

**A038 - ESAME DI STATO CONCLUSIVO DEL SECONDO CICLO DI ISTRUZIONE**  
Indirizzo ITIA - INFORMATICA E TELECOMUNICAZIONI ARTICOLAZIONE "INFORMATICA"  
(Testo valevole anche per gli indirizzi quadriennali IT32)  
Disciplina: SISTEMI E RETI

***Il candidato svolga la prima parte della prova e due tra i quesiti proposti nella seconda parte.***

**PRIMA PARTE**

**Gestione eventi con grandi folle**

Una città italiana di interesse turistico internazionale ha deciso di sperimentare un nuovo sistema di monitoraggio del flusso delle persone in occasione di grandi eventi (culturali, artistici, sportivi). A tali eventi, che si svolgono in un preciso luogo della città, si potrà accedere unicamente mediante biglietti a pagamento o anche gratuiti.

Nell'intera area del comune saranno presenti punti di informazione automatici (totem), basati su touch screen, dove l'utente potrà informarsi su uno o più eventi e acquistare il biglietto in autonomia.

Per la gestione del sistema di monitoraggio del flusso delle persone in occasione di un evento, viene messa a disposizione una sede operativa composta da due piani; al primo piano sarà presente un'area dedicata all'assistenza pre- e post- vendita dei biglietti, dove gli operatori potranno svolgere le loro mansioni; al secondo piano sarà presente la sala di controllo dove il personale addetto, attraverso telecamere di sorveglianza, potrà visionare le immagini in diretta dei luoghi interessati dagli eventi. Uno degli obiettivi è quello di ridurre il sovraffollamento nelle aree critiche e poter intervenire con prontezza in caso di necessità.

In punti strategici della città, verranno infatti collocate telecamere di monitoraggio e dispositivi azionabili a distanza (per esempio semafori, barriere a scomparsa, pannelli informativi o altro) che permetteranno di gestire al meglio il flusso di persone verso il luogo dell'evento, anche con l'ausilio di personale in loco. I dispositivi, azionabili a distanza, verranno gestiti attraverso un server HTTP interno al dispositivo stesso, accessibile da remoto.

Nell'area circostante l'evento (ad esempio un concerto) sarà presente personale addetto alla validazione degli ingressi all'evento, all'assistenza e al pronto intervento. Per lo svolgimento delle proprie mansioni, il personale in loco sarà dotato di un dispositivo mobile con il quale può comunicare con la sede operativa ed essere costantemente aggiornato sullo stato dei dispositivi azionabili a distanza sopra citati.

Il candidato analizzi la realtà di riferimento e, formulate le opportune ipotesi aggiuntive, svolga i seguenti punti:

1. sviluppi una descrizione di massima, anche supportata da uno schema grafico che presenti il sistema (organizzazione della rete informatica della sede operativa, modalità di connessione con le telecamere per il monitoraggio e i dispositivi remoti e loro attivazione e gestione), e ne ponga in evidenza i vari componenti hardware e software necessari, motivando le scelte effettuate;
2. descriva in modo dettagliato le possibili modalità di comunicazione tra la sede operativa ed il personale in loco dedicato alla gestione del flusso delle persone partecipanti all'evento, anche in relazione alla validazione dei biglietti di ingresso;
3. definisca le tecnologie di comunicazione tra la sede operativa e i punti di informazione (totem) dislocati sull'intera area del comune;
4. descriva la modalità attraverso le quali sarà possibile evitare interruzioni di servizio.

## SECONDA PARTE

- I. In relazione al tema proposto nella prima parte, si consideri la gestione dei filmati e delle immagini che vengono trasmessi dalle telecamere per il monitoraggio, e si propongano soluzioni per il relativo salvataggio all'interno dell'infrastruttura della sede centrale oppure nel cloud, definendone vantaggi e svantaggi.
- II. In relazione al tema proposto nella prima parte, si discuta come possono essere attivati e gestiti i dispositivi remoti dotati di server HTTP interno, utilizzando i metodi propri di questo protocollo, fornendo opportune esemplificazioni
- III. Il candidato illustri caratteristiche e possibili campi di applicazione di due tecnologie di comunicazione wireless a corto raggio quali, ad esempio, sistemi basati su RFID, NFC, Bluetooth Low Energy (BLE), IEEE 802.15.4.

