Protocolli per sistemi cloud federati sicuri e affidabili

Borsista: Dott. Giacomo ODOARDI

Tutor: Ch.mo Prof. Luca SPALAZZI

UNIVERSITÀ POLITECNICA DELLE MARCHE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

cini Cyber Security National Lab

7° Borsisti Day

20/01/2016

Roma – Consortium GARR

Borse di Studio Orio Carlini Consortium GARR

Motivazione

- Cloud federato: integrazione di piattaforme cloud gestite da diversi provider.

- Sfida: sicurezza e affidabilità, specialmente per lo storage
  - senza degradare le prestazioni

Stato dell'arte

- Approcci:

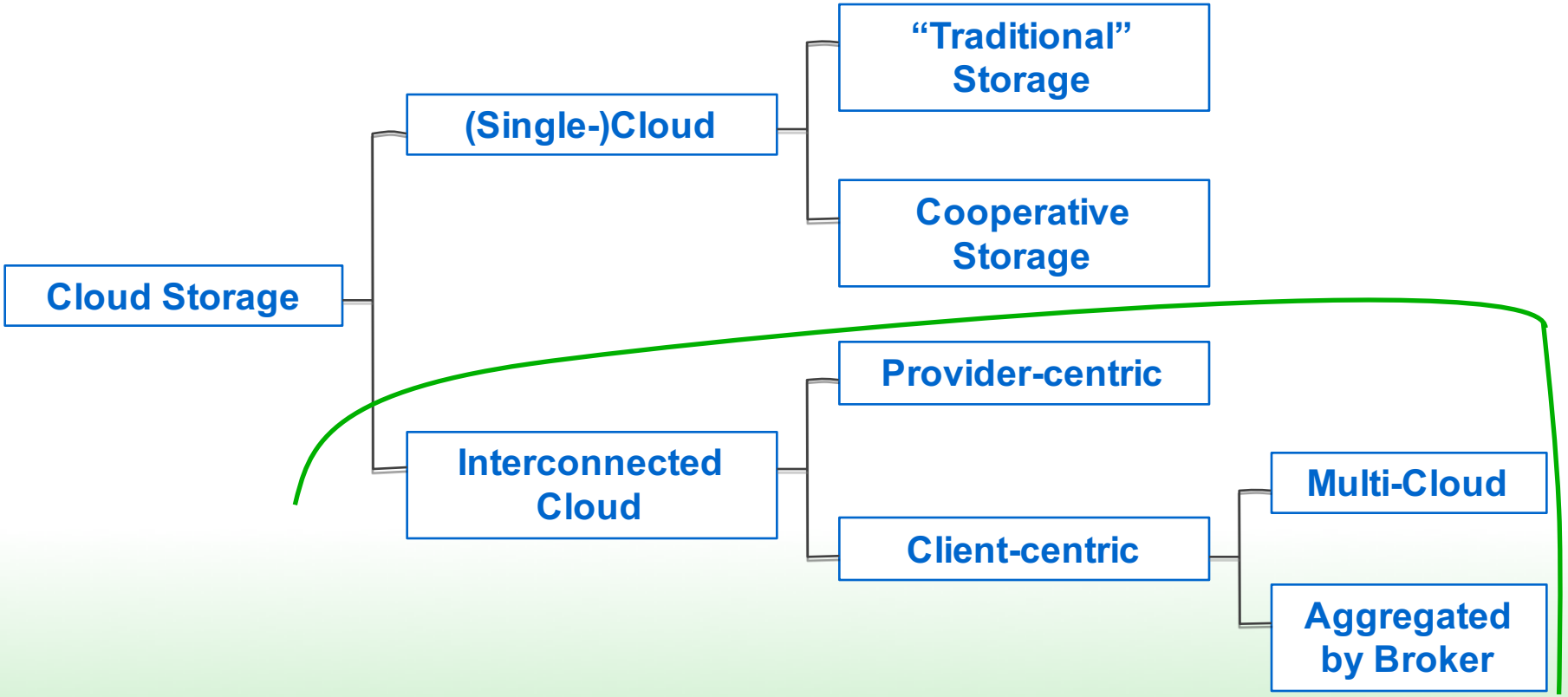
  1) Contrattuale (Service Level Agreement) ⟶ difficoltà legali
  2) Terza parte fidata ⟶ possibile riduzione flessibilità
  3) Algoritmico:

     a) crittografia tradizionale
     b) secure multiparty computation

     c) **codifica e dispersione dell'informazione**

Stato dell'arte (2)

