International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 11369-11374

http://www.ripublication.com

Trusted Architecture For Cloud Computing - A New Way of Access Control

Mr. Krishnamoorthy G.[1,a], Dr. UmaMaheswari N.[2,b] ,Dr. Venkatesh .R[3,c]
**Asst.Prof.,Dept.ofIT,Ratnavel Subramnaim College of Engg,&Tech.,Dindigul,Tamil Nadu, India [1]*
Professor, Dept. of CSE, P.S.N.A. College of Engg., & Tech., Dindigul, Tamil Nadu, India[2]
Professor, Dept. of IT, P.S.N.A. College of Engg., & Techn., Dindigul, Tamil Nadu, India[3]
pnggkrishnamoorthy@gmail.com [a] numamahi@gmail.com [b] rlvenkatesh@gmail.com

Abstract

Cloud computing is an emerging technology that provides various resources such as storage space, processing cycles, software as service .we take in to consideration only the storage service offered by the cloud providers , here since our data are stored in a space provided by the third party service providers , Access control is an major issue in the context of cloud, we built an architecture based on the concepts of trusted computing and introduce a new model of access control build on the traditional Role based Access control which provides solution to a specific kind of scenario and pave way for other related issues

Keywords: cloud computing, Access control

Introduction

Cloud computing being the currently evolving computing methodology various organizations are moving their enterprise towards the cloud, the major cloud providers currently in the market are Amazon, Google, salesforce.com, IBM, oracle and Microsoft[1], they provide cloud services in various aspects such as the IaaS , PaaS, SaaS and in different types such as the Public , Private and Hybrid cloud, this new technology also creates a lot of security issues in various levels , in the following sections we will see the various major security issues in cloud Computing and in particular the Access control problem and how various cloud service providers meet these challenges and how the proposed solution is used to solve the issue.

Major Security Issues

Cloud security alliance [2] have identified 13 major domains in cloud where security issues can arise these domains can be broadly classified as follows so that the concept of trusted computing can be applied to them, they are *Securing data in data centers, Securing data in transition, User authentication, User isolation, Legal issues, Incident response and user behaviour*. Our focus here is on the securing data in the data centres.

Related Work

From the period when data was first ever created by mankind Access control problem persists, though there exists various Access control Mechanism we discuss them in the context of cloud computing. Access control Matrix is of its first kind that provides access control over the stored objects, now in the context of cloud , cloud security alliance provides the cloud security alliance matrix (CCM)[3] which act as a guide to both the cloud vendor and the users, the second method is the Access control List basically provides a table specifying which user can access which object, now it has been used by many cloud service providers such as Google [4] , Discretionary Access control is based on the Access control List and it is data owner centric , which leads to various problems such as the increased probability of unauthorized users to access the data and maintenance of list when the number of users increases, Ravi S. Sandhu [5] , discussed about the Mandatory access control which provides the security levels for the users, subject and objects based on which the access control is provided, the drawback of this method is dynamic changing of the security level assigned to a user. Role based access control[8][9] is model that has been in use for a long but currently it is being used in cloud environment, Microsoft azure[10] uses this concept and we will design a slight variation of this method.

Problem Scenario

Consider an institution, where access of records (objects) are based on the roles and attributes assigned to the person belonging to the institution, here the following assumptions are made, we consider a private cloud and the data of the organization is stored in the cloud, each worker of the organization is assigned with a role, based on the role assigned the user is provided permission to access a record which we call here as object, so each user has a role assigned to him/her, consider the head of the institution is assigned privilege to access a particular object, now in case of emergency if Assistant Head of the institution wants to access a particular object which can only be accessed by the Head of the institution , he/she is not able to do it. This kind of scenarios is common in many applications such as health care, educational institutions etc., our proposed method will address such kind of issues.

Proposed Architecture

As we specified earlier the basic idea of our work is from Trusted computing, which uses the concepts of PEP (policy enforcement point) , PDP (policy Decision Point) , which have predefined policies based on which the request grant or request deny is decided, studies have shown that the concepts of XACML is very similar to that of the concept of the trusted computing, so with the idea of implementing our work completely based on software we use the concepts of XACML .The proposed architecture is as follows.