- IV. In una rete locale è presente un host con la seguente configurazione:

```
hostname:      pcserverlab
IP address:    192.168.1.15/24
Default Gateway: 192.168.1.1
DNS1:         192.168.1.2
DNS2:         212.14.128.1
```

Effettuando da un altro PC della rete il ping all' IP Address di tale host, con il comando:

```
C:\Users\admin>ping 192.168.1.15 si ottiene in risposta
```

Esecuzione di Ping 192.168.1.15 con 32 byte di dati:

```
Risposta da 192.168.1.15: byte=32 durata=41ms TTL=56
Risposta da 192.168.1.15: byte=32 durata=32ms TTL=56
Risposta da 192.168.1.15: byte=32 durata=52ms TTL=56
Risposta da 192.168.1.15: byte=32 durata=38ms TTL=56
...
```

mentre effettuando il comando `C:\Users\admin>ping pcserverlab` si ottiene in risposta

*Impossibile trovare l'host pcserverlab. Verificare che il nome sia corretto e riprovare*

Inoltre, effettuando il comando `C:\Users\admin>ping www.istruzione.it` si ottiene la risposta:

```
Risposta da 92.123.181.19: byte=32 durata=20ms TTL=49
Risposta da 92.123.181.19: byte=32 durata=26ms TTL=49
Risposta da 92.123.181.19: byte=32 durata=214ms TTL=49
Risposta da 92.123.181.19: byte=32 durata=18ms TTL=49
...
```

Il candidato discuta le possibili cause di tale anomalia; ipotizzando di essere il responsabile dell'infrastruttura di rete, discuta quali passi successivi compirebbe per identificare il problema e porvi rimedio.

## Soluzione prima parte

### Commento

La traccia descrive il sistema informatico che una "città italiana di interesse turistico internazionale ha deciso di sperimentare" per gestire la sicurezza degli eventi con grandi folle che si svolgono in un preciso luogo della città.

Il tema è:

- attuale e interessante perché la cultura e i problemi della sicurezza sono sempre più al centro dell'attenzione pubblica e istituzionale
- azzeccato per la prova di esame di Sistemi e Reti perché la sicurezza degli eventi viene realizzata attraverso la rete integrata di diversi elementi (ambiente, strumenti, tecnologie e infrastrutture informatiche, processi e persone) interconnessi tra di loro

### Schema del sistema

Il sistema è composto da una sede operativa e da una serie di dispositivi di campo (totem touch screen, telecamere IP, dispositivi IoT azionabili e dispositivi mobili forniti al personale) connessi a Internet e interagenti tra di loro tramite una web application e un database MySQL

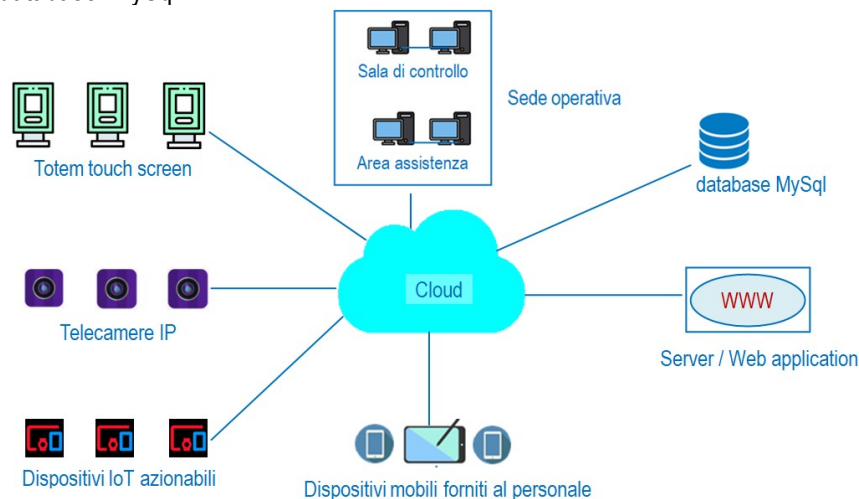


Fig. 1

La web application, in esecuzione su un server remoto:

- consente agli utenti di interagire con i totem touch screen per ricevere informazioni e prelevare i biglietti di accesso degli eventi di loro interesse
- monitora e analizza in tempo reale i video provenienti dalle telecamere IP installate in luoghi strategici della città, (l'area degli eventi e le strade di accesso principali) con l'obiettivo di controllare le situazioni di sovraffollamento e di pericolo
- comanda da remoto i dispositivi azionabili (varchi, semafori, pannelli informativi, sistemi di segnalazione, ecc.) utili a gestire al meglio il flusso di persone verso l'area degli eventi
- comunica digitalmente con i dispositivi mobili, smartphone o tablet, in dotazione del personale presente nell'area degli eventi con le mansioni di validazione degli ingressi, assistenza e pronto intervento

Prendendo in considerazione le prestazioni, i costi e le esigenze di sicurezza e affidabilità, l'architettura del sistema può essere scelta tra le seguenti tipologie:

