International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Activity Based Access Control Model for Cloud Computing

Salil Ajgaonkar[†*], Harish Indalkar[†] and Jaya Jeswani[†]

[†]Information Technology Department, Xavier Institute of Engineering, Mahim (W), Mumbai, India

Accepted 10 March 2015, Available online 15 March 2015, **Vol.5, No.2 (April 2015)**

Abstract

Cloud computing is a new generation technology that provides a number of services with great efficiency and performance by removing any forms of restrictions imposed by the limitations of user's hardware and software. However such an advanced technology comes with a risk of having loop holes in its sophisticated design that makes the system vulnerable to attacks and failure in its purpose of design. Thus security forms one of the important aspects in cloud computing. One of the most fundamental requirements in cloud computing is access control which has the paramount responsibility of providing smooth and easy access to authorized users as well as, at the same time, preventing access to any unauthorized users. Not only users but the system is also prone to insider attacks by those who are familiar with the architecture of the system. Traditional models like Mandatory access model (MAC) and Discretionary access model (DAC) may prove suitable for applications run on computer hardware but not for cloud computing applications. This paper presents a detailed analysis for access control in cloud computing, points out certain requirements not met by conventional access control model and a possible solution to these drawbacks.

Keywords: *Cloud computing, Security, Access Control, Roles, Task, Insider Attacks, Encryption, Cryptography*

1. Introduction

In recent years Cloud Computing has become a core example of new age technology in the field of Information technology industry and Computer Sciences. Cloud computing provides good performance, efficiency and low cost in providing on-line services in the domains of Platform as a service (PaaS), Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Storage as a Service.

However in spite of all these benefits, being a relatively new technology, cloud computing faces a number of milestones in its development and practical application. Data accessibility, data security and cyber-attacks are the most common forms of such milestones. Such threats are best prevented at the very start rather than coming up with remedies to prevent theft after the attackers have breached the security and have gained access.

The Activity based access control model is a type of access control model that provides the user access to data depending on the information of the organization he works for his designation and the activity he is currently performing. This model not only provides a strict security policy to prevent un-authorized access to data but also provides a concise view and access to the data and files that are relevant to the activity the user is currently performing.

This idea, however, is only limited to prevent un-authorized access externally. The system is still under threat from an insider attack, someone who manages the cloud system itself and hence is not bound by the general access control policies. The insider may leak confidential data to an outsider to gain monetary benefits. This can be prevented by encrypting the data that is being stored on the cloud. This encryption is brought about by using RC4 symmetric key algorithm which is the most simple and efficient encryption algorithm. There is also the chance of an attacker getting his hands on the key while it is being transmitted from server to client this is prevented by using RSA encryption algorithm on the key being sent.

2. Related work

A number of models were previously proposed to control user access. Each satisfied some of the requirements of present access control in cloud computing, but these models also brought in some of their own drawbacks and features that were not suitable to the comprehensive list of users of cloud applications. We feel these models are not suitable for cloud applications as they pose certain drawbacks on certain issues. Also these models may protect from unauthorized user access but do not provide any satisfactory solution to insider attacks.

2.1 Previously proposed models

2.1.1 Mandatory Access Control Model

In this model access to data is controlled by using the sensitivity of data as the prime criteria to decide who

[*]Corresponding author: **Salil Ajgaonkar**

can access it. A Central Authority assigns the data a security level based on its sensitivity and importance. It also assigns a security clearance level to users. Only those users can have access to the data who have security clearance level greater than the security level of the data.

Disadvantages: It does not guarantee complete secrecy of data. The central authority is vulnerable to attack since it is the one that assigns the security levels. Also this model is difficult and expensive to implement and does not support separation of duties.

2.1.2 Discretionary Access Control Model

The security of data in this model is dependent on the owner of the data. The owner decides who can access data based on certain attributes he has in common with other users.

Disadvantages: This model does not provide high level of security. The model does not provide any solution to risk awareness and management of improper rights. This model is also prone to Trojan horse attacks and is not scalable enough to implement in a cloud computing.