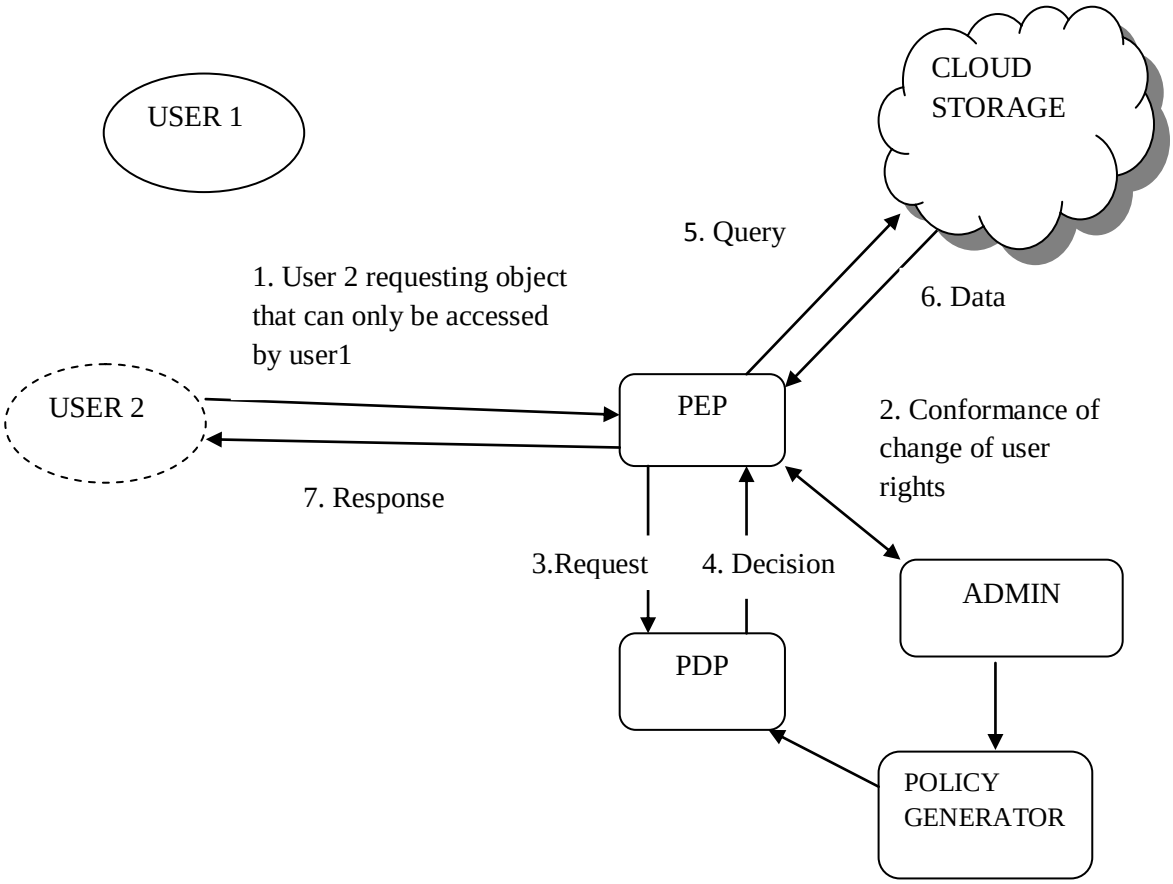


Figure 1: Architecture depicting the proposed steps for access control

The above figure represents the actual process of our proposed work , the following entities are taken in to consideration for clear understanding.

User 1: ***original user***

User 2: ***alias user*** of user 1

Object: o1

As discussed in our problem scenario in case of emergency if the user 2(alias user) wants to access object o1 which can only be accessed by user1 (original user), then the following things has to be done.

