Progettare ed ottimizzare reti di Computer Vision dedicate all’individuazione e classificazione di ostacoli all’interno di immagini o video, al fine di supportare la navigazione autonoma e la sicurezza del sistema.

**TITOLO: “Progettazione e Difesa di Sistemi di Rilevamento Ostacoli contro Attacchi Cyber”**

Questa tesi si propone di esplorare l’intersezione tra **Computer Vision per la rilevazione e classificazione di ostacoli** e il dominio della **Cybersecurity**, con l’obiettivo di costruire sistemi non solo **accurati** ma anche **robusti e resilienti** contro attacchi informatici e manipolazioni.

**1. Contesto applicativo**

* Sistemi di **navigazione autonoma** (veicoli, droni, robot).
* **Videosorveglianza intelligente** in ambienti critici (aeroporti, magazzini, ospedali, data center).
* **Smart infrastructure** (parcheggi intelligenti, smart home).

**2. Obiettivi principali**

1. **Progettazione di reti di Computer Vision dedicate all’individuazione di ostacoli**:
   * definizione delle architetture più adatte (CNN leggere, reti multimodali, modelli ottimizzati per edge).
   * valutazione di prestazioni (accuratezza, latenza, consumo).
2. **Analisi delle vulnerabilità specifiche per il dominio Computer Vision**:
   * attacchi di tipo *adversarial* (immagini o patch che ingannano la rete).
   * *data poisoning* e *model extraction* (furto del modello o manipolazione dei dati).
   * *spoofing* e *replay attacks* sui feed video.
   * minacce legate all’uso di cloud/edge computing (esposizione dati sensibili, leakage dai modelli) (cloud computing, i dati e le elaborazioni vengono eseguiti in server remoti, accessibili via internet. La telecamera/sensore invia i dati ad un server nel cloud, dove un modello di intelligenza artificiale li elabora e restituisce il risultato. I vantaggi risiedono in una capacità di calcolo elevata, aggiornamenti centralizzati, accesso da qualsiasi dispositivo connesso. Svantaggi invece per latenza più alta, richiede connessione stabile e veloce e possibilità dii esposizione ai dati sensibili) (Edge computing, i dati vengono elaborati vicino alla fonte, viene eseguito il modello di computer vision senza inviare tutti i dati al cloud. Latenza bassa, maggiore privacy dato che i dati sensibili non lasciano il dispositivo, riduzione del traffico di rete. Svantaggi in capacità di calcolo limitata ed aggiornamenti sicuramente più complessi dei modelli) ( Approccio ibrido )
3. **Classificazione delle minacce in scenari reali** (quelli che abbiamo elencato: magazzini, aeroporti, ospedali, smart home, ecc.) con focus su come un attacco può compromettere:
   * **la sicurezza fisica** (es. un ostacolo non rilevato da un veicolo).
   * **la sicurezza logica** (es. furto o manipolazione di dati video).
   * **la privacy** (es. profiling o data leakage).
4. **Studio di contromisure**:
   * tecniche di robustezza dei modelli (adversarial training, input sanitization, modelli leggeri resistenti a manipolazioni).
   * meccanismi di sicurezza architetturale (esecuzione sicura in *secure enclave*, cifratura omomorfica per dati sensibili).
   * protocolli di monitoraggio e detection di attacchi.

**3. Contributo atteso**

La tesi non solo costruisce un sistema di Computer Vision per la rilevazione di ostacoli, ma ne valuta la **resilienza a minacce cyber**. Il contributo sarà:

* un **framework di analisi delle vulnerabilità** in scenari applicativi concreti;
* un **confronto sperimentale** su tecniche di difesa (es. robustezza del modello, secure enclaves vs cloud tradizionale);
* linee guida per la **progettazione sicura di sistemi CV in contesti critici**.