1. **locale:** server e database si trovano fisicamente all'interno della sede operativa. Questa soluzione consente il controllo totale sul server e sui dati ma richiede investimenti iniziali e costi di gestione e manutenzione molto rilevanti
2. **cloud pubblico:** l'infrastruttura è di proprietà di un provider di servizi hardware e software. Il server e il database si trovano sul cloud e sono facilmente accessibili via Internet, non occorrono investimenti iniziali e si pagano solo i servizi di cui si usufruisce. La gestione dei backup è demandata al provider ed è possibile integrare la web application con servizi avanzati di archiviazione e analisi video, di mappe interattive e di Intelligenza Artificiale

3. cloud ibrido: è un ambiente misto di archiviazione, elaborazione e servizi condiviso tra il cloud computing pubblico di un provider e il server ospitato fisicamente nella sede operativa. E' una soluzione diffusa e flessibile ma complessa da configurare

Tenendo conto dei vantaggi di poter disporre di servizi avanzati di Intelligenza Artificiale (AI), mappe interattive e Analisi Video Intelligente (IVA) integrabili nella web application, si sceglie una soluzione di cloud pubblico in cui il server, la web application e il database sono ospitati su una piattaforma di cloud computing come AWS, Microsoft Azure e Google Cloud.

## Sede operativa

*“Per la gestione del sistema di monitoraggio del flusso delle persone in occasione di un evento, viene messa a disposizione una sede operativa composta da due piani; al primo piano sarà presente un'area dedicata all'assistenza pre- e post- vendita dei biglietti, dove gli operatori potranno svolgere le loro mansioni; al secondo piano sarà presente la sala di controllo dove il personale addetto, attraverso telecamere di sorveglianza, potrà visionare le immagini in diretta dei luoghi interessati dagli eventi”.*

Un'unica rete locale privata (ad esempio una LAN con indirizzo IP 192.168.1.0), con connettività in fibra ottica FTTH (Fiber To The Home) ad alta velocità, consente agli operatori del primo e secondo piano di accedere ad Internet e di utilizzare la web application che gestisce il sistema.

Per evitare che gli operatori del primo e del secondo piano condividano lo stesso dominio, si segmenta (subnetting) la LAN in due sottoreti isolate tra di loro ma connesse a Internet tramite il medesimo router. Per ottenere questo risultato, la rete originaria 192.168.1.0/24 (maschera di rete 255.255.255.0) viene suddivisa in due sottoreti /25 ciascuna con 128 indirizzi IP (126 utilizzabili).

Gli host di ciascun segmento (pc, stampanti, scanner ecc.) vengono configurati modificando la maschera di sottorete come segue:

### Sottorete1 (primo piano - Area assistenza)

Indirizzo di rete: 192.168.1.0/25

Maschera di sottorete: 255.255.255.128

Intervallo IP: da 192.168.1.1 a 192.168.1.126

Indirizzo di broadcast: 192.168.1.127

Host disponibili: 126

Indirizzo gateway: 192.168.1.1

### Sottorete2 (secondo piano – Sala di controllo)

Indirizzo di rete: 192.168.1.128/25

Maschera di sottorete: 255.255.255.128

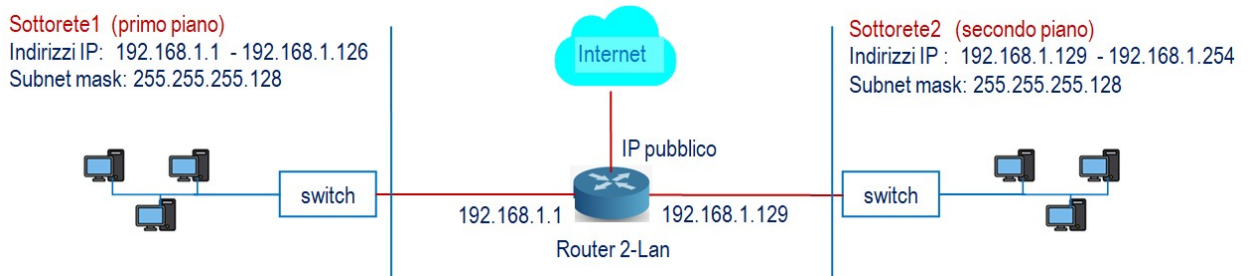
Intervallo IP: da 192.168.1.129 a 192.168.1.254

Indirizzo di broadcast: 192.168.1.255

Host disponibili: 126

Indirizzo gateway: 192.168.1.129

Il router che consente la connessione Internet è dotato di due porte LAN, una per ogni sottorete, configurate con gli indirizzi IP 192.168.1.1 (gateway sottorete1) e 192.168.1.129 (gateway sottorete2)



La sede operativa pur essendo molto importante dal punto di vista organizzativo e funzionale, è solo uno dei componenti del sistema, al pari dei dispositivi di campo con i quali condivide la web application in cloud. Non esiste un collegamento diretto tra la sede operativa e i dispositivi di campo che però interagiscono tra di loro attraverso la web application e i dati archiviati sul database MySQL in cloud

## **Totem touch screen**

Forniscono agli utenti informazioni sugli eventi (programmi, indicazioni e mappe per accedere) e consentono il prelievo dei biglietti di accesso (gratuiti o a pagamento).

