

MARTINA PALMUCCI

Consortium
GARR

THE ITALIAN
EDUCATION
& RESEARCH
NETWORK

Estensione del servizio di database SQL di Openstack con crittografia basata su attributi



BORSISTI DAY

lunedì 27 febbraio 2023

Outline

- **Introduzione**
 - **Protezione dei dati**
 - **Cloud storage**
- **Proposta**
 - **Attribute-based encryption**
 - **Openstack**
- **Risultati attesi**

Outline

- **Introduzione**
 - Protezione dei dati
 - Cloud storage
- **Proposta**
 - Attribute-based encryption
 - Openstack
- **Risultati attesi**

Outline

- **Introduzione**
 - **Protezione dei dati**
 - **Cloud storage**
- **Proposta**
 - **Attribute-based encryption**
 - **Openstack**
- **Risultati attesi**



Protezione dei dati

La quantità di dati memorizzati nei nostri dispositivi digitali è in costante aumento. Al giorno d'oggi, dobbiamo **proteggere** i nostri **dati** non solo dagli attacchi esterni, ma anche da quelli interni.

Inoltre, la legislazione recente, in particolare il **GDPR** (Regolamento generale sulla protezione dei dati) [1] e il CDR (Diritto dei dati dei clienti) ha iniziato a imporre misure tecniche per la protezione dei dati.



Outline

- **Introduzione**
 - **Protezione dei dati**
 - **Cloud storage**
- **Proposta**
 - **Attribute-based encryption**
 - **Openstack**
- **Risultati attesi**

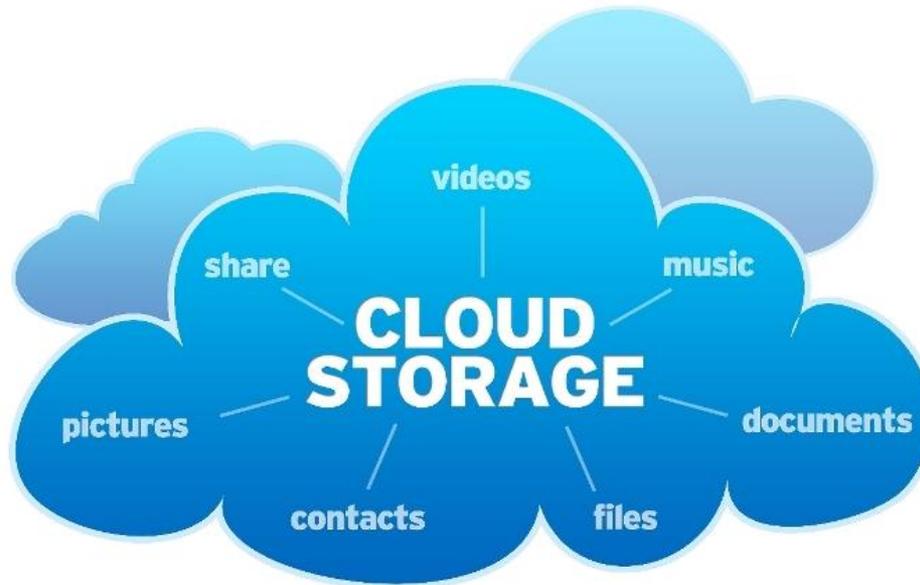
Outline

- **Introduzione**
 - Protezione dei dati
- **Cloud storage**
- **Proposta**
 - Attribute-based encryption
 - Openstack
- **Risultati attesi**



Cloud storage

L'**archiviazione** dei **dati nel cloud** è un tipo di archiviazione dei dati che utilizza server remoti e la tecnologia Internet per archiviare e gestire i dati digitali.





Cloud storage - Vantaggi

L'archiviazione dei dati nel cloud offre diversi **vantaggi** rispetto alle tradizionali soluzioni di archiviazione on-premise. In particolare,

- **Scalabilità**, consentendo loro di espandere o ridurre facilmente la capacità di archiviazione secondo necessità, senza aver bisogno di hardware aggiuntivo.
- **Accessibilità**, fornendo la possibilità di accedere ai propri dati da qualsiasi luogo con una connessione Internet.



What
about
security?



Cloud storage - Svantaggi

L'archiviazione dei dati nel cloud porta, tuttavia, anche a degli **svantaggi**. Tra quelli legati alla **sicurezza**, troviamo

- **Violazioni dei dati**, l'archiviazione dei dati nel cloud può renderli vulnerabili a violazioni dei dati, hacking e altri attacchi informatici.
- **Privacy dei dati**, i provider di archiviazione cloud possono avere accesso ai dati archiviati sui loro server.
- **Problemi di conformità** dell'archiviazione dei dati nel cloud, con conseguenti problemi legali e di conformità.



