A Survey on Enhancing Cloud Security through Access Control Models and Technologies

P.Chinnasamy
Department of Computer Science and Engineering, Kalasalingam University, KrishnanKoil, India
chinnasamyponnusamy@gmail.com

P.Deepalakshmi
Department of Computer Science and Engineering, Kalasalingam University, KrishnanKoil, India
deepa.kumar@klu.ac.in

***Abstract*— Among the up-and-coming technologies, cloud computing provides an elastic, self-service computing infrastructure for a wide range of applications. It's all about transforming resources from the single desktop computer/personal laptop/data centers to web. The user's data can be placed, within the cloud storage and it can be accessed by the clients whenever they like and from anywhere they need. Here so many security problems can be raised. Managing and controlling identities and access control for a data with an authoritative or unauthorized way is still a greatest challenges in cloud security. In a cloud environment, the data proprietor and cloud service provider have ability to monitor the data access activities in order to prevent from unauthorized access. In this article, we give attention to a variety of access control techniques, their performance, properties and implementation for cloud environments.**

Keywords- access control, cloud computing, cloud security, XACML, SAML

I. INTRODUCTION

Cloud computing is a new technology for gaining computing solutions and services. In a cloud, the resources, like storage, platforms and software, are dynamically accessed in the course of (public) networks. Cloud is a most modern technology used by both organizations and individuals. Both industry and government have invested lot of money with huge attention. Users can store their data within the cloud and there is lot of personal information and sensitive data are stored on their personal computer and now this information is moved to the cloud. While moving this type of sensitive data, all organizations need to check cloud trust and manage control over the data [1]. Among the cloud security issues, controlling and managing access for data is one of the key challenging task.

A. Architecture of Cloud Computing

Cloud computing is web based control, whereby shared resources , application, and information are provided in order to computers and other devices (such as smart phones) on demand over the web.

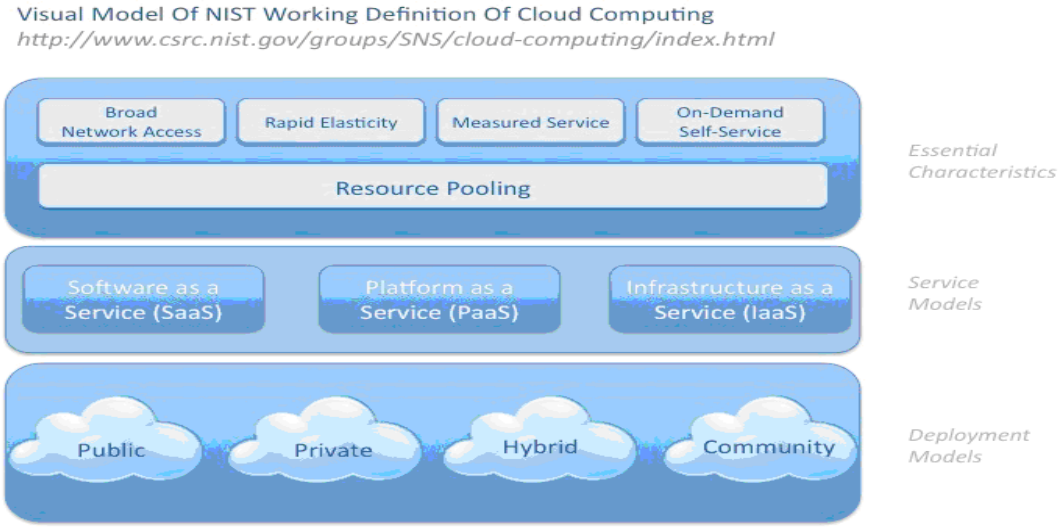

Fig.1.1 Architecture of Cloud Computing

B. Service Models

1) Software-as-a-Service (SaaS)

Here an application is organized as a service to the user/customer [1], [2] who accesses it over the web/internet. When the software is organized off-site, the user doesn't need to retain or support this.

