An Attribute-Based Protection Model for JSON Documents

Prosunjit Biswas, Ravi Sandhu and Ram Krishnan
Department of Computer Science
Department of Electrical and Computer Engineering

10th International Conference on Network and System Security

September 28th, 2016

Outline

- Summary
- Motivation
- Background
- JSON protection model
- Labeling JSON elements
- Implementation
- Q/A

Summary

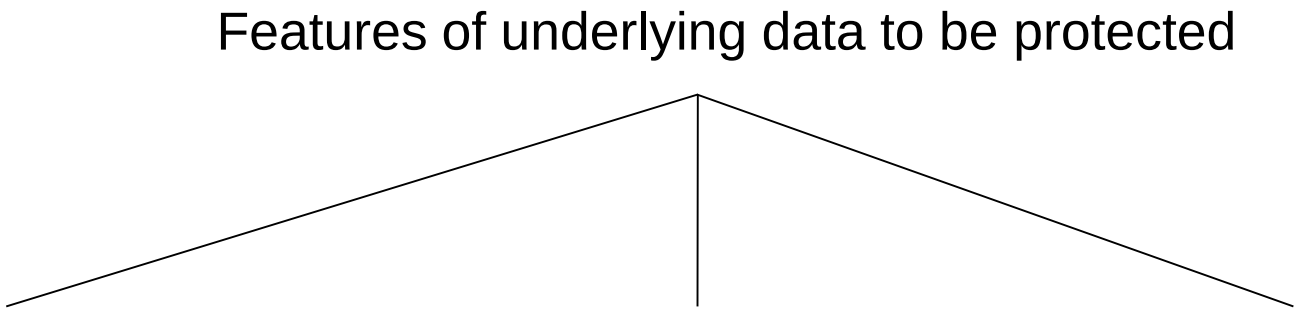
- We have presented an attribute based protection model and labeling schemes for securing JSON documents.

Motivation

- **Why JSON documents?**

Motivation (continuing)

- **Why not reuse XML protection models?**



Hierarchical relationship
(e.g. house-no, street, town)

Semantic association
(e.g. phone-no, email, fax, mobile)

Scatteredness
(due to redundancy/duplicity)

- Considered in XML protection models

- Not considered

Motivation (continuing)

❑ Existing XML models vs proposed model

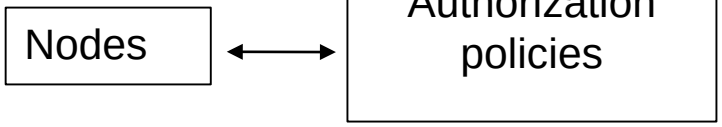


Fig 1 (a): Existing XML protection models

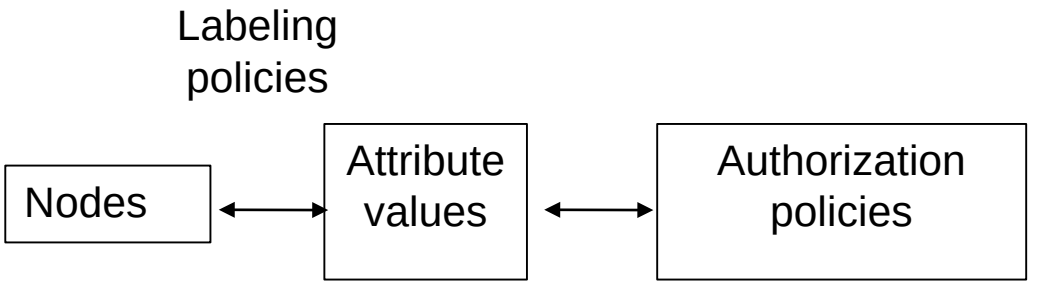


Fig 1(b): Proposed JSON protection model

Background - JSON

- **JSON data forms a rooted tree hierarchical structure (like XML)**

```
{
“emp-rec”:{
“name”: “...”,
“con-info”:{
        “email”:
“...”,
        “work-phone”:
“...”
        },
“emp-info”:{
        “mobile”: “...”,
        “EID”:  “...”,
        “salary”: “...”
}
“sen-info”: {
        “SSN”: “...”,
        “salary”: “...”
        }
}
}
```