- Cloud storage (deployment models)

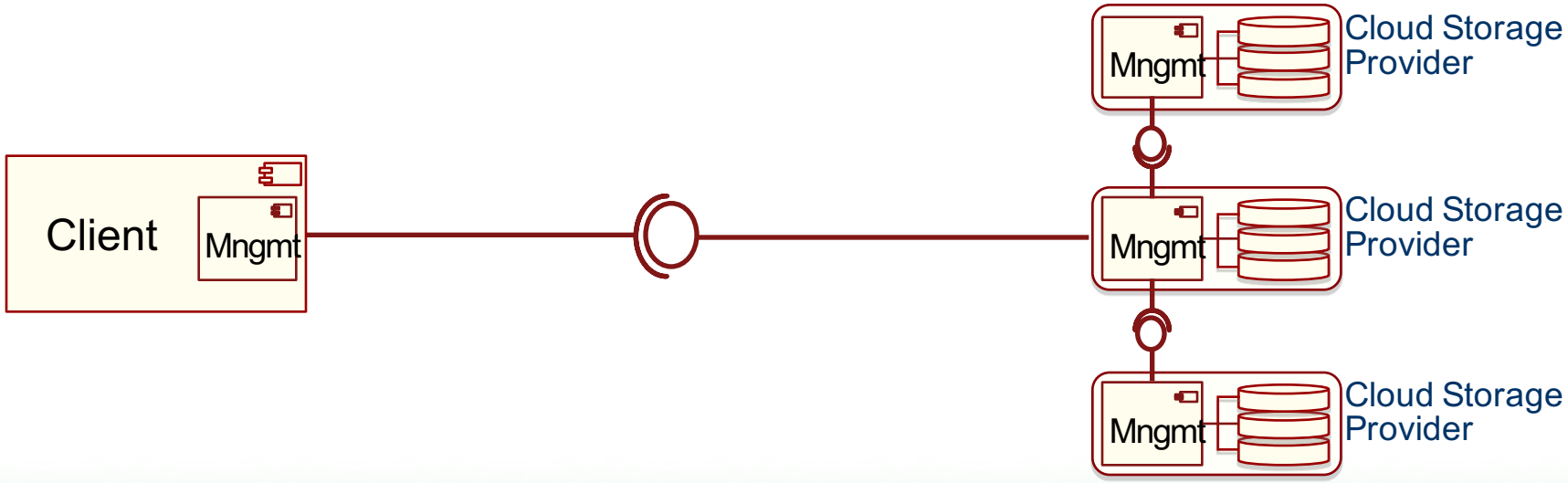


Stato dell'arte (3)

- Single-Cloud Storage

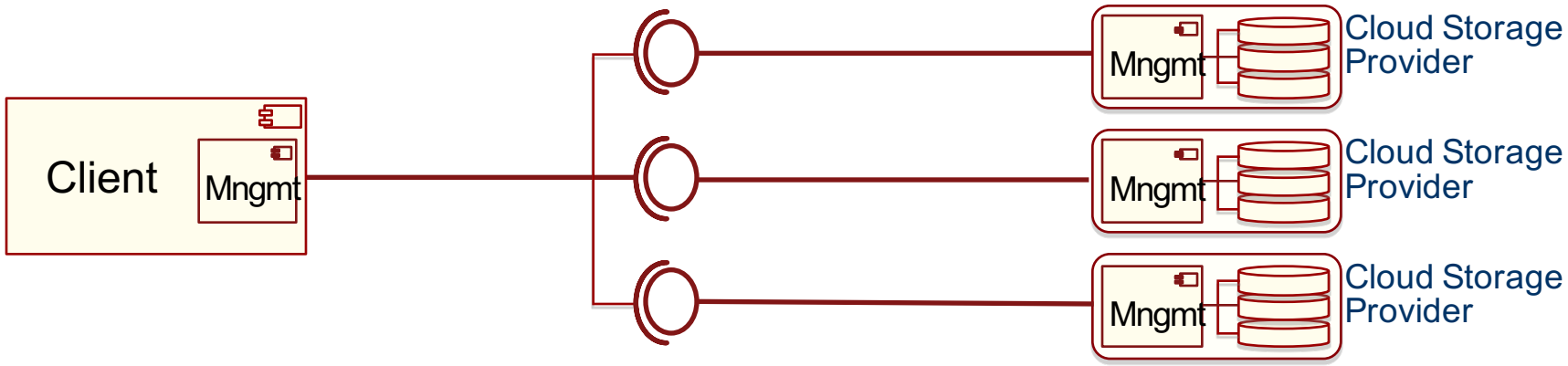
Stato dell'arte (4)

