ISSN:0975-9646

Private Cloud Security using DLSC

Jothimani S, Arul Sangeetha.S

Assistant Professor, Department of computer engineering
Nehru Institute of Engineering and Technology

Abstract: The computing resources can be easily accessed by cloud computing. The cloud computing services may be software as a service, platform as a service, and infrastructure as a service. Here we discuss the security methods to access the private cloud computing. This paper aims to give the some security mechanism to protect the private data over the cloud. It gives the ways to increase the protection of data against the attackers. In this paper we introduce the DLSC data protection against hackers

Keyword:- Private Cloud, Security, attackers, DLSC

1. Introduction

Cloud computing is networked infrastructure software and have capacity to provide resources to users in an on-demand environment. The information is stored in the centralized servers and it is dispatched to the clients includes desktop, notebooks, laptop and handheld systems. The company data centers or an external company resource can have cloud infrastructure within it. The virtual computer which allows the users to access the service whenever it is needed. The cloud computing is flexible and elastic offering.

Figure 1 cloud computing

Cloud computing is delivering hosted services over the Internet. It is used to a Platform and type of Application.

One of the key characteristics of cloud computing is the flexibility and scalability. This refers to the ability of a system to settle in and scale to changes in workload. Cloud technology allows for the automatic provision of resource as and when it is required, thus ensuring that the level of resource available is as closely coordinated to current demand as possible. This is a defining characteristic that differentiates it from other computing models where resource is delivered in blocks (e.g., individual servers, downloaded software applications), usually with fixed capacities and upfront costs. By using cloud computing, the end user usually pays only for the resource they use and so avoids the inefficiencies and expense of any unused capacity.

Private Cloud

A private cloud provides more control over the company's data, and it ensures security, notwithstanding with greater potential risk for data loss due to natural disaster. The organization implementing the private cloud is in charge for running and managing IT resources instead of passing that responsibility on to a third-party cloud provider.

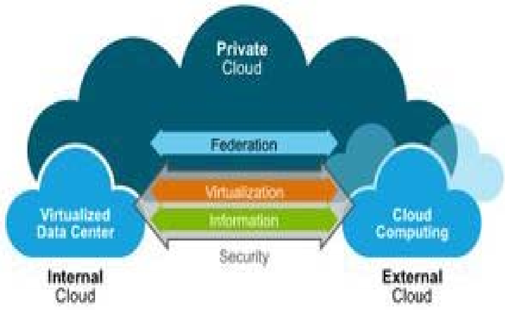

Figure 2 private cloud

Unlike a public cloud, a private cloud project remains within the corporate firewall and under the control on the company’s IT department. As a result, a private cloud provides more control over the company’s data, and it ensures security, notwithstanding with greater potential risk for data loss due to natural disaster.

Launching a private cloud project involves analyzing the need for a private cloud, formulating a plan for how to create a private cloud, developing cloud policies for access and security, deploying and testing the private cloud infrastructure, and training employees and partners on the cloud computing project.

Cloud computing opens up a new world of opportunities for businesses, but mixed in with these opportunities are several security challenges that need to be considered and addressed prior to committing to a cloud computing policy. Cloud
Computing security challenges fall into three broad categories:

- Data Protection: Securing data both at rest and in transit
- User Authentication: Limiting access to data and monitoring while accesses the data
- Disaster and Data Breach eventuality Planning

PRIVATE CLOUDS CHALLENGES

- Private Cloud administrators need to work with service administrators (e.g., mail services, collaboration services, database services) to make sure proper configuration of network access controls.
- The most deleterious security problems come from inside the organization and therefore we should treat the traffic inside the Internet perimeter with as much security as the traffic outside.
- To ensure that virtual machines only communicate with virtual machines that they communicate with, ensure that network level authentication and encryption mechanisms are used.
- Dedicate a physical interface for over-the network communications with the host operating system for management purposes.
- The host operating system must be free from malware, and mechanisms, such as anti-malware software, must be in place to detect potential compromise.
- In a Private Cloud environment, guest virtual machines belonging to different security zones should not be hosted on the same virtual server.