Fig 2 (a): JSON data

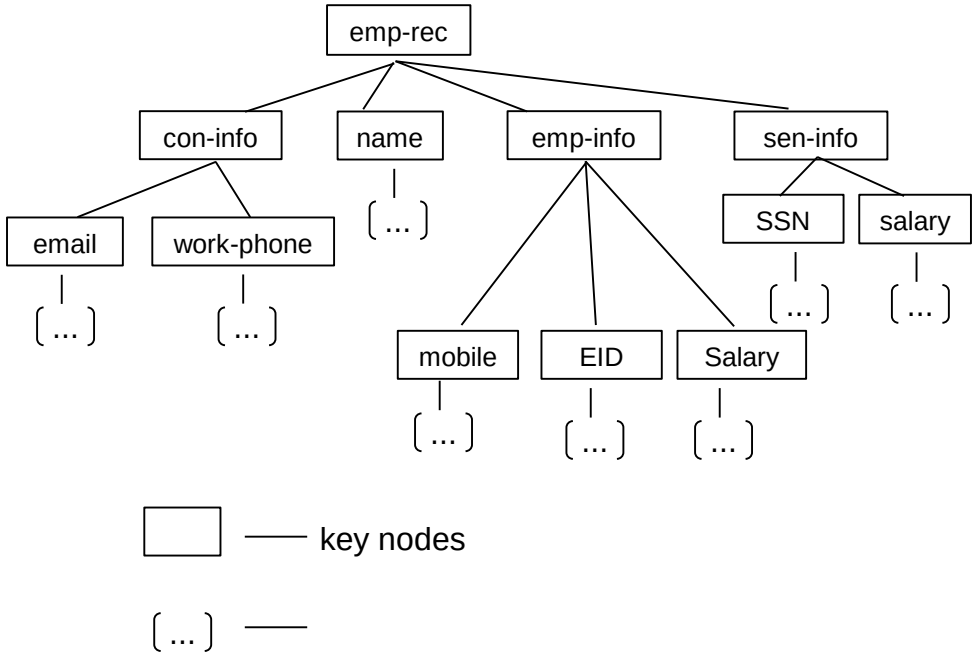


Fig 2 (b): Corresponding JSON tree

JSON protection model

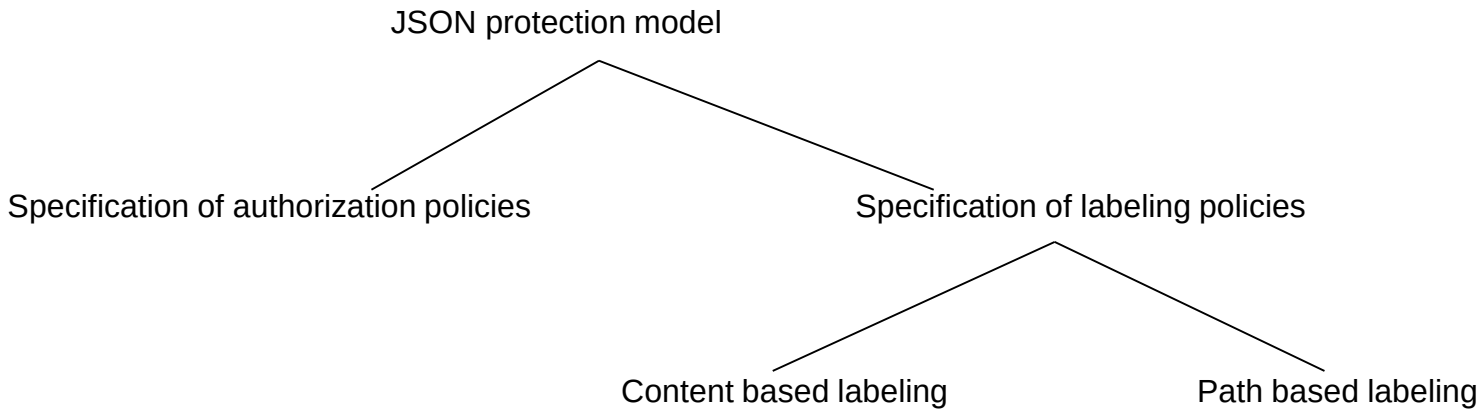


Fig 3: Scope of the JSON protection model

JSON protection model (continuing)

