Gestione della Privatezza dei Dati Acquisiti in Ambiente Smart-Home

Relatore: Prof. Claudio BETTINI

Correlatore: Dott. Gabriele CIVITARESE

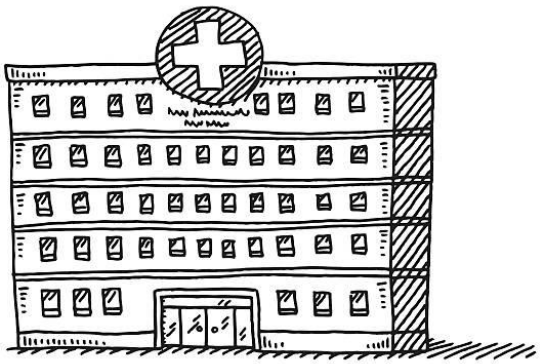
Tesi di Laurea di:

Teresa TANZI

Scenario

Memorizzazione
in cloud non fidato

Riconoscimento di
attività in smart-home



Monitoraggio
medico

Tecniche basate su indici

Attività

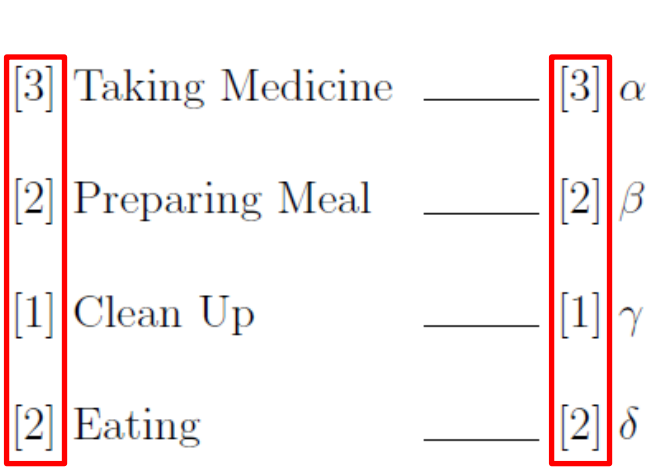
Tipo	Data	Inizio	Fine	Eventi
Taking Medicine	01/01/2016	20:00:00	20:05:00	$[e_1, e_2, \dots]$

