

- EMAIL: NELL'OGGETTO METTERE [IoT-2024]
- ESAME: 90 MINUTI, SCRITTO, 16 A CROCETA (2 PUNTI)
SE SI SBAGLIA -0,66, NON RISPOSTA 0
- 23 FEB 10 AM
6 FEB 2 PM
18 GIUGNO 2 PM
3 SET 2 PM
- LIBRO: INTERNET OF THINGS: CONCEPTS AND SYSTEM DESIGN → MILAN MILENKOVIC

CAPITOLO 1

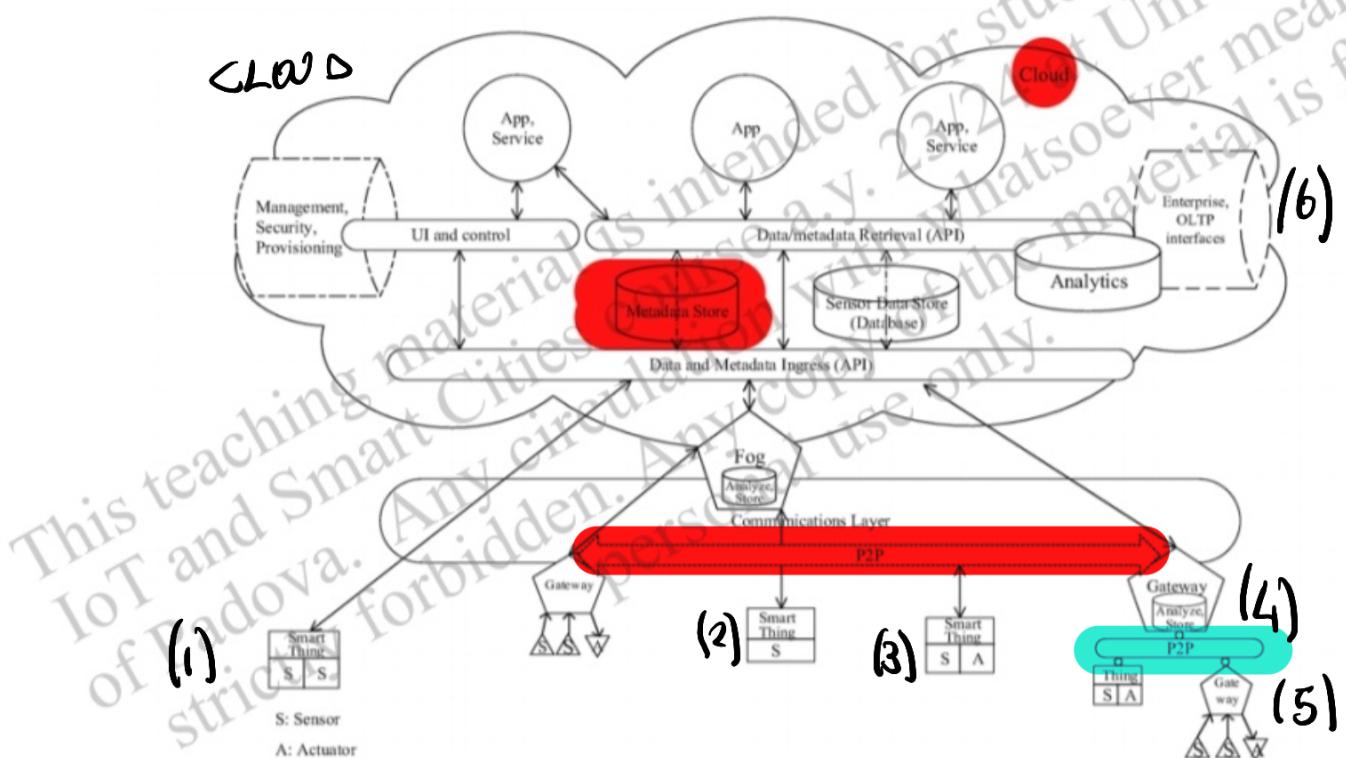
- Cos'è l'IoT!
- L'INTERNET OF THINGS È UNA QUALCOSA CHE MOSTRA = COME A OGNI "THING", REALE O VIRTUALE, È ASSEGNA = TO UN IPV6 E PUÒ ESSERE RAGGIUNTO ATTRAVERSO IL PROTOCOLLO STANDARD IP.
- IoT SYSTEM MODEL
- IL MODELLO IoT SI DIVIDE IN 2 PIANI PRINCIPALI CHE SVOLGONO FUNZIONI DIFFERENTI:
 - CONTROL PLANE: RAPPRESENTA IL PIANO DI CONTROLLO CHE INCORPORA TUTTO CIÒ LEGATO AD ESSO.
 - DATA PLANE: UN KEEPER FA =

NO PARTE DEL CONTROL PLANE
POICHE' DETERMINA DOVE
ANDRA' UN DETERMINATO PAC-
CETTO.

- DATA PLANE: RISPONDE ALLA DOMANDA "COME?"
I PACCHI VENGONO TRASPORTATI,
SI OCCUPA QUINDI SU QUALI ROUTER
FARLI PASSARE, VIENE DEFINITO
ANCHE FORWARDING PLANE.

MODELLO FONDAMENTALE IoT

IoT systems: a functional overview



- AGGIANO DIVERSI TIPI DI THING, ALCUNI POSSONO COMUNICARE DIRETTAMENTE CON IL CLOUD, COME AD ESEMPIO (1) CHE HA DUE SENSORI; ALTRI CON IL FOG, CHIAMATO ANCHE "EDGE SERVER", come (2).

POSSIAMO ANCHE AVERE UN MESH NETWORK DOVE I THING COMUNICANO TRA LORO ATTRAVERSO UN P2P NETWORK come (3).

A VOLTE PUÒ CAPITARE DI AVERE SITUAZIONI come (4) IN CUI: SI COLLEGANO SIMULTANEAEMENTE CON UN P2P, E' IL GATEWAY VERSO IL CLOUD DI UN ALTRO P2P DOVE ALL'INTERNO C'È UN'ALTRO GATEWAY A CUI SONO COLLEGATI DIRETTAMENTE SENSORI E ATTUATORI, come (5).

- SPOSTANDOCI NEL CLOUD INVECE, PARTEndo DA DESTRA NOTIAMO COME IN (6) SIA PRESENTE L'**OLTP** (ON-LINE TRANSACTION PROCESSING INTERFACES), CHE RAPPRESENTA NODI DIVERSSI PER INTERAGIRE CON UN SISTEMA, AD ESEMPIO BENCH SYSTEM, ATOMIC SYSTEM (UNA TRANSAZIONE ALLA VOLTA).

NEL CLOUD c'è ANCHE L'**ANALYTICS** CHE HA AL L'INTERNO ALGORITMI DI MACHINE LEARNING ETC.. DA UNA DELLE COSE PIÙ IMPORTANTI SONO I **DATABASE**, UNO È DESTINATO AI **METADATA** (SONO DATI DI CONTOREO CHE SERVONO A IDENTIFICARE IL PEZZO, COME AD ESEMPIO IL NUMERO DI SERIE) E L'ALTRO È DESTINATO AI **SENSOR DATA** VERI E PROPRI COME TEMPERATURE ETC... OSSIA I DATI RILEVATI. UN'ALTRA COMPONENTE IMPORTANTE È L'**API** OSSIA IL BUS CHE PERMETTE DI TRASPORTARE I DATI IN INGRESSO DAI SENSORI AI DATABASE (CHE RAPPRESENTANO LA MAGGIOR PARTE DEL DATA FLOW) MA ANCHE DI INVIARE I COMANDI DAL CLOUD AI SENSORI (PARTE MINORE DI DATA FLOW).

C'è un' **API** ANCHÉ CHE FA COMUNICARE APP E

API SERVICE CON I DATI ANNUSE.
L'ULTIMA PARTE IMPORTANTE È QUELLA DAVVOLTA
FESTIVAMENTE L'USER DEL CLOUD PUÒ LAVORARE ED È
È COMPOSTO DA MANAGEMENT, SECURITY E PROVISIONING
È INOLTRE DAL UI E CONTROL BUS (AD ESEMPIO VUO
LE MODIFICARE LA TEMPERATURA, O AGGIUNGERE UN NODO).

- **INFORMAZIONI IMPORTANTI AGGIUNTIVE DEL CAP.**
- ESISTONO DUE GRANDI DIVISIONI DELL'IOT:
 - **Critical IoT:** CI APPARTENGONO I SENSORI CON BASSA LATENZA, ULTRA RELIABILITY, BUON NUMERO DI DISPOSITIVI MA NON ENORME E UN COSTO LEGGERMENTE MAGGIORE DEI DISPOSITIVI CLASSICI.
 - ↑
 - CENTRALI NUCLEARI
 - DRONI
 - VR
 - **Massive IoT:** CI APPARTENGONO I DISPOSITIVI SENZA GARANZIA DI TIEMPO, SENZA GARANZIA DI RELIABILITY, SMART CITIES, SMART AGRICOLTURE PRODOTTI IN QUANTITÀ MASSIVE E A COSTO BASSO.
- NELL'IOT INOLTRE IL NUMERO DI SERVER È MAGGIORATO DEL NUMERO DI CLIENT, SI PARLA DI "INVERSE CLIENT TO SERVER RATIO".

CAPITOLO 2

- **IOT EDGE DEVICE**
- POSSONO ESSERE VISTI COME OGGETTI AL CONFINE TRA IL MONDO CYBER E QUELLO FISICO POICHÉ A FRONTE DI FENOMENI REALI,ESSI LI TRASFORMANO

IN DATI NEGLI TALI.

ALCUNI DI ESSI NON HANNO ABBASTANZA CAPACITÀ DI CALCOLO PER CONNETTERSI E INVIARE LE INFORMAZIONI, PER CIÒ SPESO SI AFFIDANO AL GATEWAY PER LA GESTIONE DEI DATI.

LE UNICHE FUNZIONI SVOLTE IN GENERE SONO:

- PRODURRE I RISULTATI DELLE MISURAZIONI ATTRAVERSO SEGNALI ELETTRICI;
- CONDIZIONAMENTO DEL SEGNALE, TRASFORMAZIONI E TRASFORMAZIONI A DIGITALE
- CONVERSIONE DI VALORI DIGITALI IN UNITÀ INGEGNERISTICHE.

TUTTI QUESTI SEGNALI VENGONO INVIAZI TRAMITE SERIAL BUS COME "SPI" O "I2C"

• INDUSTRIAL SENSORS & PLC

• L'INDUSTRIA DELL'AUTOMAZIONE HA STANDARDIZZATO I RAIL-MOUNTED SENSOR CON 12-24V DC E AC DI TENSIONE NOMINALE, E 4-20 mA CORRENTE NOMINALE COME SEGNALI.

ESSI POSSONO ESSERE GIÀ FORNITI CON INTERFACCIE DIGITALIZZATE VIA I2C O SPI.

QUESTI SENSORI E/O ATTUATORI POSSONO ESSERE CONNESSI AL PLC VIA I/O PORTS E MODULATI PERSEGNAKI ANALOGICI O DIGITALI.

• UN PLC È UN DISPOSITIVO PROGRAMMABILE CON INPUT E OUTPUT PINS E CONTROLLA UN ADC INTEGRATO E INOLTRE PRESENTA UN CONVERTITORE DAC PER OUTPUT ANALOGICI.

PER COMUNICARE CON ALTRI ELEMENTI UTILIZZA

NUOVI BUS INDUSTRIALI COME FIELD BUS, PRODBUS,
BACNET E PROFIBUS.

LE GERARCHIE DI QUESTI COMPONENTI FORMANO
CIO' CHE VIENE DETTO UN "DISTRIBUTED CONTROL
SYSTEM" O "DCS" CHE PUO' INCLUDERE UN
SISTEMA DETTO "SUPERVISORY CONTROL AND DATA
ACQUISITION" O "SCADA" PER LA VISUALIZZAZIONE
NEGLI UNGHE DEL PRODOTTO, O IL CONTROLLO
"PLANT-LEVEL".

- PER INTERFAZZIARSI CON QUESTI DISPOSITIVI E CON I
LORO DCS, MOLTI GATEWAY INCLUDONO SPECIALE
INTERFACCIE COME: RS 485, RS-232, RS-
422 E ETHERNET INDUSTRIALE, SONO SPESO
ACCOPPIATI CON PROTOCOLLI DI CONVERSAZIONE PER
LE COMUNICAZIONI INDUSTRIALI.

• **EDGE-NODE FUNCTIONALITY**

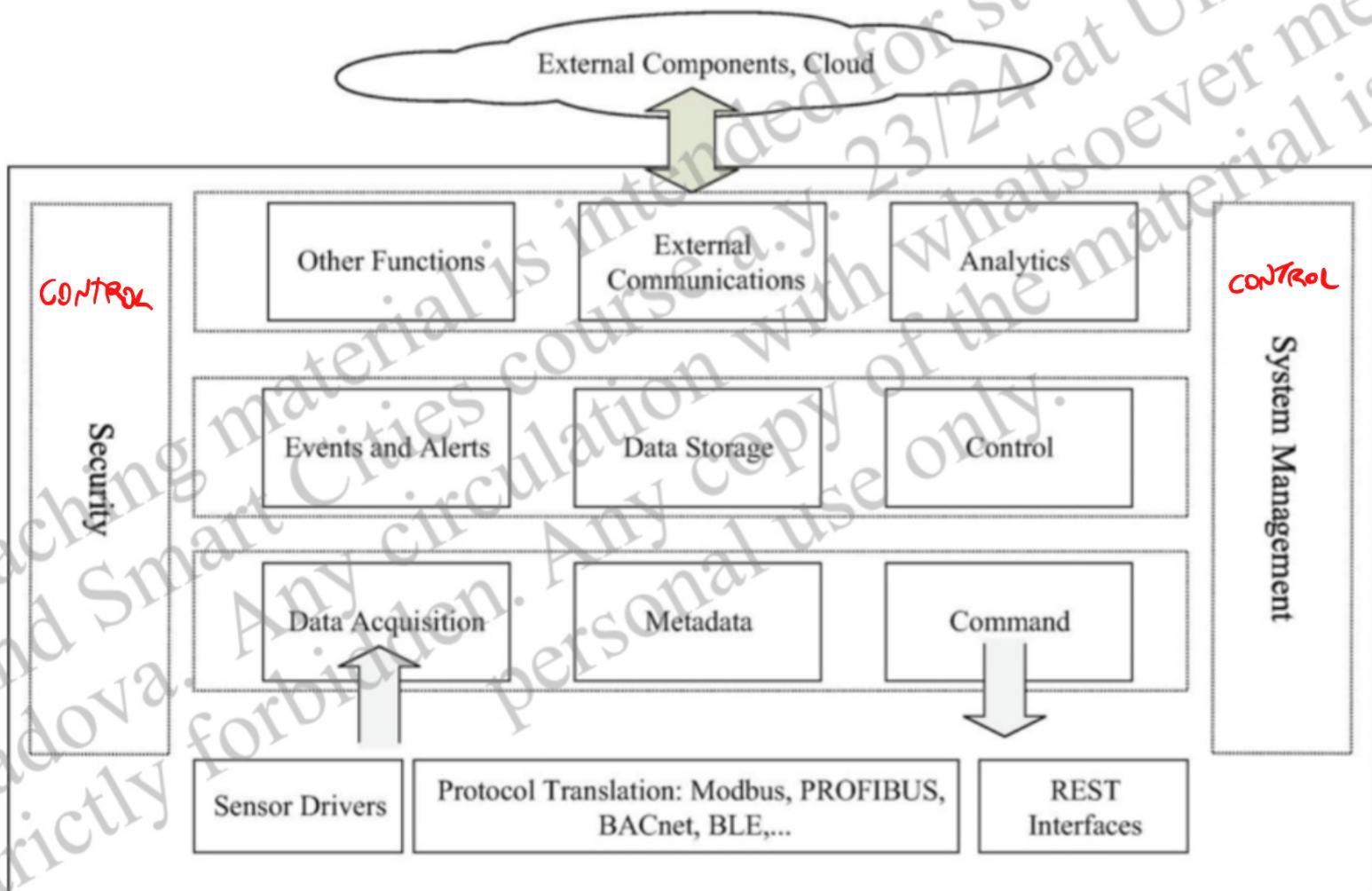
- UN GATEWAY IoT CONNETTE SENSORI/ATTUATORI/THINGS
PRESENTI NELL'EDGE CON I LIVELLI GERARCHICI
PIÙ ALTI DEL SISTEMA E/O DEL CLOUD.
SI OCCUPA ANCHE DELLA SICUREZZA TRA ESSI E
È IL CONFINE TRA PRODUZIONE E/O PROCESSO
CHIAMATO "OT" (COME PLCs E CONTROL LOGIC)
E L'IOT INFORMATION TECHNOLOGY PART CHIAMATO
"IT" DAVV AVVENGENDO I DATA PROCESSING
AVANZATI.

