

# Content Level Access Control for OpenStack Swift

Prosunjit Biswas, Farhan Patwa, Ravi Sandhu

## Quick Summary

### Swift Background:

- ✓ Storage service from OpenStack cloud platform.
- ✓ Users can upload or download an object using Swift API.
- ✓ User can Share an object with other users using Swift's ACL (Access Control List).

### Identifying Problems:

- ✓ Swift ACL is an 'all or nothing' approach.
- ✓ User either shares the whole object or cannot share at all.

### Our Solution:

- ✓ We extend Swift's access control into content level access control.
- ✓ We assign object-labels on the content level of Swift objects.
- ✓ We specify Label Based policy using object-labels and user-labels.
- ✓ We further specify different ways for applying object-labels at content level.

### Our Scope:

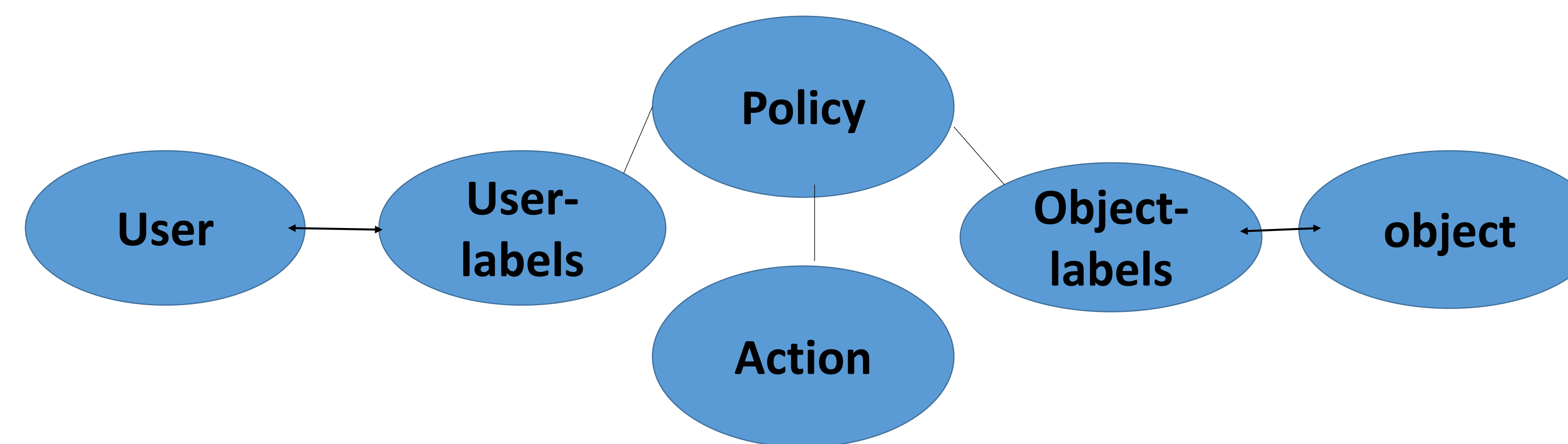
- ✓ The solution applies for JSON formatted file, in hierarchical document models (e.g. XML)

### JSON (JavaScript Object Notation)

- ✓ JSON is a hierarchical Data Model similar to XML
- ✓ We use JSON because of its increasing popularity.

