

5. Il *loader* una volta all'interno del dispositivo bersaglio lo istruisce di scaricare ed eseguire il file contenente il malware infettando i *bot*.

6. Attraverso un comando comunicato tramite il CnC, il *botmaster* ordina a tutti i *bot* di iniziare l'attacco diretto ad un *server* bersaglio con i parametri da lui decisi.

7. I *bot* eseguono l'attacco verso il server.

Molte reti IoT sono vulnerabili ad attacchi di questo genere perchè la loro struttura e i dispositivi che le compongono favoriscono la creazione di botnet: *device* come sensori o attuatori spesso sono operativi per lunghi periodi continuati, o addirittura non vengono mai spenti, questo fornisce un'ampia finestra operativa per attacchi, inoltre su di essi,

essendo numerosi, la manutenzione viene trascurata. Data la quantità di questi dispositivi e la loro potenza computazionale più che sufficiente, sono ottimali per generare attacchi DDoS, e non essendo di solito dotati di interfacce utente, gli attacchi possono passare inosservati.

Nel 2018 è stato pubblicato un articolo che propone un framework IIoT per contrastare gli attacchi DDoS, denominato Multi-Level DDoS Mitigation Framework (MLDMF) [45]. Esso è suddiviso in tre livelli (Figura 4.1): *edge computing*, *fog computing* e *cloud computing*.

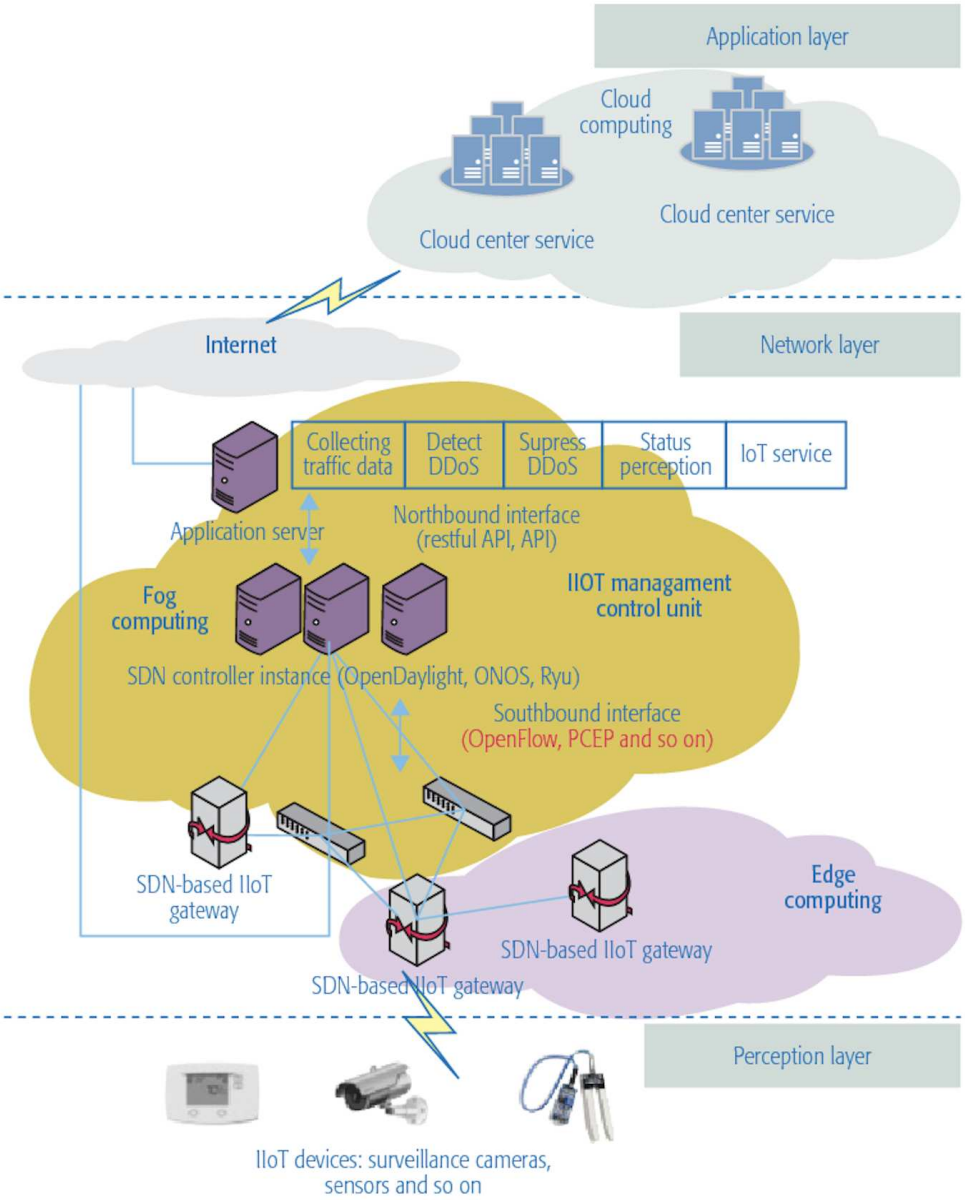

Figura 4.1: Architettura del MLDMF [45]

- Edge: formato da gateway IIoT basati su SDN (Sezione 3.2) chiamati SDN-based IIoT Gateways (SDNIGWs), che sono in grado di connettersi ai dispositivi trami-

te vari tipi di protocolli (Wi-Fi, Ethernet, ZigBee, Z-Wave, 5G). Basandosi sulla tecnologia SDN, questo livello può essere gestito dal lato software per effettuare controlli e modifiche alla rete. I SDNIGWs adottano meccanismi di protezione dei dispositivi a cui si collegano (sensori e attuatori) come il controllo degli accessi, il rilevamento di intrusioni o *software* e *firmware* maligni, filtraggio del traffico per ridurre gli attacchi, connessione automatica ai dispositivi tramite autenticazione, aggiornamento automatico del *firmware*, occultamento degli indirizzi IP e cifratura delle comunicazioni.

- Fog: consiste principalmente nelle IIoT Management Control Unit (IMCU) composte da *controller* e applicazioni SDN. A questo livello vengono raccolti i dati del traffico nella rete effettuando controlli per rilevare eventuali attacchi DDoS e rispondervi. Le funzioni di sicurezza sono programmate con SDN a livello applicazione e implementate tramite API (l'API nord le introduce nella rete e l'API sud le implementa a tutti gli effetti). A livello fog ci sono tre metodi di contrasto al DDoS: il Collect-Detect-Mitigate (CDM) in cui la IMCU raccoglie i dati del traffico analizzandolo in tempo reale, e in base al risultato ottenuto contrasta gli attacchi operando sulla larghezza di banda riducendola ove necessario; l'Honeypot-Detect-React (HDR) sfrutta l'*honeypot*, cioè un meccanismo di difesa che rileva e contrasta tentativi di accesso non autorizzati nella rete, tramite SDN l'IMCU può reindirizzare le comunicazioni all'*honeypot* per effettuare i controlli; l'ultimo metodo, il Cloud-Detect-Fog-Mitigate (CDFM) vede il livello *cloud* e *fog* operare insieme, dove il *cloud* con l'elevata potenza computazionale e quantità di dati su cui lavorare riesce a rilevare gli attacchi più efficacemente, il *fog* riceve le informazioni e contrasta l'attacco con l'aiuto del livello *edge* se opportuno.

- Cloud: il *cloud computing* risulta molto efficiente nell'IIoT. Data la quantità di dati e dispositivi coinvolti, sfruttare un sistema *cloud* con ottima capacità di elaborazione e immagazzinamento dati, con bassi costi e alta scalabilità può tornare utile anche per la sicurezza della rete. I *Big Data* affiancati a sistemi di calcolo intelligenti possono rilevare più facilmente gli attacchi DDoS. Con sistemi di calcoli intelligenti si intende l'utilizzo di modelli di intelligenza artificiale e *machine learning* (Sezione 3.2), che lavorando sui *Big Data* imparano a riconoscere le caratteristiche dei dati e la loro struttura, diventando in grado di riconoscere in parte se si tratta di dati fittizzi o artificialmente generati, aiutando il rilevamento di attacchi DDoS.

