Proc. of Int. Conf. on Current Trends in Eng., Science and Technology, ICCTEST

Trust in Security Issues and Authentication in Cloud Computing Model

Suma K
Assistant Professor, Dept. of ISE, Don Bosco Institute of Technology, Bangalore, India
ksuma91@gmail.com

***Abstract*—Trust in security and authentication plays a major issue in cloud. the scope of unite cloud computing enlarges to existing and pervasive computing, there will be a need to assess and maintain the trustworthiness of the cloud computing entities. methods which includes single encryption, multi-level virtualization, and authentication interface. Authentication intercloud is the other main role in this paper. This paper also discussed a model of authentication intercloud which based on CA and PKI model which be extended to the scenario without CA system or it crashed. Additional encrypted parameter will be an efficient technique which provides more security to the data storage in clouds.**

***Index Terms*— Private cloud, public cloud , hybrid cloud Algorithms. Data security authentication.**

I. INTRODUCTION

Cloud computing is a model for enabling 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 effort or service provider interaction".
In cloud computing, the core design principles is dynamic measurability that guarantees to cloud storage service to handle huge amounts of application data in an exceedingly versatile manner or to be promptly enlarged. By the action of multiple private and public cloud services, hybrid clouds will effectively offer dynamic measurability of service and data migration.
Integrate the information from multiple private or public providers into a backup or repository file or a service may capture the information from different services from private clouds, however the information and results are keep in hybrid clouds.
Trust is the competence of an entity to act as expected within a specific context at a given time [2]. Quality is a measure that is extracted from direct or indirect knowledge of interactions of peers and is used to access the level of trust a peer puts into another [1,2]. One entity can trust another entity in the network based on a good quality, we can use quality to build trust [3]. This means quality can serve, in the sense of reliability, as a measure of trustworthiness.

II. PROTECTION OF DATA SECURITY

As it is known, the private cloud could provide the most security for users data, and this lacks the scalability. And the public cloud could satisfy the demand of the scalability. Hybrid cloud could provide both security

Grenze ID: 02.ICCTEST.2017.1.64

and the scalability at the same time. However, there still are some problems about the data security because when user extends their application to the public cloud, the cloud computing provider could access the users privacy data.
There are some methods to protect users data on the public cloud Security at Different Levels
We need security at following levels:

- Server access security
- Internet access security
- Database access security
- Data privacy security
- Program access Security

Questions

- What is Data Security at Physical Layer?
- What is Data Security at Network Layer?
- What about investigation Support?
- How much safe is data from Natural disaster?

How much trusted is Encryption scheme of Service Provider?

III. PKI MODEL

public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. ... In a Microsoft PKI, a registration authority is usually called a subordinate CA.

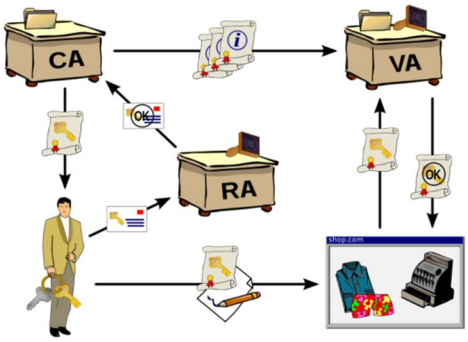

Fig. 1. PKI is emerging as the foundation for secure electronic commerce and Internet security by providing the cornerstones of security:

Authentication	The importance of authentication, verifying the identity of users and machines, becomes crucial when an organization opens its doors to the Internet. Strong authentication mechanisms ensure that persons and machines are the entities they claim to be.
Encryption	Encryption algorithms are used to secure communications and ensure the privacy of data sent from one computer to another.
Non-repudiation	PKI can be used to provide non-repudiation through digital signatures. This proves that a specific user performed certain operations at a given time.

CA – Certification Authority

- Issuer/Signer of the certificate
  - Binds public key w/ identity+attributes
- Enterprise CA
- Individual as CA (PGP)
  - Web of trust
- "Global" or "Universal" CAs
  - VeriSign, Equifax, Entrust, CyberTrust, Identrus, …Trust is the key word

IV. ATHUTHENTICATION

There are some methods to protect users data on the public cloud.

A. Single Encryption

The single encryption is based on that we could trust our private cloud totally and we could trust the public cloud conditionally. So we could store the data on private cloud directly. Single encryption means the data would be encrypted when it would be transfer to the public cloud from the private cloud, using the single encryption algorithms.

B. Authentication Interface

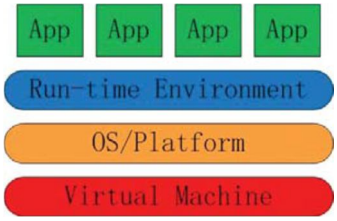

Fig. 2. Authentication Interface Model

Authentication interface is improved from multi-level virtualization model. Multi-level virtualization model is suit for the scenario that all users applications need the permission control, yet not all scenarios need this kind of control. In order to find the balance of the performance and the security, some applications would not need the permission control, so the case-based permission control is a better choice.