## Technical Details

### Label Based Access Control (LaBAC):



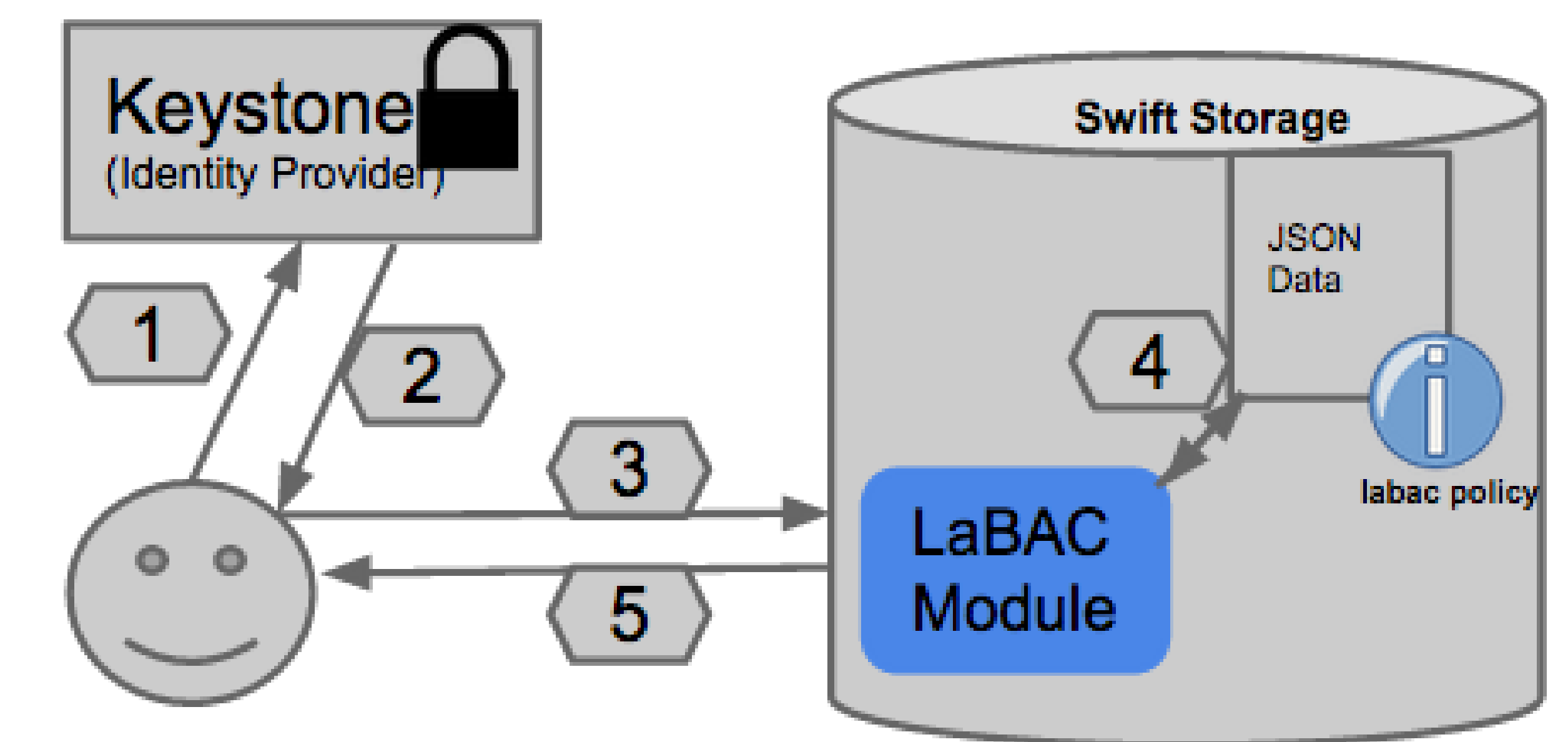
### LaBAC Policy:

- ✓ (user-labels, action, object-labels)  
e.g. ({manager},read,{'sensitive'})

### Assigning Labels at Content Level:

- ✓ Using JSONPath  
e.g. (/path/to/salary',{sensitive})
- ✓ Using JSON key/value  
e.g. (<RE-for-email>, {contact-info})
- ✓ Using Attribute to specify labels  
e.g. Records created after Jan 1<sup>st</sup> are restricted.

### Implementation & Performance:



- 1, 2: User requests and receives Identity from Keystone.
- 3: User present credential to Swift.
- 4: LaBAC decides which JSON object is accessible.
- 5: User gets Partial content.

### Required Changes:

- ✓ Extended Swift Object Server logic.
- ✓ LaBAC module intercept every Swift request and modifies response based on LaBAC policy.
- ✓ LaBAC policy and Labeling rules are stored as metadata of Swift objects.

Comparing download time of Swift objects with and without Content Level Access Control (CLAC)