I risultati del test pratico di funzionamento del framework effettuato dagli autori dimostra l'efficacia del sistema (Figura 4.2). In esso si hanno 15 *host*, i primi dieci inviano al server dei pacchetti falsi per impedirne il corretto funzionamento, gli altri cinque invece sono *host* normali, che effettuano dei comandi di ping verso il server sessanta volte per connettersi in modo da testare il *delay*, un *proxy* TCP SYN viene usato per collegare client e server. La dimostrazione è divisa in quattro casistiche: la prima (a) in cui non ci sono metodi di difesa e la seconda (b) in cui si usa SDN, l'attacco esaminato in questi due esperimenti è il *ping of death*, difendibile bloccando gli altri pacchetti maligni in arrivo. Nella figura (a) si può notare come al decimo secondo, quando viene effettuato l'attacco, il *delay* aumenti esponenzialmente raggiungendo i 3000 millisecondi corrispondenti al fallimento del *ping*; nella figura (b) invece non c'è alcun *delay*, se non per un singolo *host* all'undicesimo secondo. Nel secondo esperimento l'attacco è TCP SYN *flood*, difendibile utilizzando il *proxy* TCP SYN per scegliere un utente normale e impostare un percorso dal *client* al *server*, la casistica (c) è senza metodi di difesa, la (d) sfrutta SDN. Nella figura (c) il *delay* medio è 0.27, rispetto a 0.17 nella figura (d), dimostrando una riduzione del 37.03%.

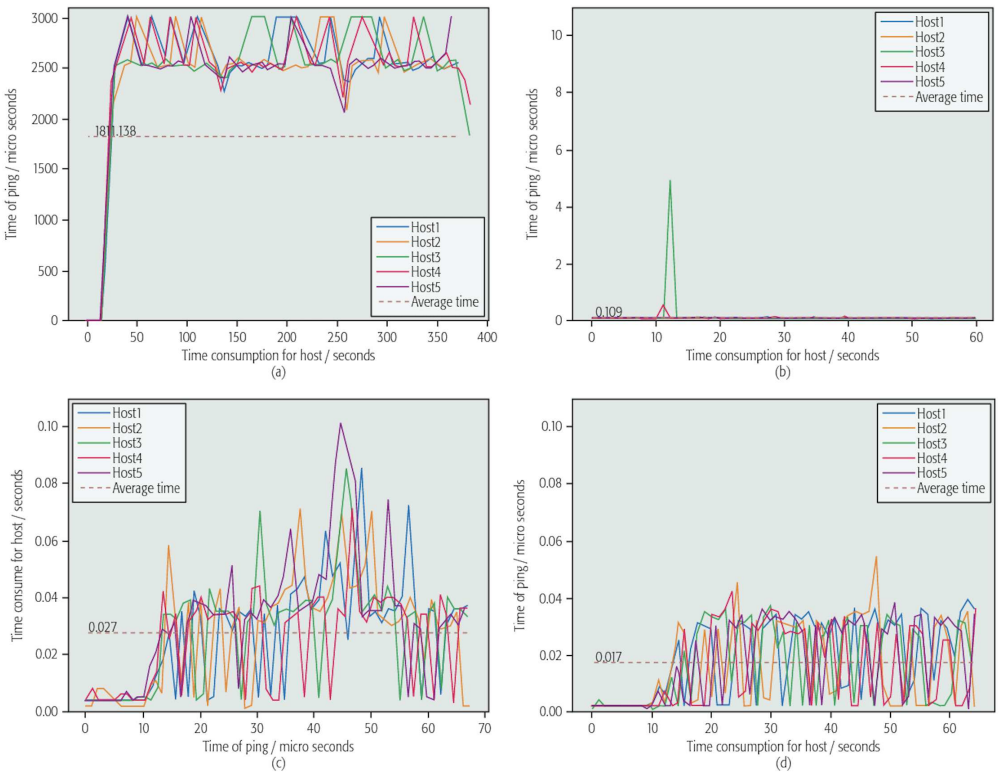

Figura 4.2: Test di efficacia del MLDMF [45]

4.2.2 Phishing

Il phishing è un particolare tipo di attacco informatico in cui colui che lo effettua impersona un altro individuo in modo da aggirare la vittima e ottenere informazioni e credenziali private. Nell'IIoT soprattutto è pericoloso perché una volta compromessa la sicurezza industriale, sono a loro volta compromessi i dipendenti e il business dal punto di vista economico, che possono essere manipolati dalla persona che ha commesso l'attacco. Spesso il movente dietro al phishing è monetario, i dati rubati sono usati per accedere a conti bancari o viene chiesto un riscatto in cambio dei dati ottenuti. Oltre alle conseguenze economiche questo porta a conseguenze operative, l'*hacker* può controllare il funzionamento industriale interrompendo le attività operative e i processi di produzione.

In [33] vengono analizzati i diversi tipi di phishing fra cui:

- *Deceptive phishing*: il criminale impersona un'organizzazione legittima, dopodiché induce la vittima a cliccare su dei link all'apparenza anch'essi legittimi per avere i suoi dati.

- *Man in the middle*: in questo caso il criminale si pone nel mezzo della trasmissione tra la vittima e il sito, così da intercettare le trasmissioni. Solitamente viene usato un *proxy* trasparente, invisibile al *client*, che ottiene i dati sul canale prima di inoltrarli alla destinazione, facendo credere al *client* di star comunicando direttamente con il destinatario previsto.

- *Evil twin*: questo attacco viene effettuato su reti WiFi, la persona che commette l'attacco crea un *hotspot* con il Set Service IDentifier (SSID) uguale a quello della rete che intende impersonare. L'utente poi si connette a questa rete diventando vulnerabile ad attacchi da parte dell'*hacker*, la facilità di questo metodo risiede nel fatto che può essere effettuato senza necessità di *hardware* particolare, ma basta anche solo un PC o addirittura uno smartphone.

- *HTTP phishing*: questo metodo consiste nella condivisione di link malevoli inviati alle vittime, che una volta che ci cliccano sopra vengono reindirizzate a pagine diverse da quelle menzionate da cui poi i loro dati vengono rubati. Questi link vengono spesso condivisi via mail o messaggi, è un metodo molto diffuso di phishing.

- *Domain spoofing*: colui che commette l'attacco impersona un'organizzazione o azienda creando un sito utilizzando un dominio il più simile possibile a quello originale, rendendo anche graficamente il sito fedele a quello vero, così facendo la vittima non si rende conto di aver a che fare con un impostore.

I metodi più semplici e talvolta efficaci per contrastare il phishing riguardano informare le potenziali vittime sui rischi, ad esempio nell'industria è opportuno sensibilizzare il personale su questi pericoli, così che siano in grado di riconoscerli in caso dovessero verificarsi, insegnargli a capire se un sito o una mail è falsa incrementa di molto la sicurezza. Inoltre usare antivirus o sistemmi di filtraggio dei contenuti limita ulteriormente il phishing, ma soprattutto è bene non condividere le proprie informazioni personali con nessuno. Esistono allo stesso tempo altri metodi sviluppati dal lato informatico che contrastano attivamente questo tipo di attacchi, come:

- Approccio basato su *data mining*, *deep learning* e *machine learning*: metodo che analizza gli URL e le pagine corrispondenti, utilizzando modelli di IA allenati per riconoscere URL sospetti. Nel marzo 2020 è stato pubblicato un articolo che propone un algoritmo basato su ML di URL Embedding (UE) [46]. Il suo scopo è di verificare la correlazione tra siti internet analizzando i vari URL tramite algoritmi, così da ottenere un coefficiente di correlazione che ne quantifica il potenziale rischio.

- Approccio Blacklisting-Whitelisting: viene utilizzata una lista nera in cui sono inseriti i domini, URL, siti e link malevoli utilizzati per il phishing. Quando un link deve essere verificato, si controlla la lista nera per assicurarsi che esso non corrisponda totalmente o in parte a voci già esistenti in essa, nel caso in cui risulti dalla lista, viene aggiunto. Tuttavia non può essere riconosciuto se la lista non comprende quella voce. In [37] è stato ideato un metodo che si basa sull'analisi del dominio. Secondo lo studio, il *domain name* è più limitante per il *phisher* rispetto all'URL, che è più modificabile a sua discrezione e quindi più facile da utilizzare per trarre in inganno le vittime, un *domain name* deliberatamente falso e ispirato ad uno reale è più individuabile. Sono stati effettuati numerosi test su vari dataset, raggiungendo un'accuratezza nel riconoscimento in tempo reale di URL utilizzati per phishing del 99,7%.

4.2.3 Attacco alla supply chain

Gli attacchi alle catene di rifornimento industriali sono pericolosi per la continuità operativa e altrettanto difficili da contrastare. Il punto debole di questo aspetto dell'industria risiede principalmente nel fatto che nella quasi totalità delle volte sono coinvolte terze parti, cioè non si occupa la stessa organizzazione di tutti i passi, ma una può gestire la produzione di componenti, una differente li assembla, e un'altra ancora vende il prodotto finale al consumatore. Questo sistema crea problemi di sicurezza, un attacco a un dispositivo diventa molto più difficile da individuare e crea un punto debole in tutta la rete IoT di cui fa parte. Un sistema operativo obsoleto, spesso utilizzato nei dispositivi IoT, può essere soggetto ad attacchi data la mancanza di aggiornamenti che lo rendono meno sicuro, allo stesso modo succede con i dispositivi stessi, che a volte vengono utilizzati per anni senza essere sostituiti.

