Information Flow Control in Cloud Computing

Ruoyu Wu, Gail-Joon Ahn, Hongxin Hu
Arizona State University
Mukesh Singhal
University of Kentucky
Outline

- **Introduction and Motivation**
  - What is Cloud Computing
  - Security Challenges in Cloud Computing

- **Our Proposed Approach**
  - Challenges in Applying Chinese Wall Security Policy (CWSP) to Cloud Computing
  - Chinese Wall in Clouds
    - Security Model
    - Security Policy Specification

- **System Design**

- **Implementation and Evaluation**

- **Conclusion**

- **Future Work**
What is a Cloud?
What is a Cloud - Cont’d

- Most popular cloud service styles
  - Infrastructure as a Service
    - Access to a collections of virtualized computer hardware resources, including machines, network, and storage.
  - Platform as a Service
    - Access to a programming or runtime environment.
  - Software as a Service
    - Access to collections of software application programs.

- Why cloud computing
  - Cost effective
  - Scalability
Security Challenges in Cloud Computing

- Authentication and identity management
- Policy Management
- Trust Management
- Access Control
  - Information Flow Problem in Clouds
Chinese Wall Security Policy

- **Purpose**
  - Makes use of subjects and objects to prevent information flows which cause conflict-of-interests.

- **Composition of Objects**

- **Simple Security Rules** [brewer’1989]
  - Access (read action) is granted to subject if the requested object:
    - is in the same company dataset as an object already accessed by that subject
    - or belongs to an entirely different conflict of interest class
Challenges in Applying CWSP to Cloud Computing

- Challenge 1: Choosing Appropriate Service Layer
  - IaaS

- Challenge 2: Definitions for Policy Components
  - Subject, Object, Access Operation


- Challenge 4: Efficient System Performance
  - Conduct system evaluation to demonstrate the overheads brought by our approach are reasonable.
Our Proposed Approach

- **Chinese Wall Security Model in Clouds**
  
  Elements in Original Chinese Wall Security Policy  
  Elements in Chinese Wall Security Model in Clouds
  
  Subject  
  Action  
  Object  

  Cloud User  
  Access Data or Services Hosted in Cloud Instances  
  Cloud Instance
Chinese Wall Security Model in Clouds - Cont’d

- **Cloud Instance**
  - A cloud instance is a virtual machine running on the cloud infrastructure. It stores customers' data and hosts various kinds of cloud services. Let \( I \) denote the set of cloud instances, \( I = \{i_1, ..., i_n\} \).

- **Security Group**
  - A security group is a named domain containing several cloud instances. Let \( G \) denote the set of security groups, \( G = \{g_1, ..., g_n\} \), where \( g_i \in I \).

- **Conflict-of-Interest (COI) Class**
  - A COI class contains several security groups that have CoI issues between each security group. Let \( C \) denote the set of COI classes, \( C = \{c_1, ..., c_n\} \), where \( c_i \in G \).

- **Object**
  - An object of the Chinese Wall security policy in the IaaS cloud computing environment is a cloud instance. Let \( O \) denote the set of objects, \( O = \{o_1, ..., o_n\} \) and an object \( o_i \in I \).
Chinese Wall Security Model in Clouds - Cont’d

– The Composition of Objects in Clouds

- Conflict of Interest Class
  - Bank COI Class
  - Airlines Company COI Class
  - Sanitized COI Class

- Security Group
  - BoA Group
  - Chase Group
  - HSBC Group
  - UA Group
  - Delta Group
  - Sanitized Group

- Individual Objects (Virtual Machine)
  - VM 1
  - VM 2
  - VM 3
  - VM 4

- Object Property 1): Any two objects which belong to the same security group belong to the same conflict of interest class.
- Object Property 2): Any two objects which belong to different conflict of interest classes belong to different security groups.
Chinese Wall Security Model in Clouds - Cont’d

- **Subjects**
  - A subject of the Chinese Wall security policy in the cloud computing environment is a user who accesses to the data or services hosted in the cloud instance. Let S denote the set of subjects, $S = \{s_1, ... s_n\}$.