RAND

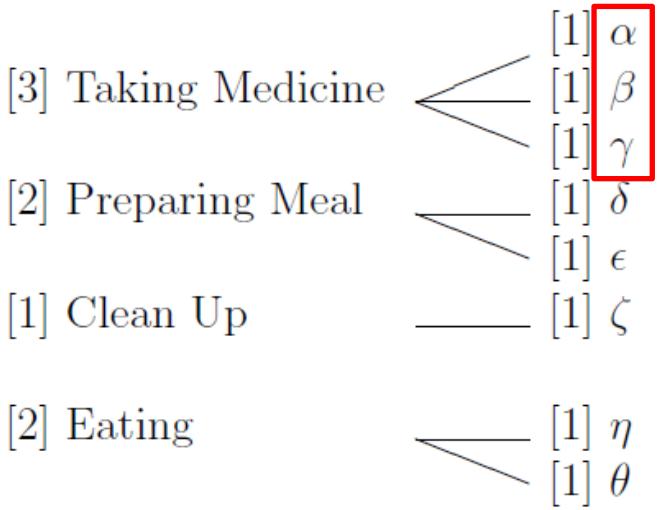
Attività^k

Etuple	I_T
dKf52gzoW7qA...	α

α



Direct



Flattened

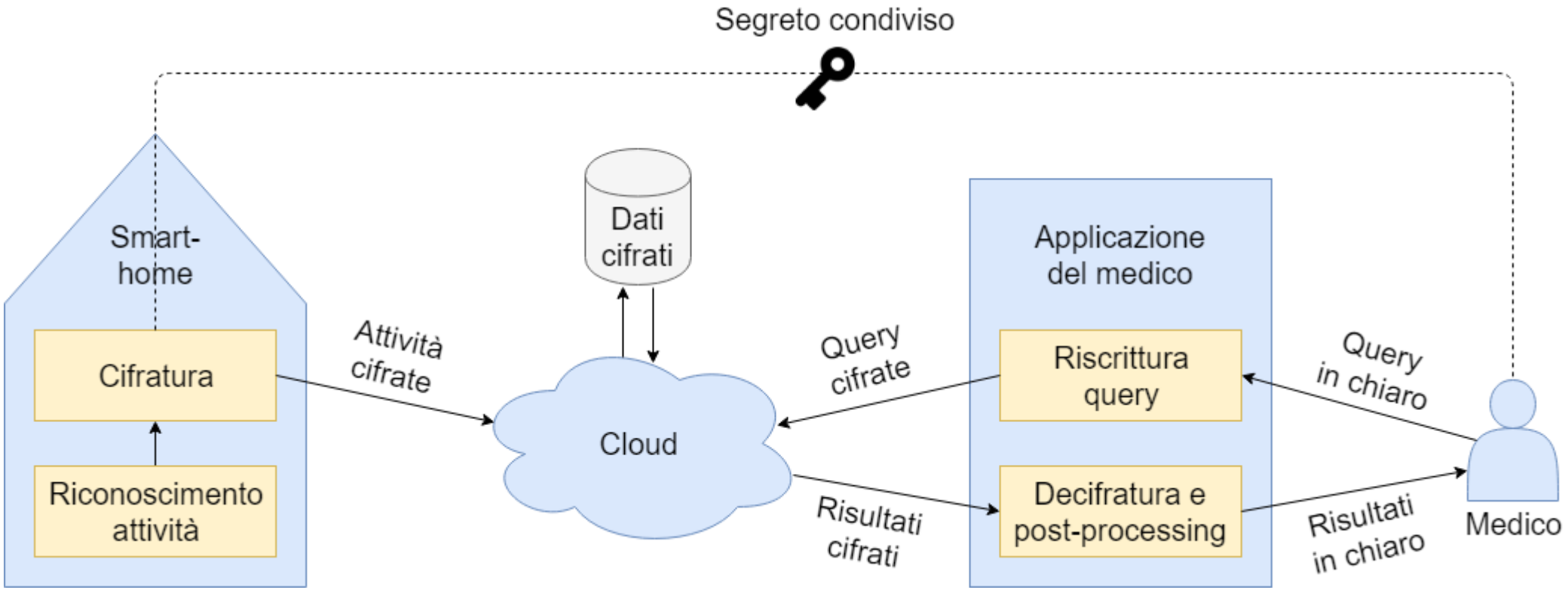
Obiettivo

Progettazione di un sistema di memorizzazione dei dati della smart-home utilizzando un servizio cloud non fidato, proteggendone la riservatezza e permettendo l'esecuzione di query direttamente sui dati cifrati.

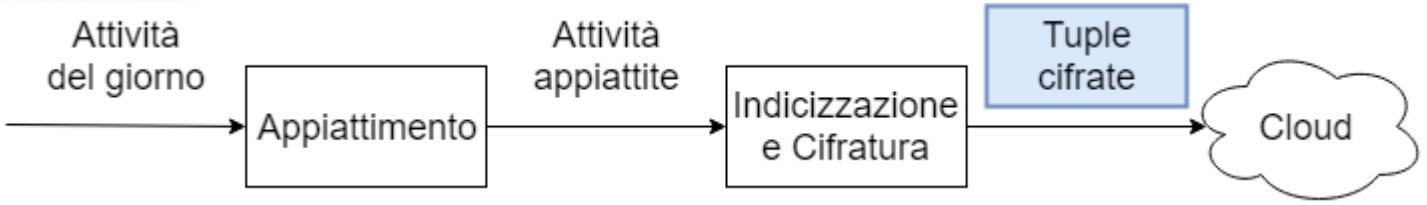
Contributi:

- Analisi del dominio applicativo e dello stato dell'arte.
- Analisi degli attacchi.
- Progettazione ed implementazione del sistema di protezione dei dati.
- Valutazione della soluzione implementata.