In [29] vengono indicate delle soluzioni preventive che possono aiutare a contrastare questi tipi di attacchi, a livello di dispositivo, di rete, e di organizzazione:

- Livello dispositivo: effettuare *product assessment*, cioè testare i *device* per assicurarsi del loro corretto funzionamento dal punto di vista della sicurezza, seguendo vari *step* di analisi esaustivi prima di inserirli nella rete; progettare i dispositivi integrandovi sistemi di autenticazione più resistenti come certificati digitali validati da chiavi crittografate, più affidabili rispetto al classico sistema di password; aggiornare i *device* risolvendo i problemi di sicurezza tempestivamente ogni qualvolta vengano rilevati.

- Livello rete: segmentare la rete è un buon metodo di prevenzione, consiste nel separare la rete più critica dal resto per proteggerla; integrare in modo sicuro nuovi elementi nella rete, controllando l'hardware o software prima dell'implementazione, in modo simile al *product assessment* al livello dei dispositivi, e utilizzando firewall per prevenire la propagazione dei danni nella rete; anche i sistemi di allarme sono utili, allertano in caso di eventi che richiedono attenzione nella rete, come cambiamenti improvvisi nei *device*.

- Livello organizzazione: il risk assessment è fondamentale ad ogni livello e per ogni elemento della *supply chain*, devono essere valutati i pericoli attribuendogli un punteggio di importanza; i dispositivi utilizzati devono rispettare gli standard industriali per conformarsi alle necessità di sicurezza; anche in questo ambito l'IA

e ML vengono sfruttate per analizzare il traffico e rilevare eventuali pericoli nella rete in modo intelligente.

In [43] viene proposta una struttura di *supply chain* basata su blockchain per trasmettere dati in modo sicuro fra gli individui che compongono la catena, i dati caricati sulla blockchain sono raccolti dai dispositivi IIoT e salvati tramite *smart contract*, sui quali vengono impostati requisiti di accesso, così facendo solo chi li soddisfa può accedervi e vedere i dettagli della transazione. Quest'ultimo aspetto è realizzato con l'Attribute-Based Encryption (ABE), in particolare Cyphertext-Policy Attribute-Based Encryption (CP-ABE), è un approccio crittografico che permette un accesso granulare ai dati basato su degli attributi predeterminati. Il modello denominato Blockchain-based Supply Chain System (BSCS) aiuta a migliorare vari aspetti della *supply chain*, da quelli di rete a quelli di gestione aziendale.

Nel BSCS sono definiti cinque ruoli (R={Ra, Rs, Rm, Rc, Rr}) con i corrispondenti nodi (N={Na, Ns, Nm, Nc, Nr}):

- *Administrator* (Ra): è l'individuo con la capacità di inizializzare il BSCS, esiste un unico nodo amministratore (Na) nel sistema.
- *Supplier* (Rs): è colui che fornisce le risorse necessarie alle aziende o individui presenti nel BSCS per entrare nel sistema deve ricevere la firma a uso singolo dall'*admin*.
- *Manufacturer* (Rm): si tratta dell'azienda produttrice, per entrare nel sistema deve ricevere una firma a uso singolo dal *supplier*.
- *Carrier* (Rc): il corriere incaricato di trasportare i prodotti fino al luogo concordato, necessita della firma del *manufacturer* per partecipare al sistema.
- *Retailer* (Rr): rappresenta l'intermediario fra l'intero processo di produzione e il consumatore finale col compito di vendergli il prodotto. La firma di accesso gli viene fornita dall'operatore al momento della registrazione al sistema.

I processi nel sistema avvengono in sei passi distinti:

1. l'*admin* del canale di comunicazione inizializza il sistema eseguendo l'algoritmo di *setup* tramite *smart contract*;
2. l'*admin* fornisce le politiche di accesso tramite *smart contract*;

3. le firme del delegatore (l'individuo che ha compiuto l'ultima azione) vengono trasmesse tramite canale sicuro;

4. il *master node* del *supplier*, *manufacturer*, *carrier* o *retailer* si registra usando la firma e fornendo gli attributi per l'ABE;

5. vengono inizializzati anche i nodi figli dei *master node*, che rappresentano i sensori della rete IIoT;

6. i nodi sono in grado di eseguire automaticamente gli *smart contract*, i quali hanno politiche di accesso per assicurarsi che i nodi li possano eseguire; i nodi caricano automaticamente i dati nella blockchain scrivendoli come record su un blocco che viene aggiunto alla catena, i dati possono poi essere scaricati dai nodi che ne hanno accesso, colui che crea transazioni nella blockchain è il *master node*.

Questo modello unisce IIoT, blockchain e ABE per garantire un livello adeguato di privacy e sicurezza durante tutte le fasi della *supply chain*, in questo modo le transazioni possono avvenire in modo sicuro, soprattutto in ambienti decentralizzati dove più operatori si dividono i compiti.

Capitolo 5

Safety

L'IIoT introduce molti vantaggi nell'industria, come l'aumento della produttività ed efficienza con nuovi sistemi tecnologici interconnessi, che permettono l'automazione dei processi e la manutenzione predittiva, al contempo però sorgono nuove sfide dal punto di vista della sicurezza sul posto di lavoro, anche detta "*safety*". L'interazione fra l'uomo e i nuovi dispositivi può creare problemi se l'implementazione dei macchinari non è effettuata correttamente; se si incorre in malfunzionamenti possono nascere numerosi rischi, allo stesso modo i problemi possono derivare da errori di comunicazione fra i dispositivi o errori nel *software*. L'affidabilità dei *device* rappresenta un punto focale nei processi industriali, e per garantirla devono essere effettuati degli *audit*, cioè dei controlli periodici per rilevare problematiche e verificare il corretto funzionamento del sistema; i lavoratori devono essere istruiti sia su come utilizzare gli strumenti sia su come rispondere ad eventuali imprevisti. Grazie ai sistemi IIoT questi processi sono semplificati e più precisi, numerosi *framework* sono stati ideati per aiutare la loro integrazione nell'industria in modo sicuro, ed il loro principale obiettivo è di aiutare a tutelare la salute dei lavoratori in ambienti ad alto rischio come quello minerario o manifatturiero.

5.1 Standard di safety

Sono stati pubblicati nel corso degli anni vari standard che delineano principi e metodologie per assicurare un livello adeguato di *safety*, fra cui l'ISO 31000 sulla gestione del rischio [18] e l'IEC 61508 in relazione all'utilizzo di macchinari [5].

5.1.1 ISO 31000 - Risk management

Si tratta di una norma rilasciata nel 2009 dall'International Organization for Standardization (ISO) che fornisce delle linee guida di carattere generale sull'attuazione di misure di gestione del rischio. Sono definite cinque clausole [22]:

1. Portata: la portata della normativa è definita come ampia e generica, in modo da non sostituire quelle già esistenti e potersi affiancare a quelle future;

2. Termini e definizioni: sono fornite definizioni di 29 termini utilizzati nel documento;

3. Principi: sono elencati 11 principi di gestione del rischio;

4. *Framework*: individua una struttura per l'implementazione della gestione del rischio in azienda;

5. Processo: definisce un processo ciclico di gestione dei rischi.

I principi enfatizzano l'utilità di questo processo gestionale, che crea valore all'interno di un'azienda, deve però essere effettuato in tutte le sue fasi e processi, da quello organizzativo a quello produttivo, ogni figura all'interno di un'organizzazione deve essere consapevole dei rischi e di come rispondervi. Deve anche essere sistematico e ben definito, devono esserci delle regole precise e non ambigue da seguire tenendo conto di tutti i fattori presenti, da quelli umani a quelli tecnologici.

L'obiettivo del *framework* proposto è di aiutare le organizzazioni, ed indica nella sua prima fase (Figura 5.1) come siano necessari impegno e attenta pianificazione su tutti i livelli da parte del settore gestionale [18]. La fase di progettazione (*design*) del *framework* invece richiede la comprensione del contesto interno ed esterno: il contesto interno consiste, ad esempio, negli obiettivi, le politiche, la struttura e i processi dell'organizzazione; il contesto esterno consiste nell'ambiente politico, territoriale e competitivo in cui l'organizzazione si colloca, insieme alle sue relazioni con esso e le influenze che ne possono derivare. Bisogna poi stabilire una politica di gestione del rischio che chiarisce gli obiettivi e l'impegno relativi ad esso; l'organizzazione in seguito assicura che vi sia responsabilità, autorità e adeguate competenze nell'insieme dei processi. Tutto ciò deve essere integrato in ogni processo organizzativo dell'azienda in modo da renderlo efficace, allocando le risorse necessarie. Infine devono essere stabiliti dei meccanismi di comu-

nicazione interna ed esterna per situazioni di bisogno o per mantenere informata ogni parte interessata.