PER QUESTA RAGIONE IN GENERE I GATEWAY INCLUI-

DONO UN APPROPRIATO PROTOCOLLO (TCP/IP O HTTP).
PER ESSERE CERTI CHE IL PROPRIO DISPOSITIVO
SIA SICURO BISOGNA VERIFICARE CHE ABbia LE
ANNESSE CERTIFICAZIONI.

- LE FUNZIONI DATA PLANE DI UN GATEWAY O EDGE NODE SONO:
 - ACQUISIZIONE, TRASMISSIONE E ATUAZIONE DATI;
 - (A VOLTE) DATA STORAGE, ALGORT PROCESSING, EVENTI E CONTROLLO AUTOMATIZZATO;
 - ~ (SOLO IN CASI RARI E PARTICOLARI) ANALISI DATI.
- LE FUNZIONI CONTROL PLANE SONO:
 - SI CUREZZA E SISTEMI MANAGEMNT.

• DATA PLANE FUNCTION



- NELLO SPECIFICO UNA FUNZIONE DEL DATA PLANE E CATURARE, CON UNA CORRETTA SINCRONIA (CHE SPESO SO DEVE ESSERE CONDIVISA CON DIVERSI DISPOSITIVI), I DATI CHE ARRIVANO DA UNA MULTITUDINE

DI SENSORI DIFFERENTI.

LA SINCRONIA AVVIGNE CON UN CLOCK INTERNO (SPRESSO 32 KHZ) CHE PERMETTE DI SCHEDARE I DATI CON IL LORO RELATIVO ORARIO DI CATTURA PER Poi ESSERE INVIAZI AD ALTRI PARTI (COME LO STORAGE).

QUESTO METODO DI ATTIVAZIONE O "STILE ARCHITETTURALE" PER SISTEMI DISTRIBUITI È DENOMINATO REST E I NODI CHE LO USANO POSSONO AVERE I LORO SPECIFICI TIPI DI DATO PEr Poi ESPORLI PERO' TRAMITE REST APIs.

• METADATA

- CON METADATA CI SI RIFERISCE AL MANAGEMENT E STORE DI INFORMAZIONI CONTESTUALI CHE POSSONO ESSERE UTILIZZATE PER AGGIUNGERE INFORMAZIONI "DI FABBRICA" UTILI QUANDO VENGONO CHIESSI DALL'ESTERNO.
ESEMPI: TIPO SENSORE, TIPO DI DATO IN CUI VENGONO INVIATI I DATI (C^o , F^o , K^o), ACCURATEZZA, RANGE MASSIMO E MASSIMO/MINIMO VALORE.
NELL'IOT I METADATI NON SONO "WELL-DEFINED" E STRUTTURATI.

• EXTERNAL DATA COMMUNICATIONS

- GLI INPUT CHE ARRIVANO AL GATEWAY POSSONO ESSERE POLICY UPDATES, ALGORITHM UPDATES, COMANDI PER ATTUATORI, CAMBIO SETTAGGI ETC... IL DATO PIÙ COMUNE O PAYLOAD È IL REPORT DATO CHE ARRIVA DA UN SENSORE.
QUI SI EFFETTUÀ ANCHE LA SERIALIZZAZIONE (PER I DATI IN USCITA) E LA DESERIALIZZAZIONE (PER I DATI IN INGRESSO).

{ "id": "150a3c6e-bef0ee0e", "temp": "n:77.6" "unit": "°F", "DateTime": "t:2019-07-15T14:50:07Z UTC"}

- I MESSAGGI INVIATI < RICHIESTI AL SENSORE IoT POSSONO ESSERE TRASMESSI ATTRAVERSO PULL / PUSH REQUEST.

CON IL PULL L'USER CHIEDE SERVIZIO AL SERVER CON UN API-STYLED "GET DATA", CON IL PUSH IL SERVER INVIA DATI ALL'USER DOPO IL VERIFICARSI DI UN "EVENT".

QUESTI SCambi DI MESSAGGI API NECESSITANO DI SINCRONIA CHE PERMETTE DI ESSERE GESTITA IN modo sincrono con un SW o in modo asincrono = NO DOVE IL RICEVITORE È NOTIFICATO QUANDO IL MESSAGE È STATO RICEVUTO.

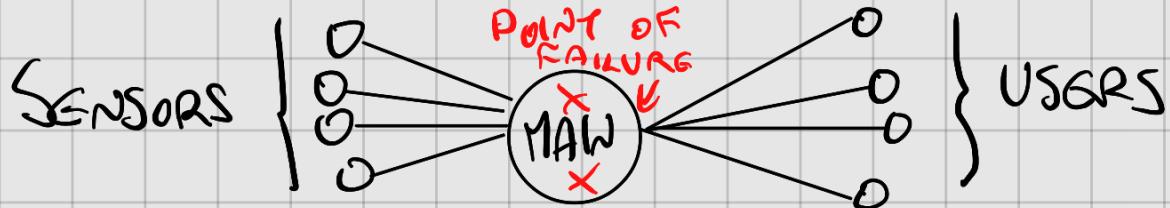
NELLE NOTIFICHE PUSH IL GATEWAY RICEVE DATI DAL SENSORE SECONDO UNA LOGICA STABILITA DA ENTRAMBI ATTRAVERSO UN'ACCORDO; CHE PUÒ ESSERE sincrono o asincrono, il primo ad esempio con HTTP PUT E INDIRIZZO & PORTA SPECIFICATA, IL SECONDO METODO DEPOSITA I MESSAGGI IN UNA QUEUE DA CUI Poi, UNA VOLTA PRONTI, VERRANNO RIPRESI.

QUESTO È UNO DEI MAGGIORI vantaggi NELL'IOT CHE GRAZIE A QUESTA QUEUE PUÒ DISACCOPPIARE IL LAVORO DEL SENDER E RECEIVER PER PERMETTERE SISTEMI COME PIPELINING ETC...

- UN SISTEMA DI SCAMBIO ORmai ACCETTATO UNIFORMEMENTE È IL PUBLISH - SUBSCRIBE DOVE I DISPOSITIVI PUBBLICANO I DATI IN UN RECIPIENTE DOVE Poi SOLO DETERMINATI UTENTI POSSONO ACCEDERE, IL RECIPIENTE SI OCCUPA DI GESTIRE TUTTO E QUINDI È UN SISTEMA Scalabile.

I SISTEMI PIÙ FAMOSI SONO ANDROP, DOS, XMP e
M&T CHE È ANCHE IL PIÙ UTILIZZATO.

DRUGS TO SYSTEMS HAVE A SINGLE POINT OF FAILURE.



• LOCAL CONTROL

IL CONTROLLO LOCALE È INTEGRATO NEI SISTEMI DOVE LA BASSA LATENZA È FONDAMENTALE. QUASI SEMPRE QUESTI SISTEMI SONO POSTI IN PROSSIMITÀ DELLA FONTE DEI DATI PER RIDURRE APPUNTO DISTANZA & TEMPO. QUESTI SISTEMI NECESSITANO DI AVERE UN' AUTONOMIA COSTANTE PER RIMANERE SEMPRE OPERATIVI.

PER QUESTI USI SONO DEFINITI I CONTROL ALGORITHMS CHE SONO REGOLE SOTTO FORMA DI SCRIPTS.

I PLCs USANO molti CONTROL PROGRAMMING LANGUAGES CHE SPESO MOLTO DIAGRAMMI O LADDER LOGIC.

NELL' USO COMUNE QUESTI PROGRAMMI USANO LA LOGICA "IF THIS THEN THAT" O IFTTT COME AD ESEMPI ALEXA O GOOGLE ASSISTANT.

NON C'È UNO STANDARD PER QUESTI PROGRAMMI, MA
UN PROGRAMMA **FLOW-BASED VISUAL PROGRAMMING**
TOOL CHE È DIVENTATO POPOLARE SI CHIAMA NODE-RED.

• DATA STORAGE

- IN GENERALE LO STORAGE PUÒ ESSERE LOCALE O NEL CLOUD, L'ESISTENZA DI UNO STORAGE LOCALE PERMETTE LA FLESSIBILITÀ DI CONSERVARE E NON UTILIZZARE TROPPO NETWORK BANDWIDTH E RIDURRE IL CAVORO SUL CLOUD.

• EDGE ANALYSIS

- I PROCESSI DI ANALISI NEI SENSORI E' NON SOLO NEI CLOUD STANNO PRENDENDO PECHE PERCHE' PERMETTONO DI RIDURRE IL CARICO SUL CLOUD.
QUESTI PROCESSI POSSONO ESSERE SVOLTI (COME AD ESEMPIO AI E MACHINE LEARNING ALGORITHMS) SIA DA SPECIFICI NODI CHE IN CONCOMITANZA CON IL CLOUD, COME SPesso ACCADE.

• FUNCTION PLACEMENT IN IoT SYSTEM

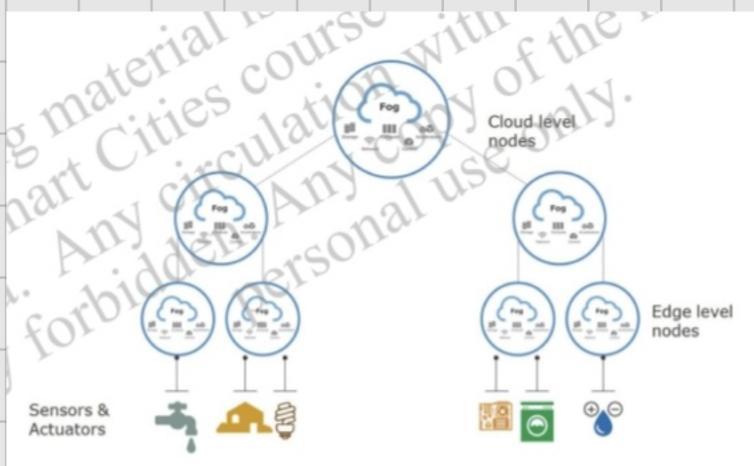
- ALL'INIZIO SI USAVA UN SISTEMA IoT IN CUI I NODI AVVANO IL COMPITO DI COLLEZIONARE DATI PER Poi INVIALI AL CLOUD DOVE SI SVOLGEVANO TUTTE LE COMPUTAZIONI.

QUESTO APPRECCIO STA VENENDO MODIFICATO IN DIREZIONE DI UN MAGGIORE BILANCIMENTO DI DATA PROCESSING TRA EDGE NODE E CLOUD: INFATI IL POSIZIONAMENTO OTTIMALE DELLE FUNZIONI RELATIVE AL DATA E AL PROCESSING VIGNE BASATO SUL RAPPORTO COSTO/EFICIENZA.

- QUESTE CONSIDERAZIONI SI BASANO SU DIVERSI FATTORI:
 - DISPONIBILITA' E COSTO DEL DATA-RATE;
 - LATENZA RICHIESTA DAI REQUIREMENTS;
 - AUTONOMIA LOCALE, INCLUSI I NODI DISCONNESSI CHE RIMANGONO OPERATIVI;
 - SICUREZZA, DATA CONTROL E PRIVACY NECESSARIA;
 - COSTO E COMPLESSITA' DI SVILUPPO E MANAGEMENT;
- GLI UNICI POSTI DOVE E' POSSIBILE POSIZIONARE I VARI PROCESSI SONO:
 - NEGLI EDGE, VICINO A DOVE SI RILEVANO I DATI;
 - NEI LOCALI INTERNI ALL'AZIENDA;
 - NELLE INFRASTRUTTURE DI COMUNICAZIONE;

- NEL CLOUD;

- FOG NODES
- I FOG NODE SONO DEI NODI PIÙ POTENTI CHE PRESENTANO STORAGE E POTENZA DI CALCOLO UTILI PER ESEGUIRE SERVIZI CHE POSSONO ESSERE RICHIAMATI QUANDO CI SONO NUOVI REQUIREMENT O LOAD VARIATIONS.



SONO MOLTO UTILI QUANDO È NECESSARIO UN RIBILANCIMENTO DEI SERVIZI PERCHÉ MAGARI IN QUEL MOMENTO IL CLOUD È COMPLETAMENTE SATURATO.

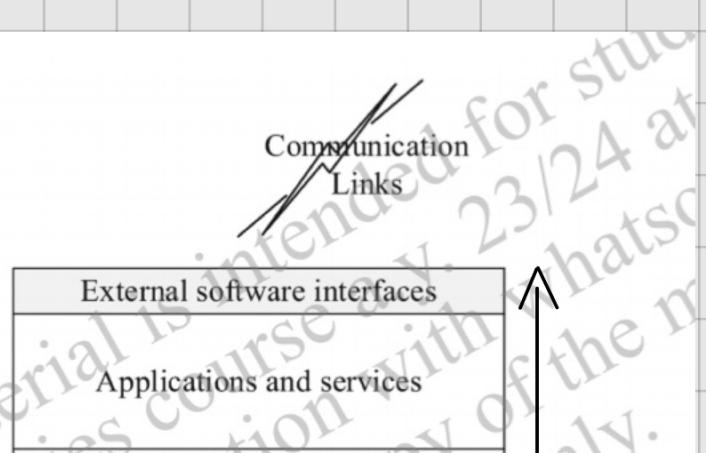
• CONTROL PLANE: SECURITY AND MANAGEMENT

- CHI SI OCCUPA DEL SETTAGGIO INIZIALE DEGLI EDGE NODE, DEFINITO BRINGING UP, È IL CONTROL PLANE. IL SUO PRIMO COMITI È LA SECURITY E MANAGEABILITY, MA ANCHE INSTALLATION E PROVISIONING; IN GENERALE QUESTI COMITI LAVORANO SU QUESTI CAMPI:
 - FAULT MANAGEMENT → TROUBLESHOOTING, ERROR LOGGING AND RECOVERY.
 - REMOTE MONITORING, CONTROL, ADMINISTRATION E DIAGNOSTICS
 - REMOTE FIRMWARE E SOFTWARE UPDATES
 - SECURITY UPDATES
 - METRICING (MISURAZIONE) DI NETWORK BANDWIDTH E SOFTWARE USAGE.

