RUSLAN BONDARUC

Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Security Assurance in Ambito IoT attraverso Infrastruttura Edge/5G

GIORNATA DI INCONTRO
BORSE DI STUDIO GARR
"ORIO CARLINI"
ROMA

Università degli Studi di Milano – Dip.to di Informatica

Tutor: Prof. Marco Anisetti

23/02/2022

IoT

L’IoT alimenta la
rivoluzione digitale

Diffusione

+10%

34 MILIONI
CONNESSIONI
CELLULARI

93
MLN

59 MILIONI
CONNESSIONI TRAMITE
ALTRE TECNOLOGIE

+15%

+100%

RETI LOW POWER
WIDE AREA (LPWA)

SPINTA POSITIVA DEL
D. L. SEMPLIFICAZIONI

Impatto economico

$830B

Agricoltura – agricoltura 4.0

$3.7T

Industria – ottimizzazione dei processi

Potenziale impatto economico IoT
$3.9 - $11T entro il 2025

$1.0T

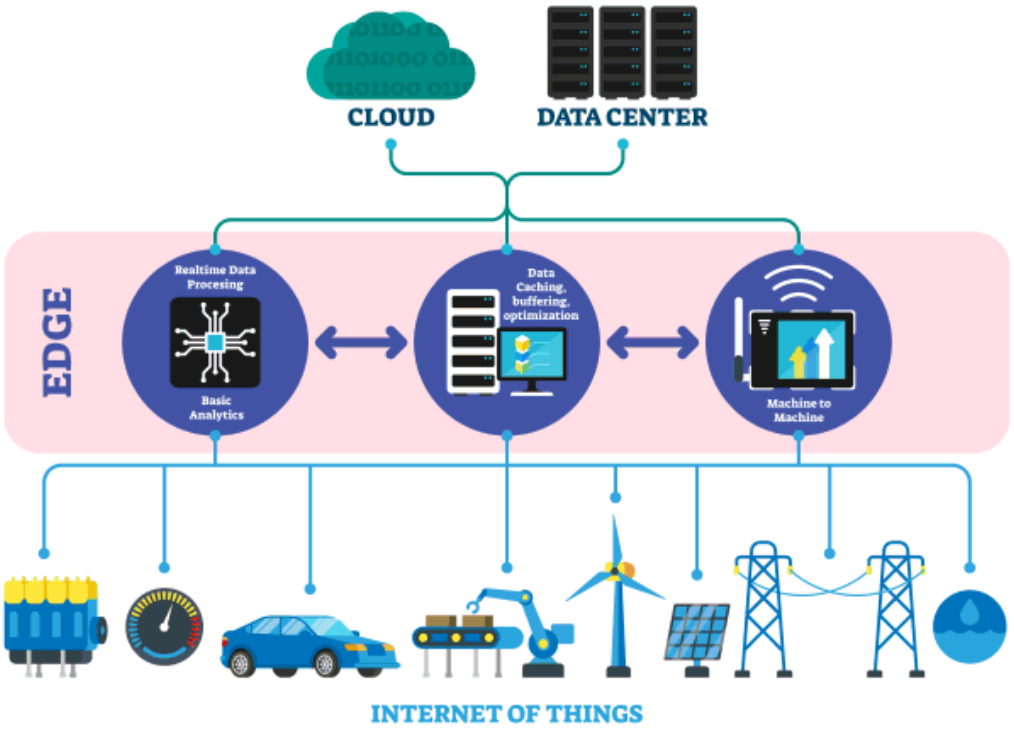
Casa e salute – sicurezza e salute & fitness