Dopo aver progettato il *framework*, si deve implementare con particolare attenzione, monitorando il suo funzionamento anche nei periodi successivi, e migliorandolo ove necessario e possibile.

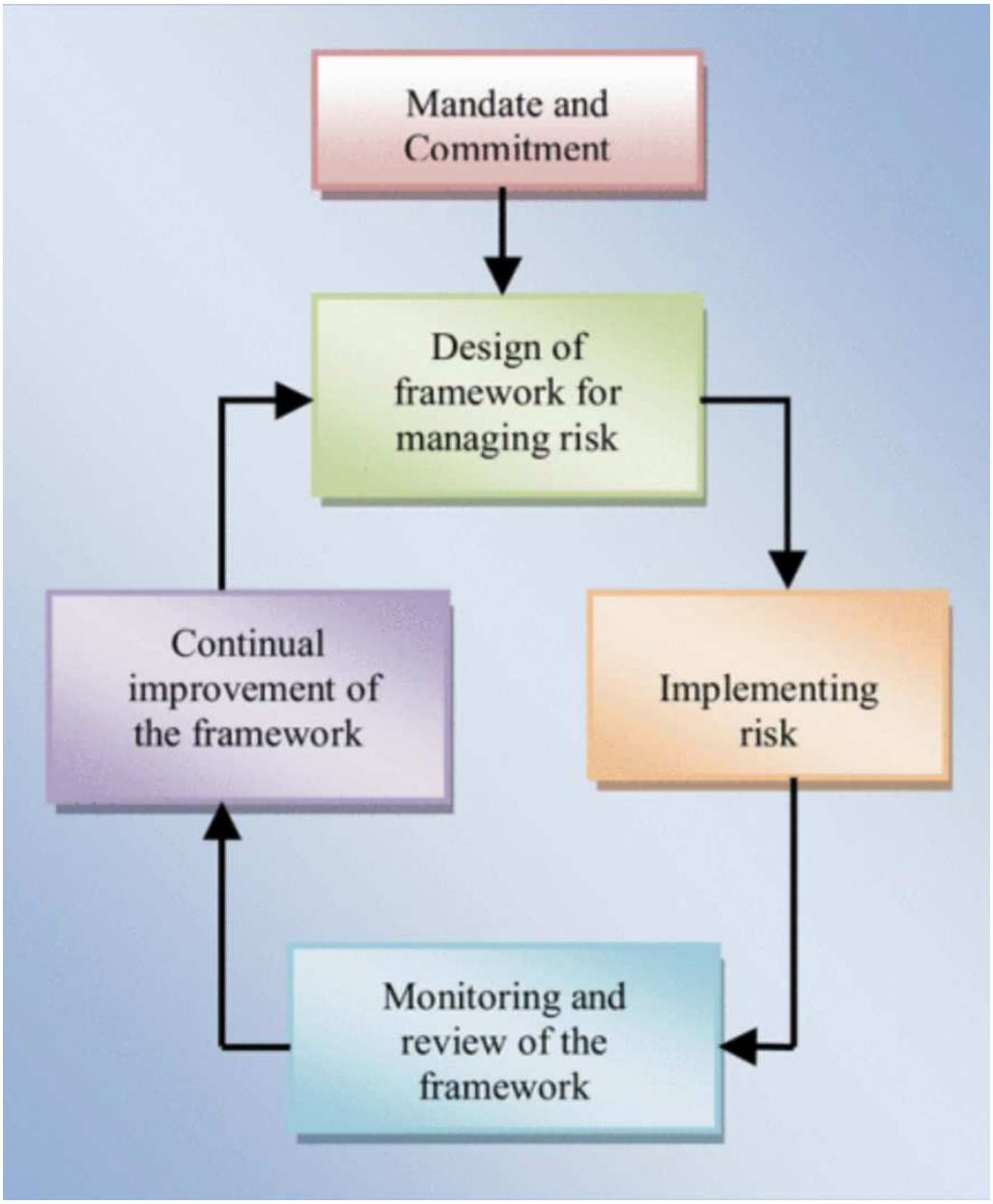

Figura 5.1: Framework di gestione del rischio [10]

Le fasi centrali del processo ciclico di gestione del rischio sono comprese nel *risk assessment*, cioè una valutazione complessiva del rischio in tutte le sue parti (Figura 5.2) [18]:

- Identificazione: l'organizzazione deve identificare tutte le fonti del rischio con le eventuali aree di impatto e potenziali conseguenze, anche se non sono del tutto

definite, bisogna essere più cauti e dettagliati possibile.

- Analisi: è la fase di comprensione del rischio, vengono analizzate le sue cause e conseguenze, sia positive che negative, e la probabilità con cui possono verificarsi. Può essere qualitativa, effettuata in fase preliminare per avere un'analisi generale, o quantitativa e più specifica.

- Valutazione: aiuta a prendere decisioni basandosi sull'analisi effettuata, come la priorità di trattamento di un rischio e il bisogno o meno di trattarlo.

Una volta valutato, il rischio viene trattato, in caso il suo livello residuo non sia tollerabile (cioè dopo tutto il processo rimane ancora un potenziale rischio), viene trattato nuovamente, fino a che il risultato non sia adeguato.

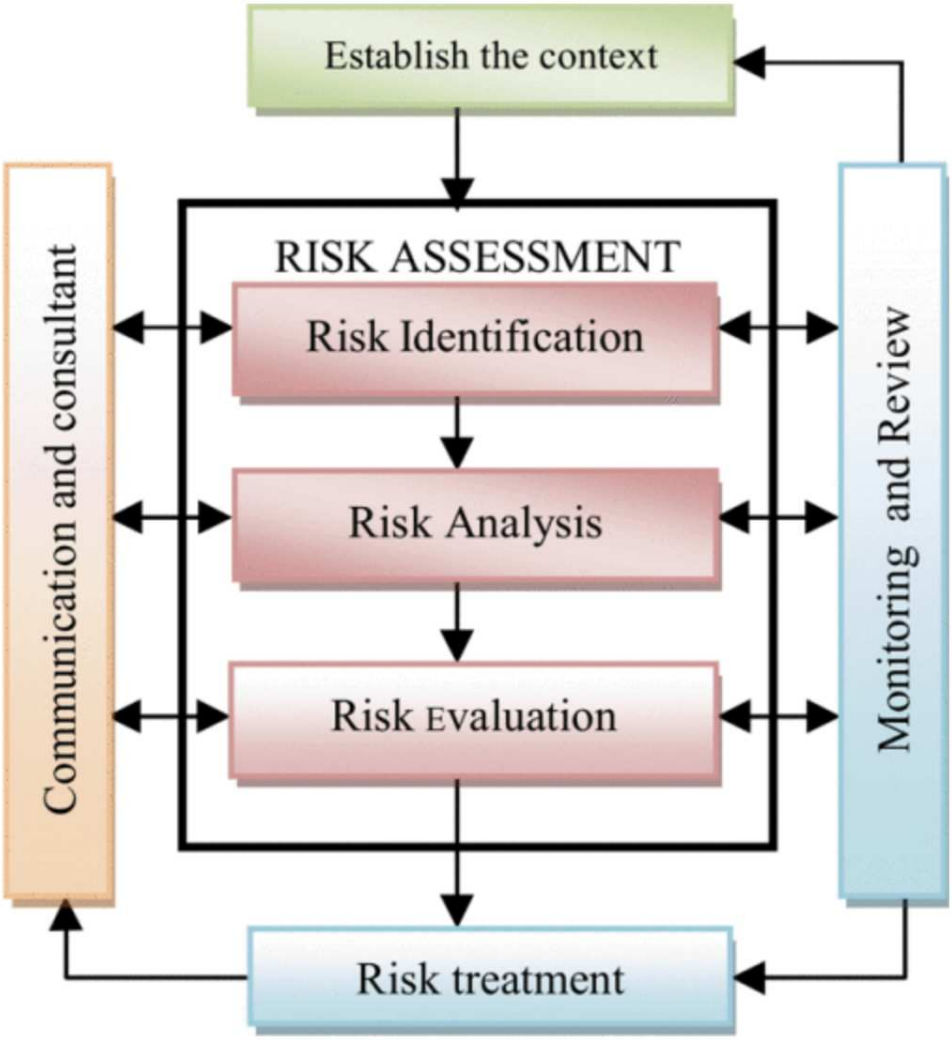

Figura 5.2: Processo di gestione del rischio [10]