PER INSERIRE UN NUOVO NODO, ESSO DEVE ESSERE REGOLO IN SICUREZZA, AUTENTICATO E REGISTRATO.

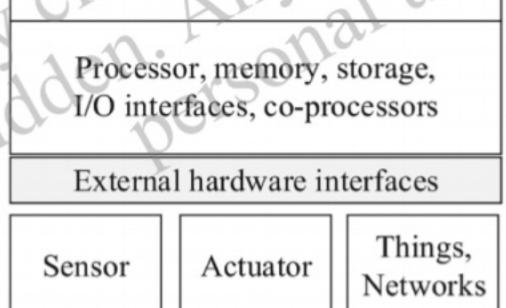
PER FARE CIÒ PRIMA IL NODO DEVE ESSERE RICONOSCIUTO E AUTORIZZATO DAGLI ALTRI NODI E DAL CLOUD, E Poi IL NODO STESSO DEVE AUTORIZZARE L'ACCESSO AGLI EXTERNAL SERVICES, E FARE I VARI UPDATES.

- IMPLEMENTATION OF AN IOT EDGE NODE
- I SENSORI IOT SONO IDEATI PER SVOLGERE OPERAZIONI AUTONOME, L'IDEA È CHE ALL'ATTO DELL'INSERIMENTO DI UN NUOVO NODO, IL SISTEMA LO RICONOSCA E SI RIPROVI CONI GUARI DI CONSEGNAZA.
Per fare ciò il nodo deve METTERE A DISPOSIZIONE DEL DATA PLANE VIA API QUESTE FUNZIONI:
 - LETTURA DEI VARI SENSORI O DEL SINGOLO;
 - LETTURA DEI SUOI METADATA;
 - INSERIMENTO DI UN COMANDO;
 - MODIFICA SETTINGS, CONFIGURATION, PROCESSING RULES, SUBSCRIPTIONS;
- I SENSORI INOLTRE DEVONO METTERE A DISPOSIZIONE DEL CONTROL PLANE LE SEGUENTI FUNZIONI:
 - LETTURA DEL SOFTWARE OS VERSION, PATCH STABILITÀ, ANTIVIRUS SIGNATURE FILE ETC...;
 - POSSIBILITÀ DI DOWNLOAD E INSTALLAZIONE DI SOFTWARE UPDATES;
 - UPDATE DI CREDENZIALI DI SICUREZZA, AGGIUNTA E RIMOZIONE AUTORIZZAZIONI;



- Con "EXTERNAL HARDWARE INTERFACES" CI RIFERIAMO ALLE GIÀ TRATTATE SPI E SERIAL INTERFACES CON BUS. SOPRA C'È TUTTO CIÒ CHE RIGUARDA IL PROCESSING CON-

Runtime system



I CRYPTOGRAPHIC PROCESSOR (ESEMPIO PROF PENNINA).

Poi c'è IL RUNTIME SYSTEM DOVE C'È L'OPERATING SYSTEM COME **FREERTOS** O **LINUX REAL-TIME** | SONO OS CHE SI OCCUPANO DI REAGIRE E ATTENERE

TE SUBITO DOPO A UNO SPECIFICO INTERRUPT).

E Poi ci sono le varie applicazioni per usarlo.

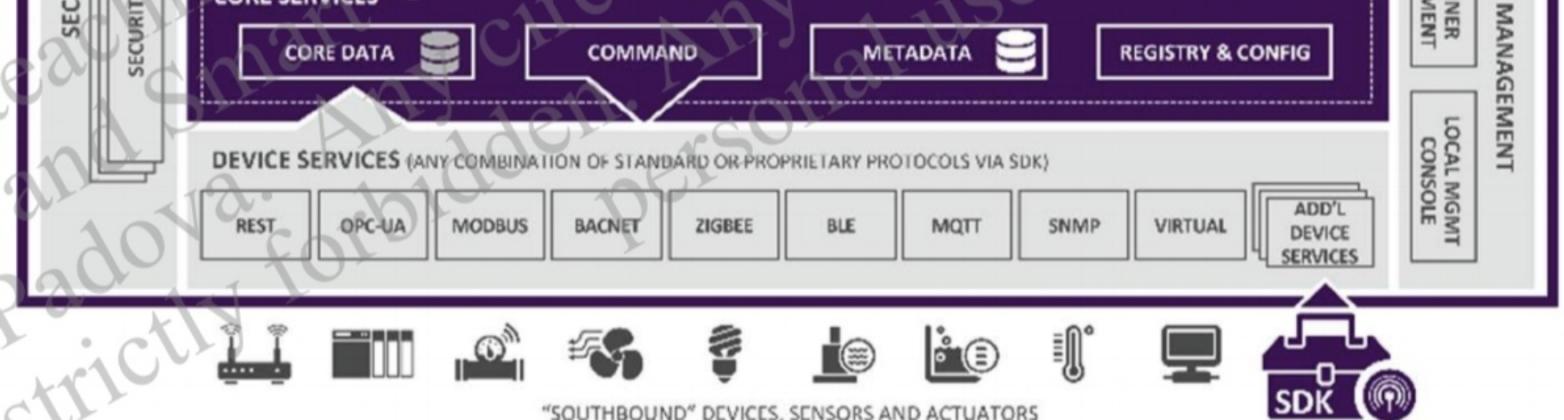
- IMPORTANTI TOPICS CHE RIGUARDANO L'IMPLEMENTAZIONE DI UN NODO SONO:

- **TPM MODULE**: CHE SONO DEI MODULI CHE PERMETTONO DI RENDERE SICURA UN DISPOSITIVO (SCHEDE SIM).
- **EDGE NODE SOFTWARE**:
 - con RUNTIME SYSTEM
 - OPERATING SYSTEM
 - ALWAYS ON OPERATION
 - WATCHDOG TIMER NOT PER I MICROCONTROLLER SEMPRE PRESENTI
 - APPLICATIONS

- AN EXAMPLE OF AN EDGE IoT NODE

EDGEX FOUNDRY™ Platform Architecture





- IN QUESTO CASO CI RIFERIAMO A UN EDGE NODE CHE COMMUNICA SIA CON IL CLOUD CHE CON I SENSORI, OSSIA UN **FOG NODE**.

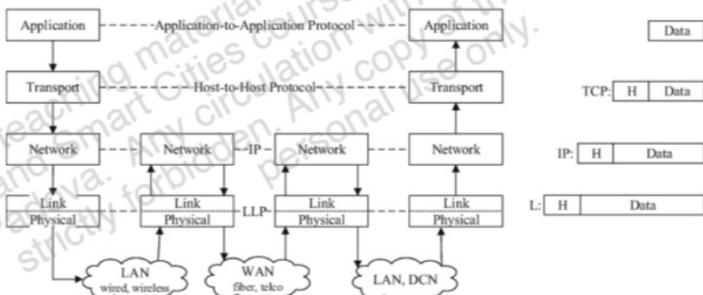
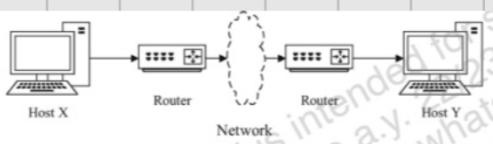
CAPITOLO 3

- **LAYERED NETWORK DESIGN**
- CON IL TERMINE **LAYERING** CI SI RIFERISCE ALL'IMPLEMENTAZIONE DI UN NETWORK CON FUNZIONALITÀ DIVISE PER LAYER APPENA; OGNI UNO DI QUESTI LAYER DEVE DARE SERVIZI AL LAYER DI SOPRA E UTILIZZARE SERVIZI DI QUELLO DI SOTTO.
QUESTA INDIPENDENZA TRA LAYER PERMETTE DI MODIFICARNE UNO SENZA RIPLETARE QUESTA DECISIONE SUGLI ALTRI.

GLI ELEMENTI BASE DI UN LAYER SONO:

- **SERVIZI**: UN SET DI AZIONI CHE UN LAYER DA AL LAYER DI SOPRA DELLA STESSA MACCHINA;
- **INTERFACCIE**: SONO I PUNTI DI ACCESSO PER USUFRUIRE DEI SERVIZI;
- **PROTOCOLLI**: SET DI REGOLE CHE UN LAYER USA PER SCAMBIARE INFORMATIVI

UN POCO DI SCARICHE, INVISUALIZZAZIONI CON LA CONTROPARTE LAYER DI UN NODO REMOTO.



Internet model	OSI model	IIC IoT model	Functions	Protocol data unit (PDU)
Application	Application		Data exchange between applications at endpoints, interoperable data	Data, information
	Presentation	Framework		
	Session			
Transport	Transport	Transport	Data segments between endpoints, segmentation, acknowledgments, multiplexing	Message (datagram), segment
Internet (network)	Network	Network	Packets transferred between endpoints, may not be on the same network, routed as needed	Packet
Link	Data link	Link	Transmission of digital frames between two endpoints connected by the physical layer	Frame
Physical	Physical	Physical	Transmission of raw bit streams between two endpoints over a shared physical medium	Symbol

Object and Data Models (HTML, XML, ... WoT, LWM2M, OCF ...)

Application (CoAP, MQTT, HTTP, SMTP)

• ANCHE
QUK

→ Transport (UDP, TCP)

Network (IPv4, v6)

Link (matching PHY)

Physical:
(PHY)

xG
cellular

802.1
TSN

802.3x
Ethernet

802.5
Token R

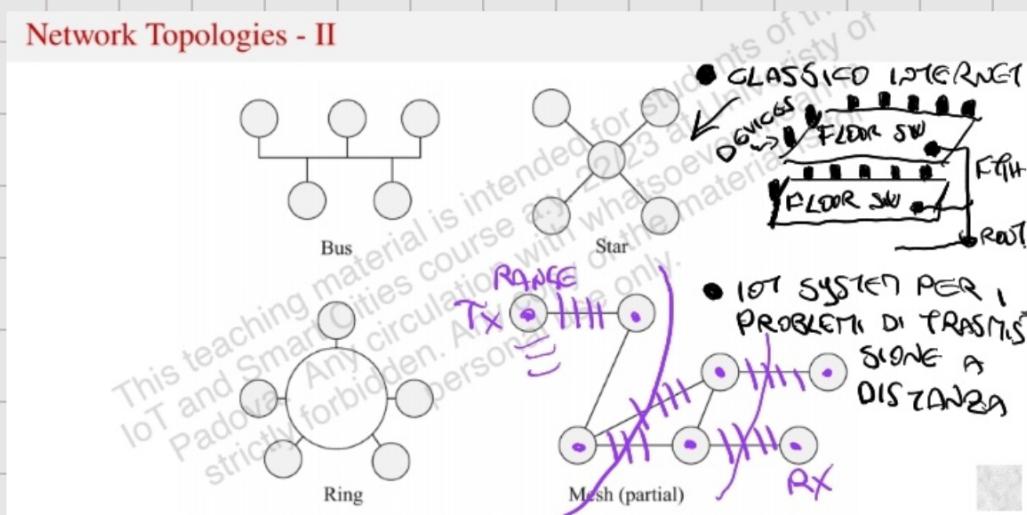
802.11x
WiFi

802.15.4x +
6 LoWPAN

Other...

- **NETWORK TOPOLOGIES**
- CI SONO NUMEROSE CONFIGURAZIONI DELLE NETWORK TOPOLOGIES E RAPPRESENTANO LA STRUTTURA LOGICA/FISICA DI UNA RETE.

Network Topologies - II



- **WIRELESS EDGE NETWORK**

- QUESTI NETWORK PRENDONO IL VANTAGGIO DI NON NECESSITARE DI UN'INSTALLAZIONE FISICA, E DI AVERE UN COSTO MINORE POICHÉ NON SI COMPRANO CAVI, INOLTRE SONO ADATTI ALL'ABILITÀ SOLO TEMPORANEA DI NODI.
IN GENERALE PERO' ANCHE I NETWORK WIRELESS PRESENTANO UN COLLEGAMENTO CABLATO NEL ROUTER / GATEWAY CHE A SUA VOLTA FORMA IL NETWORK MAGARI DI PIANO ETC...
VISTO CHE I NODI IN GENERE NECESSITANO DI CONNETTERSI A INTERNET, È IMPORTANTE CHE I PROTOCOLLI CHE UTILIZZANO GLIELO PERMETTANO.
- PER VALUTARE UN WIRELESS NETWORK VALUTIAMO:
 - RANGE DEL SEGNALE;
 - BANDWIDTH DISPONIBILE;
 - TOPOLOGIA;
 - LATENZA E SITUAZIONE → PIÙ IMPORTANTE;
 - UTILIZZO DI ENERGIA E POWER REQUIREMENT;
 - FREQUENZA;

- **RADIO SPECTRUM AND FREQUENCY ALLOCATION**
- GLI SPECTRI RADIO SI DIVIDONO IN 2 GRANDI CATEGORIE:
 - CON LICENZA → LICENSED
 - SENZA LICENZA → UNLICENSED

LE PARTI CON LICENZA SONO PREGAR SPECIFICI USER O VENDUTI A PRIVATI COME ISP, UTILIZZARE QUESTE FREQUENZE È ILLEGALE SE NON SI HA L'OK DAL PROPRIETARIO.

LE PARTI SENZA LICENZA POSSONO ESSERE UTILIZZATE GRATUITAMENTE, PERO' SONO COMUNQUE OGNISETTE...

UN REGOLAMENTATO DA NORIGI STRINGENTI IN TERMINI DI POTENZA DI SEGNALE, DURATA DI COMUNICAZIONE E CICLO DI LAVORO.

ATIENZIONE, UN SISTEMA IOT A SCOPO GLOBALE DOVRÀ ADATTARSI ALL'UTILIZZO DI SPECTRO DI FREQUENZA DELLO SPECIFICO STATO PER CHE' POTREBBE VARIARE.

- LA FREQUENZA SENZA LICENZA PIÙ UTILIZZATA NELL'IOT È LA **2,4 GHz** CHE È USAZIA DALL'IEEE 802.11 Wi-Fi NETWORKS, BLUETOOTH G IEEE 802.15.4 WPANS.
UN'ALTRA FAMOSA È LA **868 ÷ 915 MHz**
(HA UN RANGE PERCHE' VARIA DA NAZIONE A NAZIONE \rightarrow EU = 868 MHz | USA = 915 MHz)
QUESTE FREQUENZE PIÙ BASSE IN GENERALE HANNO LA POSSIBILITÀ DI INVIARE IL SEGNALE A MAGGIORI DISTANZE, A SCAPITO PERO' DELLA VELOCITÀ DI INVIO DATI.
PER I NETWORK IOT SI USANO SPESO FREQUENZE SENZA LICENZA CON LA FORTUNA DI NON DOVERLE PAGARE MA DI DOVER FARE I CONTI CON IL FATTO CHE È UNA FREQUENZA MOLTO UTILIZZATA E CHE QUINDI HA PERFORMANCE MINORI.

- **CONSTRAINED DEVICES AND NETWORKS**
- I CONST. DEVICES SI DIFFERENZIANO, PER GRANDEZZA DI DATO DI INVIO E PER IL CODE SIZE, IN 3 CLASSI:

Classification of constrained devices

Name	Data size, e.g., RAM	Code size, e.g., flash	Functionality
Class 0, CO	<<10 KB	<<100 KB	Very constrained devices, e.g., sensor-like motes. Cannot communicate with the Internet directly, need help of larger proxies, gateways, or servers

Class 1, C1	~10 KB	~100 KB	IP and security capable, cannot easily communicate using full Internet Protocol stacks, such as HTTPS. May be able to use CoAP over UDP; can be integrated as peer nodes into larger IP networks
Class 2, C2	~50 KB	~250 KB	Support most of protocol stacks used on notebooks and servers; constrained, can benefit from lightweight and energy-efficient protocols and from consuming less bandwidth

- I NETWORK DI QUESTO TIPO SONO CARATTERIZZATI DA BASSI CONSUMI E ALTE PERDITE, INFATTI SONO DEFINITI "LOW-POWER AND Lossy NETWORKS" OPPURE (LLNs).