Architettura



Rilascio dei dati



Activities

Activity	Type	Date	Time
a_1	Eating	01/01/2016	08:00:00
a_2	Preparing Meal	01/01/2016	12:30:00
a_3	Eating	01/01/2016	12:45:00
a_4	Preparing Meal	01/01/2016	19:30:00
a_5	Eating	01/01/2016	19:50:00

[3] Preparing Meal ——— [3] α

[3] Eating ——— [3] β

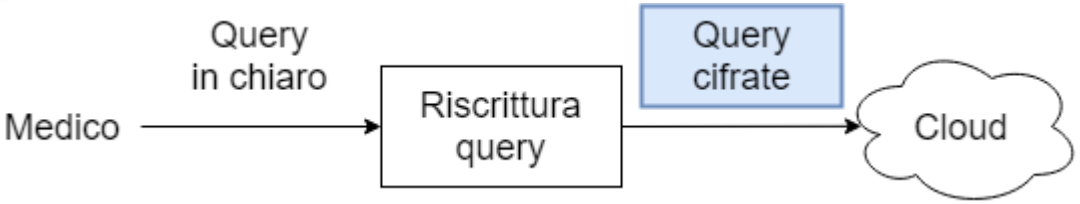
Activities

Activity	Type	Date	Time
a_1	Eating	01/01/2016	08:00:00
a_2	Preparing Meal	01/01/2016	12:30:00
a_3	Eating	01/01/2016	12:45:00
a_4	Preparing Meal	01/01/2016	19:30:00
a_5	Eating	01/01/2016	19:50:00
f_1	Preparing Meal	01/01/2016	-

Activities^k

Etuple	Type^k	Date
a_1^k	β	01/01/2016
a_2^k	α	01/01/2016
a_3^k	β	01/01/2016
a_4^k	α	01/01/2016
a_5^k	β	01/01/2016
f_1^k	α	01/01/2016

Interrogazione dei dati



SELECT *
FROM Activities
WHERE Type = 'Preparing Meal'
AND Time ≥ 12:00:00
AND Time ≤ 14:00:00

SELECT Etuple
FROM Activities^k
WHERE Type^k='α'

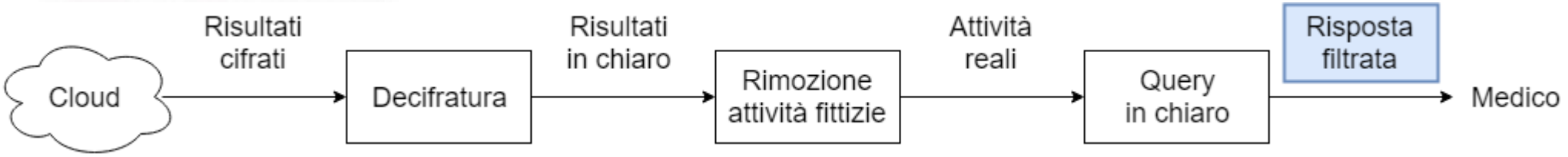
Activities

Activity	Type	Date	Time
a_1	Eating	01/01/2016	08:00:00
a_2	Preparing Meal	01/01/2016	12:30:00
a_3	Eating	01/01/2016	12:45:00
a_4	Preparing Meal	01/01/2016	19:30:00
a_5	Eating	01/01/2016	19:50:00

Activities^k

Etuple	Type^k	Date
a_1^k	β	01/01/2016
a_2^k	α	01/01/2016
a_3^k	β	01/01/2016
a_4^k	α	01/01/2016
a_5^k	β	01/01/2016
f_1^k	α	01/01/2016

Interrogazione dei dati



Activities^k

Etuple	Type^k	Date
a_2^k	α	01/01/2016
a_4^k	α	01/01/2016
f_1^k	α	01/01/2016

Activities

Activity	Type	Date	Time
a_2	Preparing Meal	01/01/2016	12:30:00
a_4	Preparing Meal	01/01/2016	19:30:00
~~f_1~~	~~Preparing Meal~~	~~01/01/2016~~	~~-~~