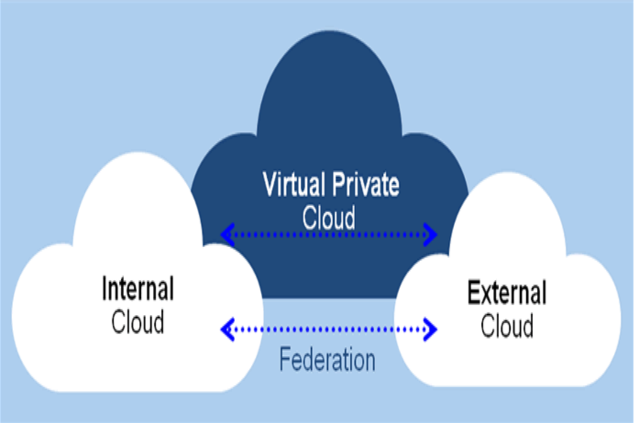

Figure 3 private cloud structure

EXSISTING SECURITY MECHANISMS

Applications must be designed so that they:

- Expose a reduced attack surface
- Run with least privilege
- Validate input
- Require user authentication
- Enforce authorization policies
- Encrypt data on disk
- Encrypt data over the network
- Encrypt data at the client application

This process, is referred to as the Security Development Lifecycle.Many organizations are sprouting virtualized infrastructure into private clouds - internal shared services running on virtualized infrastructure. Security architecture, policies, and processes will need to acclimatize to work within a cloud infrastructure, as well, and there are many changes that security and operations teams will need to accommodate to ensure assets are protected.

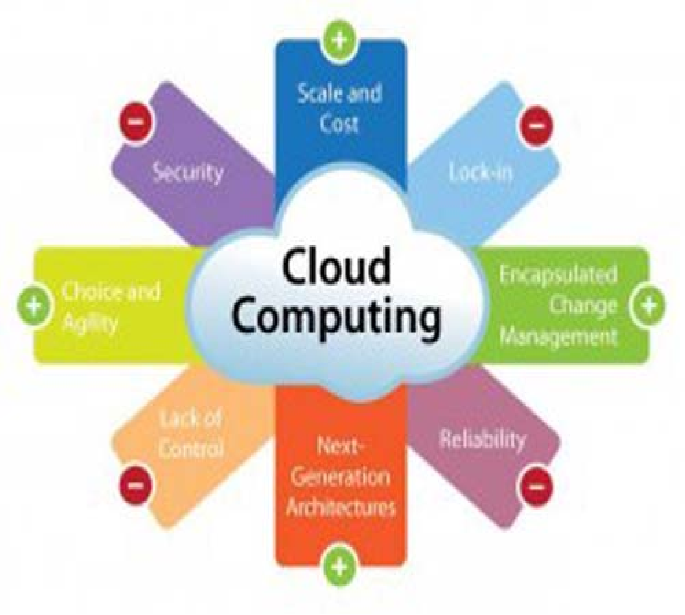

Figure 4 Private cloud issues

1) **Performance**: application performance is the major problems with the cloud computing technique. In a cloud environment, all sites are competing for the hardware resources, and if multiple websites pierce unconsciously, it may cause disorder resulting in everyone slowing down. So when we take network latency into account, we find the performance of our applications suffers a lot.
2) **Security**: Cloud hosting does not provide much secure environment as you need. If anybody is looking to achieve and maintain data privacy requirements for PCI compliance, HIPAA compliance, SOX, E-commerce, and so on, then cloud hosting is not considered as the right solution
3) **Redundancy**: One of the misconceptions of cloud hosting is that it's hosted "in the sky and not in a datacenter," which is not true. Cloud hosting resides in a single datacenter. Recently a large hosting provider's data center went down leaving a lot of cloud hosted Web sites in the dark. The site owners had a huge reality check and quickly learned of the single-points of failure within a cloud environment.
4) **Cost**: One of the misconceptions of cloud hosting is that it is cost effective which is partially true. No doubt the cloud gives businesses a hands-free method to scale their hosting, however some problems may arise that are really financially surprising. There is a need to become quite attentive towards the clouds usage. Some usage methods won't take your site to let down but will keep your server very busy and hence will take more time to accomplish any action. Since you pay for usage with cloud hosting, your costs can spin wildly out of control.
5) **Sometimes frustrating**: searching of next-generation IT models requires a thrill-seeking strength of mind and technical perceptiveness. If anyone don't have the human capital that's willing to stretch and learn new things, in that scenario, cloud computing becomes very frustrating for them.