- **Access Operations**
  - An access operation includes accessing data or services hosted in the cloud instance by a subject. Let
    - $ACC \subseteq S \times O$ be a many-to-many subject-to-object access relation. A subject-to-object access relation can be represented by $(s_i, o_j) \in ACC$, where $s_i \in S$ and $o_j \in O$, which means the subject $s_i$ has accessed the object $o_j$.
    - $ACC \to \text{Boolean}$ be a function that maps a subject-to-object access relation to a Boolean value, where
      - $Access((s_i, o_j)) = \text{true}$ if $(s_i, o_j) \in ACC$,
      - $Access((s_i, o_j)) = \text{false}$ if $(s_i, o_j) \notin ACC$. 
Chinese Wall Security Policy Specification

- **Policy Specification**
  - Let \( OA \) is a function mapping each subject to a set of objects, \( OA(s_i) = \{ o_j \mid o_j \in O \text{ and } Access(s_i, o_j) = \text{true} \} \) and \( O_s \) is a set of all sanitized objects. Then a subject \( s_i \in S \) can access an object \( o_j \in O \) if and only if any of the following requirements holds:
    - There is an object \( o_j' \in O \) such that \( Access(s_i, o_j') = \text{true} \) and \( SG(o_j) = SG(o_j') \);
    - For any object \( o_j' \in OA(s_i) \), \( COI(o_j) \neq COI(o_j') \);
    - \( o_j \in O_s \).
  where, initially \( OA(s_i) = \emptyset \), and the initial access request is assumed to be granted.
System Design

- System Architecture
System Design - Cont’d

- System Architecture
  - System Management Layer
    - Registration module
    - Authentication module
    - Image management module
    - Instance management
    - Security group management module
    - COI class management
  - Cloud Fabric Layer, built based Eucalyptus open-source software
    - Cloud Controller
    - Cluster Controller
    - Node Controller
  - Infrastructure Layer
Implementation

- System Workflow
Implementation - Cont’d

- Update COI Classes and Monitor Cloud Instances
Implementation - Cont’d

- **A Scenario**

  Step 1. Administrator sets up cloud environment

  Step 2. Alice can access any instance when first time login

  Step 3. Alice downloads a SSH key associated with instance i-4510678C in BoA group

  Step 4. After Alice accesses the instance in BoA group, instances which cause COI issues are disabled for access
Evaluation

- Analyzing the overheads brought by our approach with the three measurement criteria
  - Authorization Time
  
  ![Graph showing the relationship between the number of security groups and average authorization time](image)

  - Memory Utilization and CPU Utilization

<table>
<thead>
<tr>
<th></th>
<th>With Cloud Management Modules</th>
<th>Without Cloud Management Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Memory Utilization</td>
<td>413MB</td>
<td>378MB</td>
</tr>
<tr>
<td>(megabytes)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average CPU Utilization</td>
<td>14.8%</td>
<td>13.5%</td>
</tr>
<tr>
<td>(percentage)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Related Work

- **Securing outsourcing data and computations**
  - Encrypt the information and use hash values and digital signatures to guarantee information integrity [Miller’2002]
  - Propose SiRiUS which is layered over existing file systems providing end-to-end security [Goh’2003]
  - Enforce access control on published XML documents [Miklau’2003]
  - Exploit and combine techniques of KP-ABE, proxy re-encryption (PRE), and lazy re-encryption (LRE) to delegate most of the computation tasks to untrusted cloud service providers [Yu’2010]
  - Trusted cloud computing platform (TCCP) [Santos’2009]
  - Predicate the placements of VMs in the Amazon cloud and discussed potential side-channels and their implications [Ristenpart’2009]

- **Adopting Chinese wall security policy to distributed environment**
  - Propose the scalable enforcement of a Chinese Wall policy under the inherently decentralized Law-Governed Interaction mechanism [Minsky’2004]
  - Propose a Chinese Wall security policy for the decentralized workflow environment [Atluri’2001]
  - propose a Chinese Wall Process Confinement offering application-level distributed coalitions with a mandatory access control mechanism [Katsuno’2007]
Conclusion

- We first identified the information flow problem which could raise conflict-of-interest issues in cloud computing environments.
- We articulated challenges in specifying and enforcing information control policies in cloud computing.
- To address the identified problem and challenges, we proposed an approach to enforce the Chinese Wall security policy at the IaaS layer of a cloud.
- We implemented a prototype system based on Eucalyptus open-source software to prove the feasibility of our approach while measuring the performance of our prototype.
Future Work

- We would improve our approach to support more fine-grained control with generic policy management modules.
- A practical delegation mechanism is another essential component for cloud computing.
Questions

The work of Ruoyu Wu, Gail-J. Ahn and Hongxin Hu was partially supported by the grants from National Science Foundation (NSF-IIS-0900970 and NSF-CNS-0831360) and Department of Energy (DE-SC0004308 and DE-FG0203ER25565).