Outline

- **Introduzione**
 - Protezione dei dati
 - Cloud storage
- **Proposta**
 - Attribute-based encryption
 - Openstack
- **Risultati attesi**

Outline

- **Introduzione**
 - Protezione dei dati
 - Cloud storage
- **Proposta**
 - **Attribute-based encryption**
 - Openstack
- **Risultati attesi**



Perché la crittografia è una buona idea?

Un **database crittografato** offre una migliore **sicurezza dei dati**. I dati del database vengono trasformati in "testo cifrato" (testo illeggibile) dalla procedura crittografica utilizzando un algoritmo.

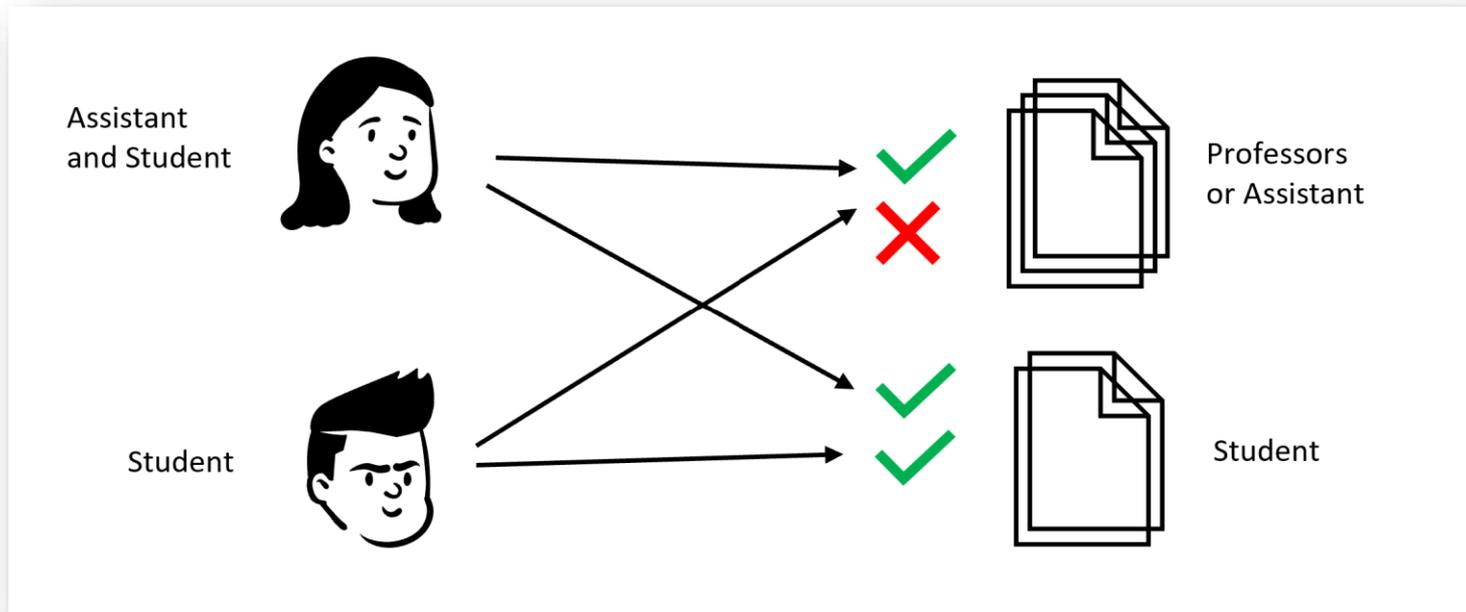
Gli **attacchi alla sicurezza** sono **inevitabili**, ma con tecniche di crittografia e sicurezza dei dati migliorate, gli hacker potrebbero non essere in grado di analizzare o decifrare i dati per comprenderli meglio.





Crittografia basata su attributi

Attribute-Based Encryption (**ABE**, in italiano Cifratura basata su attributi) è una tecnica crittografica che consente l'**accesso** ai dati **in base** ad attributi o **caratteristiche dell'utente**, piuttosto che a identità specifiche [2].