$2.4T

Città e veicoli – sanità pubblica, trasporti e guida autonoma

Scenario

Modello computazionale multi-tiered



Nuove sfide di sicurezza

Garantire il corretto comportamento

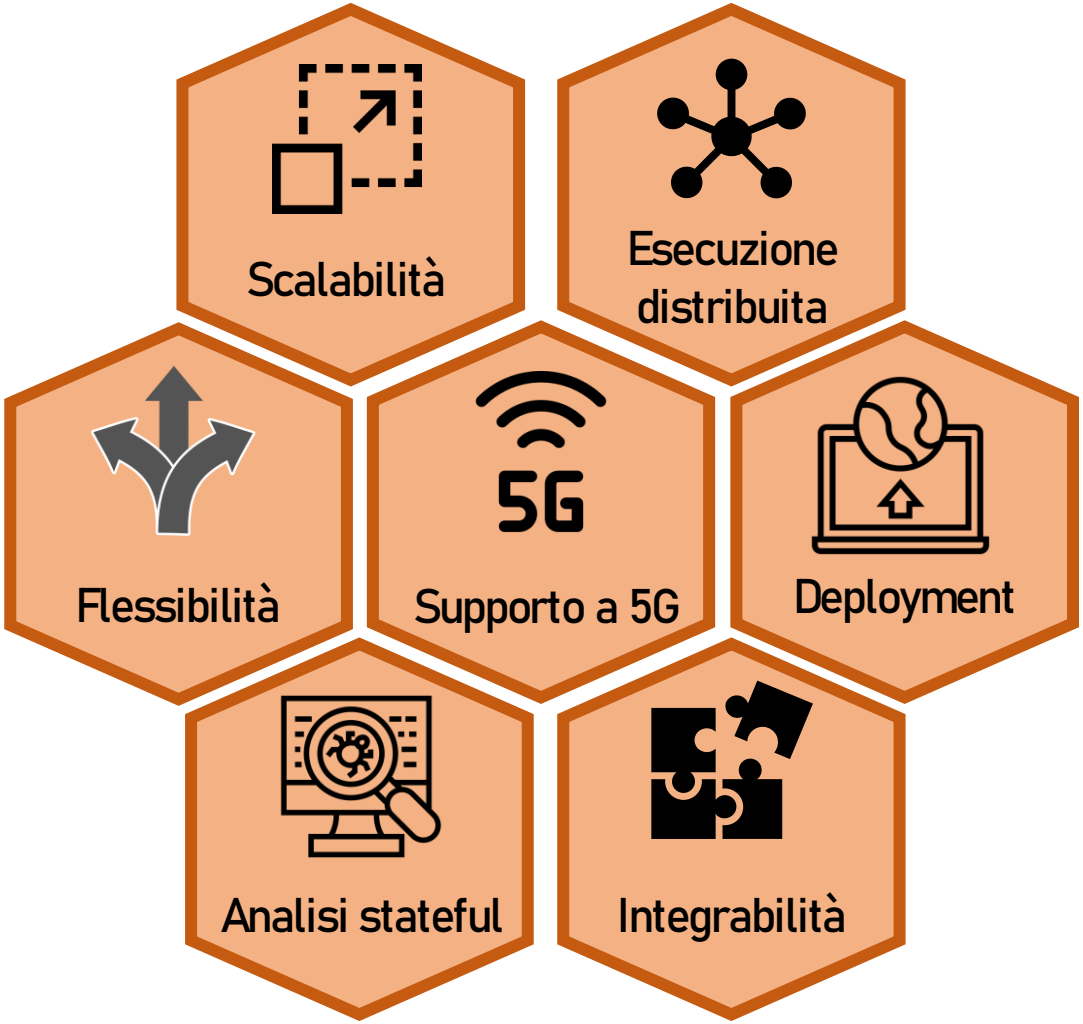
Maggiore complessità difficile da gestire

Assurance di sicurezza:
«lo strumento per ottenere la ragionevole certezza che il sistema presenta delle proprietà di sicurezza»

...Ma i framework convenzionali sono inadatti a questo scenario

Definizione e implementazione di un framework di security assurance per sistemi edge/IoT

Requisiti


Scalabilità
Esecuzione distribuita
Flessibilità
5G
Supporto a 5G
Deployment
Analisi stateful
Integrabilità

Requisiti

Scalabilità
Esecuzione distribuita
Flessibilità
5G
Supporto a 5G
Deployment
Analisi stateful
Integrabilità

Requisiti

Scalabilità
Esecuzione distribuita
Flessibilità
5G
Supporto a 5G
Deployment
Analisi stateful
Integrabilità

Requisiti

Scalabilità
Esecuzione distribuita
Flessibilità
5G
Supporto a 5G
Deployment
Analisi stateful
Integrabilità

Requisiti

Scalabilità
Esecuzione distribuita
Flessibilità
5G
Supporto a 5G
Deployment
Analisi stateful
Integrabilità