- Interconnected Cloud Storage
  Provider-Centric



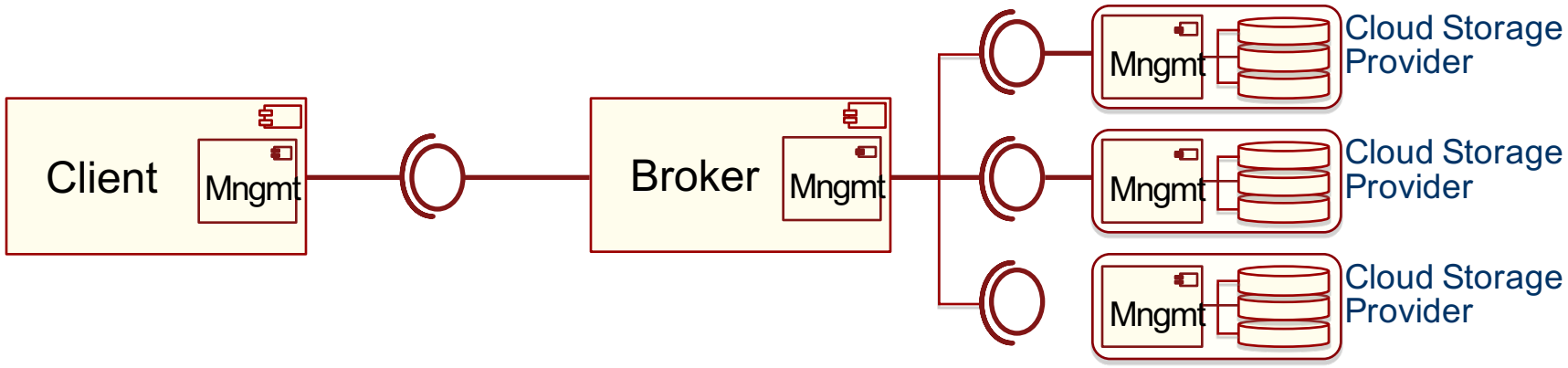
Stato dell'arte (5)

- Interconnected Cloud Storage
  Client-Centric – MultiCloud



Stato dell'arte (6)

- Interconnected Cloud Storage
  Client-Centric - Broker



Stato dell'arte (7)

- Approcci & Architetture

Approcci / Architetture	Contrattuale	Terza parte fidata	Algoritmico
Provider-centric	✓		✓
Client-centric (Multi-Cloud)			✓
Client-centric (Broker)		✓	✓

Obiettivi del progetto

- Progettazione di protocolli di sicurezza per lo storage su cloud federato basati su algoritmi di codifica e dispersione.

- Verifica della rispondenza di tali protocolli ai requisiti di sicurezza e affidabilità tramite tecniche di *Parameterized Model Checking.*

- Implementazione e configurazione di un dimostratore software con cui verificare sperimentalmente l'usabilità della soluzione proposta, anche in termini di prestazioni.

