Aspetti Crittografici nel Cloud Computing

Prof. Massimiliano Sala

Università di Trento

Trento, 10 Maggio 2013

Introduzione

Obiettivo crittografico classico:

Consentire a due utenti di comunicare su un canale potenzialmente insicuro, senza permettere ad una terza persona di comprendere il contenuto dei messaggi.

Impedire ad una terza persona di impersonare uno dei due utenti.


Alice


Bob


Eve

Crittografia a chiave privata

In linea di principio Alice e Bob si mettono d'accordo sulla funzione di cifratura da usare.

Una funziona di cifratura in realtà è un algoritmo che **deve** essere complesso per non essere ricostruibile ("attaccabile").

Sarebbe troppo oneroso mettersi d'accordo sull'intero algoritmo, quindi Alice e Bob si mettono d'accordo su un algoritmo che dipende da un parametro chiamato **chiave**.

Principali cifrari simmetrici

Oggigiorno, i principali cifrari simmetrici usati sono:

E-PAYMENT	DES 3DES
INTERNET	AES - 128 AES - 256 RC4
GSM	A5/1 A5/3

Crittografia a chiave pubblica

Non esiste solo una chiave privata, perchè siamo costretti ad usare un canale pubblico.

Diffie-Hellman
(DH e ECDH)

consente a due entità di stabilire una chiave condivisa e segreta utilizzando un canale di comunicazione pubblico.

Cifratura asimmetrica
(RSA, EL GAMAL)

consente di cifrare e decifrare usando una combinazione di chiave pubblica e privata (non condivisa).

Chiave pubblica e chiave privata

Se  e  devono comunicarsi più informazioni in modo sicuro, usano **sia** crittografia pubblica che simmetrica, con diversi scopi.

- C. Pubblica $\rightarrow$ si scambiano una chiave segreta comune che utilizzeranno nella crittografia simmetrica;
- C. Simmetrica $\rightarrow$ crittano i messaggi in chiaro e decrittano i messaggi grazie alla chiave segreta condivisa.

CRITTOGRAFIA TIPICA DEL CLOUD

Tematiche tipiche del cloud:

Distinguiamo due tipologie di cloud:

- Cloud Interno: Ad esempio, un cloud utilizzato esclusivamente dai dipendenti di un'azienda;
- Cloud Esterno: Chiunque può usufruire del cloud pagando semplicemente il servizio.

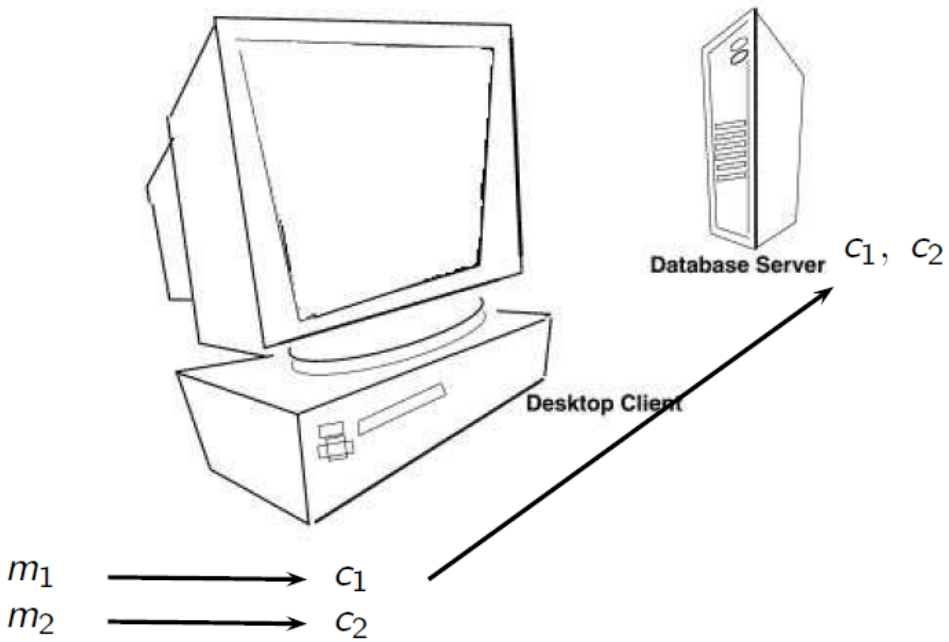
Cloud Esterno: Cifratura omomorfa

Chi deposita i propri dati sul cloud non si fida del cloud stesso (dipendenti disonesti del cloud, hacker).