Esistono due tipi di totem touch screen:

1. autonomi in modalità kiosk. Funzionano come chioschi self-service, si collegano a Internet ed eseguono un'applicazione integrata a bordo, molto specifica, innovativa e performante
2. web client. Non hanno un'applicazione installata a bordo, ma collegandosi a Internet funzionano come semplici client della web application che gira sul server in cloud

Nel nostro caso, in virtù delle scelte progettuali iniziali, si adotta la soluzione web client; significa che i totem si collegano alla web application sul server in cloud, che a sua volta interagisce con il database cloud MySQL per l'archiviazione e la gestione dei dati degli eventi e dei biglietti. Questa scelta consente di eseguire gli aggiornamenti dell'applicazione una sola volta sul server ed evita i problemi e le difficoltà di aggiornare i singoli totem.

I totem sono generalmente mini pc industriali con hardware e software integrati, equipaggiati, ad esempio, con processori Intel Celeron, sistema operativo Windows e browser Chrome. Sono dotati di touch screen per interagire con gli utenti, di lettori QR/Barcode per leggere i codici degli smartphone e di lettori di badge per consentire i pagamenti con carte e dispositivi contactless.

I totem touch screen, adibiti a punti di informazione e di biglietteria automatica, sono dislocati nell'intera area comunale e sono dotati di un router LTE integrato e una SIM dedicata con IP pubblico che assicurano la connettività Internet attraverso la rete cellulare 4G/5G. Oltre ai totem, anche gli altri dispositivi di campo (telecamere, dispositivi IoT, smartphone e tablet) sono connessi a Internet tramite SIM utilizzando la rete 4G/5G. E' una buona soluzione in quanto:

- non occorre installare cavi e fibra ottica
- ogni dispositivo è autonomo e indipendente
- dal punto di vista della sicurezza nessuno può accedere alla rete della sede operativa usando un totem
- i costi dipendono dal traffico e sono relativi alla durata degli eventi

Le modalità di funzionamento del totem touch screen sono i seguenti:

- il browser si connette via rete sicura HTTPS al server remoto in cloud dove è in esecuzione la web application
- gli utenti interagiscono con il touch screen, con il QR/Barcode o il lettore di badge e i comandi vengono inviati alla web application attraverso richieste HTTP/HTTPS o Web Socket. Acquistano i biglietti ed eseguono il pagamento dei ticket
- in base alle richieste ricevute e dialogando con gli utenti, la web application invia informazioni e mappe interattive, gestisce la scelta dei posti ed emette i biglietti, valida i pagamenti e genera il QR code dei biglietti digitali, aggiorna il database in cloud

## **Telecamere IP**

Collocate in punti strategici della città e connesse a Internet tramite rete cellulare 4G/5G, trasmettono al database MySQL in cloud le immagini in diretta dei luoghi interessati ai flussi di persone che si muovono verso l'area degli eventi; la web application legge questi dati e li visualizza nei pc della sala di controllo della sede operativa. I potenti e sofisticati algoritmi IVA (Analisi Video Intelligente con il supporto dell'Intelligenza Artificiale), messi a disposizione dai provider cloud e integrati direttamente nella web application, eseguono l'analisi video delle immagini e sono in grado di contare le persone e riconoscere le situazioni di sovraffollamento e di pericolo.

Le telecamere IP sono contraddistinte da un numero IP pubblico e statico e sono pertanto raggiungibili in modo costante dalla web application di gestione in cloud. Se l'IP della telecamera non fosse statico, in caso di cambiamento il collegamento verrebbe interrotto.

## **Dispositivi IoT azionabili**

Quando gli operatori del centro di controllo della sede operativa, tramite l'analisi video intelligente delle immagini delle telecamere, rilevano una condizione anomala (sovraffollamento, assembramento, intrusione, altre situazioni di pericolo) intervengono tramite la dashboard della web application:

- a) azionando i dispositivi IoT utili per la gestione degli eventi con grandi folle (semafori, barriere a scomparsa, pannelli informativi, sistemi di allarme sonori, annunci di emergenza)
- b) avvisando il personale presente nell'area dell'evento

Attenendoci alle indicazioni della traccia *“I dispositivi, azionabili a distanza, verranno gestiti attraverso un server HTTP interno al dispositivo stesso, accessibile da remoto”*, ipotizziamo di utilizzare dispositivi basati su microcontrollori che ospitano un server web e si connettono a Internet tramite rete cellulare 4G/5G