PER OTTENERE UN COSÌ BASSO CONSUMO SI UTILIZZANO TECNICHE COME:

- COMUNICAZIONI TEMPORIZZATE CHE PERMETTONO AL NODO DI ENTRARE SEMPRE IN SLEEP MODE;
- HEADER PICCOLI E COMPRESI;
- PAYLOAD RIDOTTI COSÌ DA AVERE BASSI BIT ERROR RATE E PERMETTERE MEDIA SHARING;
- LIMITED BANDWIDTH; → LESS POWER NEEDED
- FUNZIONALITÀ ESTREMAMENTE RIDOTTI;

UTILIZZANO IP GENERE UNA CONFIGURAZIONE MESH DOVE C'È SEMPRE ALMENO UN NODO CON CAPACITÀ DI CALcolo SUPERIORE CHE FUNZIONA DA EDGE ROUTER.

• IEEE 802.15.4

- È UNO STANDARD CHE LAVORA SU FREQUENZE SENZA LICENZA CORRE $868.0 \div 868.3$ MHz o 902-928 MHz IN NORD AMERICA E 950-956 MHz IN GIAPPONE. LE FREQUENZE 2400-2483.5 MHz SONO SENZA LICENZA A LIVELLO MONDIALE.

IN BASE ALLA FREQUENZA E ALLA POTENZA DEL SEGNALE, IL NUMERO DEI CANALI UTILIZZABILI VARIA DA 1 A 16, FINO ADDIRITTURA A 30, CON UP BIT RATE DI 20, 40, 100 E 250 Kbps.

PER COMUNICARE SFRUTTANDO IL CSMA/CA, QUINDI PRI-

MA DI COMUNICARE "ASCOLTERANNO" IL CANALE PER VERIFICARE SE E' LIBERO.

L'IEGE 802.15.4 DEFINISCE L'USO DI OPTIONAL BEACONING PER PERMETTIRE UNA TRASMISSIONE CONFLICT-FREE CON UN SUPER-FRAME.

- OGNI NODO DEL NETWORK PUO' ESSERE UN FULL-FUNCTION DEVICE (FFD) O UN REDUCED-FUNCTION DEVICE (RFD).

IL PRIMO PUO' PARTECIPARE IN TUTTE LE TOPOLOGIE HA IL PROTOCOLLO COMPLETO E PUO' FUNZIONARE DA "ADMIN" DELLA RETE, VIENE CHIAMATO PAN COORDINATOR. L'RFD E' LIMITATO SOLO A FARE DA EDGE NODE NELLE STAR TOPOLOGIES O NEI P2P NETWORK.

QUESTO PROTOCOLLO PREVEDE SOLO P2P NETWORK O STAR TOPOLOGIES APPUNTO, E VISTO CHE NON DEFINISCE FUNZIONI SOPRA L'OSI LAYER 2 NON INCLUDE ROUTING.

- IL MAC LAYER SI OCCUPA DI ABILITARE LA TRASMISSIONE DEL FRANE SUL PHYSICAL CHANNEL. QUANDO RICEVE INSEGNE FA FRAME VALIDATION, ERROR DETECTION, COLLISION AVOIDANCE E DA GLI ACCESS POINT AI SERVIZI DI SICUREZZA.

IL PROTOCOLLO E' CHIARO ANCHE CON LE DIMENSIONI DEL PAYLOAD CHE DEVE ESSERE DI 127 BYTES, I MESSAGGI POSSONO ESSERE CON O SENZA ACKNOWLEDGEO. NELL'IPV6 L'HEADER E' DI 40 BYTES (SE NON VIGNE COMPRESO) OSSIA QUASI 1/3 DEL TOTALE.

NEL TEMPO CI SONO STATI DIVERSSI EMENDAMENTI E I PIU' FAMOSI SONO 2:

- ~ 802.15.4D: HA INTRODOTTO L'EFFICIENTE TIME-SLOTTED CHANNEL HOPPING (TSCH) E IL COORDINATED SAMPLED LISTENING (CSL) HA MODIFICATO ANCHE IL

PHYSICAL LAYER PER PERMETTERE UN INCREMENTO DEL RANGO NEI SUB-GHz NETWORKS;

- 802.15.4e: HA INTRODOTTO IL CHANNEL HOPPING PER AUMENTARE LA ROBUSTEZZA CONTRO LE INTERFERENZE E IL MULTIPATH FADING.

- **6LoWPAN**
- L'IDEALE SAREbbe POTER AVERE DISPOSITIVI DISLOCATI CHE FORMANO UN NETWORK COLLEGATI TRA LORO SENZA CAVI O MEZZI FISICI; MA QUESTO IMPLICA ANCHE IL LAYER NETWORK, COSA CHE GLI EDGE DEVICE RFD NON HANNO.

IL **6LoWPAN** PERMETTE DI ELIMINARE QUESTO IMPEDIMENTO TRAMITE LA COMPRESSEIONE E IL SUCCESSIVO INSERIMENTO DEGLI HEADER IPV6.

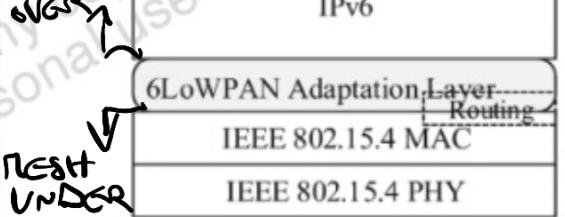
6LoWPAN STA PER LOW-POWER WIRELESS PERSONAL AREA NETWORK E DEFINISCE L'USO DELL'IP NETWORKING NELL'802.15.4.

- NEL CASO MIGLIORE IL **6LoWPAN**, DURANTE UNA TRASMISSIONE UDP, PUO' COMPRIMERE 40 B DI IPV6 ADDRESS E 8B DI HEADER UDP IN UN TOTALE DI **6 BYTES**, PERMETTENDO QUINDI UN PAYLOAD DI **108 BYTES**. VISTO CHE L'IPV6 PERMETTE UN MTU DI **1280 BYTES** E L'IEEE 802.15.4 HA UN LIMITE DI 127 B, IL **6LoWPAN** SUPPORTA LA SEGMENTAZIONE E IL RIASSSEMBLAMENTO.

Application: HTTP	IEC6F PROTOCOL	CoAP, MQTT
Transport: TCP		UDP, TCP
MESH	mesh	

- PER SUPPORTARE LE MESH CONFIGURATION PERMETTE DAL 802.15.4,

Network: IP
Link: IEEE 802.11 (Ethernet)



L'HEADER 6LOWPAN
SI OCCUPA DELLE
DISPOSIZIONI PER
IL MESH ROUTING.

QUESTO NON È IL CLASSICO IP ROUTING, INFATI SI PARLA DI
MESH-UNDER ROUTING E, IN COORDINAZIONE CON IL PRO-
TOCOLLO 802.15.4, È PIÙ EFFICIENTE A LIVELLO DI CON-
SUMO ENERGETICO ED È "NASCOSTO" DAL RESTO DEL GA-
GER IP. SE VOLESSIMO USARE IL CLASSICO IP ROUTING
PARLIAMO DI MESH-DVGR ROUTING.

- IL 6LOWPAN PRESEDE 3 TIPI DI NODO:
 - **EDGE O BORDER ROUTER**: SI OCCUPA DI CONNETTIRE IL NETWORK 6LOWPAN A INTERNET E HA 3 FUNZIONI CHE SONO
 - (1)** DATA EXCHANGE TRA NODI, INTERNET E ALTRI NETWORK 6LOWPAN,
 - (2)** DATA EXCHANGE TRA NODI DELLO STESSO NETWORK E
 - (3)** GENERA E FA MANUTENZIONE DEL 6LOWPAN RADIO NETWORK.
 - **ROUTER NODE**: SI OCCUPA DI INSTRADARE I MESSAGGI TRA NODI DEL 6LOWPAN NETWORK IN MESH CONFIGURATION E NON PUÒ MAI ENTRARE IN SLEEP.
 - **HOST NODES**: SONO GLI END NODES, NON FANNO ROUTING, POSSONO ENTRARE PERIODICAMENTE IN SLEEP PER RISPARMIARE BATTERIA.

UN VANTAGGIO NOTEVOLI DEL 6LOWPAN È QUELLO CHE NON ALTERA IL PAYLOAD, AL CONTRARIO DI ALTRI PROTOCOLLI COME BLUETOOTH O ZIGBEE CHE NON SONO CAPABILI DI MIGRARE.

PASSIBILI CON INTERNET.

I ROUTER ZIGBEE SONO STATELESS OSSIA NON MANTENGONO IN UN DETERMINATO MOMENTO LO STATO DI UNA APPLICAZIONE.

- IL ROUTING È IMPLEMENTATO CON L' IPv6 FOR LOW-POWER AND LOSSY NETWORKS (RPL) CHE SFRUTTA IL DODAG (DESTINATION-ORIENTED DIRECTED ACYCLIC GRAPH) CHE DETERMINA I VARI PATHS.
È UN MODELLO CHE SI PRESTA A CAMBIAMENTI DINAMICI DELLA CONFIGURAZIONE DI RETE.

• ZIGBEE

- ZIGBEE È UN PROTOCOLLO PROPRIETARIO CREATO E MANTENUTO DA INDUSTRY ALLIANCE.
ZIGBEE È IDEATO PER SUPPORTARE UN GRAN NUMERO DI DEVICES IN PROSSIMITÀ TRA LORO CHE SONO LOW POWER, LOW COST E LOW DATA NETWORK.

Ogni nuova versione che esce cerca di essere il più retro-compatibile possibile.

ZIGBEE È UN NETWORK SELF-HEALING, SELF-FORING OSSIA CHE SI SETTA AUTOMATICAMENTE E REAGISCE AUTONOMAMENTE ALLE VARIAZIONI DEL NETWORK STESO; SUPPORTA STAR O MESH TOPOLOGIES.

UTILIZZA LA FREQUENZA SENZA LICENZA 2.4 GHz CON 16 CANALI DA 2 MHz PER EVITARE COLLISIONI CON IL WI-FI.

A CIRCA 10 ÷ 100 m IL RAW BIT RATE È DI 250 Kbps IN BASE ANCHE ALL' AMBIENTE.

- SUPPORTA ANCHE LE ALTRE BANDE SENZA LICENZA COME 868 MHz o 915 - 921 MHz, MA L' USO DI TALI FREQUENZE ABBASSA IL

Zigbee Application Layer

SECURITY

Zigbee Network and Security Layer

SECURITY

RAW BIT RATE A 100 O 10 Kbps
RISPETTIVAMENTE DA INCREMENTAR
DO LA LING OF SIGHT FINO A 1km.

LA SICUREZZA E' PRESENTE SIA NEL NETWORK CHE NELL' APPLICATION LAYER.

- I TIPI DI NODI ZIGBEE SONO 3:
 - COORDINATOR (C): UNO PER NETWORK, NON PUÒ ENTRARE IN SLEEP (E' SEMPRE ATTACCATO ALLA CORRENTE), E' RESPONSABILE DELLA SICUREZZA, INIZIALIZZA UNA NUOVA PAN, AIUTA NEL ROUTING E SI OCCUPA DELLE VARIAZIONI DEI NODI NEL NETWORK.
 - ROUTER (R): SI OCCUPA DEL ROUTING, DOPO CHE ENTRA NELLA RETE SI OCCUPA DELLE SUO VARIAZIONI, PUÒ SUPPORTARE CHILD DEVICES, NON PUÒ MAI ENTRARE IN SLEEP.
 - END DEVICE (E): ALIMENTATI A BATTERIA POSSONO ENTRARE IN SLEEP PER RISPARMIARE RISORSE, POSSONO PARLARE SOLO CON I PARENT R E C.

IL PROTOCOLLO USATO DA ZIGBEE E' AODV (AD HOC ON-DEMAND DISTANCE VECTOR) CHE DETERMINA LA ROUTE NELL' ISTANZA IN CUI UN MESSAGGIO DEVE ESSERE INVIATO.

- IL NETWORKING LAYER SI OCCUPA DEL ROUTING VARI MA SUPPORTA ANCHE LA CRYPTAZIONE AES A 128-BIT (ADVANCED ENCRYPTION STANDARD), CHE PUÒ ESSERE ASSEGNATO SIA AL NETWORK CHE AL LINK.
C'E' UNA VERSIONE DELLO ZIGBEE CHE USÀ 6LOWPAN,

MA SOLO SU DETERMINATE APPLICAZIONI DELLA APP. LAYER.
L' APPLICATION LAYER FORNISCE ELABORATE FUNZIONI
FRAMEWORK CHE SUPPORTANO CROSS-APPLICATION IN TERMO
PERABILITÀ DEFINENDO PROFILI CHIAMATI CLUSTER
USATI PER VARIE MISURAZIONI (TEMPERATURA ETC...)

• THREAD

- THREAD È UN NETWORKING PROTOCOL STACK
Sviluppato per la domotica.
Ha l'obiettivo di fornire un network IoT affidabile senza point of failure; visto che i device devono essere low power, incorpora l'IPv6
addressability e usa il 6LoWPAN al livello network quindi necessita di un border router.
Utilizza l'UDP e AES, si focalizza sul networking e non definisce un application layer,
ma lascia questo compito ad altri framework come Zigbee.

• ISA 100.11A

- ISA 100.11A è uno standard definito dall'ISA
(INDUSTRIAL SOCIETY FOR AUTOMATION). Ha l'obiettivo di fornire operazioni wireless affidabili e sicure per monitoraggi non-critici.
Il suo network layer si basa su 6LoWPAN
IPv6 con UDP o TCP e AES.

• BLUETOOTH

- BLUETOOTH È UNA TECNOLOGIA WIRELESS IDEATA
per applicazioni low-cost, short-range; non
è compatibile con l'IP e non usa l'802.15.4.
Ci sono due release generiche:

- **BASIC RATE / ENCHANCED DATA RATE: UTILIZZATO PER (BR/EDR)**: UTILIZZATO PER DATA RATE MAGGIORI DI C'È STATA LA PRIMA VERSIONE, È PRESENTE IN DISPOSITIVI COME CUFFIE BLUETOOTH.
- **BLUETOOTH LOW ENERGY**: UTILIZZA DATA RATE MINORI, È SU DISPOSITIVI COME MOUSE.

IN GENERALE LA COMUNICAZIONE BLUETOOTH È STRUTTURATA TRAMITE **MASTER - SLAVE**.

- IN BASE ALLA POTENZA DEL TRASMETTORE, IL **RANGE** VARIA DA 0,5 A 100 M DOVE I 10 M SONO I PIÙ COMUNI. IL BIT RATE VARIA DA 1 A 3 Mbps E OPERA SULLA FREQUENZA SENZA LICENZA 2,4 GHz DOVE SI SCOSTA CON IL WI-FI CON CUI CREA A VOLTE INTERFERENZE ANCHE SE COMUNQUE HANNO IMPATTI DIVERSI A COESISTERE.

LE TOPOLOGIE CLASSICHE SONO **STAR** E **POINT-TO-POINT** CON LA **MESH** RECENTEMENTE AGGIUNTA.