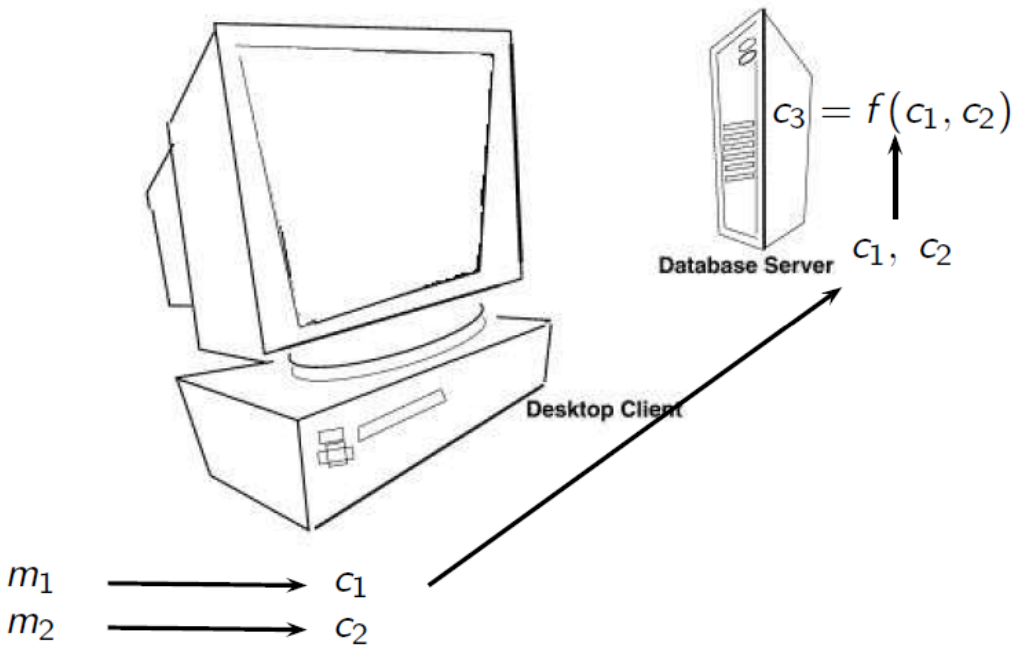
Soluzione?: I dati vengono prima cifrati e poi depositati sul cloud.
Per maneggiare tali dati, l'utente li riacquisisce dal cloud e li decifra autonomamente.

NO!

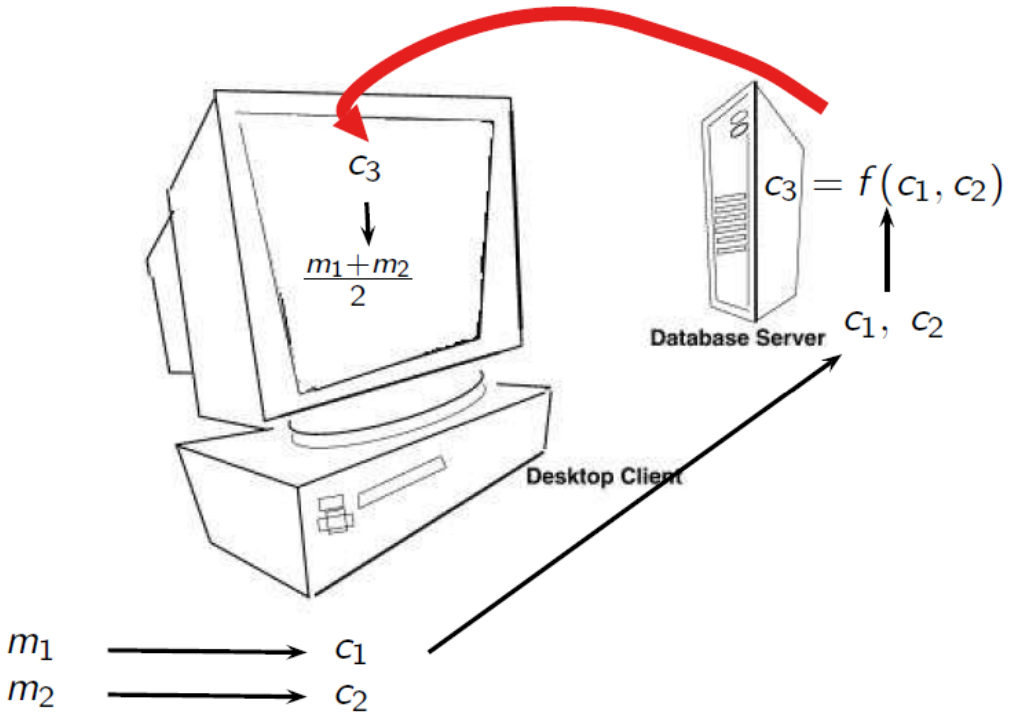
Cifre omomorfe e cloud



Cifre omomorfe e cloud



Cifre omomorfe e cloud



Cloud Interno: ABE

In un Cloud interno potremmo rifare il ragionamento precedente, ma vogliamo enfatizzare un altro aspetto.