Lo schema di un dispositivo IoT azionabile include:

- un microcontrollore, tipo Arduino, ESP32, ESP8266 e Raspberry, che contiene un server HTTP integrato ed esegue il codice di gestione del dispositivo
- i sensori che raccolgono dati (ad es. lo stato di un semaforo) e gli attuatori che eseguono i comandi provenienti dalla sala di controllo della sede operativa (ad es. “imposta rosso al semaforo X”)
- un modem, una SIM e un'antenna che consentono al dispositivo di connettersi a Internet tramite una rete cellulare. Il protocollo di comunicazione utilizzato per inviare e ricevere dati è HTTP/HTTPS

Arduino, ESP32 e ESP8266 non hanno un sistema operativo e il server HTTP è molto semplice; il Raspberry, invece, è equipaggiato con il Sistema Operativo Linux ed è in grado di eseguire un server HTTP professionale. In ogni caso i server web dei dispositivi sono accessibili da remoto e sono in grado di ricevere i comandi HTTP che gli addetti della sala di controllo della sede operativa, nel caso di situazioni di allarme riscontrati nell'area eventi, inviano tramite la web application per azionare i dispositivi attuatori (relè, motori, sirene ecc.). In alternativa, tenendo conto che la maggior parte dei dispositivi IoT remoti non ha un web server integrato, il controllo remoto può essere realizzato utilizzando il protocollo MQTT, molto diffuso in ambiente IoT e apprezzato per la sua leggerezza ed efficienza. Chi volesse approfondire quest'ultimo aspetto può consultare la sezione [Progetti ed esercizi Arduino ESP8266 IoT](#) dell'area download del sito [www.maurodeberardis.it](http://www.maurodeberardis.it)

## Dispositivi mobili forniti al personale

Per lo svolgimento delle mansioni di validazione degli ingressi, assistenza e pronto intervento, gli operatori che si trovano nell'area degli eventi sono dotati di uno smartphone o un tablet che consente loro di interagire costantemente con la sede operativa attraverso la web application in esecuzione sul server in cloud.

Le modalità di comunicazione sono le seguenti:

- dialogano con il personale della sede operativa preposto all'assistenza pre- e post- vendita dei biglietti per la validazione degli ingressi
- ricevono le notifiche relative allo stato dei dispositivi (ad es. “Telecamera 4 offline”, “Pannello informativo 2 attivato”) e alle situazioni di allarme (ad es. “Assembramento Evento X”)
- inviano comunicazioni sullo stato dei dispositivi, sulle situazioni critiche dei vari eventi e sulla loro evoluzione (ad es. “Assembramento Evento X risolto”)

E' chiaro che alcune informazioni inviate tramite web application sono ridondanti perché, ad esempio, un evento di pericolo risolto si evince anche dalle immagini delle telecamere, ma sicuramente la comunicazione diretta con un operatore sul luogo è più sicura ed immediata.

I dispositivi mobili degli operatori presenti nell'area eventi utilizzano la rete cellulare 4G/5G per connettersi a Internet. Riguardo alla tecnologia di comunicazione tra dispositivi mobili e la web app sul server, si utilizza il protocollo HTTPS. Ai fini della sicurezza la connessione è cifrata e l'accesso alla web application è gestito da una robusta procedura di autenticazione.

Un'altra modalità di comunicazione è quella che prevede l'uso di canali informali, tipo WhatsApp o WhatsApp Business, che consentono agli operatori di comunicare rapidamente con la sede operativa, di inviare foto e video su quello che succede e ricevere disposizioni su come intervenire

## Web application

La web application in cloud funge da piattaforma unica per la sede operativa centrale, i totem touch screen, le telecamere IP, i dispositivi IoT azionabili e i dispositivi personali forniti agli operatori. Tutti accedono agli stessi dati del DB MySql in cloud e la comunicazione avviene tramite i protocolli HTTPS o MQTT.

La web application, rigorosamente responsive, offre molte funzionalità a ciascuna delle quali gli utenti possono accedere in base al livello di autenticazione acquisito in fase di Login:

- gestisce gli utenti e gli accessi al sistema
- per ciascun evento, attraverso una dashboard, visualizza le immagini provenienti dalle telecamere, il numero di biglietti emessi, lo stato dei dispositivi azionabili da remoto, le richieste dai touch screen e le eventuali segnalazioni automatiche di allarme o pericolo

- localizza e visualizza le mappe interattive relative all'area degli eventi, ai totem, alle telecamere, ai dispositivi IoT azionabili e ai dispositivi mobili forniti agli operatori
- fornisce informazioni sugli eventi, gestisce la scelta dei posti e l'emissione dei biglietti
- comunica in real time con smartphone e tablet degli operatori che si trovano sul luogo degli eventi
- invia comandi ai dispositivi IoT azionabili da remoto