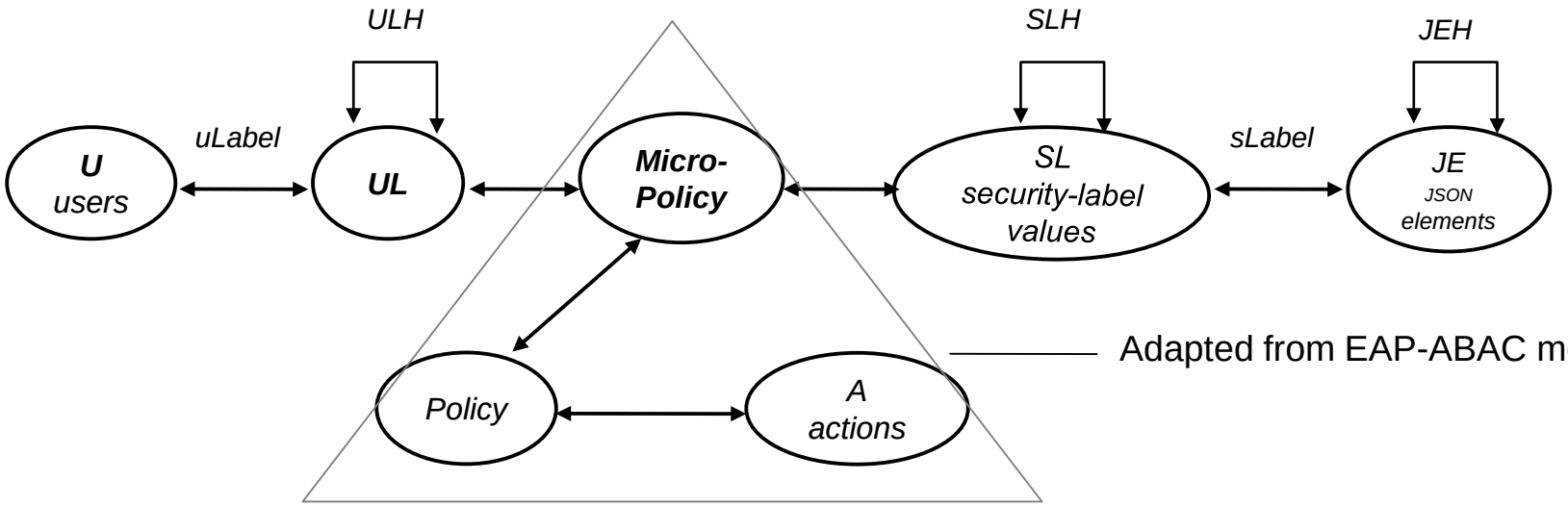


Fig 4: The Attribute-based Operational Model (AtOM)

[1] Biswas, Prosunjit, Ravi Sandhu, and Ram Krishnan. "Label-Based Access Control: An ABAC Model with Enumerated Authorization Policy." Proceedings of the 2016 ACM International Workshop on Attribute Based Access Control. ACM, 2016.