Authentication interface is integrated in the users applications, when the application running on the public cloud wish to access the data owned by hybrid cloud application (host application), it would sent permission request to the host application, host application would check the authorize list, if the request application is already authorized, the host application will give it permission to the data. And if the request application is not already forbidden, the host application would send the request back to private cloud to let the user to decide whether authorize the request or not.

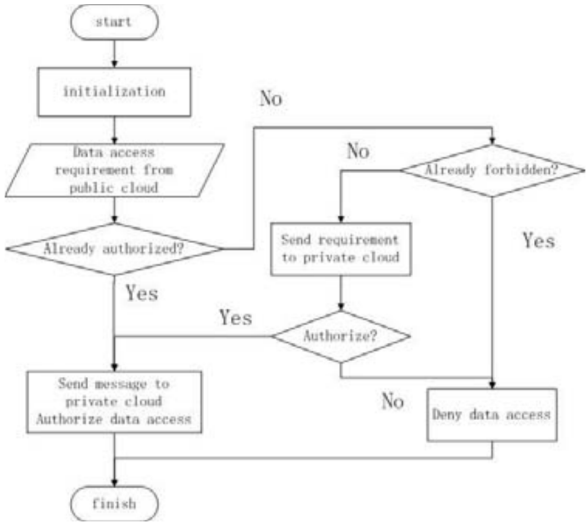

Fig. 3. Authorize Flow Diagram

V. THE GENERALIZATION OF THE AUTHENTICATION MODEL

Sometimes the cloud cannot find a CA to authenticate the other cloud provider, or the scenario of intercloud authenticate in a large cloud network, for example, a lots of clouds of a cloud computing provider.

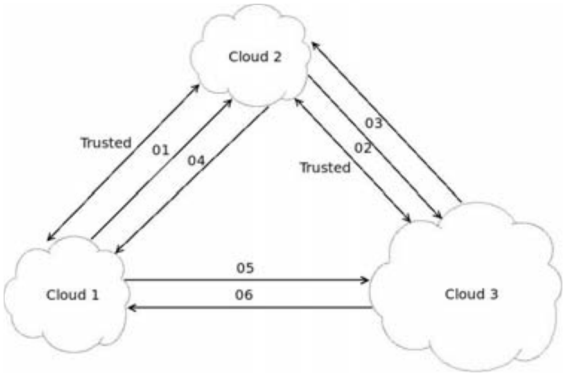

Fig. 4. Generalization of the Authentication Model

Here is a generalization of the authentication model. there is a scenario that cloud 1 is already trust cloud 2, and cloud 2 is already trust cloud 3. Now cloud 1 wishes to extend its computing capacity via connect another cloud. Here cloud 2 has some reason that cannot connect to cloud 1, so the cloud 1 has to find another cloud to connect.The cloud 1 first send a request to cloud 2 for another trustable cloud, the cloud 2 will check its trust list to find a cloud it trusts. Like the situation in the figure, the cloud 2 finds that cloud 3 could be trusted, so it will send a request to cloud 3 to find whether it could provide connection to other cloud. The cloud 3 has the extra capacity so it will send the answer to cloud 2. Then the cloud 2 will send the information about cloud 3 to cloud 1, meanwhile the cloud 3 will send the information
about itself to cloud 1. cloud 1 will check the information from cloud 2 and cloud 3, if they are same, the cloud 3 could be trust by cloud 1.
And the process of the authentication will finish, and if the information is not same, the cloud 3 would not be trusted by cloud 1.

VI. Trust Management Framework

In this section, we present a brief discussion of the main components of the inter-cloud computing architecture and the proposed mechanism for determining trustworthiness of a given resource. By autonomous we mean that no cloud has direct control and power over the actions of another cloud. For the purposes of this paper, we define a hybrid cloud computing as a subset of the universe of clouds. Cloud users require resources to deploy services and run applications. Cloud providers provide resources and services to potential users for fee or following another economic model uch as bartering. Resource providers have their cost structures and policies that govern how their resources are provisioned to a user.computing architecture that allows cloud users to deploy applications and scientific workflows that require resources beyond the capacity of their clouds. The architecture is layered in that services are provisioned to cloud users based on cloud-level by the cloud resource manager or the intercloud broker (ICB) level by two resource management policies.

VII. Discussion

During the commercialization of the cloud computing, the use of users data becomes a major problem. When user decides to establish the cloud computing for their company, the security and privacy of their commercial data would be concerned first. They need to protect their data, and the cloud computing providers may take use of the users data to analysis their commercial behavior and mine the useful information. These operations may be done without the users authorization. Cloud computing and the data mining could help the users
improve their commercial behavior, yet if the data obtained by the opponents, it could lead some legal issues. Cloud computing still has some problem of security, especially the intercloud operations. The cloud providers should get together for the standard of intercloud operation interfaces.

REFERENCE

[1] Jemal H. Abawajy, Andrzej M. Goscinski: A Reputation-Based Grid Information Service. International Conference on Computational Science (4) 2006: 1015-1022

[2] L. Peterson and J. Wroclawski. Overview of the GENI architecture. GENI Design Document GDD- 06-11, GENI: Global Environment for Network Innovations, January 2007

[3] A. Jøsang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision. Decision Support Systems, 43(2):618–644, March 2007.