2) Platform-as-a-Service (PaaS)

This supplies all the properties to make applications and expert services available in the internet, without any need model download and install software [1], [2].

3) Hardware-as-a-Service (HaaS/IaaS)

Hardware as a service can be another form of service available in cloud computing, which simply offers computer hardware so that organizations will be able to place anything they want to onto it [1], [2].

C. Deployment Models

1) Public Cloud

The public cloud is sold towards the public. In this, all the information are managed by third party. They charge the amount according to resources utilization [1], [2].

2) Private Cloud

A private cloud is enterprise owned or leased. [1], [2] Each of the resources are managed simply by enterprise itself.

3) Community Cloud

It has shared infrastructure with regard to specific community.

4) Hybrid Cloud

It is a composition of one or even more clouds.

D. Essential Characteristics

1) On Demand Self Service

-All the resources are present when user need it.

2) Broad Network Access

-It provides tons of connectivity options.

3) Resource Pooling

-Shares resources

4) Measured Service

-User have to pay for what they get.

5) Rapid Elasticity

-User get what they necessitate

II. WHY WE LOOKING FOR ACCESS CONTROL

Typically, the cloud platform helps often the tiny level organizations, government industries and educational institutions to reduce their very own financial issues of information government, data management as well as data control, since they are now able to save their data directly into cloud over the internet. Cloud gives some useful services including email, ticket reservation, use new passport services, and download the birth and death certificate and so on... over the internet.

Nowadays all the enterprise data are usually moved to cloud. To save sensitive data (Medical data), personal information (credit cards, social networks data) [1], [7], [12] in a secured approach, we need a safe and successful access control method for cloud.

Discretionary Access Control (DAC), Role Based Access Control (RBAC) [1], and Attribute Based Access Control (ABAC) are conventional access control models while the Attribute Based Encryption schemes introduce a complicated access control models that is certainly based on encryption technique. Every one of these systems are explained down below.

III. ACCESS CONTROL MODEL

Access control is a first brand of defense to protect institute information resources. Wherever users aim to access a particular resource they must provide their identity [1]. This can be a framework that dictates easy access control using various technologies. In this section, we talk about various ACM (Access Control Module) in detail.

A. Discretionary Access Control (DAC)

This is often a conventional scheme whereby consumer have the complete manges on the resources. An organization/creator can certainly recognize a set of actions and provide to an object to some group of users. The DAC is actually flexible but sophisticated since the DAC policy exchange around the user's identity and authorizationUnits

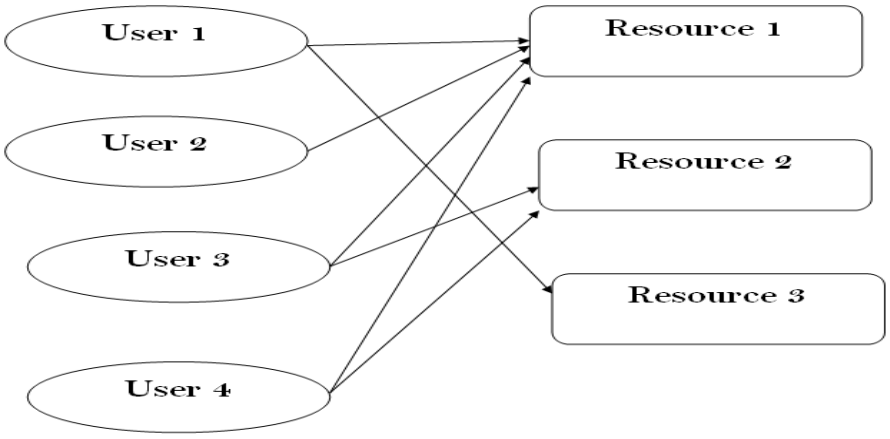

Fig.3.1. Sample Model for DAC

B. Mandatory Access Control (MAC)

In this method, the information is classified into unique categories and each category will be assigned a particular security degree. It mainly deals with secrecy of information. Each object within cloud is assigned a variety of security levels, which is used to spot the current access state of the object. For example, if resource RS comes under extremely sensitive resource in a company, it has been assigned a good "incredibly confidential" security degree. The users, who are in below level of very confidential, when attempt to access the resource (RS) [4] [12], he/she is not possible to gain access because the mismatch in the security level.