LA FREQUENZA BLUETOOTH LE è DIVISA IN 40 CANALI, ⁽¹⁾ 3 DEI QUALI POSSONO ESSERE UTILIZZATI PER PERMETTERE AI DISPOSITIVI DI INTRODURSI, FARSI RILEGUARE E STABILIRE LA CONNESSIONE; I RIMANENTI ⁽²⁾ 37 SONO PER L'INVIO DEI DATI.

QUESTO SISTEMA USA L'**ADAPTIVE FREQUENCY HOPPING** TRA I CANALI PER SELEZIONARE IL MIGLIORE.

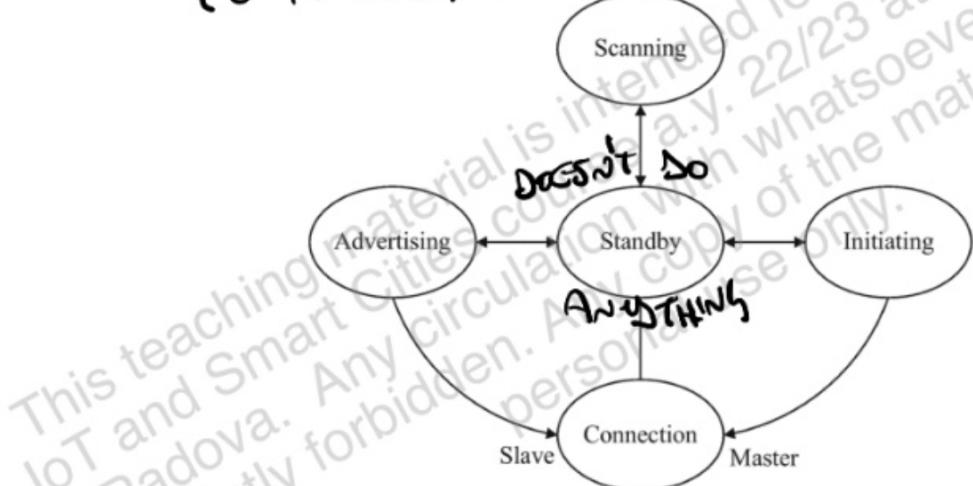
- UN BLUETOOTH **GENERIC ACCESS PROFILE** CATEGORIZZA UN DETERMINATO DEVICE COME SEGUENTE:
 - **BROADCASTER**: PUÒ INVIARE **ADVERTISING EVENTS** ⁽¹⁾

HA UN TRASMETTORE, IL RICEATORE
E' OPZIONALE;

- **OBSERVER**: RICEVE ADVERTISING EVENT, HA UN RICEVITORE, IL TRASMETTORE È OPZIONALE;
 - **PERIPHERAL**: ACCERCHIA CONNESSIONI, SI COMPORTA DA SLAVE, HA SIA RICEVITORE CHE TRASMETTORE (MOUSE, KEYBOARD ETC...);
 - **CENTRAL**: CRIDA LE CONNESSIONI, SI COMPORTA DA MASTER, HA UN TRASMETTORE E UN RICEVITORE (SMART PHONES ETC...).

I NODI POSSONO CAMBIARE RUOLO O ASSUMERNE MOLTEPLICI IN BASE ALLE CONSEGNAZIONI (PENSA AL PC CHE RICEVE DATI MENTRE ASCOLTI MUSICA).

- **SCANNING:** YOU WANT TO CONNECT TO A DEVICE AND YOU FACE TO A LIST OF THEM



N.B!! THE BLUETOOTH STABILISHMENT IS **NOT** SECURE, BUT WHEN THE CONNECTION IS STABILISHED IT BECOME SECURE.

- IL BLUETOOTH NON È COMPATIBILE CON L' IP, E FORNISCE IL SUO PROPRIO NETWORKING & APPLICATION STACK. INCLUSA UN PROTOCOLLO LOGICAL LINK E ADAPTER PROTOCOL (L2CAP) CHE SI OCCUPA DEL LINK STATE MANAGEMENT AND TRANSITION. C'È UNA SPECIFICA CHE PERMETTE DI TRASPORTARE TRAFFICO IPV6 NELLA VERSIONE BLE 3.1 E MAGGIORI.

UNO DEI GATTI UMBRI È IL PROTOCOLO DEL PAIRING.
COL STACK E' IL SECURITY MANAGER CHE SI OCCUPA DI METTRE IN SICUREZZA I DEVICES PRIMA E DOPO IL PAIRING.

IL PAIRING FORNISCE UNO SCANSIO DI CHIAVI TRA DISPOSITIVI CHE SONO Poi IMMAGAZZINATE IN UN CENTRAL-NODE, LE CHIAVI SFRUTTANO AES.

• RFID

• RADIO FREQUENCY IDENTIFICATION (RFID) E' UNA TECNOLOGIA PER L'IDENTIFICAZIONE DI OGGETTI USANDO CAMPI ELETROMAGNETICI (CARTE DI CREDITO, BADGE ETC..)
E' UN SISTEMA DI IDENTIFICAZIONE NON UN NETWORK.
E' STANDARDIZZATO DALL' ISO/IEC.

• LOW RANGE LOW-POWER WIDE-AREA NETWORKS
• NOI VOLGHIAMO POTER COMUNICARE A DISTANZA UTILIZZANDO BASSA POTENZA.

PER FARLO CIÒ CI VIENE INCONTRO LORAWAN.

DISTINZIONE: PROT. STACK



• LORAWAN

• LORA (LONG-RANGE) E' UNA WAN A BASSA POTENZA SPETTACOLARMENTE DA "LORA INDUSTRY ALLIANCE".

OPERATA NELLO SPETTRO SENZA LICENZA DI NUMEROSE BANDE DA 169 MHZ A 430 MHZ, MA ANCHE 868 MHZ E 915 MHZ IN BASE ALL'EUROPA NORD AMERICA.

IL SUO RANGE VA DA 10 Km NELLE AREE APERTE E SCENDE A 1 Km IN QUELLE CHIUSE O DENSAMENTE POPOLATE, IL SUO RAW BIT RATE ARRIVA FINO A 50 kbps. IL PAYLOAD G' DI 50÷250 BYTES IN BASE ALLA FREQUENZA. IL NETWORK E' HALF-DUPLEX.

- LORAWAN DEFINISCE 3 TIPI DI NODO:
 - BI DIRECTIONAL END DEVICE: ULTRA DURATURA, G' POSSIBILE COMUNICARE SOLO QUANDO SI SVEGLIA PER INVIARE DATI;
 - BIDIRECTIONAL END DEVICE WITH SCHEDULED RECEIVING SLOTS (CLASS B)
 - BIDIRECTIONAL END DEVICE WITH MAXIMUM RECEIVING SLOTS (CLASS C)

LORA SFUCCA LO SPREAD SPECTRUM MODULATION E SUPPORTA L' ADAPTING DATA RATE (ADR) CHE PERMETTE, IN BASE ALLA POTENZA DEL SEGNALE, BANDWIDTH E DATA RATE, DI TROVARE IL RODO DI FAR CONSUMARE PIENO A UN DISPOSITIVO.

- LA TOPOLOGIA UTILIZZATA E' STELLA DI STELLE, IL GATEWAY E' FATTO PER SUPPORTARE MIGLIORI DI DISPOSITIVI E SPESO NE HA TANTI PER POTER COPRIRE AREE MAGGIORI.
- I DISPOSITIVI LORA NON HANNO UN'ASSOCIAZIONE FISSA CON I GATEWAY, QUINDI A VOLTE SONO RICEVUTI DA PIÙ GATEWAY CHE DEVONO OCCUPARSI.

LORAWAN NON SI ISPIRA NELL'INTERNET NETWORK LAYERING.

LORA SUPPORTA IL ROAMING CON L'HOME-SERVER E HANDOFF PROCEDURE DEFINITE.

I DISPOSITIVI POSSONO ESSERE ATTIVATI OTR-THE-AIR (OTA) E CON TALE PROCEDURA, IN CASO FOSSERO COMPROMESSI, POSSONO ANCHE ESSERE DISATTIVATI.

I PACCHETTI SONO CRYPTATI CON AES E I NETWORK LORA FORNISCONO SICUREZZA NEL MAC LAYER.

LA LORA ALLIANCE SI OCCUPA DI FORNIRE CERTIFICAZIONI PER L'INTEGRABILITÀ TRA VENDITORI DIVERSI.

• IoT IN LICENSED SPECTRUM

QUANDO CI RIFERIAMO ALL'IOT NEL LICENSED SPECTRUM, IN REALTÀ, PARLIAMO DI SPECIFICHE PER L'INVIO DI DATI.

LE PIÙ FAROSE SONO:

- LTE CAT 0: HA UNA VELOCITÀ MASSIMA DI 1 Mbps IN HALF-DUPLEX CON LA POSSIBILITÀ DI ANDARE IN SLEEP PER QUILCHE SECONDO (UTILIZZATO PER LO PIÙ NEGLI ASCENSORI), BANDWIDTH 20 MHz

- LTE -n: LA BANDWIDTH VIENE RIDOTTA A 1,4 MHz, DATA RATE 200 Kbps IN HALF-DUPLEX CON SLEEPING TIME DI MINUTI.

- NB-IoT: SVILUCCATO PER LO PIÙ MANTENUTO DA HUAWEI, PARLANO DI UNA BANDWIDTH DI 180 KHz IN HALF-DUPLEX CON DATA RATE DI 30 Kbps DOWNLOAD E 60

- **CONSTRAINED APPLICATION PROTOCOL (CoAP)**
- NEL MONDO DELL' IoT NON SI POSSONO USARE PROTOCOLLI PESANTI COME HTTP; SI USA INVECE IL CoAP POICHÉ: PRESENTA HEADERS RIDOTTI, SUPPORTA REST ASINCRONI, SUPPORTA SCambi DI MESSAGGI TRA PUBLISH E SUBSCRIBER IN MACHINE TO MACHINE (M2M) COMMUNICATION. IN BREVE È' HTTP LEGGERO.

• CoAP MESSAGING

- LOGICAMENTE IL CoAP HA DUE LAYER, UNO DI SOPRA PER DOMANDE E RISPOSTE, UNO DI SOTTO PER LA MESSAGGISTICA, ENTRANGI SONO SOPRA L' UDP, CHE APPUNTO È IL PROTOCOLLO CHE UTILIZZA. POICHÉ È RAPIDO E LEGGERO A SPESA DELL' INFIDABILITÀ. PER SOPPIARE A QUESTO PROBLEMA IL CoAP PRESENTA DUPLICATE CHECK E ACKNOWLEDGMENT MATCHING ALL' INTERNO DEL MESSAGGIO; QUEST' ULTIMO È DI TIPO REQUEST - RESPONSE.
- I TIPI DI MESSAGGIO INVIAZI SONO:

Message type	Description
Confirmable	Reliable message delivery, recipient required to confirm by sending acknowledgment
Non-confirmable	Not acknowledged, delivery not guaranteed
Acknowledgment	Confirms delivery of a specific confirmable message
Reset	Indicates a message was received, but recipient is missing some context to process it properly
Piggy-backed response	Included in the acknowledgment message, provides data response, e.g., sensor reading
Separate response	Sent as a delayed response to a prior request that needed time to process

- I METODI DI INVIO SONO:

GET	Retrieves a representation of information corresponding to the specified URI
PUT	Requests that the identified resource be updated with the enclosed representation, optionally created if it does not exist
POST	Request that the enclosed representation be processed, e.g., new resource created or existing updated
DELETE	Deleted resource identified by URI

- CoAP USA LO STANDARD URIs (UNIFORM RESOURCE IDENTIFIERS) PER IDENTIFICARE IL DISPOSITIVO DA QUI ARRIVANO LE INFORMAZIONI. AL POSTO DI GET, PUT, POST, DELETE, ALCUNI FRAMEWORKS IOT USANO CREATE, RETRIEVE, UPDATE, DELETE.
- CoAP SUPPORTA BROADCAST E MULTICAST PER LA MESSAGGIISTICA IN UNA SINGOLA TRASMISSIONE. CoAP PRESENTA ANCHE CROSS-PROXIES CHE EFFETTUANO TRADUZIONI TRA ENDPOINT CHE USANO APPLICAZIONI DIFFERENTI, AD ESEMPIO POSSONO TRASFORMARE UN COAP IN HTTP MA NON VICEVERSA ESSENDO HTTP PIÙ PESANTE DI COAP.

• MESSAGING AND QUEING

- UN CLASSICO METODO DI MESSAGGIISTICA, I PUBLISHER POSTANO QUALcosa GLI SUBSCRIBER RICEVONO I DATI (E' MQTT). QUESTO MECCANISMO E' UTILE NELL' IOT POICHÉ:

- DISACCOPPIA PUBLISHER E SUBSCRIBER;
- PERMETTE COMUNICAZIONI ASINCRONE;
- E' FACILMENTE SCALABILE SE LO E' IL NODO CENTRALE;

• MESSAGE QUEUING AND TELEMETRY SYSTEM (MQTT)

- IL PUNTO FORTE DELL' MQTT E' IL SISTEMA DI PUBLISHER, BROKER E SUBSCRIBER.

UTILIZZA TCP PER UNA COMUNICAZIONE AFFIDABILE.
DEFINISCE 14 MESSAGGI PER LA COMUNICAZIONE TRA PUBLISHER E SUBSCRIBER.

Message type	Value	Description
CONNECT	1	Request to connect
CONNACK	2	Connect acknowledgment
PUBLISH	3	Publish message
PUBACK	4	Publish acknowledgment
PUBREC	5	Publish received
PUBREL	6	Publish release
PUBCOMP	7	Publish complete
SUBSCRIBE	8	Subscribe request
SUBACK	9	Subscribe acknowledgment
UNSUBSCRIBE	10	Unsubscribe request
UNSUBACK	11	Unsubscribe acknowledgment
PINGREQ	12	Ping request
PINGRESP	13	Ping response
DISCONNECT	14	Disconnect

- L' MQTT BROKER TIENE TRACCIA DEGLI STATI TRA PUBLISHER E SUBSCRIBER E SI OCCUPA DI RI SOLVERE I PROBLEMI DI NON RAGGIUNGIBILITÀ E DISCONNESSIONI.
- LA COSA PIÙ IMPORTANTE DELL' MQTT È CHE FORNISCE TRE DIFFERENTI LIVELLI DI QUALITÀ DEL SERVIZIO PER L' INVIO DEL MESSAGGIO:

- QoS 0: INVIAZIONE PASSIMO UNA VOLTA, BEST-EFFORT SENZA CONFERMA DI RICEZIONE;
- QoS 1: INVIAZIONE ALMENO UNA VOLTA, CONFERMA DI RICEZIONE, POSSIBILI DUPLICATI;
- QoS 2: INVIAZIONE ESATTAMENTE UNA VOLTA, CONFERMA DI RICEZIONE COMPLETA, NON HA DUPLICATI.

ALL'AUMENTARE DEL QoS AUMENTA L' OVERHEAD.

- MQTT SUPPORTA ANCHE I MESSAGGI "WILL" DOVE SI INDICA AL SUBSCRIBER L' ULTIMA AZIONE DA SVOLGERE PRIMA CHE LA COMUNICAZIONE VENGA INTERRUTTA; IL LINK PUÒ ESSERE CHIUSO ATTRAVV

SO UN CONTROL MESSAGE O A CAUSA DI ERRORE

(ERRORE DI RICHIESTA PER UN DATO DA TIME-TO-LIVE)

- I VARI "ARGOMENTI" DI UN SISTEMA IoT CON MQTT SONO PUBBLICATI SEGUENDO UN'ORDINAMENTO A SOTOCARTELLA TRAMITE "/".