2.1.3 Attribute Based Access Control Model

In this model access to data is decided on the attribute values of the user. The attributes of the user can be anything from the user's work like location, designation, employee ID, etc. the attributes may or may not depend on each other. Each attribute is considered as an individual discrete value. The values of these attributes are compared to those set of values defined by the model to decide whether to grant or deny access to data.

Disadvantages: This model is difficult to implement as proposing a suitable security policy for a large variety of users is difficult. So far this model has not been implemented in well-known applications.

2.1.4 Role Based Access Control Model

In this model access to data is granted based on the user's job. His designation in the company or organization determines his security clearance. However a user can play multiple roles in his organization. For example the user can be the head of management as well as a professor in an organization such as a school. This model has its own drawbacks.

Disadvantages: There may be a case where a user with multiple roles uses one of his roles that grant him more rights than it is required for him to access the data. This leads to a violation of security policy. This model also does not support active responsibilities of the staff as it does not separate tasks form roles.

2.1.5 Risk based Access Control Model

This model is usually used in big corporations. This model uses different kinds of risk levels to determine its access criteria. The risk levels are decided on certain environmental conditions. This model has a dynamic security policy that changes with the change in risk levels.

Disadvantages: This model is very difficult to implement as the logic to determine the risk levels and the security policy based on it requires a lot of analysis and planning. It also requires specially trained administrators to manage the complex model. Standardization of security policies and environmental conditions is important while making access decisions.

2.2 Security

Concerns with security in cloud computing is a very controversial issue that may be preventing its full scale adoption in present organizations. There lies an air of in-security among users in giving the responsibility of protecting their vital data to external managements.

The most common security concern in cloud computing are traditional security, data availability and third party data control.

2.2.1 Traditional Security

Traditional security concerns involve network intrusion attacks. Such attacks have become a possible threat as data is transferred through a network to the cloud application. The Cloud provider also has the responsibility to secure and protect the network used as the communication medium between the user and cloud application. Basic validation, verification and authentication do not prevent these attacks. Also investigation of illegal activities and crimes related to cloud computing becomes very difficult as the data is accessed by a large number of users spread across a wide geographic region with different national rules and regulations in cyber–crime investigations.

2.2.2 Availability

This concern centers on the all-time availability of critical applications and data in cloud. The user or organization is completely dependent on the cloud for its daily activities. Unavailability of services even for a few minutes may lead to severe damages to business. Such real-life incidents of cloud outage include Gmail's one-day outage (October 2008), Amazon S3 seven hour downtime (20 July 2008). Cloud service providers may assure that they are providing all-time availability and security but in reality they are more vulnerable as a single point of attack.

2.2.3 Third Party Data Control

The legal implications of providing data security by a third party service provider are sophisticated and complex considering the wide geographical reach of cloud computing which transcends national or even continental boundaries. There is also the lack of transparency and free communication when a third party is being involved. Cloud service providers may hype that the cloud is implementation independent but in reality regulatory compliance requires transparency into cloud. It also proves difficult in auditing a cloud since there is always a lack of control

3. Proposed System

The proposed model facilitates the principles used in role and task based models which were proposed in previous work. In this model stated as "The Activity Based Model". Users are granted access to the data depending on the activity they wish to perform. Thus, every user will be located in a security domain depending on what activity or task they are doing and will only be given access to only that data that is needed for that activity to be completed. The task that he is performing will be dependent on the role that he plays in his organization and his designated post. Every task will have certain security clearance that will grant the user access to the relevant files. A security tag engine will also be implemented which is responsible for assigning a security tag to all the data that is being stored in the cloud. Any attempts to access the data has to ensure that the user designation i.e. the role of the user and the task he is performing are genuinely related to the data to be accessed. In this model we are using security tags to compare the relation of the data to the user activity and the user information i.e. his roles and the tasks he can perform in those roles as the criteria to access the data needed for his work. The Security tag will consist of a user role, tasks, permissions, unique number and a security level.