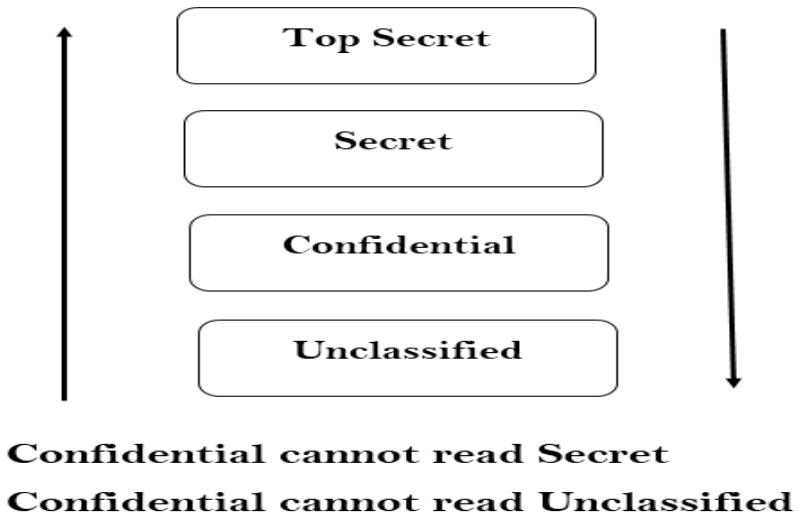

Fig.3.2 A Sample Model for MAC

C. Role Based Access Control (RBAC)

In RBAC, access resolution is based on individual or group of user responsibilities and role in the cloud environment. In this framework, the user have the ability to perform dissimilar operations, for instance, create, modify, and alter personal files. It's based on user role, depending on responsibilities and authority within the enterprise. RBAC [4] [9] is commonly used and leading easy access control model and the majority safety and security products available in market nowadays are based on RBAC only.

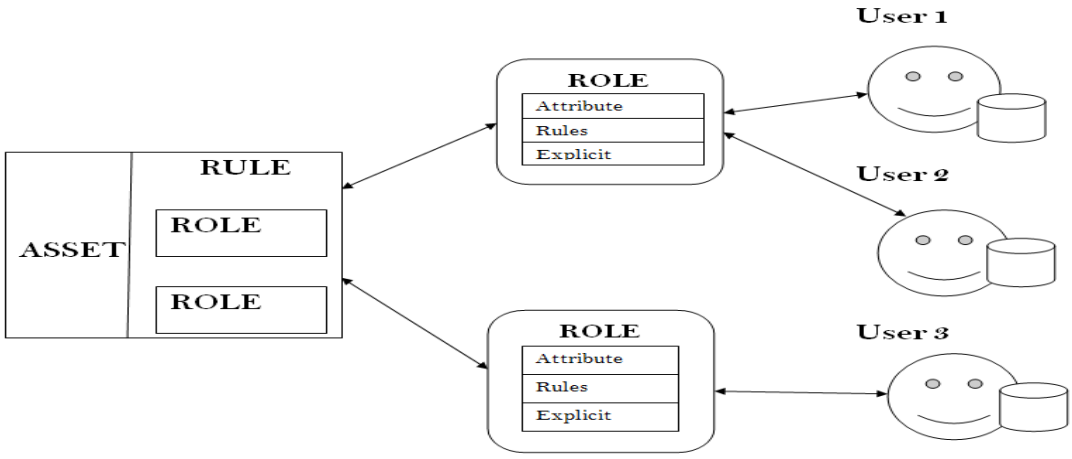

Fig.3.3. A Sample Model for RBAC

D. Attribute Based Access Control

With ABAC [6] each user will coupled among specific set of attributes. Data proprietor assigns attributes to the distinct user. Whenever the user demand resource, the owner gave permission to access only assigned features. More flexible it is, secure and scalable structure is improved. The ABAC model is shown in the Fig 3.4