Requisiti

Scalabilità
Esecuzione distribuita
Flessibilità
5G
Supporto a 5G
Deployment
Analisi stateful
Integrabilità

Requisiti

Scalabilità
Esecuzione distribuita
Flessibilità
5G
Supporto a 5G
Deployment
Analisi stateful
Integrabilità

Requisiti

Scalabilità
Esecuzione distribuita
Flessibilità
5G
Supporto a 5G
Deployment
Analisi stateful
Integrabilità

Approccio

Sistema distribuito a microservizi

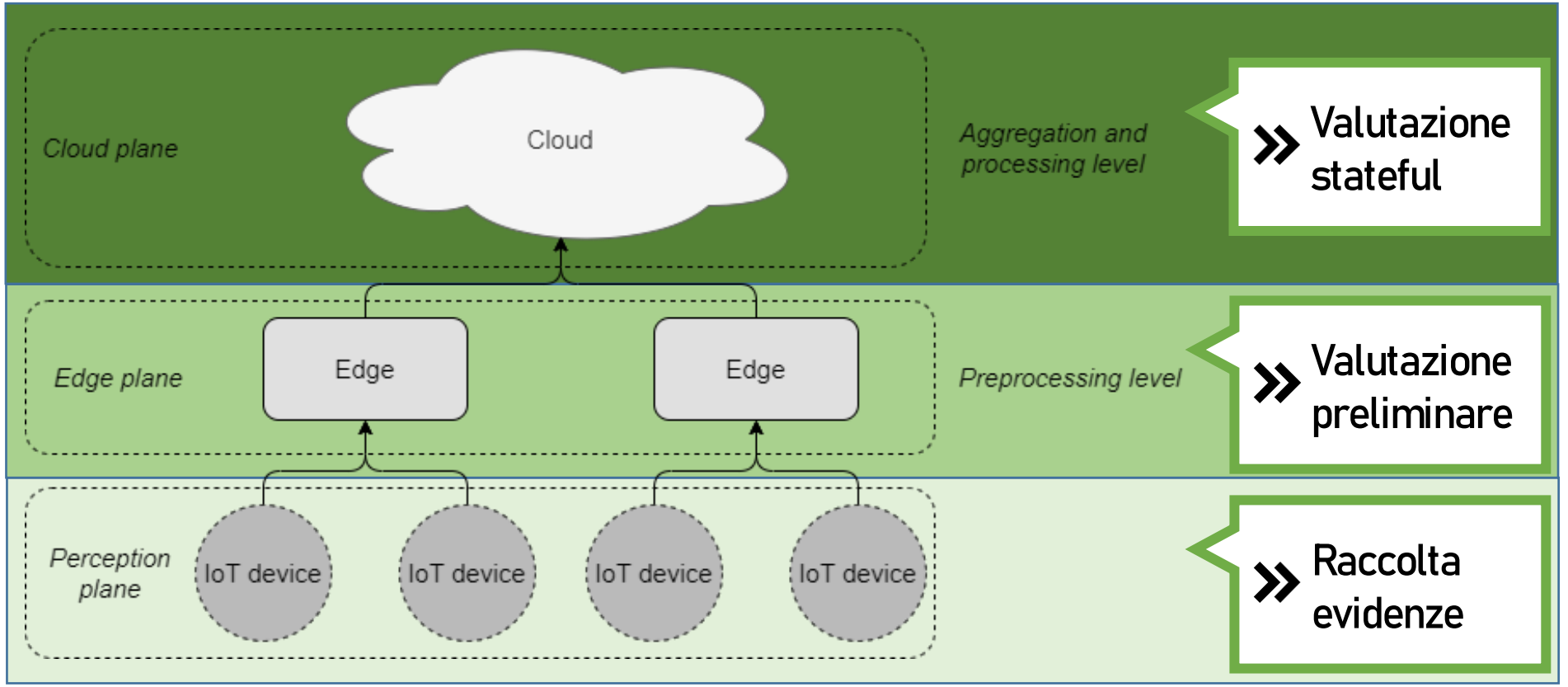
kubernetes

MOON CLOUD

Approccio

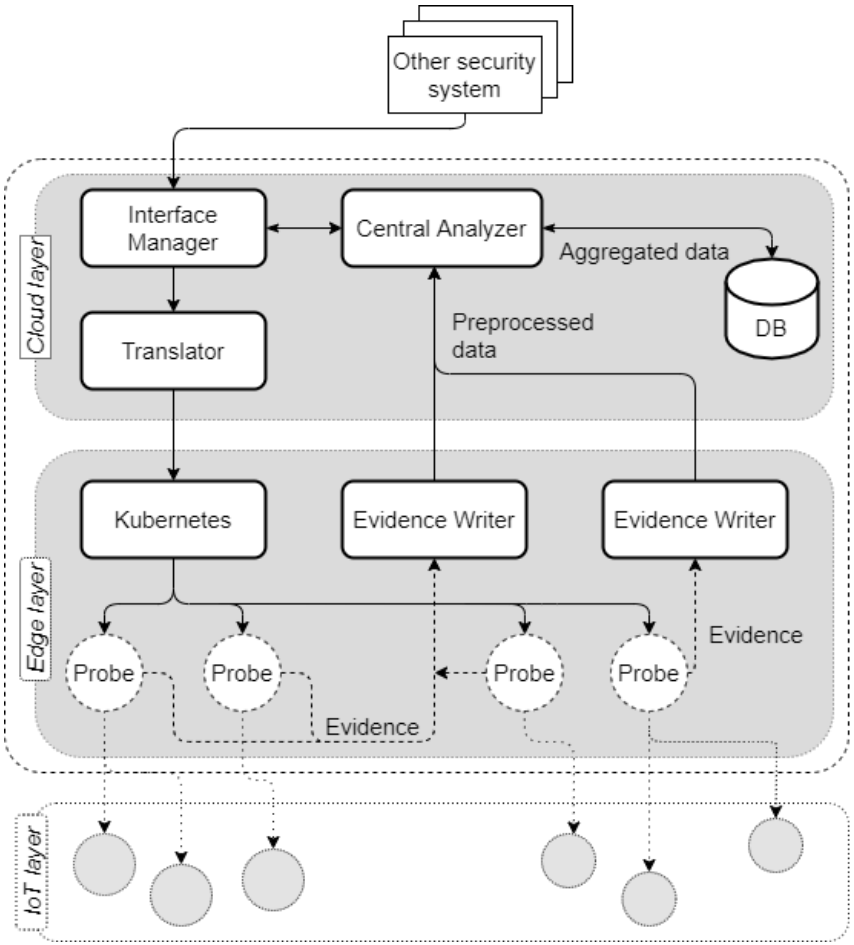
Sistema distribuito a microservizi

Approccio (2)