Activities

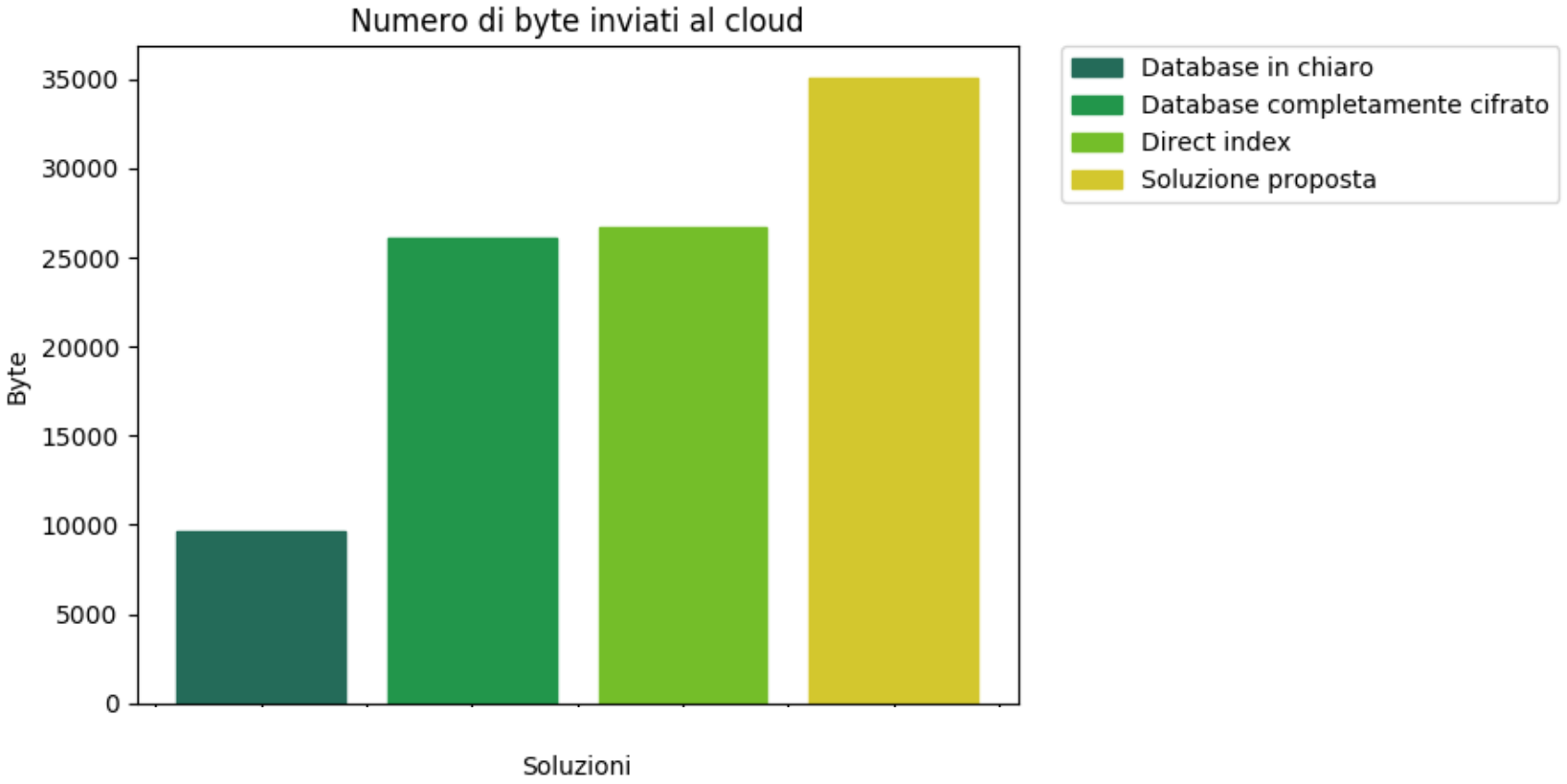
Activity	Type	Date	Time
a_2	Preparing Meal	01/01/2016	12:30:00
~~a_4~~	~~Preparing Meal~~	~~01/01/2016~~	~~19:30:00~~

```
SELECT *
FROM Activities
WHERE Type = 'Preparing Meal'
        AND Time ≥ 12:00:00
        AND Time ≤ 14:00:00
```