Tasks	Permissions	Unique Number	Security Level

Fig.1 Security Tag

3.1 Access Components

This model has the following components that play a part in its functioning:

Users (U) – It is set of users.
Roles (R) – It is a set of roles that a user can act.
Tasks (T) – It is a set of task that a user performs as his work.
Permissions (P) – Read/Write/Delete.
Data (D) – It is the set of data to be accessed.
Session (S) - It is a set of session
User Assignment (UA) – It is the set of various roles a specific user can perform.
Role Assignment (RA) – It is the set of tasks that a user in a specific role can perform.
Security Clearance (SC) – It is the attribute that defines the importance of the user in handling sensitive data.
Security Level (SL) – It is the attribute that restricts access to data based on its sensitivity.

Every user u in the model can have any number of specific roles {r1,r2,r3,r4,r5…} he can perform. Based on these roles, every specific role rn can perform any number of specific tasks {t1,t2,t3,t4,t5….}

The Security level of the data will depend on the owner of the file who specifies its sensitivity. For a user to have access to such a sensitive data he should have the value of his SC greater than the SL of the data

The SC of the user is dependent on the designation of the user in his organization i.e. his role.

Based on the role that he is performing and the value of his SC, the model will provide the user access to only that data that he requires to accomplish his job.

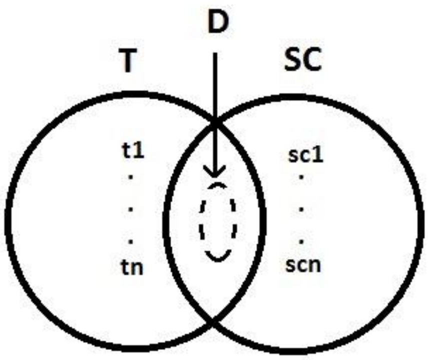

Fig 2: Data Access and User Relationship

Most of the relations in this model are many-to-many i.e. many users can have many roles; similarly many roles can perform many tasks. However only user-to-session relation is an exception which is one-to-one i.e. a user can have only one session of access at a time

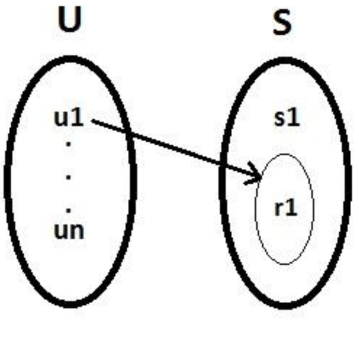

Fig 3: Assignment of only one Session for every user

3.2 Cryptography Components

The best way to protect user data from an insider attack is to encrypt it using an encryption algorithm. Currently the most secure encryption algorithm that can be used is RC4 symmetric key encryption algorithm. Encryption and Decryption is usually carried out by a third person party which is only responsible for the generation and management of keys. The third person party in no way comes directly in contact with the data. The key thus generated is then transferred to the client side from the server side. This transmission is vulnerable to a middleman attack. An intruder can get his hands on the symmetric key that is being transmitted. Using this key he can decrypt the data and get full access to the data. Thus to protect the key during transmission, it needs to be encrypted using RSA Key Encryption algorithm.

3.2.1 RC4 Symmetric Key Encryption Algorithm

The RC4 algorithm is very easy and simple to use. The RC4 algorithm is remarkably simple as it uses a look-up table containing 256 byte value permutations. Every time a byte value key stream is generated the look-up table is shuffled in such a way that the table still contains 256 permutations but in different order.