AD ESEMPIO UN SUBSCRIBER DI:

EDIFICIO 5/PIANO 3/CAMERA 305/TEMPERATURA/TI

RICEVERÀ TUTTI I MESSAGGI PUBBLICATI IN QUELLA SOTOCARTELLA (IN QUESTO CASO QUEGLI INVIAZI DAL THERMOSTATO TI).

SI PUÒ USARE ANCHE "/" CHE PERMETTE DI RICEVRE I MESSAGGI DI TUTTI I COMPONENTI DI QUELLA SOTOCARTELLA.

ESEMPIO CON TUTTI I DISPOSITIVI E SOTOCARTELLE:

ED 5/PIANO 3/CAM 305/#

SI PUÒ USARE ANCHE "+" PER SPECIFICARE SOLO UN TIPO DI MISURAZIONE (SOLA UMIDITÀ ETC.)

CAPITOLO 4

CLOUD

- IL CLOUD È DOVE SI INCONTRANO LE GRANDE QUANTITA' DI DATI IoT E LE APPLICAZIONI O SERVIZI CON LA QUALE OPERANO.

CLOUD COMPUTING

- È UN NUOVO CONCETTO PERMETTE L'ACCESSO DA RE-

NOTO A RISORSE DI COMPUTING TRA CUI SERVER, STORAGE, NETWORK E SERVIZI.

LA VELOCITÀ CON LA QUALE VENGONO GARANTITI QUESTI SERVIZI È ELEVATA E LE RISORSE SONO GESTITE NEI DATA CENTER, QUESTI ULTIMI SONO "DINAMICI E ELASTICI" NEL SENSO CHE, IN BASE ALLE NECESSITÀ, È POSSIBILE APPLICARLI FACILMENTE IN TERMINI DI POTENZA DI CALCOLO E SPAZIO.

- I SERVIZI CLOUD FORNITI DAI PRINCIPALI CLOUD PROVIDER SONO DEFINITI "PUBLIC CLOUDS" QUELLI PER AZIENDE "PRIVATE CLOUDS", E INFINE GLI "HYBRID CLOUDS" SONO UN MIX.

NEI CLOUD RETONI, SICUREZZA E PRIVACY SONO GESTITI DAI PROVIDER E QUINDI L'USUARIO NON SGRAVATO DA QUESTO COMPITO, LE FUNZIONALITÀ MIGLIORI PER L'UTENTE SONO:

- SPAZIO APPARENTEMENTE INFINTO;
- COMPUTING RESOURCE APPARENTEMENTE INFINTO;
- DIMENSIONE VARIABILE IN BASE ALLE NECESSITÀ;
- NESSUNA SPESA DI UPGRADE FISICO;
- OPERAZIONI SEMPLIFICATE DATE DAL MANAGEMENT VIRTUALE;
- AFFIDABILITÀ, SICUREZZA E RESILIENZA;

- QUESTE CARATTERISTICHE DISCENDONO DALLA VIRTUALIZZAZIONE < DAL MULTIPLEXING TRA UTENTI.

LA VIRTUALIZZAZIONE DISACOPPIA TUTTI QUESTI REQUISITI DI RISORSE ATTRAVERSO "VM" O "CONTAINERS".

IL COSTO RICHIESTO PER IL LORO UTILIZZO VARIA DALLA CAPACITÀ DI CALCOLO UTILIZZATO, SPAZIO

ETC...

QUESTA EFFICIENZA E SCALING ATTRAE SPESO STARTUPS.

IN BASE ALLA DIMENSIONE, I CLOUD PROVIDER POSSONO AVERE PIÙ DATACENTER IN PIÙ REGIONI, ANCHE PER ADEGUARSI ALLE VARIETÀ LEGGI.

GLI SVANTAGGI PRINCIPALI SONO:

- PERDITA DI UTILIZZO O CLOUD OUTAGES;
- SICUREZZA E DATI POGNSI CONTRO IL PROPRIO CONTROLLO;
- VENDOR LOCK-IN;

• MODELS OF CLOUD COMPUTING

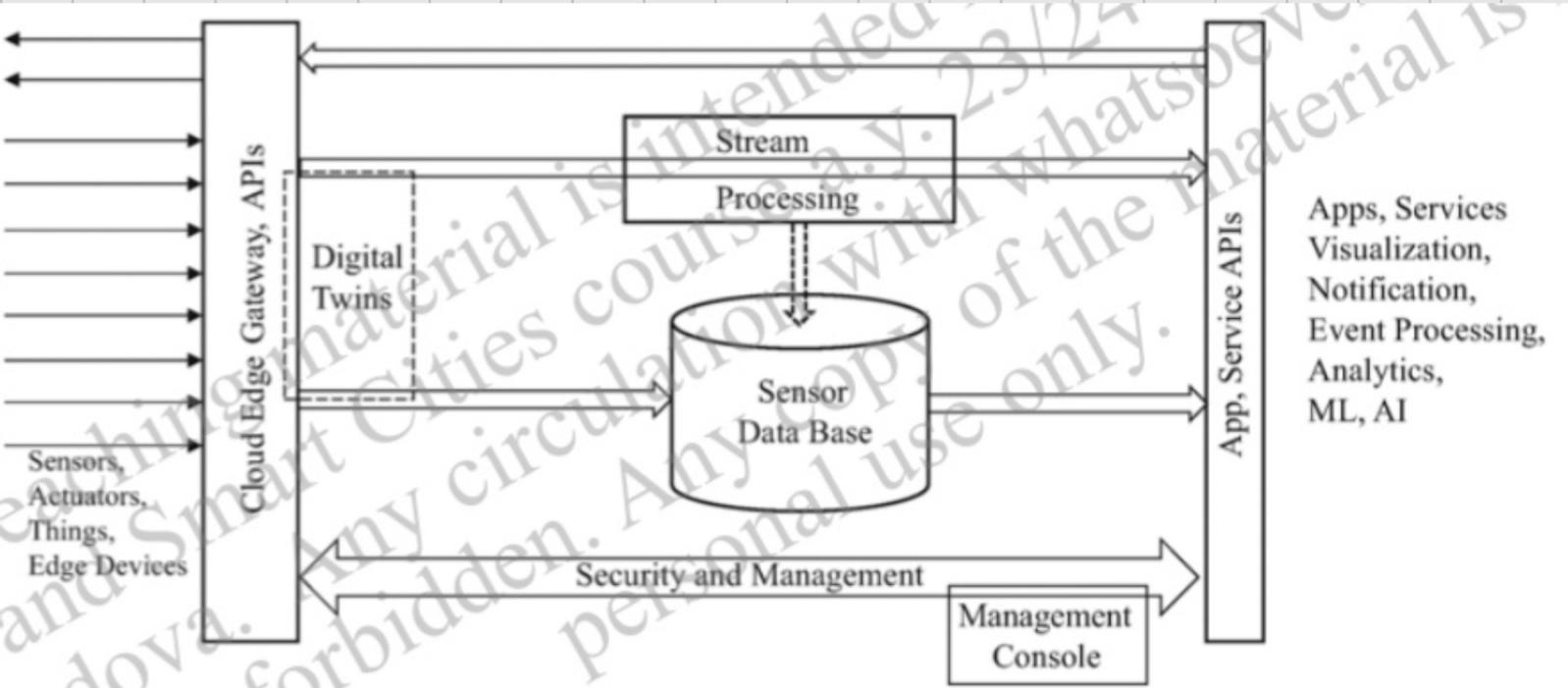
End-user applications, cloud clients

	Software as a Service (SaaS)	Serverless Computing (Function as a Service, FaaS)
Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Applications: CRM, email, office productivity, games
Language runtime, libraries, database, web servers, development tools	Virtual machines	Function instantiation, activation, scaling
Servers, storage, network		

- 1) SOLO SPAZIO, NETWORK O SERVER.
- 2) VM CON SISTEMA OPERATIVO, COME IN 1), SI CUREZZA LASCIATA ALL'UTENTE, COMPRESA LA GESTIONE DI FILE ETC... .
- 3) VIRTUAL MACHINE CON CLOUD SUPPORTING E SERVICES, CON PROCESSORI ANNESSI FORMATI, LIBRE ETC... UTILIZZATO MOLTO NELL'IOT.
- 4) VM CON POCHE APPLICAZIONI UTILIZZABILI MA

Y MOLTO POTENZE (GS. GOOGLE STUA).
VM DENG L' UTENTE IP BREVE FORNISCE
SOLO I DATI E IL CLOUD PROVIDER FA
IL RESTO.

- **IoT SYSTEM CLOUD COMPONENTS**
- ALL' INTERNO DEL SISTEMA CLOUD CI SONO COMPOGNENTI PER ACQUISIRE, PREPROCESSARE, E IMMAGAZINARE DATI PER Poi ESSERE ELABORATI.
QUESTI COMPOGNENTI SONO:
 - EDGE INTERFACE AND DATA INGESTION;
 - TIME - SERIES STREAM PROCESSING;
 - DATA AGGREGATION AND STORAGE;
 - SECURITY AND MANAGEMENT;



- ESISTONO DUE LINEE DI STREAM DATA PROCESSING,
PAOTE' (DEFINITO SCHEMA "A") POICHE' ALCUNI DATI
VENGONO USATI PER AI E NEL DIRETTAMENTE
(WARM PATH) O ALTRI VENGONO NESSI PRIMA
PELLO STORAGE E Poi UTILIZZATI IN UN SECONDO
MOMENTO (COLD PATH).

ALCUNI SISTEMI IoT IMPLEMENTANO IL DIGITAL

TWINS OSSIA UN PROGRAMMA CHE SIMULA ALLA PERFEZIONE, ATTRaverso UN MODELLO, LA REACTA FISICA ANNESSA; INOLTRE TEORICAMENTE OGNI MO^{DO} DI PRACTICA APPLICATA NEL MONDO REALE DEVE REFLETTERSI SUL DIGITAL TWIN E VICEVERSA.

IL DIGITAL TWIN SERVE PER TESTARE SITUAZIONI REALI, SENZA PERO' DOVENDO SPENDERE PER ATTIVARIE PERCHE' E' APPUNTO UNA SIMULAZIONE.

- SIA PER LE APIs DI SINISTRA (PER I DATA INJECTION) CHE PER QUELLE DI DESTRA (UTILI APP MACHINE LEARNING E AI), E' NECESSARIO CREARE APPLICAZIONI NON CHE FUNZIONINO SU SINGOLI DISPOSITIVI O A SINGOLI SCOPI, MA A USI GENERICI.

• CLOUD ED EDGE GATEWAY

- E' IL COMPONENTE TRA IL CLOUD E GLI EDGE COMPONENTS.
IMPLEMENTA SICUREZZA AVANZATA OLTRE A TUTTE LE FUNZIONALITA' DI UN CLASSICO GATEWAY.

In GENERALE IL SUO PRIMO TASK E' ACQUISIRE DATI E INVIARE COMANDI AGLI ENDPOINTS, ANCH'E SO PUO' IMPLEMENTARE DIGITAL TWINS.

• IoT DATA INGESTION

- I DATI CHE ARRIVANO DAGLI EDGE NODE, LO FANNO IN GENERE AL CONCRETIZZARSI DI DETERMINATI EVENTI.

I DATI IN INGRESSO IN GENERE CONTENGONO I TIME STAMPS DELL'EVENTO E ANCHE I ME-

TA DATI CHE SERVONO A DESCRIVERE MEGLIO L'EVENTO STESSO.

LAVORARE CON QUESTI DATI PERMETTE DI FRONTEGGIARE DINAMICHE COME SCALING, VOLUNTEERING.

- I DATI ARRIVANO ATTRAVERSO ACCESS POINT / URLs PGR HTTP, SECRETS PORT O MESSAGE BROKERS. SI IDENTIFICANO ATTRAVERSO IP-PORTA IN BASE AL PROTOCOLLO UTILIZZATO.

I DATI UNA VOLTA ARRIVATI DEVONO ESSERE INDISTRIBUITI ALLO SPECIFICO SERVIZIO RICHIESTO, CON LO SPECIFICO QoS DATO.

GLI IoT CLOUD EDGE SERVICES POSSONO INCLUDERE SERVIZI DI MESSAGE HOSTING DEI BROKERS (QUINDI DEVONO IMPLEMENTARE MQTT)

- SE I DATI ARRIVANO IN UN FORMATO NON APPROPRIATO ALLORA DEVONO ESSERE CONVERGIRE DAL CLOUD IoT GATEWAY, DALL'APPLICAZIONE CHE LI RICEVE O PROPRIO NELLA FASE DI INJECTION.

A VOLTE LE QUANTITÀ DI DATI IN INGRESSO SONO ENORMI, QUINDI SONO NECESSARI SISTEMI DI SCALABILITY.

UNO DEI PIÙ FAMOSI È "KAFKA" CHE FORNISCE HIGH-THROUGHPUT IMPLEMENTATION, HIGH RELIABILITY E SCALABILITY ATTRAVERSO PARTIZIONAMENTO E REPLICAZIONI, VENNE SVILUPPATO LA PRIMA VOLTA PER GESTIRE FLUSSI DI DATI COME QUELLI DEI SOCIAL NETWORK.

• DIGITAL TWINS

- A volte è preferibile utilizzare APPLICAZIONI

NI ACCEDENDO PRIMA AL DIGITAL TWIN, GLI INVINO
POI I COMANDI, COSÌ CHE' SIA Poi IL DIGITAL
TWIN STESSO A MODIFICARE IL MEZZO FISICO.
QUALI VANTAGGI PORTA QUESTO FATTO?

- ACCESSO PIÙ RAPIDO;
- SEMPRE DISPONIBILE AL LAVORO;
- SALVA POTENZA E BANDWIDTH;
- HA UNA RAPPRESENTAZIONE ASTRATTA DELLE
INTERFACCIE, RENDENDOLO PIÙ IMPLEMENTABILE;
- CON QUESTO TIPO DI ACCESSO CI SI ACCONTENTA DEL
L'ULTIMO STATO SALVATO, E NON DI QUELLO REALE.
LA RAPPRESENTAZIONE ASTRATTA SI RIFERISCE ALLA
CAPACITÀ DEL CLOUD DI LAVORARE CON TIPI DI DATO
DIFFERENTI RENDENDOLO QUINDI PORTABILE.

• REAL TIME STREAM PROCESSING

- VARIE FORME DI STREAMING ANALYTICS POSSONO
ESSERE MESSE IN FUNZIONE PER CONTROLLARE
E SCOPRIRE EVENTI CHE POTREBBERO ESSERE
PERICOLOSI, E CHE NECESSITANO APPUNTO DI UNA
REAZIONE ISTANTANEA.

A VOLTE CHIAMA CHE PERSISTENTI DI CONTROLLO PIÙ "SINTI
PLICI" COME I PLC BASTANO SE PLICI STRUMENTI
E/O SCRIPT COME AD ESEMPIO NODE-RED.

• SHORT-TERM STREAMING STORAGE

- ALCUNE IMPLEMENTAZIONI DEI SISTEMI IOT DI
STREAMING PROCESSING INCLUDONO ALCUNE FORME
DI FAST-ACCESS ALLA MEMORIA IN MANIERA RETI-
TAGLIATA DEI DATI RIGUARDANTI EVENTI RECEN-
TEMENTE PASSATI PER ANALISI E CONTROLLO A POSTO

RIORI, IN GENERALE QUESTI DATI SONO PESSI NEGLI SSD.