Per lo sviluppo della web application vengono utilizzate diverse tecnologie che coprono sia il frontend (il lato client ovvero l'interfaccia che consente all'utente di interagire con l'applicazione), sia il backend (il lato server ovvero la parte dell'applicazione che gestisce la logica, i dati e le operazioni sul server)

#### Tecnologie per il frontend

- HTML (HyperText Markup Language): definisce la struttura e il contenuto delle pagine web.
- CSS (Cascading Style Sheets): si occupa dello stile e dell'aspetto visivo, come colori, font e layout. Attraverso una progettazione responsive del CSS, la web application si adatta automaticamente alle dimensioni dello schermo dei dispositivi utilizzati per accedere (desktop, tablet o smartphone)
- JavaScript: aggiunge interattività e dinamismo, permettendo di creare animazioni, gestire eventi e aggiornare contenuti senza ricaricare la pagina.

Spesso alle tecnologie HTML/CSS/JavaScript vengono affiancati dei framework JavaScript quali React e Angular che consentono di velocizzare lo sviluppo frontend e realizzare web application complesse e reattive nelle quali, come nel nostro caso, il frontend e il backend comunicano tramite richieste HTTP.

#### Tecnologie per il backend

- un framework PHP, tipo Laravel o Symphony, per la gestione dei dati MySQL
- il framework JavaScript Node.js, ideale per gestire il backend real time con i totem, i dispositivi IoT e le telecamere

## **DB MySQL**

Il database in cloud ha un ruolo fondamentale perché è la memoria strutturata dove sono archiviati e condivisi tutti i dati MySQL, attuali e storici, coinvolti nel sistema e relativi a:

- a) dispositivi di campo
- b) informazioni sugli eventi
- c) richieste dai totem
- d) gestione dei biglietti
- e) immagini video delle telecamere IP
- f) situazioni di allarme e pericolo
- g) comandi ai dispositivi IoT azionabili
- h) comunicazioni con i dispositivi mobili forniti al personale

Per quel che riguarda la **continuità di servizio del sistema**, occorre prendere in considerazione la sicurezza informatica e le modalità specifiche attraverso le quali è possibile evitare interruzioni della connettività.

Si interviene su due diversi livelli:

1. il livello cloud che include server, database e web application
2. Il livello locale che include sede operativa e dispositivi di campo

A livello cloud, la scelta progettuale di adottare una soluzione cloud pubblica si rivela particolarmente azzeccata. Infatti, le piattaforme migliori e più diffuse offrono un elevato grado di sicurezza fisica e logica proteggendo i server e l'infrastruttura, i dati e il software. In particolare:

- a) garantiscono la sicurezza dei propri data center e dei database, attraverso la ridondanza dei server, la replica dei dati su più dispositivi di storage e i backup automatici
- b) usano l'intelligenza artificiale per rilevare le minacce e far fronte ad attacchi e attività malevoli
- c) forniscono soluzioni avanzate per la crittografia dei dati
- d) impediscono gli accessi non autorizzati ai dati sensibili
- e) assicurano la continuità di Internet grazie alla ridondanza a livello di infrastruttura: i data center si connettono con diversi provider di servizi Internet in modo tale da non dipendere da un singolo fornitore, Se un percorso di rete fallisce, il traffico viene dirottato su un percorso alternativo disponibile

In sintesi, la sicurezza è delegata in massima parte al fornitore di servizi cloud.

A livello locale è necessario da un lato applicare efficaci misure di sicurezza fisiche, logiche e organizzative alla sede operativa e ai dispositivi di campo, dall'altro garantire la continuità di servizio della connessione con il cloud. Infatti, anche se il cloud è perfettamente operativo ed è progettato per evitare interruzioni di servizio, se "cade" la connessione Internet locale il sistema diventa irraggiungibile.

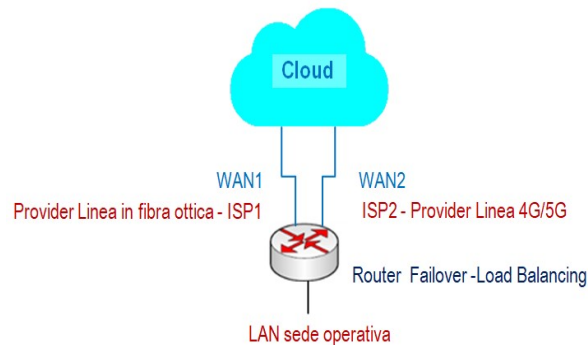
Non approfondiamo l'argomento delle misure di sicurezza informatica (generalmente ben conosciuto dagli studenti e trattato in diverse soluzioni proposte nel sito [www.maurodeberardis.it](http://www.maurodeberardis.it)) e ci concentriamo sulla continuità di servizio della connessione tra sede operativa/dispositivi di campo e cloud.