3.2.1.1 Initialization of the Permutations table

RC4 is entirely byte based. The first phase of this algorithm is to initialize the permutations table i.e. the look-up table using the key K which can be of any length from 0-256 bytes. The look-up table is defined as V. The length of the key is defined as L. The pseudo-code for initialization is defined as T. the pseudo code is only used to initialize the permutations table. These initial operations can be summarized as follows:

```
/* Initialization */
for i = 0 to 255 do
    V[i] = i;
    T[i] = K [i mod L];
next i

/* Initial Permutation of V */
j = 0;
for i = 0 to 255
    j = (j + V[i] + T[i]) mod 256;
    Swap (V[i], V[j]);
next i
i = j = 0
```

3.2.1.2 Byte Stream Generation

Once the permutations table has been initialized the key stream byte can be generated. The key stream byte k is simply XORed with the plain text to encrypt the data or XORed with the cipher text for decrypting. The algorithm for stream generation is as follows:

```
/* Stream Generation */
i, j = 0;
while (true)
i = (i + 1) mod 256;
j = (j + V[i]) mod 256;
Swap (V[i], V[j]);
t = (V[i] + V[j]) mod 256;
k = V[t];
```

3.2.2 RSA Encryption Algorithm

It involves three steps: Generation of the key, Encryption and Decryption.

The reason why RSA is so secure is that it uses factorization of large numbers as its base idea. The keys for the RSA algorithm are generated the following way:

Choose two distinct prime numbers p and q.

For security purposes, the integers, p and q should be chosen in such a way that they are two large prime numbers and should be of similar bit-length.

Compute $N = pq$.

Choose E, the encryption exponent, relatively prime to $(p-1)(q-1)$

The decryption exponent D is the multiplicative inverse of E modulus $(p-1)(q-1)$.

Thus we have $ED= 1 \bmod (p-1)(q-1)$

N is used as the modulus for both the public and private keys. Its length is the key length and is expressed in bits. In RSA encryption and decryption are carried out using modular exponentiation. Let P be the plain text and C be the Cipher text.

To encrypt the data we use;
$C = P^E \bmod N$
Where E is the encryption exponent

Similarly to decrypt we use;
$P = C^D \bmod N$

This decryption works, as proved by Euler's Theorem that

If x is relatively prime to n then $x^{\Phi(n)} =1 \bmod n$
$ED = 1 \bmod (p-1)(q-1)$
$\Phi(N) = (p-1)(q-1)$

These two factors together give us
$ED-1 = k\Phi(N)$
Where k is some integer

Therefore $C^D = M^{ED} = M^{(ED-1)+1} =M\bullet M^{(ED-1)} =M\bullet M^{k\Phi(N)} =M\bullet 1^k = M \bmod N$

The public key consists of the modulus N and the public (or encryption) exponent E. The private key consists of the modulus N and the private (or decryption) exponent D, which must be kept secret. p, q and $\Phi(N)$ must also be kept secret because they can be used to calculate D.

Table 1 Activity Based Access control model compared against conventional access control models

Criteria	MAC	DAC	ABAC	RBAC	Risk-BAC	Activity- BAC
Least Privilege principle	No	No	Yes	Yes	Yes	Yes
Separation of duties	No	No	Yes	Yes	N/A	Yes
Flexibility of Configuration	No	No	No	Yes	No	Yes
Dealing with heterogeneous users	No	No	No	No	Yes	Yes
Scalability	No	No	N/A	Yes	N/A	Yes

Table 2 Speed Comparison of stream ciphers using Pentium 2

Cipher	Key-length	Speed
DES	56	9
3DES	128	3
RC2	Variable	0.9
RC4	Variable	45

4. Present Investigation

When we initially took up the idea on proposing an access control model for cloud computing, we came across a number of different access control models that were previously proposed. It did not seem like the best choice to create a new access control model from the start. Many access models had their own advantages in certain areas while lacking in a few. Hence we decided to make a model based on the positive attributes of these previously proposed models. By implementing the positive attributes of these models we aimed at creating a secure model in all general areas of cloud computing. We used the Role Based Access Model as our general base of study as it is the most currently successful model in implementation used by various enterprises and organizations.