• CLOUD IOT DATA STORAGE

- LA MIGLIOR PARTE DEI DATI VENGONO INSERITI NELLE GRANDI MEMORIE DEL CLOUD, QUESTI DATI SONO PESI UTILI PER APPLICAZIONI COME ML O AI POICHE' QUESTE LAVORANO CON GRANDE QUANTITA' DI DATI.

• PROPERTIES OF IOT DATA

- I DATI IOT HANNO IN COMUNE CON I BIG DATA DIVERSE PROPRIETA' DEFINITE CON "V".
 - **VOLUME**: QUANTITA' DI DATI ELEVATA;
 - **VELOCITY**: VELOCITA' ELEVATA, ALTA FREQUENZA;
 - **VARIETY**: MOLTE SOURCES, MOLTI TIPI DI DATI;
 - **VERACITY**: ALTA AFFIDABILITA', RENDONDANZA, E VERIFICA DELLA PROVENIENZA CON LA CONSISTENZA.

- I DATI IOT HANNO QUINDI PROPRIETA' UNICHE TESSE:

- TIME-SERIES DATA AND METADATA
- SEMI-STRUCTURED AND UNSTRUCTURED
- LIFECYCLE MANAGEMENT AND DATA RETENTION
- DATA ACCESS PATTERNS, WRITING AND RETRIEVAL

• TYPES OF IOT DATABASES

- LE IMPLEMENTAZIONI CLOUD DI UNO STORAGE IOT SERVICE CONSISTE IN UN SISTEMA DI INPUT TRA POSTING E SUBSCRIPTIONS CHE Poi E' SCRITTO NELL DATABASE, E UN SISTEMA DI OUTPUT, CHE E' ANCHE IL CUORE DEL DATABASE, CHE SUPPOSTO DIRSI E API.

FOR IT RUGBY E PPT'S.

LA SCELTA DEL TIPO DI DATABASE E' FATTA IN BASE A COME SI VOGLIONO FARE LE QUERIES SU COME SI VOGLIONO STRUTTURARE I DATI.

• RELATIONAL DATA BASE MANAGEMENT SYSTEMS (RDBMS)

- IN GENERALE SI USANO I DATABASE DEFINITI "LEGACY RDBMS" IN CUI I DATI SEGUONO UNA STRUTTURA RIGIDA E NON MODIFICABILE E SUPPORTANO LA PROPRIETÀ "ACID" (ATOMICITY, CONSISTENCY, ISOLATION AND DURABILITY).
Una struttura rigida non va bene per i database hot, perciò si usa un database RDBMS **NON LEGACY**; sicurando sua ntagli in termini di throughput e scalability a causa dell'overhead, inoltre serve un high licensing e un alto maintenance cost.
vediamo alcuni tipi.

• NOSQL DATABASE

- I DATABASE NO SQL SONO CHIAMATI COSÌ PERCHÉ PER COME SONO STRUTTURATI NON SUPPORTANO SQL. ESSI SONO RAPIDI, SCALABILI E SONO IDEATI PER WEB-APPLICATIONS E GRANDI VOLUMI DI DATI.
- IN BASE ALLA LORO STRUTTURA VENGONO CLASSIFICATI COME:
 - KEY-VALUE STORES;
 - DOCUMENT-ORIENTED DATABASES;
 - COLUMN-ORIENTED DATABASES;
 - GRAPH DATABASES;

{ PIÙ
POPOLARI

- NEI DOCUMENT-ORIENTED I DATI POSSONO ESSERE DI QUALSIASI TIPO (XML, JSON).
- I COLUMN-ORIENTED DATABASE SONO UTILIZZATI PER APPLICAZIONI PASSIVE (RICERCHE WGB), UN ESEMPIO E' HADOOP.
- I GRAPH DATABASE SONO UTILIZZATI PER PRESENTARE STRUTTURE COMPLESSE.
- IL DATABASE NOSQL PIU' FAMOSO E' MONGODB E QUANDO SI SCEGLIE UN DATABASE BIETTI CONSIDERARE ANCHE LE DIPENDENZE.

• CLOUD IoT ANALYTICS

- QUANDO SI FA CLOUD ANALYTICS BISOGNA TENERE IN CONSIDERAZIONE DIVERSI ASPECTI, OGNIUNO DEI QUALI E' CAPITO DI UNO SPECIFICO SETTORE; ESSI SONO:
 - DESCRIPTIVE ANALYTICS: ANALIZZA UN EVENTO DOPO CHE E' ACCADUTO, RISPONDE ALLA DOMANDA "WHAT HAPPENED";
 - PREDICTIVE ANALYTICS: ANALIZZANDO LO STATO ATTUALE E QUELLI PASSATI, PROVA A PREDIRE I FUTURI, RISPONDENDO A "WHAT WILL HAPPEN NEXT";
 - PRESPECTIVE ANALYTICS: E' LA PIU' SOFISTICATA, STIMA IN CORSO D'OPERA LO STATO E NE GUIDA LA TRAIETTORIA FUTURA.
- LE ULTIME DUE SONO DOMAIN-SPECIFIC E QUINDI DIFFICILI DA RENDERLE PORTABLE E NECESSITANO DI COSTI ELEVATI.

• VISUALIZATION AND DASHBOARDS

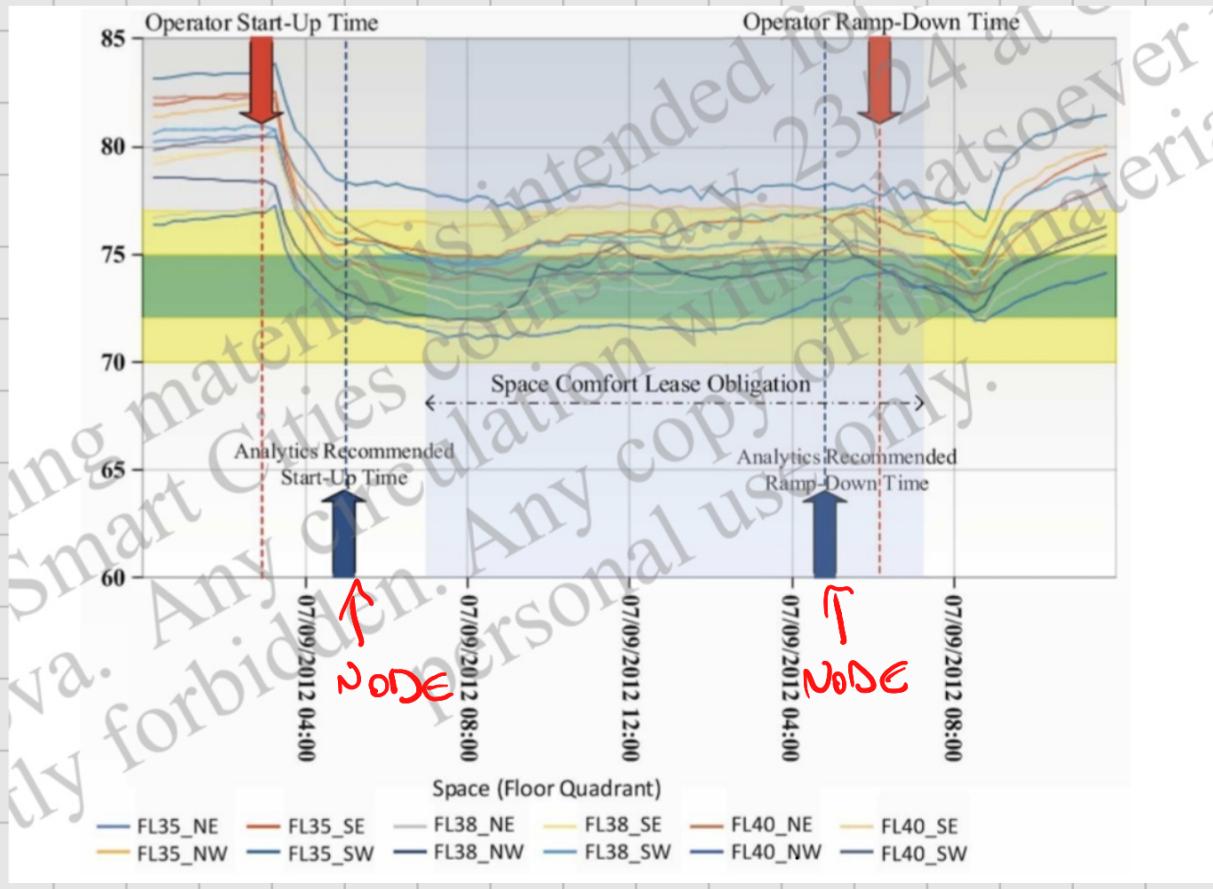
- ALCUNE OPERAZIONI NON SONO POSSIBILI DA

SVOLGERE PER UN NUOVO, QUINDI ENTRA IN LUCE IL RUOLO DEL **SYSTEM OPERATOR** OSSIA UNA PERSONA CHE, TRAMITE UNA GUI DI ALTO LIVELLO, CONTROLLA LO STATO DEL SISTEMA E SI COMPORTA DI CONSEGUENZA IN CASO DI PROBLEMI.

DIVIDIAMO PER UN OPERATORE HA DEI COSTI ELEVATI MA POSSIEDE DI AVERE UNA SICUREZZA IN ALTA GRAZIE ALLA SUA ESPERIENZA.

DI SEGUENTE UN CASO CHE MOSTRA DIFFERENZE TRA COME SI COMPORTA UN OPERATORE E UN DISPOSITIVO.

• USE OF IoT ANALYTICS



CAPITOLO 5

• SECURITY AND MANAGEMENT

IL PROBLEMA DI SICUREZZA NEL MONDO DI

E' MOLTO IMPORTANTE POICHÉ, VISTO CHE IL NUMERO DEI DISPOSITIVI E' ELEVATISSIMO, LA SUPERFICE D'ATTACCO E' MOLTO ESposta.

- UN ALTRO IMPORTANTISSIMO ASPECTO E' LEGATO ALLA PRIVACY CHE VA TENUTO IN CONSIDERAZIONE NELLO SPECIFICO.
OGNI DISPOSITIVO DOVRÀ REBBERE POTER COMUNICARE SOLO CON IL NUMERO MINIMO NECESSARIO DI DISPOSITIVI, INOLTRE LA COMUNICAZIONE BIDIREZIONALE DEVE ESSERE FATTA SOLO CON DISPOSITIVI ALCUNO SCALTI E FIDATI.
- **IoT SECURITY THREATS AND VULNERABILITIES**
 - IN GENERALE POTREMO DIRE CHE LA SICUREZZA E' LA PROTEZIONE DA ACCESSI NON AUTORIZZATI, IN REALTA' I PERICOLI SONO TANTI, E LE TECNICHE DA SALVAGUARDARE SONO:
 - **CONFIDENTIALITY**: SI ASSICURA CHE I DATI SONO DISPONIBILI SOLO DAGLI AUTORIZZATI.
 - **INTEGRITY**: SI ASSICURA CHE I DATI SONO ACCURATI E NON SONO STATI MODIFICATI DA MALEVOLI.
 - **AVAILABILITY**: SI ASSICURA CHE I DATI SIANO REPERIBILI OGNI VOLTA CHE E' NECESSARIO.
 - ESISTONO DIVERSI TIPI DI ATTACCO:
 - **PHYSICAL ATTACKS**: SU DISPOSITIVI ISOLATI CHE POSSONO ESSERE SOSTITUITI.
 - **SOFTWARE ATTACKS**: MALEVOLENT CODE INSEGNATI

TEST IN THE SOFTWARE.

- **NETWORK ATTACKS**: SPYING O DDOS, WI-FI RELESS NETWORK EXPOSED.
- **ENCRYPTION ATTACKS**: I DATI VENGONO CRYPTATI CON ANNESSO RICATTO.
- **ROUTING**: UN NODO MALEVOLO SI IDENTIFICA COME PARTE DELLA RETE.

• OPERATIONAL TECHNOLOGY (OT) SECURITY CONSIDERATION

- I LEGACY INDUSTRIAL SYSTEM (OT) PREFERISCONO PRESERVARE LA SICUREZZA DEI PROPRI MACHINARI ISOLANDOLI DALLE FONTI ESTERNE. QUESTO METODO DI AGIRE E' ERRATO POICHÉ PRENDE IN CONSIDERAZIONE SOLO IL PRIMO DI QUESTI 3 ASPETTI:

- **SAFETY**: CONTROLLO RIGOROSO DEI MACHINARI, RI-TESTING E CERTIFICAZIONI.
- **RELIABILITY**: IL SISTEMA DEVE OPERARE IN MODO AFFIDABILE CONTINUAMENTE.
- **RESILIENCE**: RESISTENZA AI FAULTS RANDOM DI TORNUARE ALLO STATO PRECEDENTE

• RISK ANALYSIS

- QUANDO SI PARLA DI RISK ANALYSIS SI PARLA DI RISK AVOIDANCE OSSIA CIÒ CHE SERVE STUDIARE E IMPLEMENTARE PER EVITARE UN ERRORE, RISK ACCEPTANCE OSSIA ACCETTARE CHE UN ERRORE POTREBBE CAPITARE SAPENDO CHE NON E' GRAVE.

SI PUO' ANCHE PAGARE EFAR GESTIRE QUESTA ANALISI A TERZI

ARMING ITSELF

• SECURITY THREAT MODELING

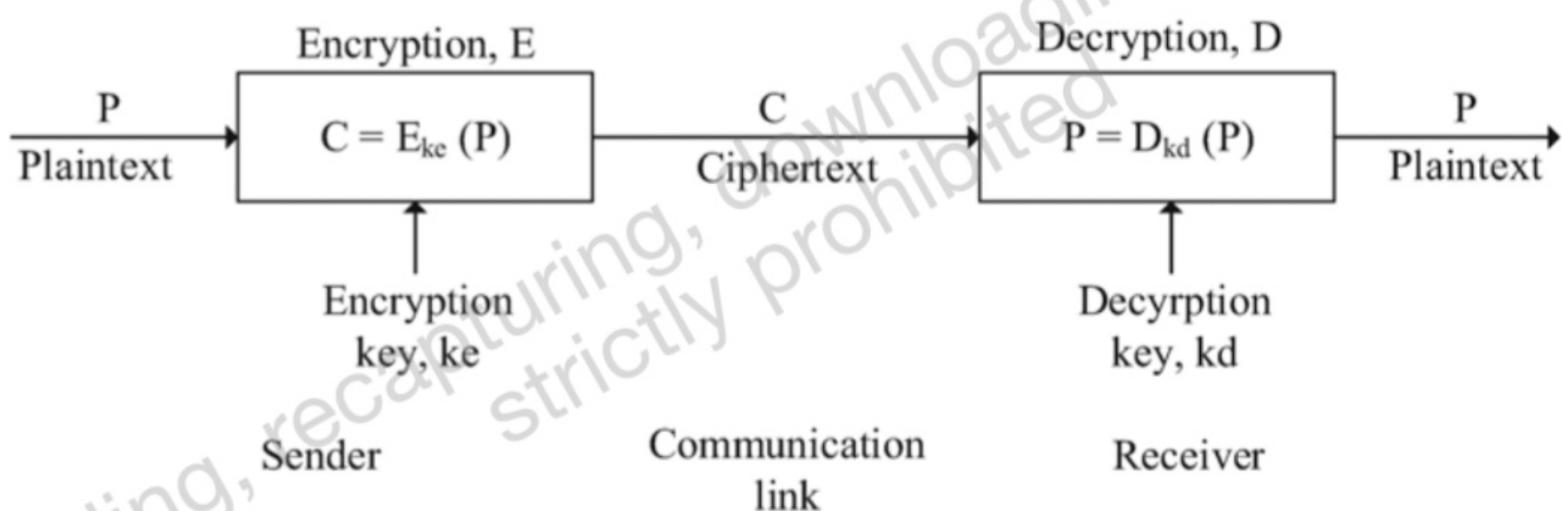
- PER PREVENIRE I PROBLEMI DI SICUREZZA, SI SEGUONO ALCUNI STEP:
 - SI MODELIA IL SISTEMA;
 - SI NUMERANO LE MINACCIE;
 - SI MITIGANO LE MINACCIE;
 - SI VALUTANO LE MITIGAZIONI;
 LE MINACCIE POSSONO ESSERE LE SEGUENTI.