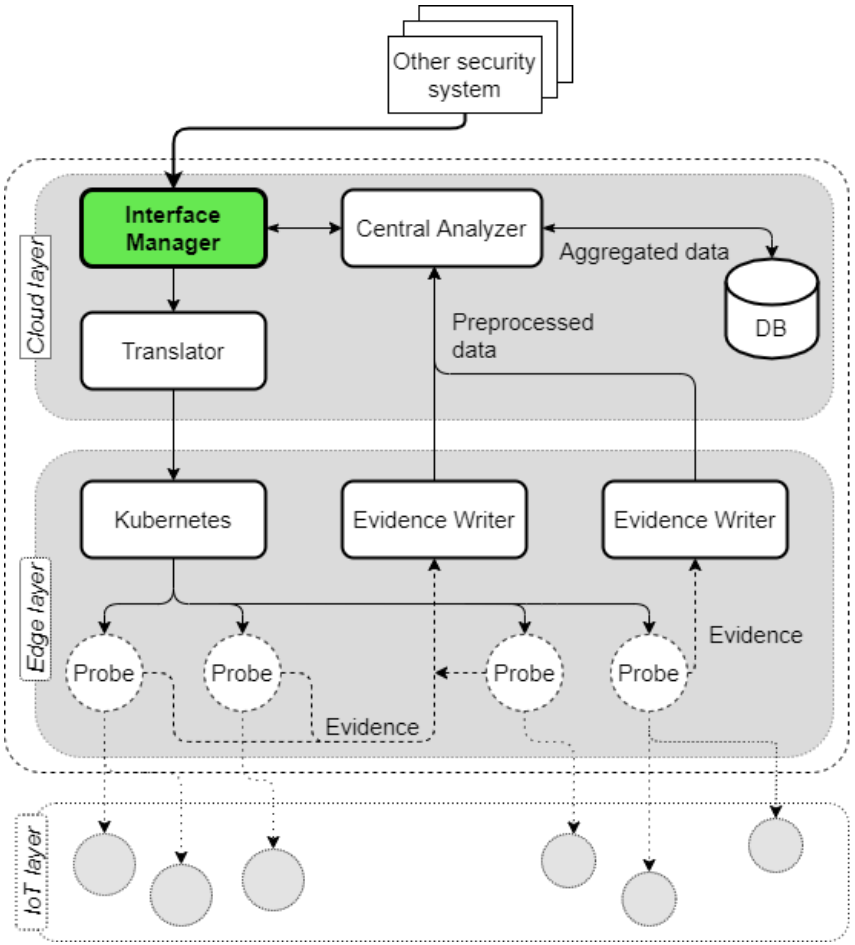


Visione olistica del sistema target

Framework

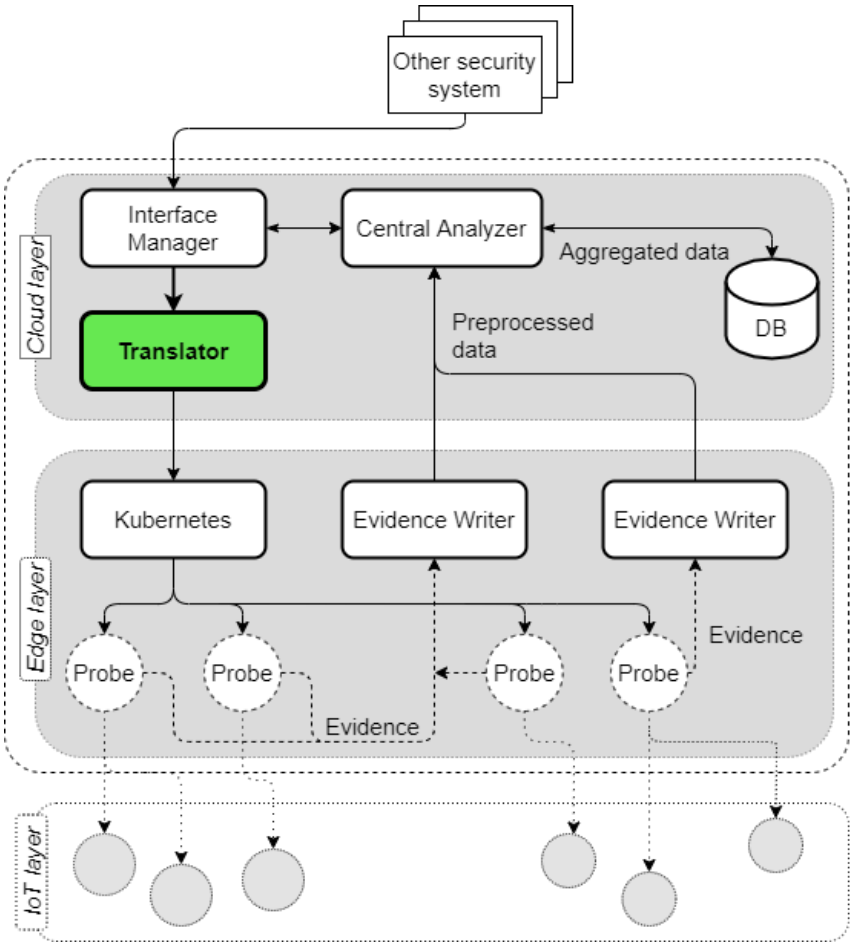

Other security system
Interface Manager
Central Analyzer
Aggregated data
DB
Cloud layer
Translator
Preprocessed data
Kubernetes
Evidence Writer
Evidence Writer
Edge layer
Evidence
Probe
Probe
Probe
Probe
Evidence
IoT layer