JSON protection model - examples

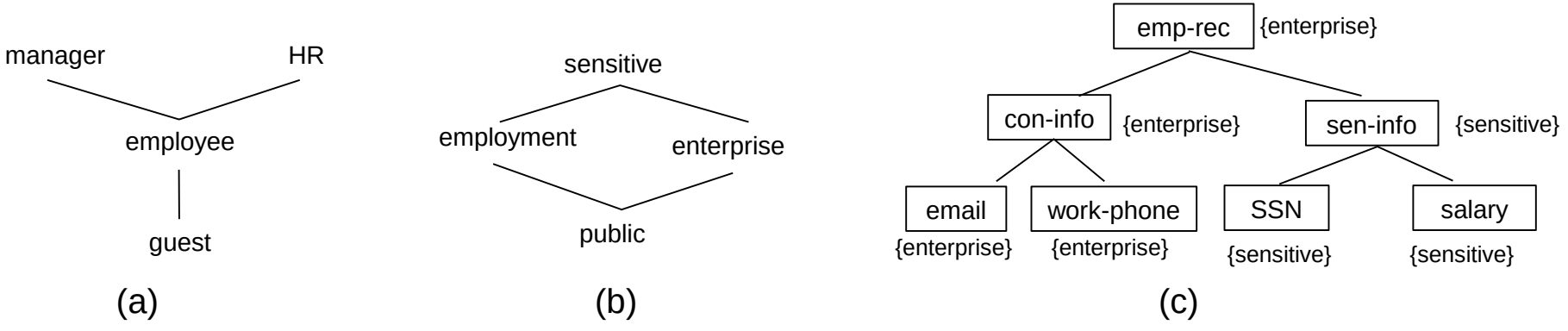


Fig 5: (a) User-label values, (b) security-label values and (c) annotated JSON tree

Example of a policy, $Policy_{read}$ =
{(manager, sensitive), (HR, employment), (employee, enterprise), (guest,public) }

Labeling JSON documents

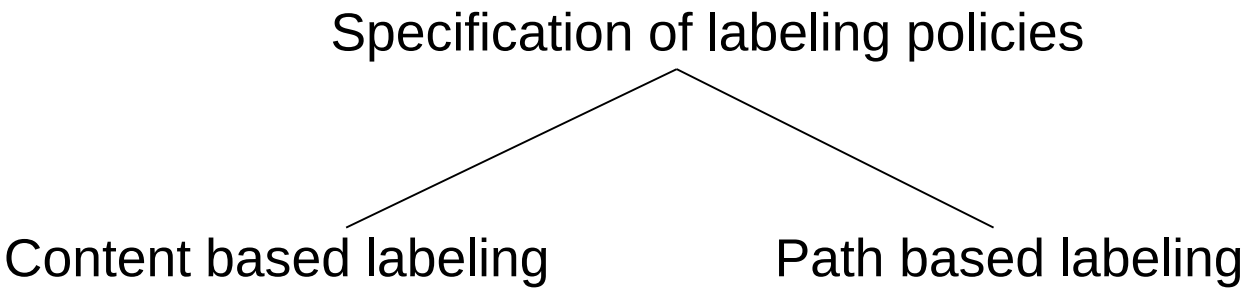


Fig 6 (a): Types of labeling policies

Labeling JSON documents (continuing)