The proposed model provides the necessary access to the data based on what the user needs. It supports Least Privilege Principal i.e. it provides limited access to the user, just enough for him to complete his work and at the same time considers the sensitivity of the data. This solves the problem faced by traditional RBAC model. This concept also prevents any damages caused by Trojan Horse attacks since only a limited data is exposed to the current user. Also unlike ABAC model, this model is suitable to cater a wide variety of users in an organization based on their role and task attribute. The comparative study of the Activity based access Control model with other models is given in Table 1.

A number of papers have been published analyzing various methods of attacks against RC4 Encryption e.g. (Kumar et al, 1997), (Mister, .S et al, 1998), (Mantin I. et al, 2001). None of these attacks are practical against RC4 if the key length of RC4 is as long as 128 bits. The authors also pointed out that the WEP protocol, that provides confidentiality on wireless LAN networks, is vulnerable to some attack approach. However in this case it is not the fault of RC4 encryption but the way in which the key was generated. This problem does not occur in other implementations of RC4. Thus RC4 was the optimum choice in selecting an encryption algorithm that protected the user data from insider attacks. A comparative study conducted by William Stalling in his paper “RC4 encryption Algorithm” 2005 () states the following advantages of RC4 over other encryption algorithms as given in Table 2.

Conclusions

Thus from this analysis we come to the conclusion that cloud, unlike, other applications, has certain special security concerns, right from getting access to data to its encryption. Though a lot of focus has been given to data encryption and protection from hacks, the area of access granting has often been left out of consideration. Granting access is also a vital part of security if not the most important. It is better to prevent someone from accessing the data from the very start rather than not letting him read it after he gets his hands on it.

A number of access control methods have been developed for a variety of applications, but none of them fully satisfy the huge security demands of cloud based applications. Due to the networking oriented structure and a wide number of users using the same facility it becomes necessary to implement a complex yet easy to use access technique.

This proposed model is suitable for all cloud applications. It provides the necessary security and protection that is needed to prevent any un-authorized user from getting access to vital and sensitive data and at the same time protecting the data from the cloud service provider himself.

Future Scope

Once implementation of the proposed model is complete there is still room for further improvement. The model requires storage of user information and information about the files to be stored. This leads to the additional creation of databases and the responsibility of handling and maintaining them. The model can be made more efficient if an alternative method of storing user and data information is found making it independent of managing large databases for large users.

The proposed model is more suited for an intra-organization cloud application instead of a worldwide user application since organizational data is needed while developing the roles to be considered while accessing the model. The model will benefit greatly if a more generalized role-task format is used which is common to all organizations throughout the globe.

The model can also become more effective if delegation capabilities are added to it.

References

Younis A.Younis, Kashif Kifayat, Madjid Merabti, *An access Control model for Cloud Computing*, School of Computing and Mathematical Sciences, Liverpool John Moores University, Liverpool L3 3AF, UK

Mohamed Nabeel, Elisa Bertino Fellow, *Privacy Preserving Delegated Access Control in Public Clouds*, IEEE

Sushmita Ruj, Milos Stojmenovic, Amiya Nayak, *Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds*, IEEE

Zahid Pervaiz, Walid G. Aref, *Accuracy-Constrained Privacy-Preserving Access Control Mechanism for Relational Data*, IEEE

Xin Dong, Jiadi Yu, Yuan Luo, Yingying Chen, Guangtao Xue, Minglu Li, *Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing*, Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai,

Ramgovind S, Eloff MM, Smith E (2010), *The Management of Security in Cloud Computing*, Page(s): 1 – 7

Simarjeet Kaur (2012) *Cryptography and encryption in Cloud Computing*

Salim Khamadja, Kamel Adi, Luigi Logrippo, *Designing Flexible access control models for the cloud*

Kumar, I (1997), Cryptology. Laguna Hills, CA: Aegean Park Press,.

Mantin, I., Shamir, A (2001), *A Practical Attack on Broadcast RC4*. Proceedings, Fast Software Encryption.

Mister, S., and Tavares, S. (1998), *Cryptanalysis of RC4-Like Ciphers*, Proceedings, Workshop in Selected Areas of Cryptography, SAC' 98.