5.1.2 IEC 61508

Questo standard ha come obiettivo la definizione di un metodo di implementazione per sistemi relativi alla *safety* basati su tecnologia elettrica/elettronica/elettronica programmabile (E/E/PE). Si tratta di sistemi che in caso di malfunzionamento mettono in pericolo i lavoratori, visto l'ampio utilizzo di sistemi informatici dedicati a questo scopo nell'IIoT, questa normativa è molto utile e importante da rispettare. Alcuni di questi sistemi possono essere antincendio, rilevamento dei gas, arresto d'emergenza di impianti a rischio, o arresto d'emergenza di macchinari operati dall'uomo. In questo documento viene introdotto il concetto di *safety* funzionale [6] definita con la funzione di *safety*, cioè una funzione che deve essere implementata da un sistema E/E/PE relativo alla *safety* per raggiungere o mantenere uno stato sicuro rispetto a uno specifico evento di pericolo. Questa funzione determina come bisogna agire, e se osservata, permette di evitare l'evento di rischio. Un sistema relativo alla *safety* invece è un sistema in grado di portare a termine i requisiti della funzione. Ogni sistema ha un determinato livello di integrità su una scala da 1 a 4, che indica la complessità delle funzioni riesce a compiere, sono denominati Safety Integrity Levels (SILs). Ci sono due modalità basate sulla frequenza di utilizzo che rappresentano come questi sistemi vengono utilizzati: la modalità a bassa domanda (Tabella 5.1) dove la frequenza di utilizzo del sistema è massimo una volta l'anno e non maggiore del doppio della frequenza stabilita nel test di utilizzo (quindi può essere usato di rado, per questo si dice a bassa domanda); la modalità ad alta domanda o continua (Tabella 5.2) prevede utilizzi oltre una volta l'anno o oltre il doppio della frequenza stabilita nel test di utilizzo (può essere utilizzato spesso). Significa dunque che i SILs indicano la soglia di utilizzo del sistema in relazione alla loro modalità di utilizzo, oltre la quale falliscono [5].

Tabella 5.1: Probabilità di fallimento della funzione in un sistema a bassa domanda

Modalità a bassa domanda	
Safety Integrity Level	Probabilità media di fallimento del sistema nel portare a termine la funzione
4	da $>= 10^{(-5)}$ a $< 10^{(-4)}$
3	da $>= 10^{(-4)}$ a $< 10^{(-3)}$
2	da $>= 10^{(-3)}$ a $< 10^{(-2)}$
1	da $>= 10^{(-2)}$ a $< 10^{(-1)}$

Questo standard delinea perciò un approccio basato sul rischio, in cui valuta la funzionalità di un sistema analizzando il rischio di malfunzionamento in relazione alla sua

Tabella 5.2: Probabilità di fallimento della funzione in un sistema ad alta domanda o continuo

Modalità ad alta domanda o continua	
Safety Integrity Level	Probabilità di fallimento all'ora
4	da $>= 10^{(-9)}$ a $< 10^{(-8)}$
3	da $>= 10^{(-8)}$ a $< 10^{(-7)}$
2	da $>= 10^{(-7)}$ a $< 10^{(-6)}$
1	da $>= 10^{(-6)}$ a $< 10^{(-5)}$

efficacia.

5.2 Studio di *framework* e sistemi di *safety* industriali

Sono stati proposti nel corso degli anni diversi framework per l'implementazione della safety all'interno di ambienti industriali, così come sistemi pratici per la gestione di situazioni specifiche in diversi ambiti, da quello minerario a quello manifatturiero. In questa sezione verranno studiati alcuni di essi per mostrare esempi pratici di come gestire e ridurre i rischi in casistiche particolari.

5.2.1 *Public Safety Framework* per IIoT

La *public safety* rappresenta la sicurezza degli individui, lavoratori e non, con lo scopo di salvaguardare la loro salute dai rischi legati ad un posto di lavoro come, ad esempio, l'industria chimica o mineraria, dove se ne possono riscontrare numerosi.

Il framework proposto in [30] , denominato IoTPS, è diviso in quattro strati (Figura 5.3) riconducibili alla suddivisione generale dell'IIoT studiata precedentemente (Sezione 3.2):

- *Data Acquisition Layer*: attraverso i dispositivi IoT installati sui macchinari industriali, vengono raccolti i dati, trasmessi poi allo strato superiore passando per i *gateway*.
- *Edge Computing Layer*: è uno strato intermedio dove vengono processati e monitorati in tempo reale i dati raccolti.
- *Cloud Computing Layer*: qui i dati vengono immagazzinati nel *cloud*, in modo da effettuare analisi a lungo termine e accedervi quando necessario. L'analisi a lungo termine aiuta a studiare più nel dettaglio le informazioni per valutare i rischi.

- *Application Layer*: in questo strato i dati sono accessibili tramite interfaccia utente, possono essere effettuate decisioni di controllo e gestione dei processi, basandosi sulle informazioni raccolte tramite le applicazioni disponibili a questo livello.

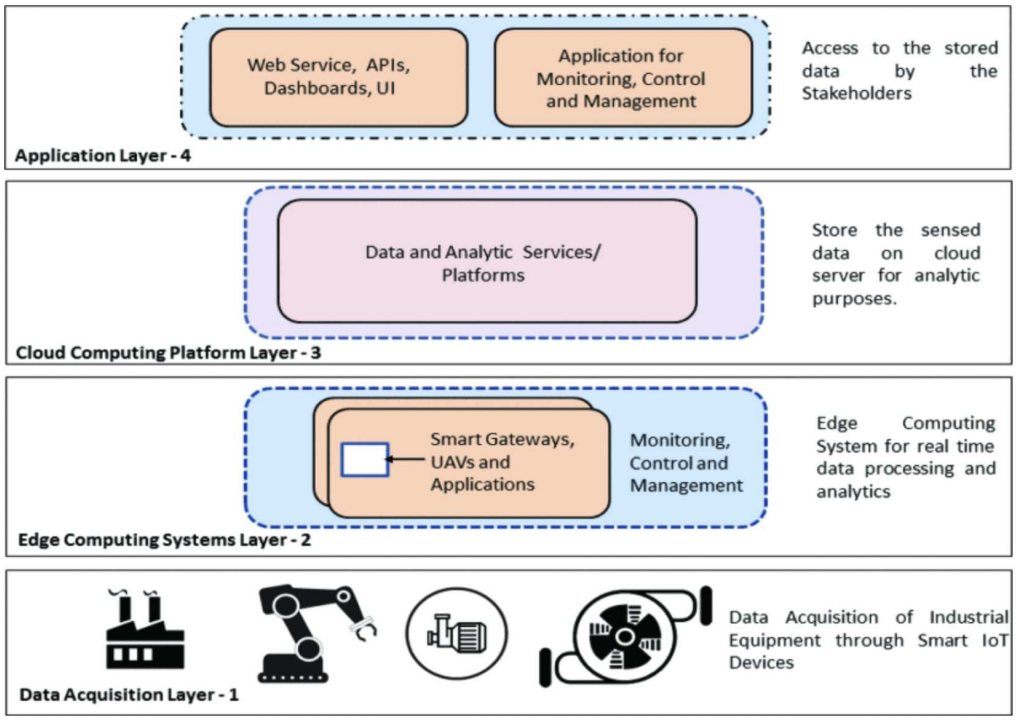

Figura 5.3: Public Safety Framework [30]

Le caratteristiche principali dell'IoTPS descritte in [30] sono:

1. Rilevamento tempestivo di eventi anomali: grazie alla rete di dispositivi comunicanti, eventi anomali come interruzione di servizi, attacchi esterni o problematiche nei macchinari o lavoratori, vengono rilevate in tempi brevi.

2. Generazione di allarmi: in caso di situazioni pericolose, le persone interessate vengono avvertite, fornendo indicazioni e una sensazione di sicurezza.

3. Localizzazione del sito dell'evento e della manodopera: grazie alla consapevolezza della struttura della rete fornita dalla comunicazione fra i dispositivi, si ha una mappatura accurata dell'impianto industriale, consentendo di localizzare il luogo di un evento dannoso in modo facile e rapido.

4. Notifica ai fornitori di servizi di risposta alle emergenze: il *framework* è progettato per inviare messaggi automatizzati agli individui interessati agli eventi pericolosi, come i lavoratori stessi, e i fornitori di servizi di emergenza come polizia, vigili del fuoco e ambulanza.

5. Comunicazione ad-hoc: per mantenere i processi comunicativi attivi in ogni condizione, venogno usati gli Unmanned Aerial Vehicle (UAV), cioè droni che non richiedono il comando umano e che, in caso di problematiche nella rete, consentono il mantenimento delle comunicazioni permettendo all'utente di accedere alla rete usandoli come intermediari.