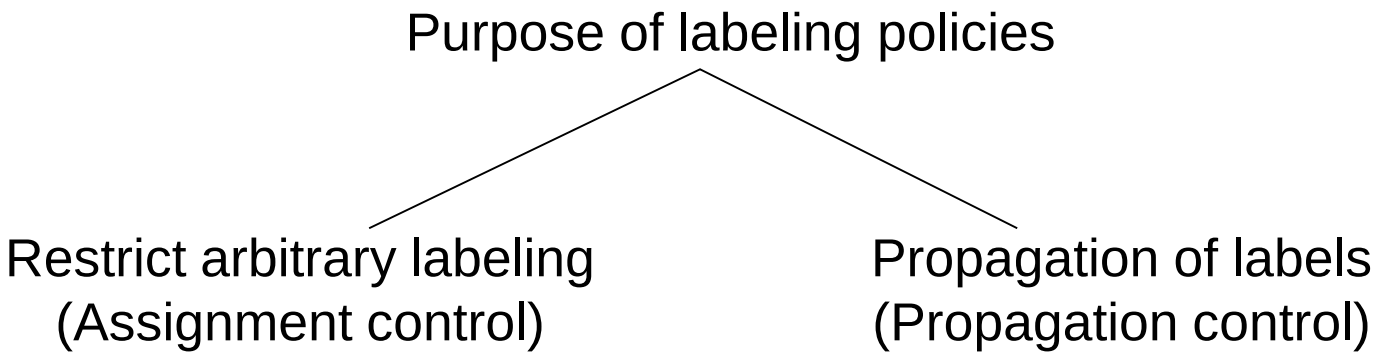


Fig 6 (b): Purpose of labeling policies

Labeling JSON documents – Assignment control

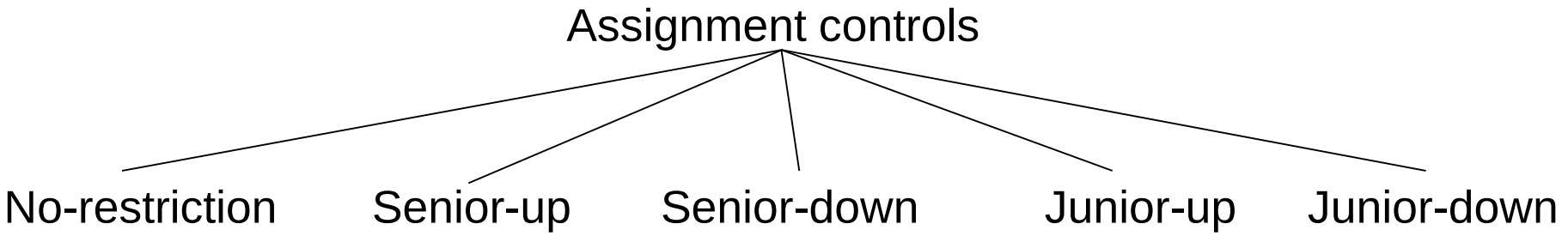


Fig 7 (a): Different types of Assignment controls

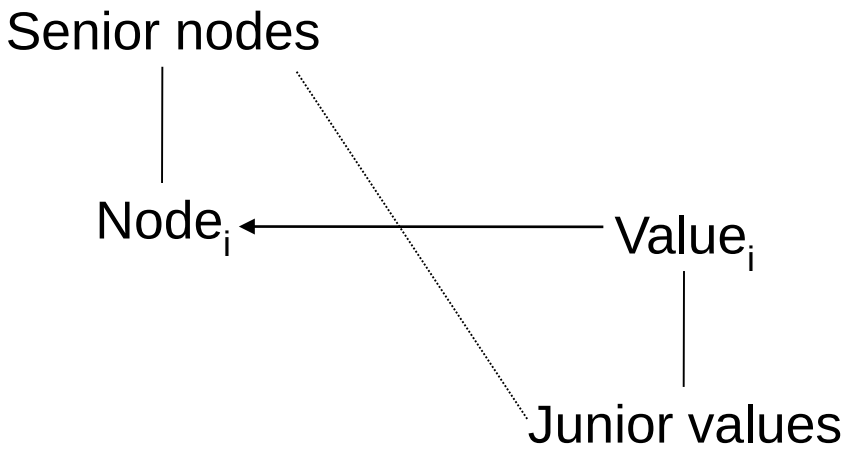


Fig 7 (b): Junior-up assignment control

Assignment

Senior nodes of **Node$_i$** must be assigned junior values of **Value$_i$**

Labeling JSON documents – Propagation control

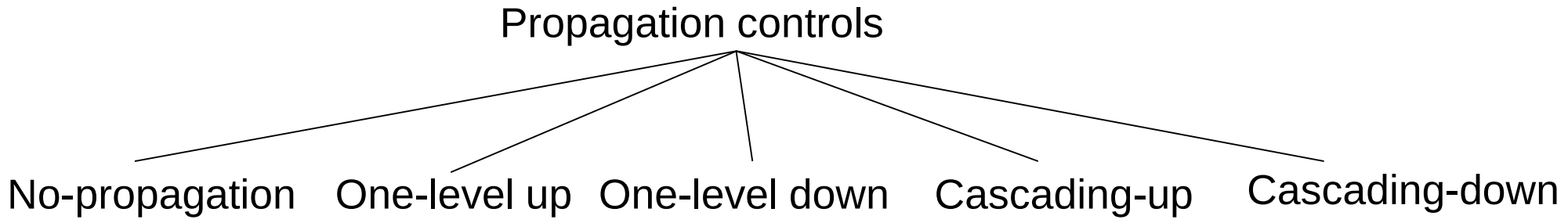