- Providing privilege to the alias user for accessing o1
- Dynamic generation of policy that allows alias user to access the o1

When generating the dynamic policy the following ***constraints*** are taken in to account

- The alias user can access only the object o1, he/she should not be permitted to access any other objects that can be accessed by the original user, this helps preventing accessing of other unauthorized data
- The alias user can access object o1 only for a particular time, this constraint is taken in to consideration because at any later point of time the alias user should not access the same object

Taking in to consideration the above specified constraints we have implemented our work , though there is numerous numbers of policy definition languages[6] we have used XACML for defining policies and its related components (PDP, PEP). The steps that are involved in this model after the admin allows the alias user to access the object that can be accessed only by user 1 is as follows,

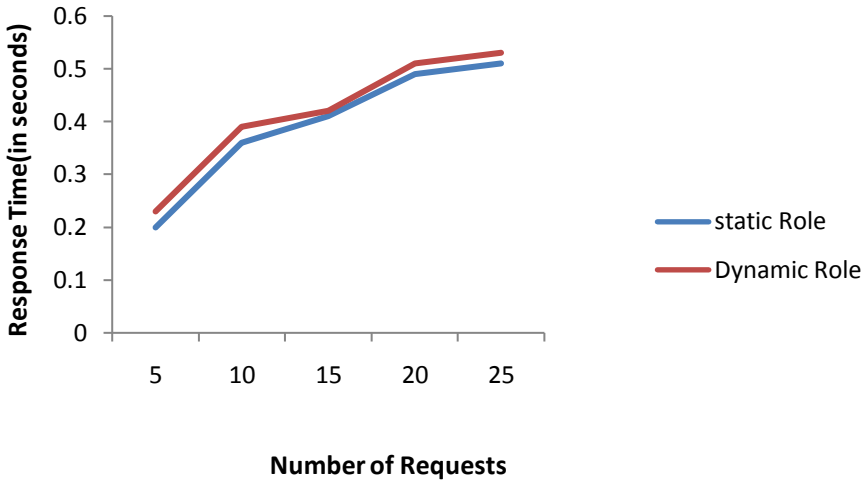
Generate Dynamic policy taking in to consideration the following.

- User2 should only be able to access the Object o1.
- User2 can access Object o1 only for the specified session
- Apply all Constraints to user2 that is applicable for user1

These things should be done before the request is generated by user2.

Implementation Details & Experimental Results

The work was implemented by considering a data space in a remote system as cloud, the system is equipped with i3 processor and 300 GB Hard disk. The policy language used here is XACML[7] and the other implementation of creating users and generating Requests from the user, sending request and getting the Decision are all implemented in Java, thanks to the basic syntax of the Language that provides facilities of adding attributes to the elements , we use this concept for the specifying the session in which the user2 should access the Object o1 and user2 can access only o1 .we have tested our work with varying number of Requests and the time taken to provide permission or deny it. The following graph shows the result.



Obviously from the above graph we can understand that the Response time when using the Dynamic role is negotiable, but the use of the dynamic Role paves way for the various other access control scenarios that may be based on the temporal, contextual etc.

Conclusion & Future Work

This paper depicts the possibility of providing the solution to the various Access Control Scenarios that would arise in the cloud and we have demonstrated a simple scenario in Access control and we can also able to apply such Methodologies to various other scenarios in the cloud, in our future work we create an mathematical Model for the above explained work and also adding dynamic Attribute based Access Control with this.

References

[1]. Danish Jamil, Hassan zaki, cloud computing security, 2011International Journal of Engineering Science and Technology (IJEST)

[2]. http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[3]. https://downloads.cloudsecurityalliance.org/initiatives/ccm/ccm-v3.0.1.zip

[4]. https://cloud.google.com/storage/docs/access-control#About-Access-Control-Lists

[5]. Ravi s. Sandhu " Access control Principles and Practices" IEEE Communications, September 1994

[6]. weili Han , chang Lei " A Survey on Policy Languages in network and Security Management " Elsevier, 2011

[7]. https://www.oasis-open.org/committees/xacml/repository/cs-xacml-specification-1.1.pdf

[8]. David F. Ferraiolo and D. Richard Kuhn "Role based Access control" 15th National computer security conference ,USA, 1992

[9]. Ravi s. Sandhu et. al " Role Based Access Control Models" IEEE Computer , 1996

[10]. Charlie Kauffman and ramanathan venkatapathy "windows azure security overview v1.01 " 2011