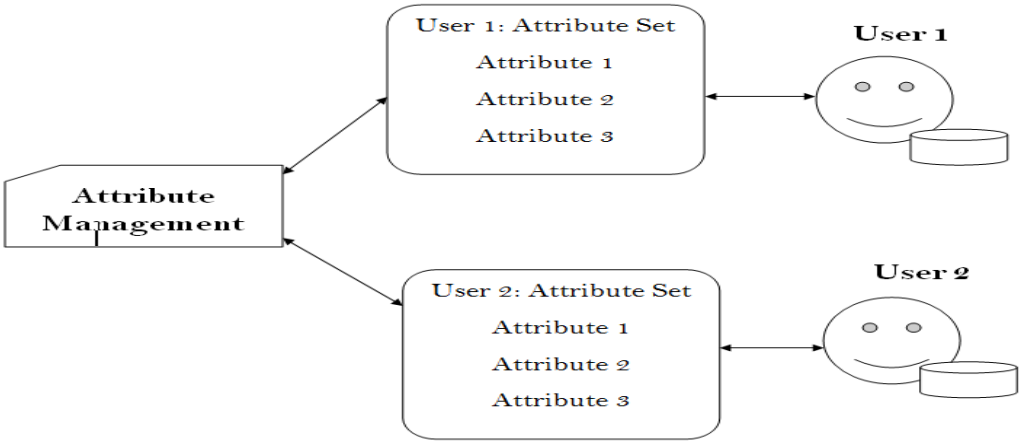

Fig.3.4. A Sample Model for ABAC

IV. ADVANCED ACCESS CONTROL MODEL

These kinds of advanced access models are based on two distinct encryption techniques [11]. They are Identity Based Encryption and Attribute Based Encryption.

1) Identity Based Encryption (IBE)

The IDE was proposed by Adi Shamir in 1984. The IBE [10] ended up being wished-for cipher text security and safety and it's a kind of general public key encryption. In this, typically the distinctive information with reference to user's identity act as public key (i.e. email id) and secret key is made by known identity from the user.

2) Attribute Based Encryption

The ABE standard was proposed by Amit Brent and Sahai Waters in 2005. The new kind of public key security in which personal key as well as secret message are dependent with user's attributes. Typically the decryption can be done only if the client attributes satisfy with matching cipher text attributes. In this particular scheme the data owner able to use user general public key to encipher the data. This is certainly one of the important drawbacks associated with ABE [7],[10]. So to overcome this nagging problem, various ABE based access control systems were developed.

B. Key Policy Attribute Based Encryption (KP-ABE)

It may be one of the modified versions associated with traditional model of attribute based encryption. In KP-ABE cipher text is correlated amongst a set of attribute and user's decipher key [8] is correlated amongst a monotonic tree accessibility structure. Only if the cipher texts associated attributes fulfill the access tree structure, have the ability to decrypt the cipher text messages.

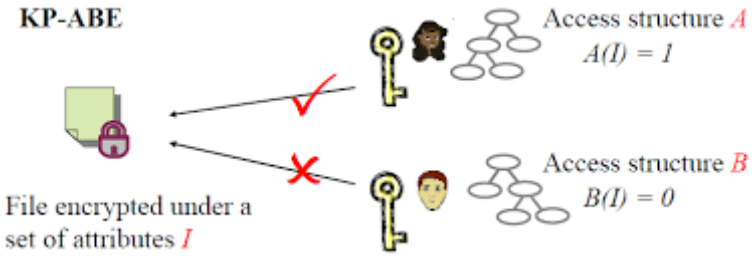

Fig.4.1 A Sample Model for KP-ABE

C. Cipher Text Policy Attribute Based Encryption (CP-ABE)

CP-ABE is another modified version connected with ABE. It's mainly used to encrypt the data that are saved on an untrusted server [6]. The important key is associated to arbitrary number of attributes. On the other side, whenever an owner encrypts any message he should identify the related access framework over attributes.