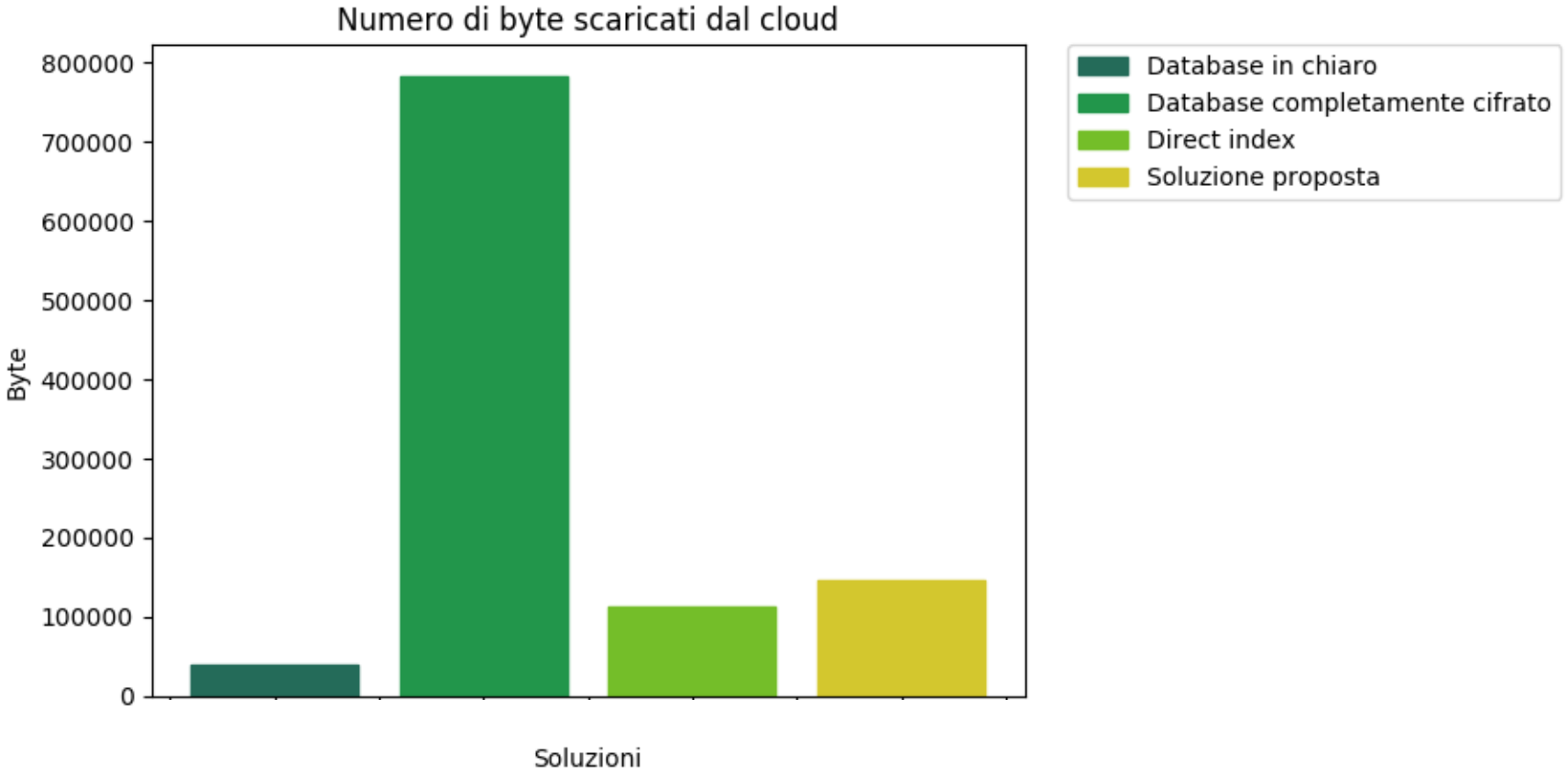
Activities

Activity	Type	Date	Time
a_2	Preparing Meal	01/01/2016	12:30:00

Valutazione



Valutazione



Conclusioni e lavori futuri

La soluzione proposta difende dalla maggior parte degli attacchi, è costosa in fase di cifratura ed invio dei dati, ma è vantaggiosa in fase di esecuzione delle query.

Lavori futuri:

- Ampliare l'insieme delle query eseguibili direttamente in cloud, aggiungendo un indice sul tempo.
- Proteggere da analisi dei pattern d'accesso.
- Aggiungere informazioni sulle anomalie.
- Testare su un dataset più ampio.

Grazie per l’attenzione