Comparative Analysis of Access Control Models

Usvir Kaur¹, Dheerendra Singh²
1Assistant Professor, Dept. of Computer Science & Engineering,
Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab India
2Professor, Dept. of Computer Science & Engineering
Shaheed Udham Singh College of Engineering and Technology, Tangori, Mohali, Punjab, India.

Abstract: - Cloud computing is becoming most promising paradigm in information technology industry. Due to dynamic relationship between users and resources, service providers and users. Security has became one of the main hurdle in the growth of cloud computing. Access Control model can achieve security by controlling access to resources by users. Different access control models have different methods to achieve security. In this paper comparative analysis of different access control models are done.

Keywords: Access control model, security, trust.

I. Introduction

Introduction: cloud computing is an evolving paradigm for security and delivery services to the users. According to NIST definition, “cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management.” Access control basically termed as policy or procedure which allows or delivers or restricts to a system [1]. Security is one of main hurdle or challenge in adoption of cloud computing. Access control models helps us to resolve these issues. It checks unauthorized access to a system. Different access control models such as mandatory access control model, discretionary access control model and role based access control(RBAC) are known as identity based access control models.[1] In these access models users are known as subjects and resources are objects identified by unique names. Characteristics of information security such as integrity, availability and confidentiality are associated with access control. These access control models provide controlled access to users and resources therefore achieve security. However, access control is more than just controlling users (subjects) can access which is computing and network resources. It also provides additional facilitates such as access control manages users files and other resources. From the access control perspective cloud computing should provide Control access to the service features of the cloud based on the specified policies and the level of service purchased by the customer. (ii) Control access to a consumer’s data from other consumers in multi-tenant environments. (iii) Control access to both regular user functions and privileged administrative functions. (iv) Maintain accurate access control policy and up to date user profile information.[6] Main hurdle in cloud computing access control diverse set of users with different sets of security requirements such as dynamic performance and mobility features, authentication, scalability, trust, heterogeneity, quality of service, interoperability, flexibility, virtualization and sharing of physical resources. In this paper comparative analysis of various access control models are done.

II. Literature Review

In Cloud Computing paradigms, there is necessity to define methods with the help of which clients can discover, request and use resources .Zhou[2] propose a new RBE SCHEME which helps in achieving efficient user revocation. After that cloud storage architecture based on RBAC is presented which allows an organization to store data securely on a public cloud while maintaining sensitive information on private cloud. Authors propose a practical access a policy based on role in a flexible manner and provides secure data storage. This system has several characteristics such as cipher text and decryption key. Vidyalakshmi(2013)[3] proposed a model trust based access control model for mobile devices such as smartphones. Trust is calculated based on direct interaction between host and client peer. In absence of direct interaction trust is calculated using recommendations ever assigning weights to categories and context. This is manageable, flexible and effective way of access control for large number of files.
Vidyalakshmi[4] et. al proposed access control model by exploiting it with KP-ABE and lazy encryption and proxy encryption. This model helps us to achieve fine-graininess, data confidentiality, scalability, user secret key accountability, user access privilege. Younis et. al[5] proposed a access control model based on requirements of cloud computing such as mobility features, dynamic performance, scalability, interoperability, flexibility, virtualization .It facilitates role and task principles to make assigning privileges dynamic and easy. Their proposed it utilizes temporal and delegation constraints Users are assigned to security domains which relate to roles and actual jobs.

Security classifications are done according to users and roles. RB-RBAC [6] model was proposed by khatani to dynamically assign users to roles based on finite set of rules. The proposed model will be beneficial in dynamically assignment of roles. Capability based delegation model in RBAC [7] model was proposed for flexible and dynamic resource management in environment. Authors proposed an access control model CRBAC integrating capability based access control into RBAC96 model. Due to flexibility of capability based access control model supported both delegation of roles and permission in capability.