6. Linee guida per portare al sicuro le persone: le linee guida per rispondere a determinati eventi devono essere precise ed appropriate, per svilupparle è necessario adempiere alla fase di valutazione del rischio in modo esaustivo.

5.2.2 *Safety* nell'industria mineraria

Nell'industria mineraria la sicurezza dei lavoratori è sempre stata un aspetto complesso, dati i pericoli che i lavoratori incontrano ogni giorno. Trattandosi di lavoro svolto per la maggior parte sotto terra, più la distanza dal punto di uscita aumenta, più il rischio cresce, e controllare lo stato di salute di tutto il personale in miniere molto ampie e diradate è estremamente complesso. In [27] viene proposto un sistema di monitoraggio dello stato del personale e dell'ambiente utilizzando dispositivi IIoT basati su tecnologia Long Range Wide Area Network (LoRaWAN) [14]. Si tratta di una tecnologia basata su Low Power Wide Area Network (LPWAN), cioè tecnologie a basso consumo che coprono una vasta area operativa. LoRaWAN supporta anche basse velocità di trasmissione dati, quindi è ottimale per reti IoT con *device* come i sensori che inviano pacchetti di dimensioni ridotte. I bassi costi di implementazione rendono le reti basate su LoRaWAN molto flessibili (adattabili a diversi ambienti) e scalalabili.

Il *framework* ideato in [27], prevede l'utilizzo di tre tipi di sensori: di respirazione, del battito cardiaco e di fumo.

- Sensore di respirazione: posizionato solitamente sui vestiti nella zona dell'addome o del torace in modo saldo, così da rilevare l'espansione e contrazione in fase di inspirazione ed espirazione, per fare ciò il sensore viene posto sul corpo con una cintura in materiale non elastico, se non in piccola parte, questa breve zona elastica serve appunto a misurare l'ampiezza della respirazione. Questo rilevamento aiuta a comprendere lo stato dei polmoni del soggetto e lo stato mentale, lo stress infatti può causare irregolarità nella frequenza di respiro.

- Sensore del battito cardiaco: sono progettati in modo da produrre un segnale digitale in output del battito quando il dito viene posizionato su di esso. Il sensore rileva piccoli cambiamenti di contenuto del sangue nel tessuto del dito, i quali indicano la presenza e frequenza di battito.

- Sensore di fumo: il sensore di gas utilizzato in questo sistema si chiama MQ-8, è molto sensibile e rileva i gas mischiati ad idrogeno presenti nell'aria con un ampio raggio, è dotato di proprietà di anti-interferenza così da non corrompere i dati rilevati a causa di gas diversi dall'idrogeno.

Un esempio di impostazione di rete sensoriale è mostrata nella tabella seguente (Tabella 5.3) [27], che mostra come i valori rilevati dai diversi sensori, se superata una certa soglia (ad esempio una frequenza cardiaca troppo elevata maggiore di 100 battiti al minuto), attivino una segnalazione inviata agli individui interessati, come i soccorsi incaricati di mettere in sicurezza la persona e valutarne le condizioni.

Tabella 5.3: Condizioni di allerta.

Sensore	Valore	Segnale	Stato
Fumo 1	> 500	ON	Anormale
Fumo 1	< 500	OFF	Normale
Fumo 2	> 500	ON	Anormale
Fumo 2	< 500	OFF	Normale
Respiratorio	< 12	ON	Anormale
Respiratorio	> 18	ON	Anormale
Respiratorio	$12 < val < 18$	OFF	Normale
Battito	< 60	ON	Anormale
Battito	> 100	ON	Anormale
Battito	$60 < val < 100$	OFF	Normale

5.2.3 Sistema di risposta alla emergenze nelle aree di produzione

In [26] viene proposto un sistema di *safety* per le officine nell'industria manifatturiera, basato su rilevamento sensoriale e *Machine Learning*. Le aree di produzione industriali possono risultare rischiose, per via dei numerosi macchinari utilizzati e i materiali trattati, la mancata adozione di sistemi di tutela dei lavoratori mette in pericolo il personale e il *business* dell'azienda. I sensori adoperati in questo modello sono di respirazione e movimento, di vibrazione, e Light Detection and Ranging (LIDAR):

- Ultra-Wide Band (UWB): il sensore UWB viene utilizzato per il monitoraggio del processo respiratorio e del movimento. Lavora nella banda 7-9 GHz e il suo scopo è rilevare i movimenti all'interno di un raggio di rilevamento (in questo caso l'officina); i dati sono raccolti in modo alternato, cioè vengono rilevati i movimenti del personale, e quando essi cessano, o è presente una sola persona nell'officina, viene rilevata la respirazione, se nessuno è presente, entrambi i valori saranno a zero. Questa scelta deriva dal fatto che la respirazione è necessario controllarla se l'individuo è solo, dato che in caso di problemi non può essere soccorso da qualcuno nelle vicinanze.

- G-Link-200: si tratta del sensore per il rilevamento delle vibrazioni, è alimentato a batteria e comunica con il *gateway* per la trasmissione di dati tramite tecnologia *wireless*. In Figura 5.4 si notano tre esempi di segnali, il primo da sinistra in cui le vibrazioni sono quasi assenti, il secondo con moderate vibrazioni e il terzo dove sono intense. Essendo un sensore triassiale rileva vibrazioni nelle tre direzioni dello spazio (lunghezza di colore rosso, altezza di colore verde e larghezza di colore blu), per questo motivo sono presenti tre curve.

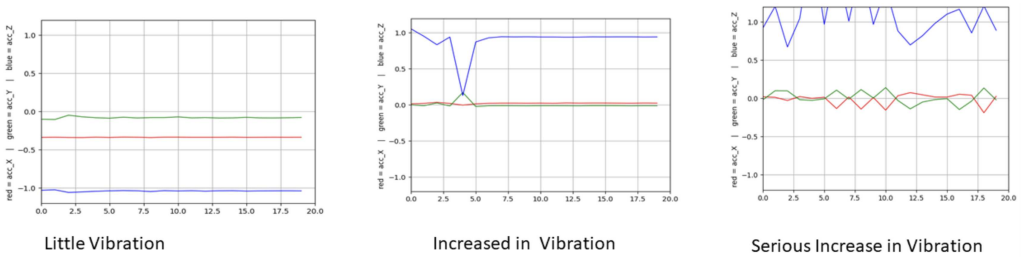

Figura 5.4: Rilevamento dati tramite G-Link-200 [26]

- RP-LIDAR A1: è un sensore LIDAR sviluppato da RoboPeak adottato nel modello proposto, è usato per localizzare il lavoratore in un raggio a 360 gradi fino a 100 metri a seconda dell'ambiente. L'output dei dati raccolti è la distanza dell'individuo dal sensore, la sua angolazione, la qualità della misurazione e il *flag* di inizio rilevamento (booleano). Di questi, la distanza e l'angolazione sono i dati rilevanti per identificare la posizione dell'operaio.

Il funzionamento di questa rete dipende dall'analisi dei dati rilevati da tutti questi sensori: il sensore UWB rileva il movimento indicandolo con un coefficiente che varia da 100 a 4800 (a seconda del numero di persone e del tipo di movimento) se è presente più di un lavoratore con un coefficiente di rilevamento della respirazione a 0 (come detto

in precedenza non controlla la respirazione se rileva già il movimento). Conta, se il lavoratore è isolato, il numero di respiri al minuto (dato variabile dai 6 ai 40), e allo stesso tempo il sensore LIDAR ha il compito di angolare la sua posizione, tutto questo consente di controllare lo stato di una persona isolata; il sensore di vibrazione aiuta a capire se un oggetto o una persona è caduta individuando quindi situazioni di eventuale pericolo.

Per l'analisi dei dati viene utilizzata una Convolutional Neural Network (CNN), spesso adottata in sistemi di riconoscimento facciale, classificazione delle immagini e individuazione di *pattern* comportamentali. La rete neurale descritta in questo sistema è formata da più strati con ruoli differenti come l'estrazione e la mappatura delle caratteristiche.

Per essere utilizzabili dal CNN, i dati devono prima essere processati e trasformati in un formato da essa elaborabile, ovvero un'immagine, da cui vengono poi estratte le caratteristiche fondamentali dei dati su cui operare, una volta estratte vengono classificate (Figura 5.5).