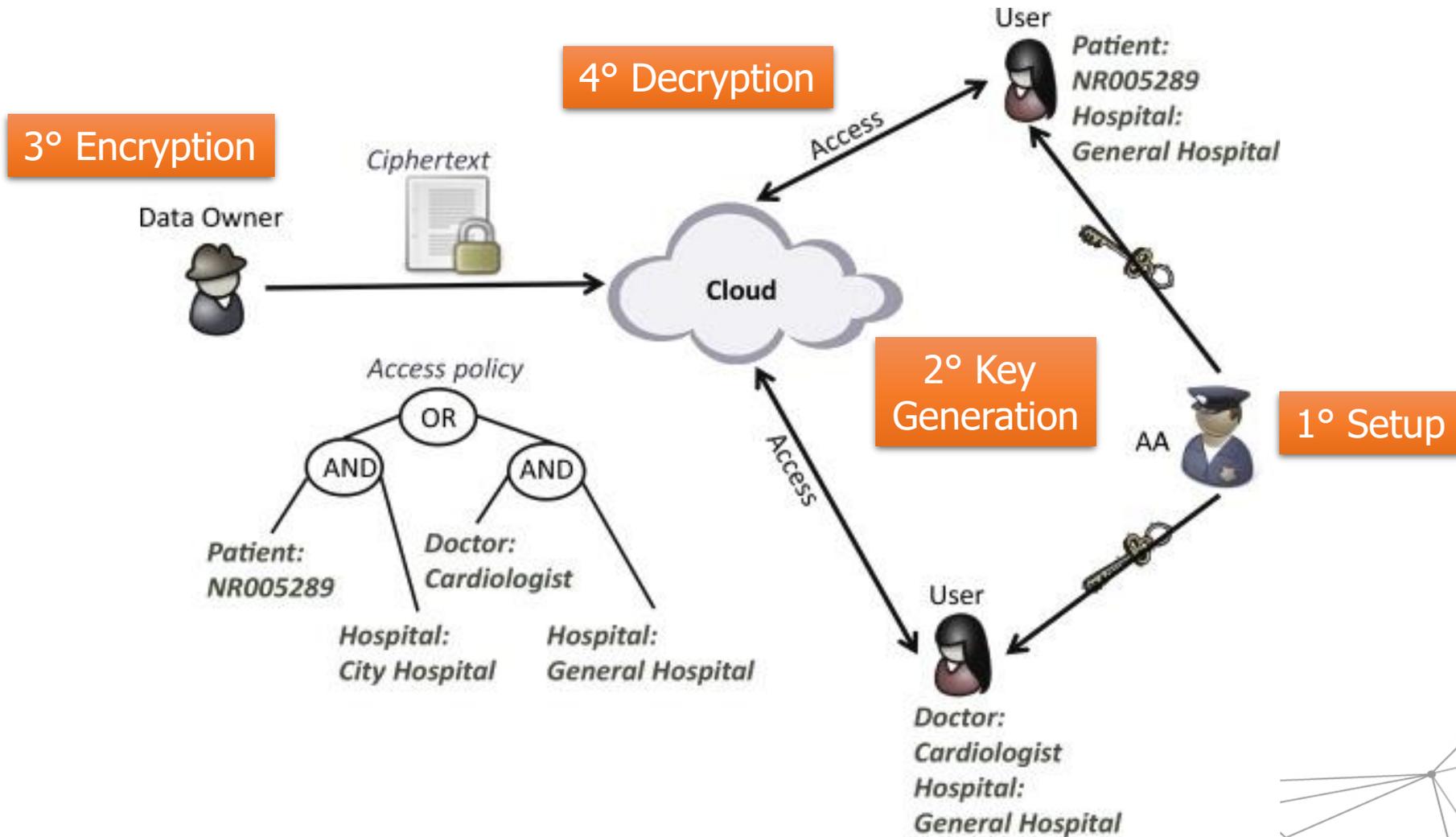


Perché ABE è una buona idea?

- 1. Controllo granulare dell'accesso** ai dati, in cui l'accesso può essere concesso o negato in base a un'ampia gamma di attributi.
- 2. Condivisione sicura dei dati** tra più utenti o gruppi con diversi livelli di accesso in base ai loro attributi, proteggendo allo stesso tempo i dati sensibili da accessi non autorizzati.
- 3. Protezione della privacy** dei dati tramite la crittografia e l'accesso ai dati solo da parte di utenti autorizzati con gli attributi richiesti.
- 4. Politiche di accesso flessibili** in base agli attributi, il che fornisce un approccio più dinamico e adattivo al controllo degli accessi.



Schema CP-ABE



Outline

- **Introduzione**
 - Protezione dei dati
 - Cloud storage
- **Proposta**
 - **Attribute-based encryption**
 - Openstack
- **Risultati attesi**

Outline

- **Introduzione**
 - Protezione dei dati
 - Cloud storage
- **Proposta**
 - Attribute-based encryption
 - **Openstack**
- **Risultati attesi**



OpenStack: piattaforma di cloud computing open source

OpenStack è una **piattaforma di cloud computing** open source, flessibile e scalabile che offre un'ampia gamma di servizi per la creazione e la gestione di cloud privato e pubblico.