In un'organizzazione molto grande, con chiare esigenze di sicurezza, il Cloud si potrebbe usare come un repository in cui mettere i documenti (cifrati) di interesse per più utenti. Il modo per farlo è di usare Attribute Based Encryption

ABE

Con ABE è possibile:

- cifrare i documenti marcandoli con degli attributi;
- consegnare a ogni singolo utente una chiave di decifratura, di modo che la chiave apre un documento solo se l'utente possiede almeno gli attributi del documento.

In questo modo si semplifica enormemente il problema della condivisione di informazioni riservate.

SHE - Somewhat Homomorphic Encryption

Fissato uno schema di cifratura SHE, solo alcune operazioni sono possibili sui cifrati. È quindi necessario decidere in anticipo che tipo di dati saranno protetti e quali elaborazioni andranno fatte: da ciò dipenderà la scelta dello schema di cifratura.

Esempi

- Query semplici su un database;
- Calcoli statistici come media, varianza, etc.;
- Funzioni di autenticazione/verifica.

FHE - Full Homomorphic Encryption

Sui cifrati, **tutte** le operazioni sono possibili.

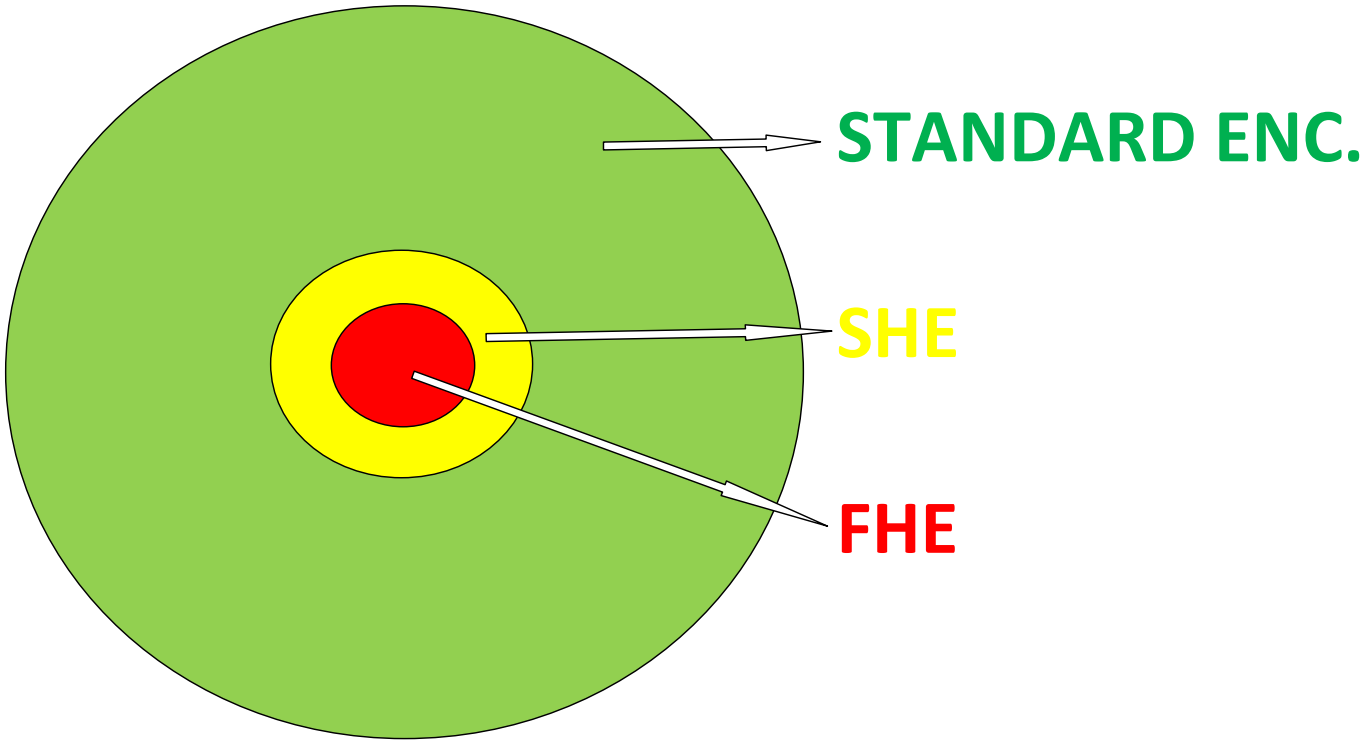
Il **grosso problema** è che l'FHE è **costosissimo**, sia in termini di complessità computazione che in termini di memoria.

Ciò nonostante l'uso di FHE può essere giustificato in presenza di dati ad altissima sensibilità.

Architettura Proposta

- Dati poco sensibili (la maggioranza);
- Dati sensibili (pochi);
- Dati molto sensibili (pochissimi).

Architettura Proposta



Osservazioni

SHE per funzionare devi aver deciso a priori quali sono le operazioni che ti interessano.

Un cloud a **3 stadi di sicurezza** è un valore aggiunto.

Grazie per l'attenzione