Threat	Property violated	Description
Spoofing	Authentication	Impersonating someone or something else, e.g., a device
Tampering	Integrity	Altering hardware, data (in motion or at rest), or code
Repudiation	Nonrepudiation	Denial of performing an action (inability to trace)
Information disclosure	Confidentiality	Exposing information to unauthorized parties
Denial of service	Availability	Deny or degrade services, e.g., through excessive resource consumption
Elevation of privilege	Authorization	Gain capabilities without proper authorization, e.g., system access

• CRYPTOGRAPHY

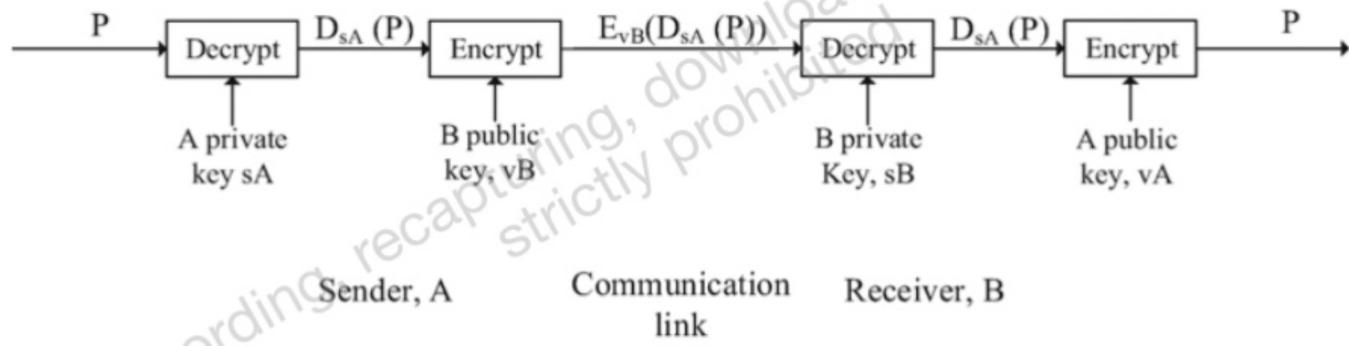
- LA CRIPTOGRAFIA È UN SISTEMA PER RENDERE UNA COMUNICAZIONE CONFIDENZIALE, INTEGRATA E AUTENTICA.

PER PRIMA COSA È SUGGERITO DI USARE TRUST WORTHY LIBRARIES.



- QUANDO AVVIENE UNA COMUNICAZIONE CI SI SCAVIA UNA CHIAVE DI SICUREZZA PUBBLICA, SE LO SCAMBIO È SIMETRICO DYNUNO USA LA STESSA CHIAVE PER CRYPTARE E DECRYPTARE, MA È MENO SICURA;
- SE LO SCAMBIO È ASSIMETRICO SI OTTE NC UNA MAGGIORE SICUREZZA.

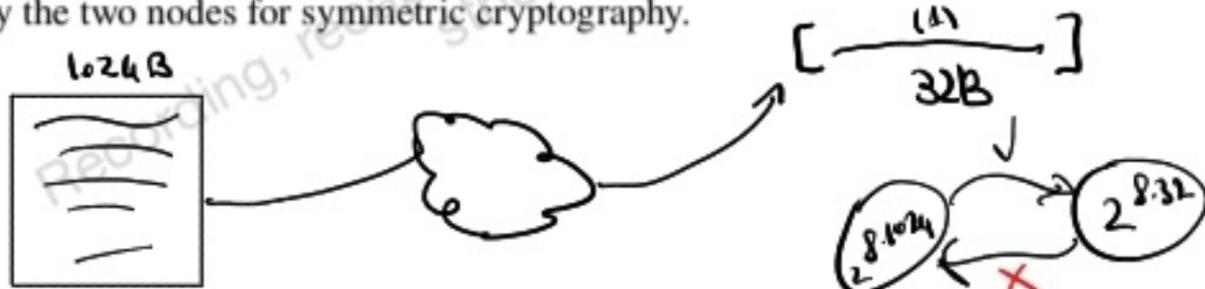
Public key cryptography can achieve simultaneously confidentiality, integrity and authentication using a double transformation.



- THIS USE AGS 128 BITS WITH A CHACE OF KEY LENGTHS: 128, 192 & 256 BITS.

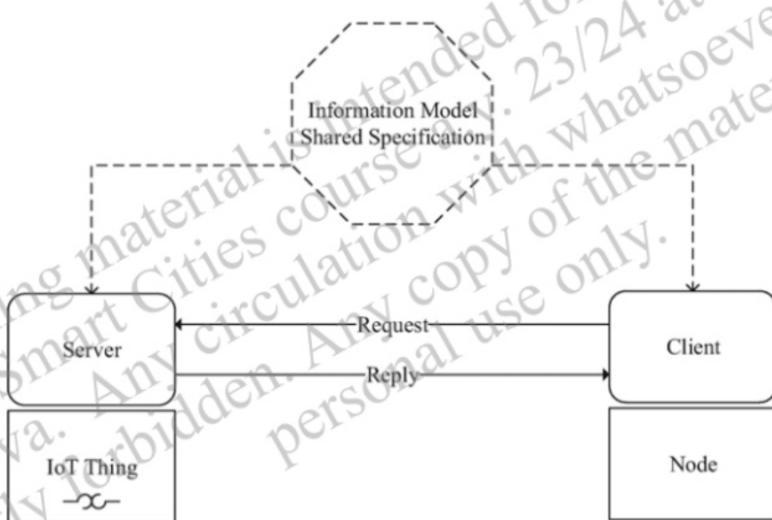
Cryptographic Scheme	Confidentiality	Integrity	Authentication	Digital signature
Asymmetric, $E_{vB}(P)$	Yes	Yes	No	No
Asymmetric, $E_{sA}(P)$	No	Yes	Partial, yes w MAC	Yes
Double transformation	Yes	Yes	Yes	Yes
Symmetric, shared key	Yes	Yes	Partial, yes w MAC	No

Cryptographic message authentication is a secure way to ensure that the received message corresponds to its actual original, i.e., the plaintext sent by A. This is accomplished by creating a message authentication code(MAC). Authentication based on MAC requires that senders and receivers share the secret authentication key, preferably a different one than the shared key that may be used by the two nodes for symmetric cryptography.



CAPITOLO 6

- IoT DATA MODELS AND METADATA
- LA SFIDA MIGLIORE DEL MONDO IoT, CHE PROV= RERRE UN INCREMENTO DI VENDITE DEL 40%, E' OTTENERE L'INTEROPERABILITÀ TRA SISTEMI E TIPI DI DATO DIFFERENTI.
IL VERO PROBLEMA E' CHE NON CI SONO AL M= MENTO STANDARD O DEFINIZIONI UNIVERSALMENTE ACCETTATE.
- IoT DATA AND INFORMATION MODELS
- IL MODELLO DI UN SENSORE LO DEVE DESCRIVERE FISICAMENTE ATRAVERSO UN'AUTRAZIONE IN TERMINI DI DATI E NESTA DATI.
PER ESSERE UTILI, QUESTI DATI DEVONO CONTENERE IMPORTANTI INFORMAZIONI COME UNITÀ DI MISURA, MODELLO ETC..., INOLTRE BISOGNA SPECIFICARE LE CONDIZIONI IN CUI IL DATO E' STATO CATTURATO E ACCESS METHODS.
- INTEROPERABILITY USING A SHARED INFORMATION MODEL



- I SOFTWARE CHE RAPPRESENTANO I Dati POSITIVI, SONO IMMAGAZINATI ALL'INTENSO DELL'IOT SERVER E CONNESSIONE TE SONO DRIVERS. IN PIÙ DEV'IMPLEMEN= TARE LE AZIONI

ASSOCIATE AL DEVICE PGR POTERVI ACCEDERE.
IN BASE AL SISTEMA IL SERVER POTREBBE RISIENE-
RE IN UN PROXY DEVICE.

- **DATA SEMANTICS**
- IL PRIMO OBIETTIVO DI UN MODELLO IoT È FA-
TARE L'INTEROPERABILITÀ SEMANTICA.
A VALIG UTILIZZANO TECNICHE CON L'ONTOLOGIA
PER DESCRIVERE MEGLIO IL COMPORTAMENTO
DI UN DISPOSITIVO.
LA SEMANTICA WEB USA RDF (RESOURCE DEFINI-
TION FRAMEWORK) E ANCHE WOL (WEB ONTOLOGIES
LANGUAGE); OSSIA PERMETTONO DI UTILIZZARE
E RAGGIUNGERE UN DISPOSITIVO PUR NON CO-
NSCENDOLO, MA ANDANDO A PRENDERE IL LORO
MODELLO DA QUESTE APPLICAZIONI.
- **STRUCTURE OF IoT INFORMATION MODEL**
- UN DISPOSITIVO IoT PRESENTA IL SUO MODELLO
MODELLATO ATTRAVERSO OOP (OBJECT ORIENTED
PROGRAMMING) POICHÉ SI PRESTA NELLA
MAGGIOR PARTE DEI CASI A QUESTO MONDO.
CI SONO 4 TIPI DI MODELLI (GENERALMENTE
UTILIZZATI):

Element	Description
Object type	Physical thing being modeled (endpoint, device)
Properties, attributes	Object attributes, data, metadata
Interactions	Ways to interact with object, access points, actions
Links	To other objects, compositions, and collections

- **OBJECT TYPE**
- CON QUESTA TIPOLOGIA SI PUOLE MODELLARE UN OGGETTO DIVERSO, ED E' MODELLOATO TRAMITE UNA CLASSE.
A OGUNA SI ASSEGNA UN NOME UNIVOCO PER IDENTIFICARLA, GS. "BEDROOM 28".

• PROPERTIES AND ATTRIBUTES

- SONO I DATI PER LA LETTURA, AD ESEMPIO SE SI USA F° O C°, E SONO **READ-ONLY**.

• INTERACTIONS

- LE INTERAZIONI INCLUDONO INTERFACCE E NEI TUTTI CHE SUPPORTANO REQUEST E RESPONSE, INCLUDONO ANCHE PORTI PER I PROTOCOLLI CHE SPESO SONO APIs CHE A VOLTE PERMETTONO IL DATA RETRIEVAL OF ATTRIBUTES AND VALUE.

• LINKS

- E' UN NODO PER COLLEGARE VIRTUALMENTE PIU' DISPOSITIVI, E' MOLTO UTILE PER DEFINIRE COMPONENTI ASTRATTE CHE SONO DESCritte DA PIU' DATI CONTEMPORANAMENTE, GS. CONFORTO → VLINGUE DI TEMPERATURA, UVIDITÀ E LUCE VISUA.

• PAYLOADS AND DATA SERIALIZATION

- I MESSAGGI NECESSITANO DI ESSERE SERIALIZZATI COSICHE' IL RICEVITORE POSSA ANALIZZARLI CORRETTAMENTE.

IN GENERALE SI USA JSON CHE ESPRIME I DATI IN TERRINI DI "NON CI VALORE", AD ESEMPI:

```
{  
  "id": "150a3c6e-bef0ee0e"  
  "sensor": "m:",  
  "temp": "m:",  
  "curVal": "n:77.6",  
  "unit": ".F"  
  "DateTime": "t: 2019-07-15T14:50:07Z UTC"  
}
```

HAYSTACK
COMPLIANT
NOTATION
WITH JSON

- UN ALTRO NODO PIÙ COMPATTO È BINARIO PER SERIALIZZARE I DATI È UTILIZZARE CBOR (CONCISE BINARY OBJECT REPRESENTATION)

• IoT FRAMEWORKS

- PER OTTIME NGRE L'INTEROPERABILITÀ DESIDERATA SI UTILIZZANO I FRAMEWORK, OSSIA UNA SERIE DI PROTOCOLLI E DI MECCANISMI DI SERIALIZZAZIONE.

I FRAMEWORKS POSSONO CONTENERE BRIDGES E PROTOCOL CONVERETERS.

I FRAMEWORKS OPERANO TRA TRANSPORT LAYER E APPLICATION LAYER.

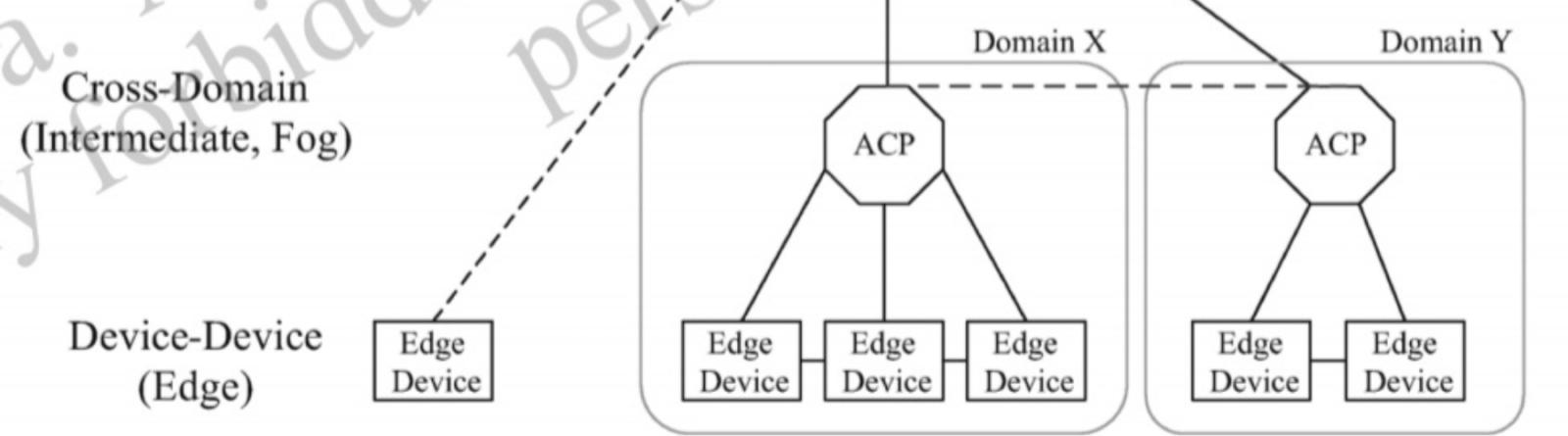
I FRAMEWORK IoT DEFINISCONO COME AVVENGONO I MECCANISMI DI NAMING E ADDRESSING.
GLI OGGETTI POSSONO SEGUIRE UN'IDENTIFICAZIONE URI, URL, URN.

ALCUNI FRAMEWORK UTILIZZANO SIMIL-DNS.

• SCHEME OF INTEROPERABILITY

Big-Data Aggregation
(Cloud)





FINE