Per garantire la continuità di Internet non è sufficiente affidarsi a un Provider di qualità perché anche le tecnologie più sicure non sono esenti da rischi e problemi e si possono comunque verificare black-out e disservizi.

Nei casi in cui la connettività deve essere assicurata sempre (always-on) si può adottare la soluzione di utilizzare una seconda linea, preferibilmente con tecnologia di trasmissione differente dalla prima.

#### Sede operativa

La linea principale in fibra ottica viene affiancata da una linea 4G/5G fornita da un altro Provider; le due linee convergono in un unico router Dual-Wan con le funzionalità di "Failover automatico" e "Load Balancing" che permettono di condividere dinamicamente le due linee e di ottimizzare la connettività totale. Con questa configurazione se "cade" la linea principale in fibra ottica, il router in pochi millisecondi passa automaticamente alla rete 4G/5G (Backup 4G/5G) che, seppure in modo meno performante, assicura la continuità del servizio Internet.



#### Dispositivi di campo

Utilizzano la rete cellulare 4G/5G che è notoriamente molto stabile. Ogni rete mobile però non è infallibile, può avere zone d'ombra e presentare guasti o malfunzionamenti. Anche in questo caso occorre una ridondanza che si ottiene utilizzando una Dual SIM che consente di avere due SIM attive in ogni momento. La SIM sceglie automaticamente il miglior operatore e se un operatore "cade" passa all'altro.

Ancor più performante è la soluzione dei router industriali Dual SIM che funzionano esattamente come i router con failover visti per la sede operativa: se "cade" una rete mobile, in pochi secondi la connessione viene spostata automaticamente sull'altra rete.

## Soluzione seconda parte

Quesiti I - III

- I. *In relazione al tema proposto nella prima parte, si consideri la gestione dei filmati e delle immagini che vengono trasmessi dalle telecamere per il monitoraggio, e si propongano soluzioni per il relativo salvataggio all'interno dell'infrastruttura della sede centrale oppure nel cloud, definendone vantaggi e svantaggi.*

Il sistema di gestione eventi con grandi folle proposto nella soluzione della prima parte si basa su un'architettura di cloud pubblico e il salvataggio dei filmati e delle immagini trasmessi dalle telecamere viene effettuata sul cloud.

I filmati integrali delle telecamere scorrono nei display della sala di controllo della sede operativa e gli addetti possono esaminare in diretta tutte le immagini dei luoghi interessati agli eventi e, grazie ai servizi aggiuntivi di Intelligenza Artificiale (AI) e di Analisi Video Intelligente (IVA) integrati nella web application di gestione, sono in grado di valutare facilmente le situazioni di sovraffollamento, pericolo ed emergenza.

E' una scelta che garantisce il controllo costante delle telecamere e presenta i vantaggi specifici del cloud: costi generalmente ridotti (non si deve creare né gestire alcuna infrastruttura), ridondanza dell'hardware e dei dati, sicurezza elevata, scalabilità e accessibilità da ogni luogo e con qualsiasi dispositivo.

Tuttavia, poiché i costi del cloud dipendono in misura importante dalla quantità dei dati che vengono salvati, la soluzione proposta è ottimale solo se il numero di telecamere è basso e il traffico generato è limitato a pochi TeraByte; con un numero elevato di telecamere che nell'arco temporale della durata degli eventi inviano un flusso continuo di immagini, l'upload video è molto pesante e troppo costoso. In questi casi è necessario ridurre la mole di dati inviati al cloud; si utilizzano, a tale scopo, telecamere smart, dotate di microprocessore, software per l'Analisi Video Intelligente (IVA) e Intelligenza Artificiale, in grado di acquisire i flussi video in tempo reale, analizzare le immagini e inviare al cloud, oltre alle fotografie istantanee ogni X minuti, solo i video relativi a situazioni di allarme, incidenti e sovraffollamento. In altre parole, si utilizzano telecamere smart che non inviano al cloud tutto il flusso video ma solo le immagini degli eventi significativi; in tal modo la quantità dei dati trasmessi è drasticamente più bassa e i costi di storage diventano sostenibili.

- III. *Il candidato illustri caratteristiche e possibili campi di applicazione di due tecnologie di comunicazione wireless a corto raggio quali, ad esempio, sistemi basati su RFID, NFC, Bluetooth Low Energy (BLE), IEEE 802.15.4.*

Le tecnologie di comunicazione wireless a corto raggio sono sistemi che permettono lo scambio di dati tra dispositivi vicini senza utilizzare cavi, tipicamente entro distanze che vanno da pochi centimetri a qualche decina di metri.