Codifica e dispersione dell'informazione [*]

1) applicazione sui dati di una trasformazione di tipo All or Nothing
2) suddivisione dell'output in k slice
3) applicazione algoritmo correzione d'errore n=k+r slice
4) dispersione delle n slice nei vari nodi di storage

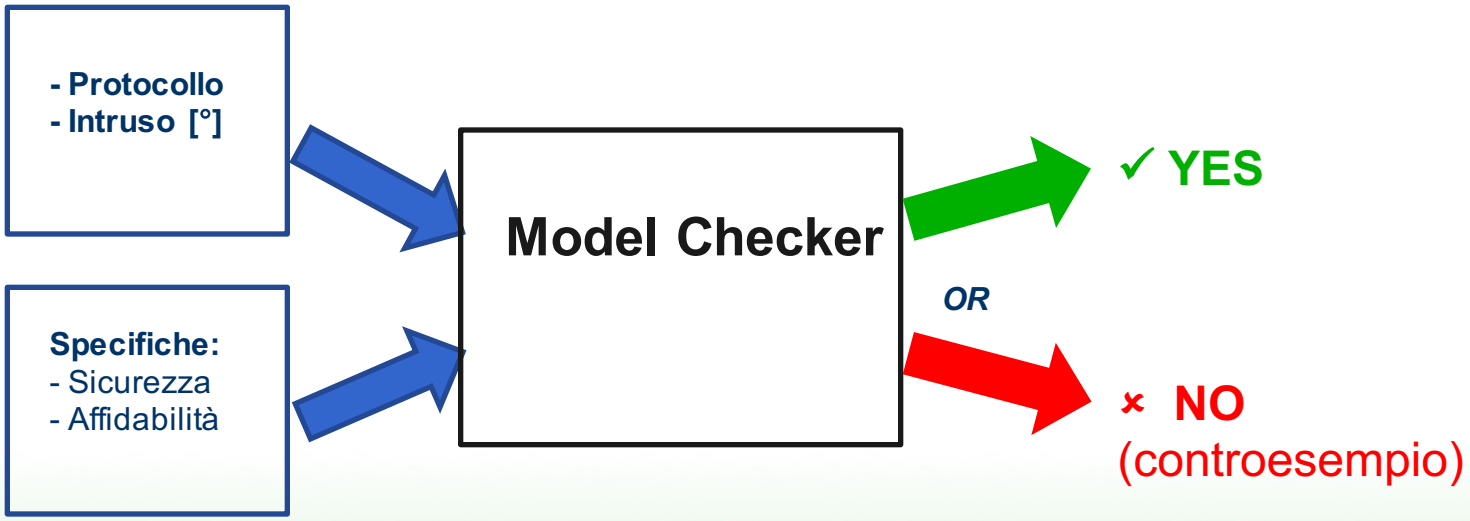
- Trasformazione invertibile ⟺ possesso di almeno k slice!

- Algoritmi finora usati con successo da protocolli di sicurezza per storage distribuito e cooperativo.

- Mai usati su un cloud federato, scenario nuovo ma con almeno gli stessi requisiti di sicurezza ed affidabilità dei precedenti!
- [*] M. Baldi, et al, "AONT-LT: A data protection scheme for cloud and cooperative storage systems", Proc. HPCS 2014, Bologna, Italy, 2014

Model Checking

- Tecnica automatica con cui verificare la rispondenza di un sistema (modellato opportunamente) a determinati requisiti (espressi in un linguaggio formale).



[°] D. Dolev, A. Yao, "On the security of public key protocols", IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198–208, 1983

Fasi del lavoro

1. Approfondita analisi dello stato dell'arte:
   a) cloud federato e relativi protocolli di storage
   b) algoritmi di codifica e partizionamento dei dati
   c) tecniche di model checking (parametrico e non)
2. Scelta di un appropriato scenario di riferimento (focus su ambito sanitario – collaborazione in atto con F.I.M.M.G.), per poi individuarne i requisiti di sicurezza e affidabilità.
3. Progettazione protocolli di memorizzazione e recupero dati per lo scenario su indicato.
4. Verifica del rispetto dei requisiti tramite *Parameterized Model Checking* (*"modello dell'intruso"* di Dolev-Yao).
5. Implementazione dei protocolli su piattaforma reale con controller di federazione (software usato: OpenStack).

Risultati attesi

1. Definizione di protocolli di storage/retrieval dati per cloud federato basati su algoritmi di codifica e dispersione.

2. Dimostrazione formale sicurezza e affidabilità di tali protocolli.

3. Dimostratore software con cui verificare l'usabilità della soluzione proposta.

Grazie per l'attenzione !