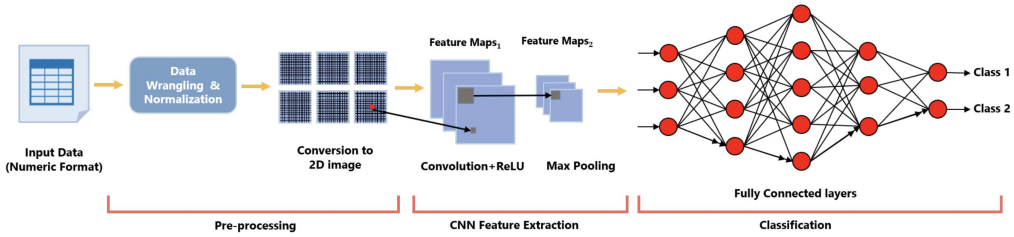

Figura 5.5: Processo di analisi dati con CNN [26]

In (Figura 5.6) è riportata l'accuratezza nei rilevamenti del modello basato su CNN in fase di *training* e validazione, dimostrando un'elevata efficienza.

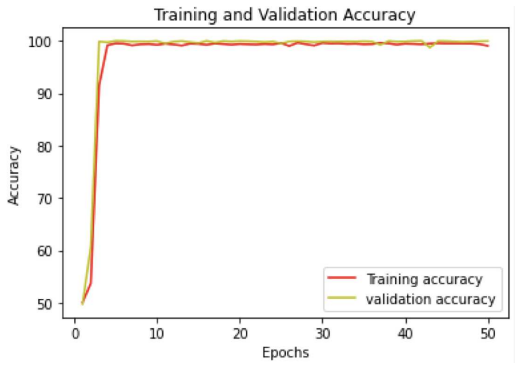

Figura 5.6: Accuratezza del modello CNN [26]

Capitolo 6

Conclusioni

In questo elaborato sono stati analizzati i principi fondamentali e il funzionamento pratico delle reti IoT, con particolare attenzione all'IIoT. La sua utilità risiede nel fornire la possibilità di creare ambienti intelligenti e comunicanti in ambiti industriali, consentendo di aumentare la produttività garantendo allo stesso tempo la sicurezza. Quest'ultima deve essere osservata sia nell'ambito informatico che fisico, la protezione da attacchi *hacker* assicura la continuità del *business* aziendale, e l'utilizzo di nuove tecnologie come *Blockchain* e *Machine Learning* possono essere implementate nelle reti IIoT per adempiere allo scopo. La diffusione di attacchi DDoS che sfruttano ad esempio il *botnet* Mirai, o il *Phishing* che attacca principalmente facendo leva sulla disattenzione o fiducia umana nel prossimo, e quelli alla *Supply Chain* con ripercussioni su tutta la catena operativa, rappresentano alcuni dei pericoli maggiori per l'industria. Lo studio dei *framework* di sicurezza effettuato in questo documento ha lo scopo di presentare delle soluzioni a queste problematiche ponendo l'attenzione su più ambienti. Allo stesso modo ci sono varie architetture di rete conformi agli standard sulla *safety* e la gestione del rischio (ISO 31000 e IEC 61508) per mantenere il luogo di lavoro sicuro, preparandosi adeguatamente alle fasi di risposta e prevenzione di eventi imprevisti e salvaguardando la salute dei lavoratori. Il ruolo dell'IIoT sotto questo aspetto è contribuire a migliorare in modo sostanziale la tutela del personale; varie industrie mettono in pericolo i dipendenti, talvolta non per disattenzioni o poco riguardo per la sicurezza, ma per la natura stessa del lavoro svolto, perciò affiancargli degli strumenti che monitorano il loro stato di salute come i sensori di rilevamento del battito cardiaco o della respirazione, e metodi di automazione dei soccorsi o di allerta può avere un grande impatto positivo.

Acronimi

IoT Internet of Things

IIoT Industrial Internet of Things

RFID Radio Frequency IDentification

IP Internet Protocol Address

IAB Internet Architecture Board

ASP Application Service Provider

UDP User Datagram Protocol

TCP Transmission Control Protocol

CoAP Constrained Application Protocol

SDN Software-Defined Networking

WSN Wireless Sensor Networks

ML Machine Learning

PoW Proof of Work

PoS Proof of Stake

IA Intelligenza Artificiale

API Application Programming Interface

CMfg Cloud Manufacturing

CIA Confidentiality Integrity Availability

DES Data Encryption Standard

TDES Triple DES

AES Advanced Encryption Standard

RSA Rivest-Shamir-Adleman

DSA Digital Signature Algorithm

ECC Elliptical Curve Cryptography

SHA Secure Hash Algorithm

DOA Data Owners Application

DCAs Data Consumer Applications

CSS Cloud Storage Service

DOs Data Owners

DCs Data Consumers

P2PFS Peer to Peer File System

DDoS Distributed Denial of Service

CnC Command and Control server

MLDMF Multi-Level DDoS Mitigation Framework

SDNIGWs SDN-based IIoT Gateways

IMCU IIoT Management Control Unit

CDM Collect-Detect-Mitigate

HDR Honeypot-Detect-React

CDFM Cloud-Detect-Fog-Mitigate

SSID Set Service IDentifier

UE URL Embedding

ABE Attribute-Based Encryption

CP-ABE Cyphertext-Policy Attribute-Based Encryption

BSCS Blockchain-based Supply Chain System

ISO International Organization for Standardization

SIL Safety Integrity Level

UAV Unmanned Aerial Vehicle

LoRaWAN Long Range Wide Area Network

LPWAN Low Power Wide Area Network

LIDAR Light Detection and Ranging

UWB Ultra-Wide Band

CNN Convolutional Neural Network

Bibliografia

[1] Tommaso Addabbo, Ada Fort, Marco Mugnaini, Lorenzo Parri, Stefano Parrino, Alessandro Pozzebon, and Valerio Vignoli. An IoT Framework for the Pervasive Monitoring of Chemical Emissions in Industrial Plants. In *2018 Workshop on Metrology for Industry 4.0 and IoT*, pages 269–273, 2018. doi:10.1109/METROI4.2018.8428325.

[2] Monika Agrawal and Pradeep Mishra. A comparative survey on symmetric key encryption techniques. *International journal on computer science and engineering*, 4(5):877, 2012.

[3] Sarah A. Al-Qaseemi, Hajer A. Almulhim, Maria F. Almulhim, and Saqib Rasool Chaudhry. IoT architecture challenges and issues: Lack of standardization. In *2016 Future Technologies Conference (FTC)*, pages 731–738, 2016. doi:10.1109/FTC.2016.7821686.

[4] Kevin Ashton et al. That 'internet of things' thing. *RFID journal*, 22(7):97–114, 2009.

[5] Ron Bell. Introduction to IEC 61508. In *Acm international conference proceeding series*, volume 162, pages 3–12. Citeseer, 2006.

[6] Simon Brown. Overview of IEC 61508 Design of electrical/electronic/programmable electronic safety-related systems. *Computing and Control Engineering Journal*, 11(1):6–12, 2000.

[7] Naresh Babu Bynagari. Industrial Application of Internet of Things. *Asia Pacific Journal of Energy and Environment*, 3(2):75–82, 2016.

[8] Lucas Santos Dalenogare, Guilherme Brittes Benitez, Néstor Fabián Ayala, and Alejandro Germán Frank. The expected contribution of industry 4.0 technologies for industrial performance. *International Journal of production economics*, 204:383–394, 2018.

[9] Liyanage C De Silva, Chamin Morikawa, and Iskandar M Petra. State of the art of smart homes. *Engineering Applications of Artificial Intelligence*, 25(7):1313–1321, 2012.

[10] Tati Ernawati, Suhardi, and Doddi R. Nugroho. IT risk management framework based on ISO 31000:2009. In *2012 International Conference on System Engineering and Technology (ICSET)*, pages 1–8, 2012. doi:10.1109/ICSEngT.2012.6339352.

[11] Xenofon Foukas, Georgios Patounas, Ahmed Elmokashfi, and Mahesh K. Marina. Network Slicing in 5G: Survey and Challenges. *IEEE Communications Magazine*, 55(5):94–100, 2017. doi:10.1109/MCOM.2017.1600951.

[12] Arthur Gervais, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 3–16, 2016.

[13] Carles Gomez and Josep Paradells. Wireless home automation networks: A survey of architectures and technologies. *IEEE Communications Magazine*, 48(6):92–101, 2010. doi:10.1109/MCOM.2010.5473869.

[14] Jetmir Haxhibeqiri, Eli De Poorter, Ingrid Moerman, and Jeroen Hoebeke. A survey of LoRaWAN for IoT: From technology to application. *Sensors*, 18(11):3995, 2018.

[15] Brian Hayes. Cloud computing, 2008.

[16] Naser Hossein Motlagh, Mahsa Mohammadrezaei, Julian Hunt, and Behnam Zakeri. Internet of Things (IoT) and the energy sector. *Energies*, 13(2):494, 2020.

