# CoMPAC: Collaborative Multi-Party Access Control for OSN

**Panagiotis Ilia**

**pilia@ics.forth.gr**

## Problem

Privacy settings of shared data are set entirely by the owner.

Related users cannot control access to shared data.

- Not considered as co-owners of data objects.
- Not given any rights on shared data objects.
- Their privacy concerns are not taken into account.

Shared data are disclosed to **a large number** of OSN users, **despite the privacy concerns of the related users**.

## Requirements

- Related users are considered as co-owners of the objects.
- Co-owners collaboratively specify the access control policy.
- The policy is enforced by the trusted friends of co-owners.
- Co-owners and their trusted friends are held **responsible** and **accountable** for access control decisions.
- OSN:
  considered trusted for securely computing joint values
  not take part on specification or enforcement of the policy.

## Proposed Model

Based on mature and widely used cryptographic techniques.

Employs a **secret sharing scheme** and **selective encryption**.

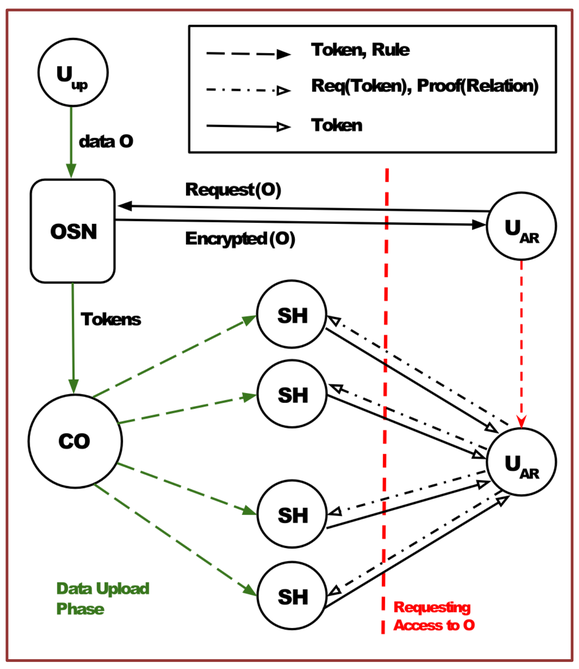
Two distinct phases:

- Data Object **Upload** phase
- Data Object **Access** phase

Uploaded data objects are encrypted by the OSN.

Tokens are created and distributed to co-owners.

Each co-owner distributes the tokens to trusted friends (SH).




The Access requesting user:

Receives the encrypted data object from OSN.

Contacts trusted friends (SH) to collect the tokens.

Reconstruct the encryption key – decrypts object

## System Design

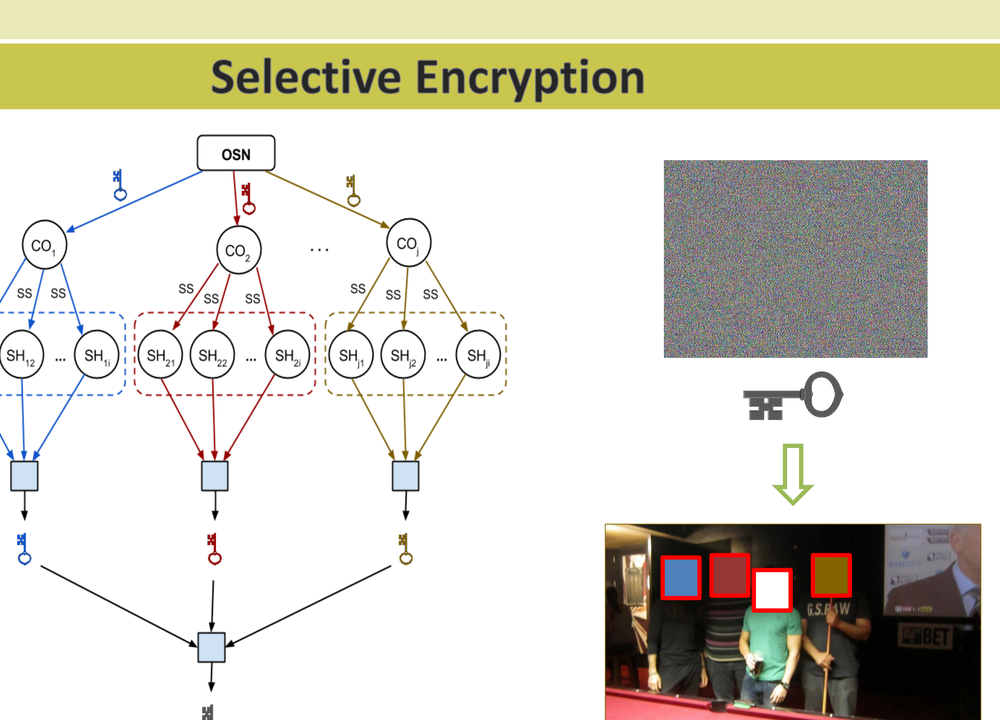
Each co-owner submits random **encryption** and **secret keys** and the desired **sensitivity** value.

OSN generates keys and calculate sensitivity from submitted values.

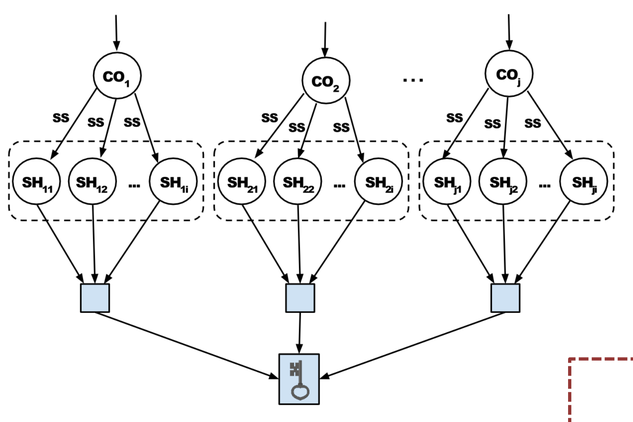
OSN creates **shares** from the secret key (tokens) and disseminates them to co-owners.

The secret key is reconstructed only if a sufficient number of shares are combined together.

The **sensitivity** value determines the number of shares and the threshold value.

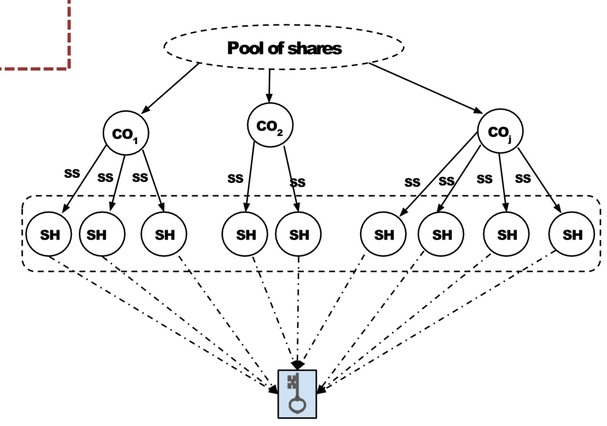



## Pool Approach vs 2-level Approach




**Pool Approach**

Shares belong to a pool
Supports weighted decisions
Supports hierarchy




**2-level Approach**

Each CO has a single "**key-share**"
Distributes "**sub-shares**"
Supports selective encryption

## Selective Encryption




Top-level shares can be used as **personal keys** for **selective encryption**