Fig 8: Different types of propagation controls

Labeling JSON documents – Path-based labeling model

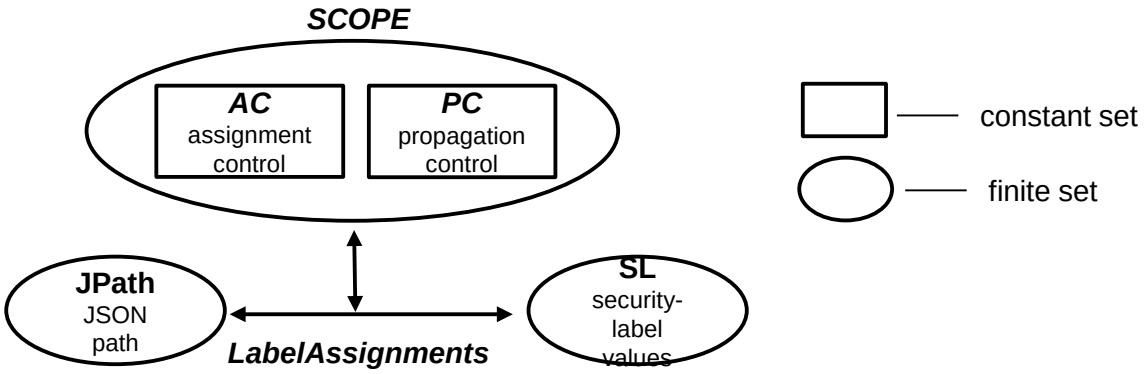


Fig 9: Model for path-based labeling of JSON data

I. JSONPaths
- path-to-email=$.emp-rec.con-info.email
- path-to-salary=$.emp-rec.sen-info.salary
II. LabelAssignments
- LabelAssignments= { (path-to-email, (no-prop, unrestricted), {enterprise}), (path-to-salary, (no-prop, unrestricted), {sensitive}) }

