**Privacy and Data Protection in Emerging Scenarios**

**Privacy in Data Outsourcing**

Il mondo è diventato sempre più tecnologico e interconnesso, smart tutto.

I vantaggi sono: miglior protezione, disaster recovery, prevenzione

Gli svantaggi sono: aumento di attacchi, perdita di controllo sui dati e processi, maggiore complessità.

Così tanti dispositivi che comunicano e si scambiano informazioni appunto provocano una perdita di contorllo, i dati intanto sono diventati la risorsa più cara al mondo e per questo è necessario che vada protetta.

Il cloud permette ad aziende e a singoli individui di avere processi e storage space e scalabilità, il problema principale è la perdita di controllo sui dati. Non vogliamo che ciò accada.

Vogliamo che il provider ci fornisca i servizi in totale sicurezza senza che avvenga leakage dei dati a nostra disposizione.

Le privacy policies messe in pratica (utilizzate) da coloro che offrono servizi cloud proteggono i dati da attacchi esterni ma non dall’utilizzo che può farci il possessore del servizio cloud.

Vogliamo poter dare i nostri dati al cloud service provider (CSP) in modo da non preoccuparci dei dati e in modo che esso ci possa fornire i servizi richiesti. In questa ottica solo il comportamento del data owner è considerato trusted.

Confidenzialità: proprietà delle informazioni di non essere rese disponibili o divulgate a individui, entità o processi non autorizzati.

(non rendere disponibili informazioni a chi non è autorizzato)

**Characterization of Data Protection Challenges**

3 dimensioni caratterizzano il problema: (vedere slide 31)

1. Security properties
2. Access requirements
3. Architectures

Security properties:

1. Confidentiality (protezione ad utilizzi non autorizzati)
2. Integrity (validità dei dati)
3. Sla (service-level agreement) compliance (certificazioni) (availability), mi impegno che i servizi funzionino sempre per i miei clienti, servizio rispetto al quale ho firmato

Access requirements:

1. Data archivial (upload/downlaod)
2. Data retrieval (queries)
3. Data update

Architectures:

1. 1 user- 1 provider
2. N users - \*provider (authorization and access control)
3. \*users – n providers (controlled data sharing and computation)

Le dimensioni vengono combinate per la creazione di nuove challanges/problemi che possono sorgere.

I providers possono essere: curious, lazy, malicious

Trustworthy: il provider fornisce correttamente integrità e availability ma la confidenzialità la devo garantire io.

Honost but curious: il provider è trustworthy però devo mantenere i miei dati confidenziali anche rispetto a lui, non è un misbehaviour da parte sua. Ex non posso mettere dati sanitari in chiaro ad un provider esterno.

In lazy e malicous cade il fatto di essere trustworthy quindi anche rispetto a integrità e availability

Lazy: il provider non fa effort a comportarsi male, lo fa solo male.

Malicous: si impegna a comportarsi male