[17] Marco Iansiti, Karim R Lakhani, et al. The truth about blockchain. *Harvard business review*, 95(1):118–127, 2017.

[18] I Iso et al. Risk management–Principles and guidelines. *International Organization for Standardization, Geneva, Switzerland*, 2009.

[19] Benish Sharfeen Khan, Sobia Jangsher, Ashfaq Ahmed, and Arafat Al-Dweik. URLLC and eMBB in 5G Industrial IoT: A Survey. *IEEE Open Journal of the Communications Society*, 3:1134–1163, 2022. doi:10.1109/OJCOMS.2022.3189013.

[20] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. DDoS in the IoT: Mirai and Other Botnets. *Computer*, 50(7):80–84, 2017. doi:10.1109/MC.2017.201.

[21] Heiner Lasi, Peter Fettke, Hans-Georg Kemper, Thomas Feld, and Michael Hoffmann. Industry 4.0. *Business & information systems engineering*, 6:239–242, 2014.

[22] Matthew Leitch et al. ISO 31000: 2009-The new international standard on risk management. *Risk analysis*, 30(6):887, 2010.

[23] Bin Liu, Xiao Liang Yu, Shiping Chen, Xiwei Xu, and Liming Zhu. Blockchain Based Data Integrity Service Framework for IoT Data. In *2017 IEEE International Conference on Web Services (ICWS)*, pages 468–475, 2017. doi:10.1109/ICWS.2017.54.

[24] Akseer Ali Mirani, Gustavo Velasco-Hernandez, Anshul Awasthi, and Joseph Walsh. Key challenges and emerging technologies in industrial IoT architectures: A review. *Sensors*, 22(15):5836, 2022.

[25] Radouan Ait Radouan Ait Mouha et al. Internet of things (IoT). *Journal of Data Analysis and Information Processing*, 9(02):77, 2021.

[26] Cosmas Ifeanyi Nwakanma, Fabliha Bushra Islam, Mareska Pratiwi Maharani, Jae-Min Lee, and Dong-Seong Kim. Detection and classification of human activity for emergency response in smart factory shop floor. *Applied Sciences*, 11(8):3662, 2021.

[27] T. Porselvi, Sai Ganesh CS, Janaki B, Priyadarshini K, and Shajitha Begam S. IoT Based Coal Mine Safety and Health Monitoring System using LoRaWAN. In *2021 3rd International Conference on Signal Processing and Communication (ICPSC)*, pages 49–53, 2021. doi:10.1109/ICSPC51351.2021.9451673.

[28] Tie Qiu, Jiancheng Chi, Xiaobo Zhou, Zhaolong Ning, Mohammed Atiquzzaman, and Dapeng Oliver Wu. Edge Computing in Industrial Internet of Things: Architecture, Advances and Challenges. *IEEE Communications Surveys & Tutorials*, 22(4):2462–2488, 2020. doi:10.1109/COMST.2020.3009103.

[29] V Venkateswara Rao, R Marshal, and K Gobinath. The IoT Supply Chain Attack Trends-Vulnerabilities and Preventive Measures. In *2021 4th International Con-*

ference on Security and Privacy (ISEA-ISAP), pages 1–4, 2021. doi:10.1109/ISEA-ISAP54304.2021.9689704.

[30] Faheem Reegu, Wazir Zada Khan, Salwani Mohd Daud, Quratulain Arshad, and Nasrullah Armi. A Reliable Public Safety Framework for Industrial Internet of Things (IIoT). In *2020 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET)*, pages 189–193, 2020. doi:10.1109/ICRAMET51080.2020.9298690.

[31] Al Reshan and Mana Saleh. IoT-based Application of Information Security Triad. *International Journal of Interactive Mobile Technologies*, 15(24), 2021.

[32] Karen Rose, Scott Eldridge, and Lyman Chapin. The internet of things: An overview. *The internet society (ISOC)*, 80(15):1–53, 2015.

[33] Ashina Sadiq, Muhammad Anwar, Rizwan A Butt, Farhan Masud, Muhammad K Shahzad, Shahid Naseem, and Muhammad Younas. A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0. *Human behavior and emerging technologies*, 3(5):854–864, 2021.

[34] Seref Sagiroglu and Duygu Sinanc. Big data: A review. In *2013 International Conference on Collaboration Technologies and Systems (CTS)*, pages 42–47, 2013. doi:10.1109/CTS.2013.6567202.

[35] Fahad Saleh. Blockchain without waste: Proof-of-stake. *The Review of financial studies*, 34(3):1156–1190, 2021.

[36] Jothi Prasanna Shanmuga Sundaram, Wan Du, and Zhiwei Zhao. A Survey on LoRa Networking: Research Problems, Current Solutions, and Open Issues. *IEEE Communications Surveys & Tutorials*, 22(1):371–388, 2020. doi:10.1109/COMST.2019.2949598.

[37] Hossein Shirazi, Bruhadeshwar Bezawada, and Indrakshi Ray. "Kn0w Thy Doma1n Name" Unbiased Phishing Detection Using Domain Name Based Features. In *Proceedings of the 23nd ACM on symposium on access control models and technologies*, pages 69–75, 2018.

[38] Pushkar Singh and Sanghamitra Saikia. Arduino-based smart irrigation using water flow sensor, soil moisture sensor, temperature sensor and ESP8266 WiFi module.

In *2016 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, pages 1–4. IEEE, 2016.

[39] Emiliano Sisinni, Abusayeed Saifullah, Song Han, Ulf Jennehag, and Mikael Gidlund. Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Transactions on Industrial Informatics*, 14(11):4724–4734, 2018. doi:10.1109/TII.2018.2852491.

[40] Fei Tao, Ying Cheng, Li Da Xu, Lin Zhang, and Bo Hu Li. CCIoT-CMfg: Cloud Computing and Internet of Things-Based Cloud Manufacturing Service System. *IEEE Transactions on Industrial Informatics*, 10(2):1435–1442, 2014. doi:10.1109/TII.2014.2306383.

[41] Hannes Tschofenig, Jari Arkko, Dave Thaler, and Danny R. McPherson. Architectural Considerations in Smart Object Networking. RFC 7452, March 2015. URL: https://www.rfc-editor.org/info/rfc7452, doi:10.17487/RFC7452.

[42] R. Weinstein. RFID: a technical overview and its application to the enterprise. *IT Professional*, 7(3):27–33, 2005. doi:10.1109/MITP.2005.69.

[43] Quansi Wen, Ying Gao, Zhiling Chen, and Dapeng Wu. A Blockchain-based Data Sharing Scheme in The Supply Chain by IIoT. In *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, pages 695–700, 2019. doi:10.1109/ICPHYS.2019.8780161.

[44] Wenfeng Xia, Yonggang Wen, Chuan Heng Foh, Dusit Niyato, and Haiyong Xie. A Survey on Software-Defined Networking. *IEEE Communications Surveys & Tutorials*, 17(1):27–51, 2015. doi:10.1109/COMST.2014.2330903.

[45] Qiao Yan, Wenyao Huang, Xupeng Luo, Qingxiang Gong, and F. Richard Yu. A Multi-Level DDoS Mitigation Framework for the Industrial Internet of Things. *IEEE Communications Magazine*, 56(2):30–36, 2018. doi:10.1109/MCOM.2018.1700621.

[46] Xiaodan Yan, Yang Xu, Baojiang Cui, Shuhan Zhang, Taibiao Guo, and Chaoliang Li. Learning URL Embedding for Malicious Website Detection. *IEEE Transactions on Industrial Informatics*, 16(10):6673–6681, 2020. doi:10.1109/TII.2020.2977886.

[47] Chen Yang, Weiming Shen, and Xianbin Wang. Applications of Internet of Things in manufacturing. In *2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pages 670–675, 2016. doi:10.1109/CSCWD.2016.7566069.

[48] Muneer Bani Yassein, Shadi Aljawarneh, Ethar Qawasmeh, Wail Mardini, and Yaser Khamayseh. Comprehensive study of symmetric key and asymmetric key encryption algorithms. In *2017 international conference on engineering and technology (ICET)*, pages 1–7. IEEE, 2017.

[49] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer networks*, 52(12):2292–2330, 2008.

[50] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi. Internet of Things for Smart Cities. *IEEE Internet of Things Journal*, 1(1):22–32, 2014. doi:10.1109/JIOT.2014.2306328.

[51] Weiqin Zou, David Lo, Pavneet Singh Kochhar, Xuan-Bach Dinh Le, Xin Xia, Yang Feng, Zhenyu Chen, and Baowen Xu. Smart Contract Development: Challenges and Opportunities. *IEEE Transactions on Software Engineering*, 47(10):2084–2106, 2021. doi:10.1109/TSE.2019.2942301.