Table 1: Example of path-based labeling

Prototype implementation

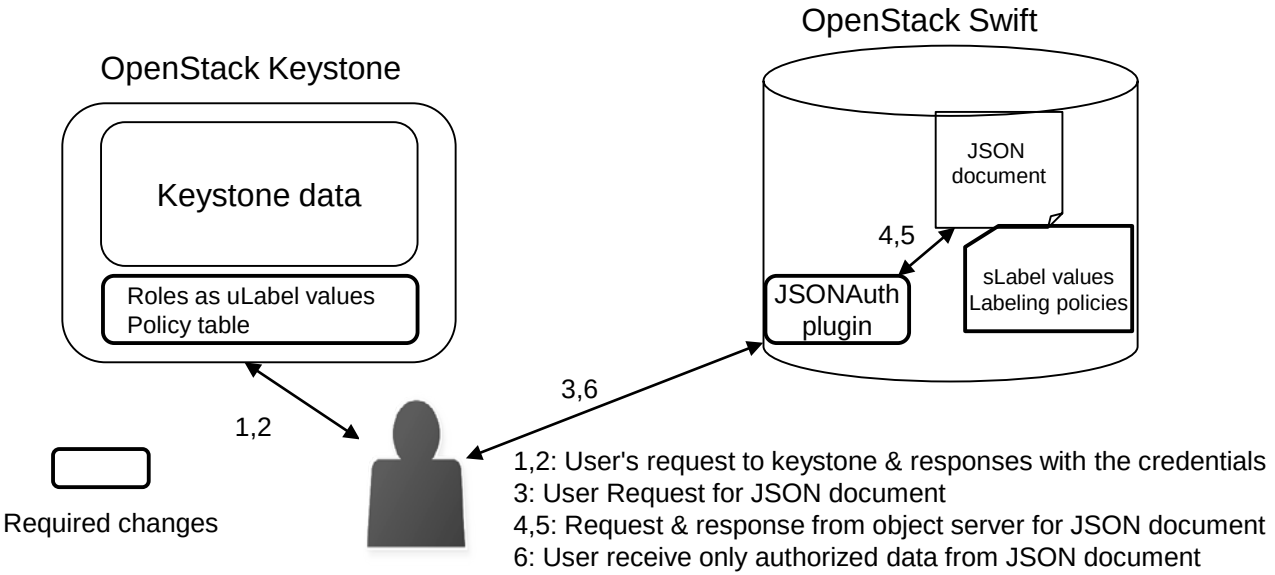


Fig 10: Implementation in OpenStack Cloud

Implementation - evaluation

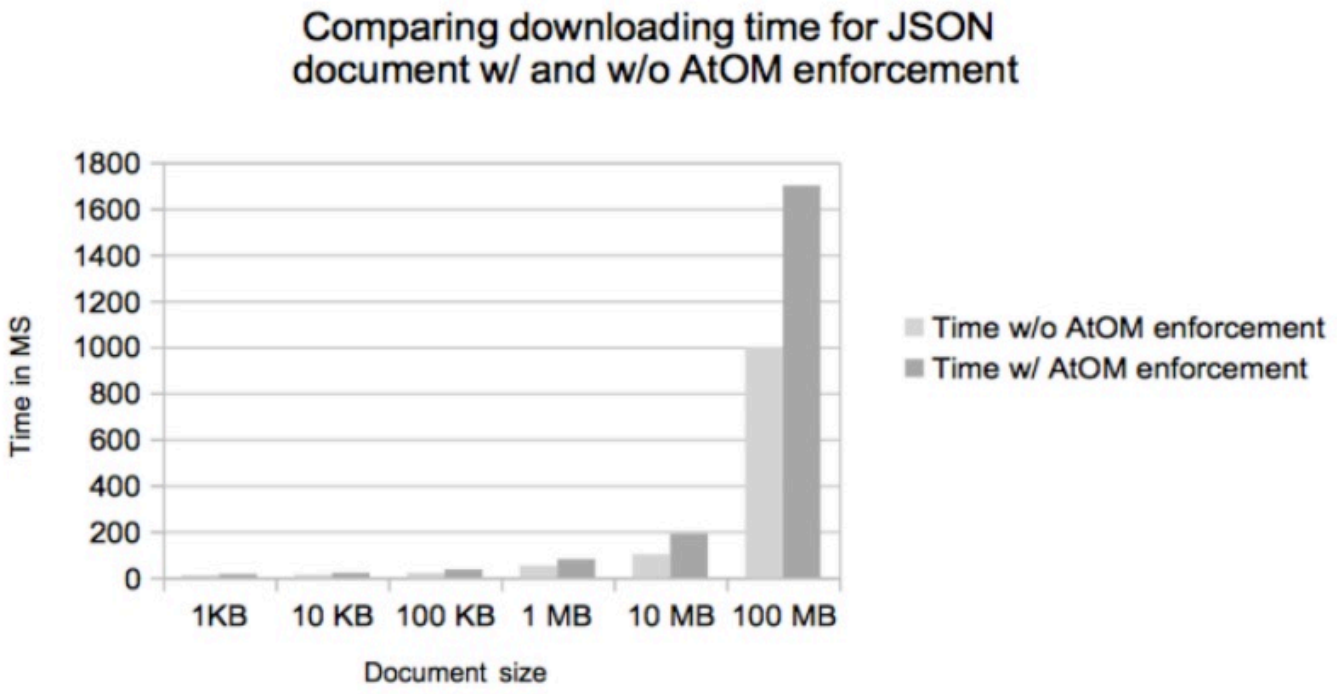


Fig 11: Performance evaluation

I·C·S
The Institute for Cyber Security

UTSA