ADVANCED SECURITY CONTROL

Since there are many security issues associated with the private cloud we need to protect the cloud in safe manner. Hence in this paper we introduce the two layered security control mechanism.

This method involves in two steps.

The very first step to protect the data is to covering of it using the strongest password which should contain the letters and the images and special letters. The smallest and complex images are preferable. The image should be kept confidential with us. Then whenever we want to access the data have to use the image as password contains with the text and letters.

The second step to create the puzzles using the images to protect the passwords. Hence our data will be safer with the double layered protection.

DLSC

The Dual Layered Security Control (DLSC) which contains the password including images and the puzzle to protect the password.

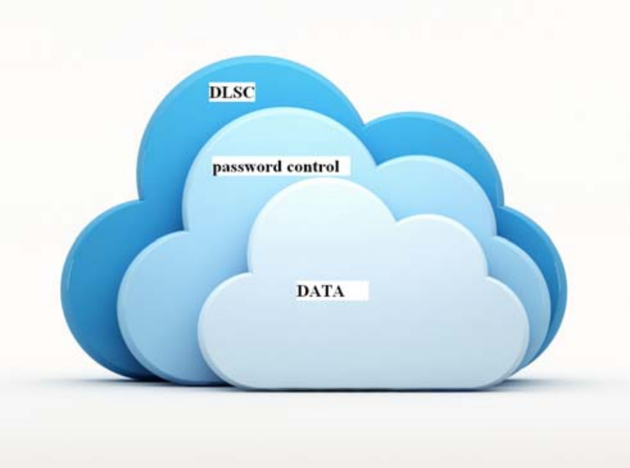

Figure 5 DLSC control

The second layer protection which contains the puzzles on images is the strongest method to protect the data. The solving of puzzle should be pre computed and the attempt of steps to move the slides to arrange the puzzle also pre computed and it should be stored. The user should solve and open the puzzle with the given number of time and the number of slide movement.

The attempt to solve the puzzle is controlled to three times. When the user failed to solve the puzzle in the first time the chance of opening the puzzle second time is harder than the first time. Hence the hackers are not capable of open the puzzle in the same allotted time and the movement leads to protection stronger.

ALGORITHM

```
Initialize a=3,m=5,t=10s;
if a<= 3
   For t=0 to 10
         For m=0 to 5
           Solve the puzzle;
            Print "authorized"
             If(authorized)
                 For i=0 to i=3
                    Use image password to access the Data
                                   If(i>3)
                                   Print "unauthorized"
                                   Exit;
                            Exit
         Exit
Exit

Else
Print "unauthorized user"
```

CONCLUSION:-

The private cloud has number of increased control and monitoring of resources, flexibility of customization, facility to recover from failure, and the capability to scale up or down depending upon demand. Private cloud is less vulnerable to hackers' attack by blocking unauthorized access and restricting its resources to authorized users and administrators alone.

REFERENCES

1. http://blogs.gartner.com/thomas_bittman/2010/05/18 /clarifying-private-cloud-computing/
2. "Adopting Cloud Computing: Enterprise Private Clouds", Shyam Kumar Doddavula and Amit Wasudeo Gawande, SETLabs Briefings, VOL 7 NO 7 2009
3. http://www.cisco.com/en/US/solutions/collateral/ns3 40/ns517/ns224/ns836/ns976/white_paper_c11-543 729.html
4. Cloud Computing: A Study of Infrastructure As A Service (Iaas), Sushil Bhardwaj, Leena Jain, Sandeep Jain, International Journal Of Engineering And Information Technology.
5. http://www.esri.com/technology-topics/cloud-gis/pub lic-vs-private.html
6. http://www.tatvasoft.com/blog/2011/04/what-is-clou d-computing. html