Framework



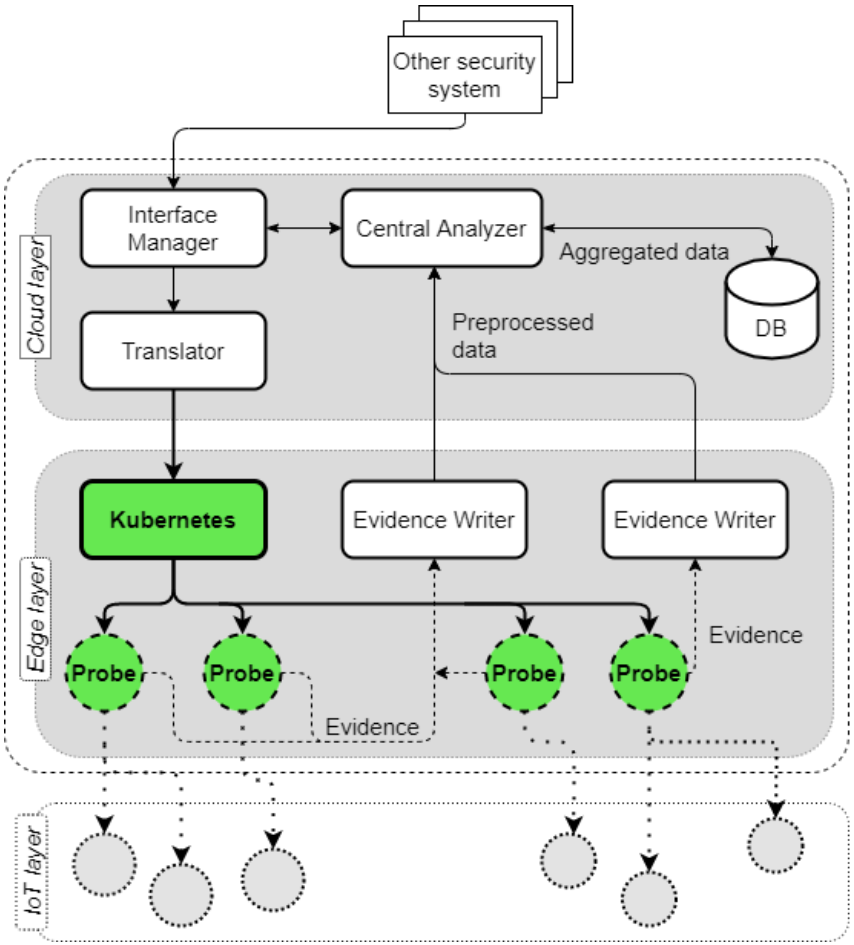
1. Interface Manager: interazione tra framework e ambiente esterno (utenti, altri sistemi di sicurezza, ecc.)

Framework



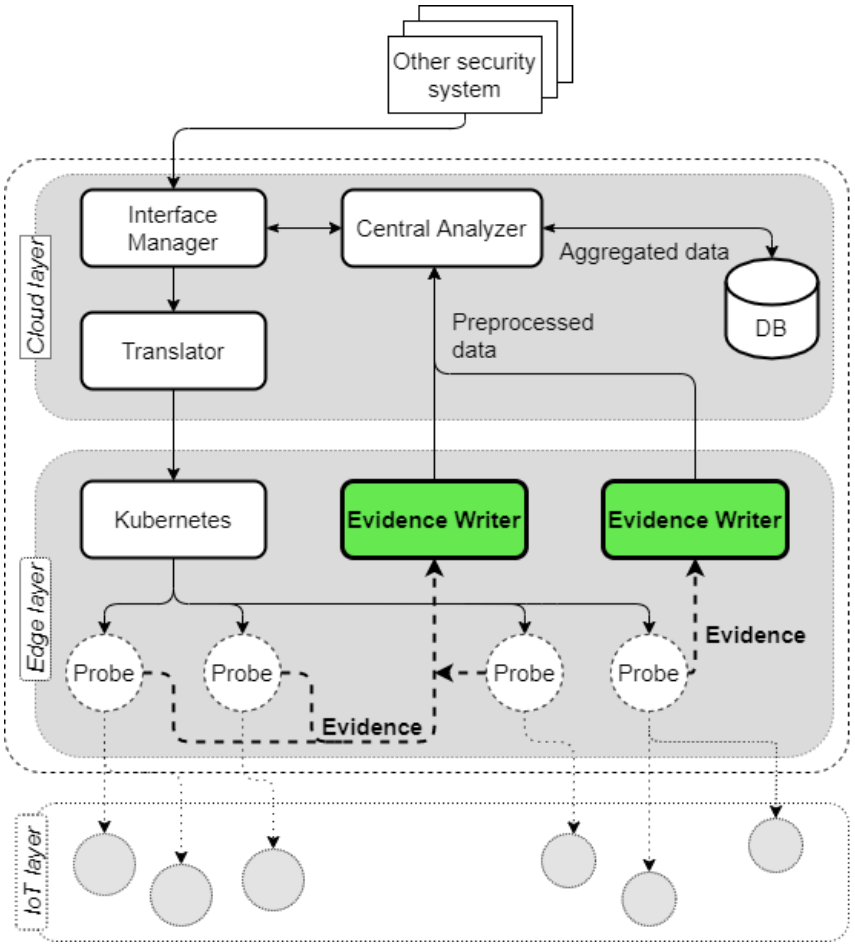
1. Interface Manager: interazione tra framework e ambiente esterno (utenti, altri sistemi di sicurezza, ecc.)
2. Translator: mappa le richieste di assurance in richieste a Kubernetes