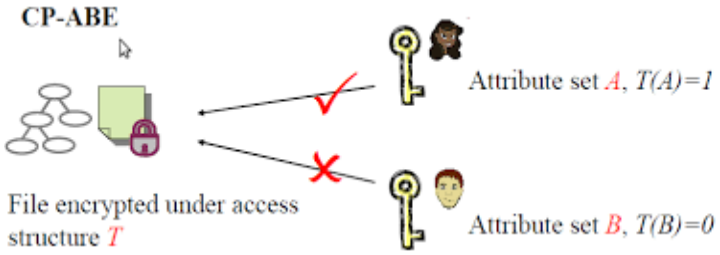

Fig.4.2. A Sample Model for CP-ABE

D. Hierarchical Attribute-Based Encryption (HABE)

HABE was invented simply by Wang et'al in 2012. It composed of root master (RM) that correlated users/clients to trusted third party (TTP), domain users (DMs) in which best level DMs correlated users/clients to enterprise user and sub users that correlated for all personnel in organizations. It is used to generate keys in hierarchical order [5].

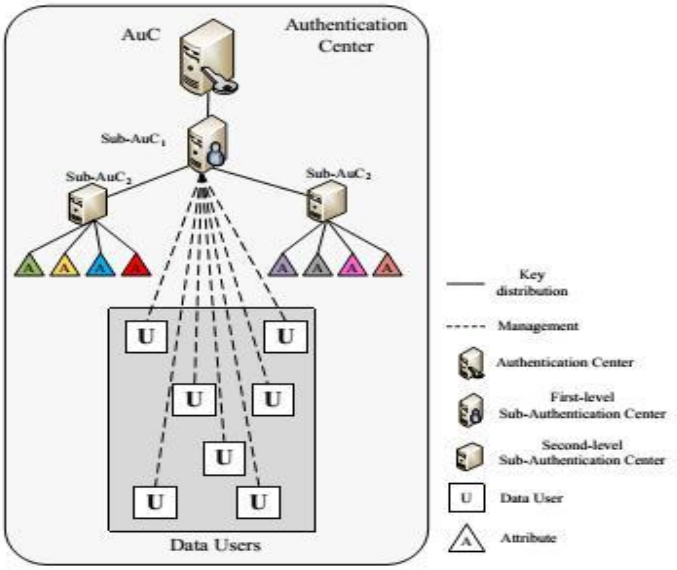

Fig.4.3. A Sample Model for HABE

V. ACCESS COTNROL TECHNOLOGIES

In this section we focus on about implementation technologies associated with access control model.

A. Security Assertion Markup Languages (SAML)

SAML is a XML based standard, used to exchange details between identity provider as well as service provider [13].

B. Service Provisioning Markup Languages (SPML)

SPML is a rising standard that can help organizations to handle provisioning of user details for cloud services [13] (e. g., an application or services running at a customer internet site requesting Salesforce. com for first time)

C. eXensible Access Control Markup Language (XACML)

XACML is an OASIS-ratified, general-purpose, XML [13]-based access control language to get policy access and management decisions.

D. Open Authentication (OAuth)

OAuth [13] is an open up protocol and it was created using the goal of enabling authorization via a secure API. It is a simple and typical method for desktop, mobile, as well as web applications.

TABLE 1: COMPARISON OF TRADITIONAL ACCESS CONTROL

Access Control Attributes	**ABAC**	**RBAC**	**MAC**	**DAC**
Performance	Good	Good	It relies on Security level	Low
Role Assignment	Not Mentioned	Multi-Node	Single Node	Not Mentioned
Single Point Failure	-	Less	Less	Authorization failure
Authentication Failure	Less	Based on Job Role	Depend on Distributed Environment	Less

TABLE II: COMPARISON OF ABE BASED ACCESS CONTROL

Parameters	**HABE**	**CP-ABE**	**KP-ABE**	**ABE**
Fine grained access control	Excellent	Normal	Fair, Excellent when the present of re-encryption technique.	Fair
Efficient	Flexible	Normal, not efficient for modern apps	Normal, Good for broadcast type system	Normal
Collision Resistant	Excellent	Excellent	Excellent	Normal

VI. CONCLUSION

Cloud computing is a leading research technology in both industries and IT. In cloud, access control is an important and basic research area to offer a security to the customer data. A powerful access control model makes a secure cloud environment. In this article, we studied with regards to various access control model and explain them in a very easiest manner to understand by the researchers.