- **Ampia rete** di utilizzatori, tra cui organizzazioni, dalle piccole imprese alle grandi aziende.
- **Personalizzabile**, può essere utilizzato per creare cloud privati per uso interno o cloud pubblici per uso esterno.





Proposta iniziale

«Estensione del servizio di database SQL»

Tuttavia, la **modifica del codice sorgente** di OpenStack può avere diversi svantaggi, tra cui:

- **Complessità:** piattaforma complessa e altamente integrata [3,4].
- **Manutenzione:** difficile da mantenere e aggiornare [5].
- **Compatibilità:** problemi di compatibilità con altri componenti o servizi dell'ecosistema OpenStack o con integrazioni di terze parti [6].
- **Sicurezza:** potenziale introduzione di vulnerabilità [7].

DISADVANTAGE





Servizio di cifratura basato su attributi

«Integrazione del servizio di **cifratura**»

- Superare i limiti precedenti prediligendo l’**approccio modulare**.
- Applicazione del servizio di cifratura basato su attributi per controllare l'accesso alle **risorse di rete** in OpenStack.
- Applicazione del servizio di cifratura basato su attributi ai dati archiviati in **Swift**, servizio di object storage di Openstack, oppure a **servizio cloud esterni**.

Outline

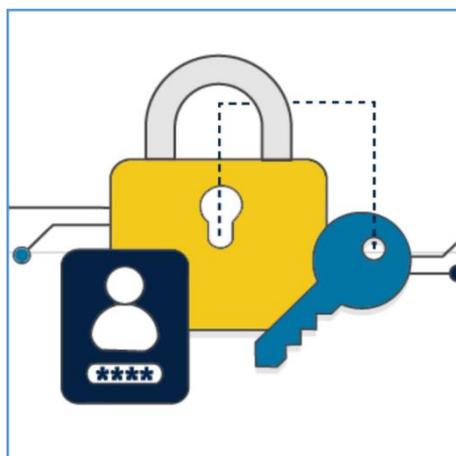
- **Introduzione**
 - Protezione dei dati
 - Cloud storage
- **Proposta**
 - Attribute-based encryption
 - Openstack
- **Risultati attesi**



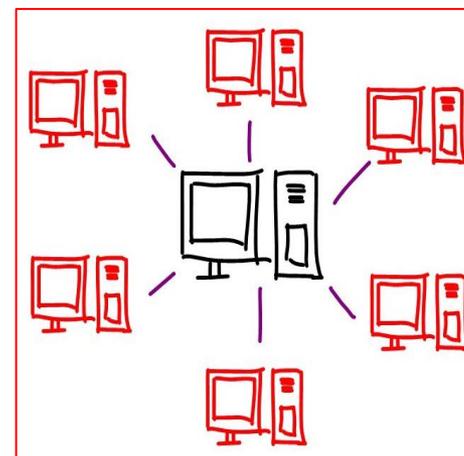
Risultati attesi



Rispetto delle normative



Protezione capillare di dati e risorse



Predisposizione a sistemi decentralizzati



Riferimenti

1. EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
2. Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." *Proceedings of the 13th ACM conference on Computer and communications security*. 2006.
3. "Modifying OpenStack Code: An Exploration of Challenges" by Aditya Manthramurthy, Prajakta Kalmegh, and Nalini Natarajan. *Proceedings of the 2017 IEEE International Conference on Cloud Engineering (IC2E)*, 2017.
4. "An Analysis of the Code Complexity of the OpenStack Cloud Computing Platform" by C. D. Parson, L. Liu, and D. C. Wilkins. *Proceedings of the 2015 IEEE International Conference on Cloud Computing (CLOUD)*, 2015.
5. "Maintenance and Upgrade of OpenStack Cloud Computing Platform: A Survey" by S. M. Ferdous, M. Y. Aalsalem, and I. A. H. Fathalla. *International Journal of Computer Applications*, vol. 170, no. 1, pp. 1-9, 2017.
6. "OpenStack Operations Guide" by Tom Fifield, Diane Fleming, Anne Gentle, Lorin Hochstein, Jonathan Proulx, and Everett Toews. O'Reilly Media, 2014.
7. "OpenStack Security Guide" by OpenStack Security Project. OpenStack Foundation, 2019.



Grazie per l'attenzione!