III. Comparison of access control models

Following table describe different access control model their techniques, advantages and their limitations

<table>
<thead>
<tr>
<th>Name of model</th>
<th>Description</th>
<th>Advantages</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification based access control</td>
<td>These were based on user’s identity. This is referred as identification based access control model.</td>
<td>Easy to implement. Simplify</td>
<td>• It weakens on large number of users.</td>
</tr>
<tr>
<td>Role based access control model</td>
<td>In this client access to system resources is determined on the basis of job role provided to the user. Role is determined on basis on permissions or functionalities for job.</td>
<td>• More powerful than IBAC • Flexible enough to be managed at a access level that to organize in policy and structure.</td>
<td>• Difficult to assign permissions • Became problematic across extended administrative domains.</td>
</tr>
<tr>
<td>Attribute Based Access control Model</td>
<td>Access is granted on attributes such as date of birth, national security number. Etc</td>
<td>• Subject does not have to be known in advance to the system.</td>
<td>• Difficult to make an agreement on set of attributes.</td>
</tr>
<tr>
<td>Trust Based Access Control Model[2]</td>
<td>P2P access control model for smart based trust. Trust component is based on direct interaction of host with client peer. In absence of direct interaction trust is calculated using recommendations weights assigned to categories and contexts.</td>
<td>• Manageable • Flexible • Effective way of access control of large number of files.</td>
<td>Complex calculations are to be done using weights.</td>
</tr>
<tr>
<td>Secure, Scalable Fine grained</td>
<td>Three advanced cryptographic techniques</td>
<td>• Scalability</td>
<td>• Heavy computation</td>
</tr>
<tr>
<td>Access Control Model</td>
<td>Description</td>
<td>Pros</td>
<td>Cons</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| such as KP-ABE, lazy encryption, are combined with access control model. | - Fine grainness  
- Data confidentiality  
- User Access  
- Secret key accountability | Overhead  
- Cumbersome Online Burden towards data owner | |
| Mandatory Access Control Model       | Central authority is in command of giving access decisions to a subject(users) that requests access to objects(resources) or information in objects | - Security levels are assigned for each information  
- Secure access | - Not guarantee complete secrecy of information  
- Expensive to difficult to deploy  
- Does not support separation of duties  
- Dynamic activation of rights is not supported  
- Does not support time and location constraints |
| Discretionary Access Control Model   | Grants the owner of objects ability to restrict access to their objects.     | - Easy to deploy | - Less Secure  
- No Mechanism to facilitate the management of improper rights  
- Does not have ability to control information  
- Trojan horses can inherit access permissions. |
| Task Role based Access Control Model | It assigns permissions to tasks instead of roles. In this model are assigned roles whenever assigned tasks that have | Easy to deploy  
Manageable  
Flexible. | - Do not differentiate between sensitive or insensitive information.  
- Does not support delegation principle  
- Does not support active responsibilities staff as it does not support tasks from roles. |
| Policy based Access Control Model    | Subjects needs authentication itself that provides its attributes.          | Easy to implement. | - Difficult to reach an agreement what kind of attributes should be used.  
- How many attributes should be used. |
<table>
<thead>
<tr>
<th>Rule Based –Role Based Access Control model</th>
<th>Dynamically assign users to roles based on finite set of rules.</th>
<th>● Automatic assignment managing users to roles rather than manually</th>
<th>Difficult to reach an agreement about different kind of roles should be used.</th>
</tr>
</thead>
</table>
| Quantified Risk Adaptive Access Control (QRAAC) | risk = V*P,  
- V is the information value that reflects the sensitivity level of the resource,  
- P is the probability of unauthorized disclosure, which reflects the trustworthiness of the user. | ● The security policy in this model is dynamic; it is changed according to a variety of risk levels  
- stated on the security policy. | ● difficult to be deployed in cloud  
- computing.  
- number of systems to be merged to compute risk levels.  
- It needs expertise that can deal with the model.  
- Security policies and environmental conditions need to be standardized. |

V. Conclusion
According to above analysis, it is found that different access control models have different technique to implement security. Traditional access control models such as discretionary, mandatory use central authority to manage access. While others some access control models also use different encryption techniques such as lazy encryption, KP-ABE etc. to provide security. Thus, after doing review of different access control methods it is seen that access control model must support dynamic performance and mobility features, authentication, scalability, heterogeneity, interoperability, computation complexity, response time, interoperability, virtualization and sharing of physical resources, delegation of capabilities, policy management.

References