### Tecnologia RFID

RFID è l'acronimo di "Radio Frequency Identification" ovvero "identificazione a radiofrequenza" e si riferisce a una tecnologia in base alla quale i dati digitali codificati in un tag RFID vengono acquisiti da un dispositivo di lettura (reader) tramite onde radio.

Le tecnologie RFID sono contrassegnate da un codice univoco (UID), e quindi da un'identità digitale, e rappresentano una delle leve principali per lo sviluppo dell'automazione industriale e dell'Internet delle cose (IoT). L'RFID è simile al codice a barre ma presenta il grande vantaggio che i dati dei tag RFID possono essere letti in prossimità anche senza "contatto visivo": al contrario i codici a barre devono essere allineati con uno scanner ottico.

Un sistema RFID è costituito da due componenti principali:

- un transponder a radiofrequenza (tag RFID) inserito nell'oggetto che si vuole identificare: il tag contiene un microchip, che memorizza ed elabora le informazioni, e un'antenna, che consente la ricezione/trasmmissione di dati a corto raggio senza contatto fisico. Il tag è generalmente un dispositivo passivo, ovvero non contiene una batteria
- un ricetrasmittitore (reader) controllato da un microprocessore ed usato per leggere le informazioni contenute nel Tag



Le frequenze RFID si suddividono in:

- LF (Low Frequency, ~125-134 kHz): letture fino a pochi cm (tessere, portachiavi)
- HF (High Frequency, 13,56 MHz): letture fino a 1m (smartphone, carte di credito)
- UHF (Ultra High Frequency, 860-960 MHz): letture fino a 10-20 m (logistica, magazzini).
- Microonde (Frequenze molto alte, ad es. 5.8 GHz): letture fino a 10-15 m (Telepass: in questo caso il tag è attivo, ovvero alimentato da una batteria, per garantire che nei caselli autostradali i lettori identifichino i veicoli in modo certo, sicuro e veloce)

Il funzionamento di un sistema RFID con tag passivo è il seguente:

- il tag viene posizionato in prossimità del reader (non deve necessariamente trovarsi "a vista" del reader)
- il reader genera un campo elettromagnetico variabile che induce una corrente nell'antenna del tag e alimenta il chip
- il chip tramite un segnale radio trasmette al reader le informazioni memorizzate al suo interno
- il reader rileva e interpreta il segnale radio ricevuto e, attraverso un'interfaccia periferica seriale, invia i dati a un computer o ad un microcontrollore (nella figura di esempio sopra ad Arduino), che li gestisce per realizzare gli scopi dell'applicazione

La tecnologia RFID offre vantaggi rilevanti:

- i dispositivi sono robusti e molto economici
- la lettura dei tag, rapida e senza contatto, elimina gli errori umani e velocizza i processi
- i dati memorizzati nei tag sono difficili da duplicare

e i campi di applicazione sono vastissimi:

- automazione
- logistica e trasporti
- sanità
- sistemi di pagamento
- ...

In particolare, facendo riferimento al tema della gestione di eventi con grandi folle, la tecnologia RFID è ampiamente usata per gestire gli accessi in modo affidabile, sicuro e veloce. In situazioni con migliaia di persone, in tempi rapidissimi i varchi RFID leggono i tag dei biglietti e inviano i codici identificativi UID al sistema che verifica la validità dei biglietti, autorizza l'accesso e comanda l'apertura dei tornelli.

### Tecnologia NFC

NFC (Near Field Communication) è una tecnologia wireless a corto raggio basata sullo standard RFID HF a 13.56 MHz e progettata per consentire comunicazioni interattive e sicure tra due dispositivi compatibili (smartphone, smartwatch, lettori) avvicinandoli a pochi centimetri l'uno dall'altro.

In pratica NFC è un sottoinsieme specializzato della tecnologia RFID HF a 13,56 MHz creato per l'utilizzo con gli smartphone e per consentire transazioni sensibili e sicure.

NFC è utilizzata largamente per pagamenti contactless (Google Pay) e condivisione di file.

In particolare, quando si utilizza lo smartphone (o lo smartwatch) per effettuare un pagamento o per l'accesso ad un evento, lo smartphone entra in modalità di emulazione di una smart card NFC e viene riconosciuto e identificato dal lettore (POS, tornello, ecc.) come se fosse una carta fisica.

I dispositivi NFC sono sicuri grazie alla distanza operativa ridotta (max 4cm), che rende difficile l'intercettazione, e la cifratura avanzata AES; inoltre sono molto veloci e quasi sempre integrati nativamente negli smartphone.

Al pari degli RFID i campi di applicazione della tecnologia NFC sono molto ampi:

- comunicazione NFC tra due smartphone (peer to peer)
- pagamenti contactless
- biglietti elettronici
- parcheggi
- trasporti ed eventi
- badge aziendali e accessi
- ...