Framework



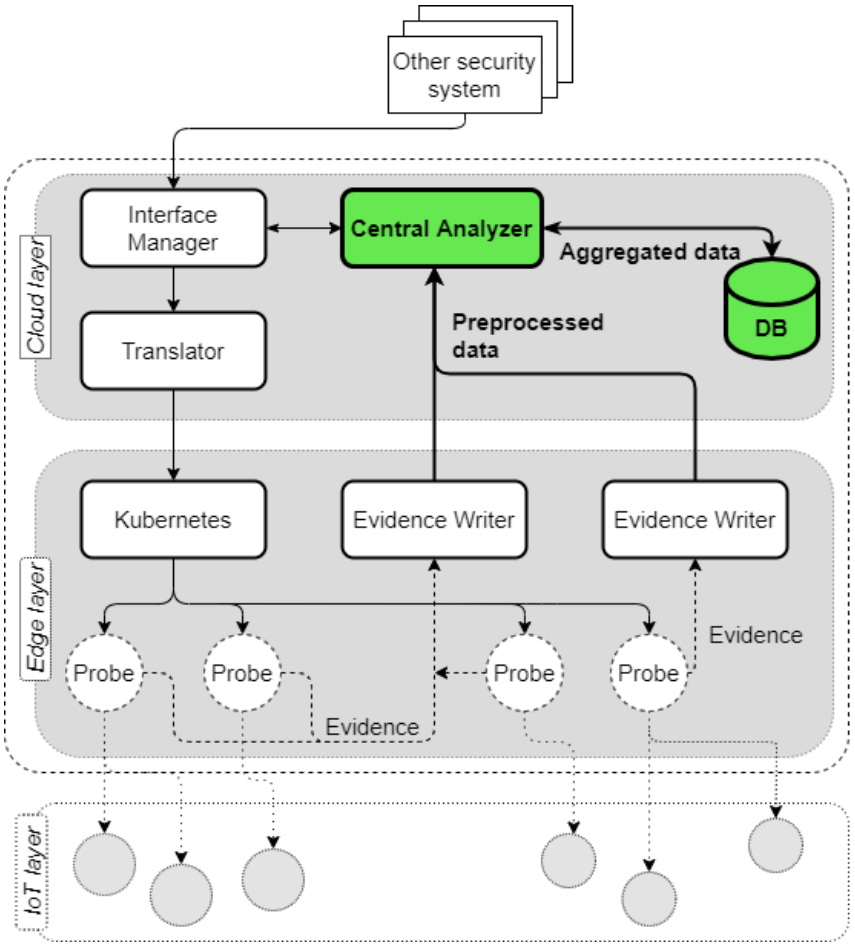
1. Interface Manager: interazione tra framework e ambiente esterno (utenti, altri sistemi di sicurezza, ecc.)
2. Translator: mappa le richieste di assurance in richieste a Kubernetes
3. Kubernetes: esegue le Probe per la raccolta delle evidenze

Framework



1. Interface Manager: interazione tra framework e ambiente esterno (utenti, altri sistemi di sicurezza, ecc.)
2. Translator: mappa le richieste di assurance in richieste a Kubernetes
3. Kubernetes: esegue le Probe per la raccolta delle evidenze
4. Evidence Writer: riceve ed elabora le evidenze