In this article, we become experienced in various access models including DAC, MAC, RBAC, ABAC, ABE, RBE, KP-ABE, HABE and CP-ABE with simple model diagrams. From these we can certainly identify that each and every access design has different mechanism to provide a security level. This short article aimed to deliver basics associated with access control model as well as its technologies to enhance the cloud security.

VII. REFERENCES

[1] Subra Kumaraswamy, Sitaraman lakshminarayanan, Michael Reiter, Joseph Stein,Yvonne Wilson, Guidanace for Identity & Access Management, Cloud Security Alliance,2010.

[2] Toby Velte, Anthony Velte, and Robert Elsenpeter. 2009. *Cloud Computing, a Practical Approach (1 ed.)*. McGraw-Hill, Inc., New York, NY,USA.

[3] Qi Yuan, Chunguang Ma and Junyu Lin, Fine-Grained Access Control for Big Data Based on CP_ABE in Cloud Computing, Springer, pp – 344 – 352, 2015.

[4] Rajanikanth Aluvalu and Lakshmi Muddana, A Surey on Access Control Models in Cloud Computing, Advances in Intelligent Systems and Computing- Springer, Vol. 1, pp 653-664, 2015.

[5] Guojun Wnag, Qin Liu and Jie Wu, Hierarchial Attribute-based Encryption for Fine-Grained Access Control in Cloud Storage Services.

[6] Vincent C. Hu, D.Richard Kuhn and David F.Ferraiolo, Attribute- Based Access Control, IEEE Computer Society, pp -85-88,2015.

[7] Vincent Hu, David F.Ferraiolo,D.Richard Kuhn,Raghu N.Kacker, Yu Lei, Implementing and Managing Policy Rules in Attribute Based Access Control, 2015 IEEE 16th International Conference on Information Reuse and Integration, pp 518-525, 2015.

[8] Afsha Pathan, M.D.Ingle. Survey Paper on User Anonymous Authentication Scheme for Decentralized Access Control in Clouds, International Journal of Science and Research (IJSR), Vol. 4, Issue 11, pp 2024-2027, 2015.

[9] Chirag Langaliya, Rajanikanth Aluvalu, Enhancing Cloud Security through Access Control Models: A Survey, International Journal of Computer applications, Vol.112, Issue No 7, 2015.

[10] B.K.Ugale, R.N.Phursule, A Survey on Access Control and Encryption Mechanisms for Cloud Computing, International Journal of Computer Science and Information Technologies, Vol. 6, pp 5363- 5366, 2015.

[11] Iqbalinder Singh Sohal, Amardeep kaur, Review on advanced access control model in cloud computing, The Research Journal, Vol. 2, Issue 4, pp -1-5, 2016.

[12] Vinay Purohit, Authentication and Access Control, pp 1-10,2008

[13] Tim Mather, Subra Kumaraswamy, and Shahed Latif. 2009. *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. O'Reilly Media, Inc..

AUTHORS PROFILE

CHINNASAMY P is a PhD student at Kalasalingam University. His research interests include cloud computing, cloud security, cryptography. Chinnasamy has a master's degree in computer science and engineering at Kalasalingam University. Contact him at chinnasamyponnusamy@gmail.com

Dr.P.DEEPALAKSHMI is currently working as professor and head in department of CSE, Kalasalingam University, Tamil Nadu, India. Her area of interest include routing in wireless networks, optimization techniques, software defined networking and distributed computing. Contact her at deepa.kumar@klu.ac.in