Framework



1. Interface Manager: interazione tra framework e ambiente esterno (utenti, altri sistemi di sicurezza, ecc.)
2. Translator: mappa le richieste di assurance in richieste a Kubernetes
3. Kubernetes: esegue le Probe per la raccolta delle evidenze
4. Evidence Writer: riceve ed elabora le evidenze
5. Central Analyzer: aggrega e crea la visione olistica

Paper

"Towards an Assurance Framework for Edge and IoT Systems"

- pubblicazione presso IEEE International Conference on Edge Computing 2021 (IEEE EDGE 2021)
- tematiche affrontate:
  - definizione di criticità e requisiti
  - descrizione del framework

Proroga – motivazioni

Metodologie di assurance tradizionali su IoT risultano inadeguate

- limitata ad analisi puntuale
- tecniche specifiche assenti
- necessità di valutazioni distribuite
- mancanza di lavori in questo ambito

» Necessità di rivedere le convenzionali tecniche alla base dell'assurance alla luce del nuovo scenario

Proroga – obiettivi

01: analisi comportamentale basata su intelligenza artificiale (AI)

- modelli generati in modo automatico
- ...ma non sempre trustworthy

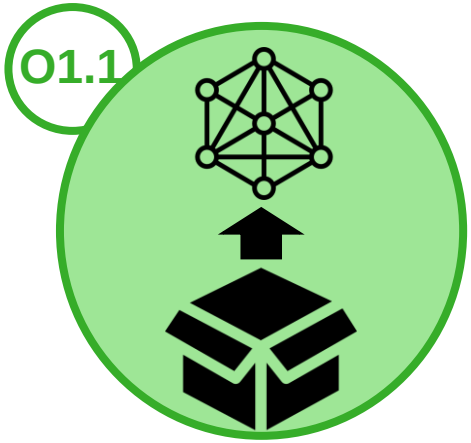
02: sperimentazione e validazione attraverso scenari reali

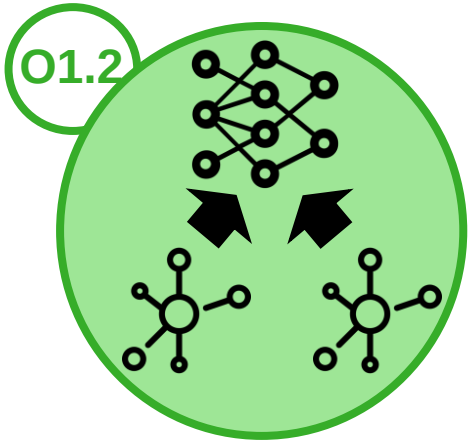
- parte architetturale e metodologica

Proroga – assurance con AI

Sviluppo di tecniche di assurance basate su

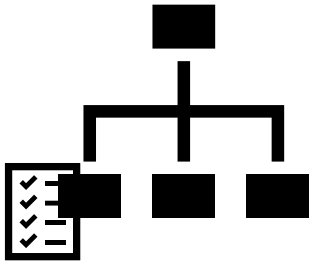
- O1.1: eXplainable AI (XAI)
  - trasparenza
  - obblighi normativi
- O1.2: apprendimento multi-modello
  - modelli multipli
  - aggregazione di valutazioni intermedie





Proroga – sperimentazione

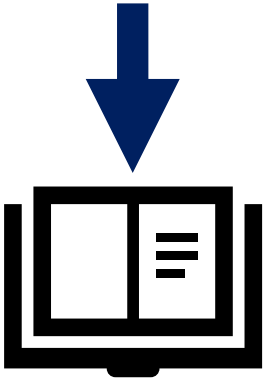
Testing architetturale



Scenario applicativo

MAINFLUX
Internet of Things Solutions

Testing metodologico



Pubblicazione (in fase di scrittura)

Conclusioni

Framework di assurance di sicurezza per sistemi edge e IoT

- adeguato a scenari applicativi moderni
- adattabile alla complessità dei sistemi target
- costruito su un'architettura distribuita basata su Kubernetes

Sviluppi futuri

- analisi comportamentale che sfrutti tecniche di AI
  - spiegabili
  - distribuite
- valutazione sperimentale che misuri
  - qualità dell'assurance
  - risposta ai requisiti

Grazie per l'attenzione