International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 9, November- 2012

Security In Cloud Computing Using File Encryption

Mr.Tejas P.Bhatt[*1], *Asst. Prof. Ashish Maheta*[#2]

** C.S.E. Department, Government College of Engineering, Gandhinagar*
Gujarat Technology University, Gujarat, India.

 # I.T. Department, Indus Institute of Technology, Ahemadabad
Gujarat Technology University, Gujarat, India

Abstract

In cloud computing, Security of file or data is provided to the end user in the private cloud environment. The main concern is to provide the security to end user to protect files or data from unauthorized user. Difference is that the research is done in cloud, but security related issue can't be resolved yet. Security is the main intention of any technology through which unauthorized intruder can't access your file or data in cloud. Thus, we can give maximum effort to avoid the issues of security occurs. We have designed one proposed design and architecture that can help to encrypt the file and decrypt it. In this research paper, we have used the AES Algorithm for the encryption.

Keywords: cloud *computing, security, file encryption*

1. Introduction

Cloud Computing:

Cloud computing is the next stage in the Internet's evolution, providing the means through which everything — from computing power to computing infrastructure, applications, business processes to personal collaboration — can be delivered to you as a service wherever and whenever you need[1].

The "cloud" in cloud computing can be defined as the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a service. Cloud services include the delivery of software, infrastructure, and storage over the Internet (either as separate components or a complete platform) based on user demand.

Cloud computing has four essential characteristics: elasticity and the ability to scale up and down, self-service provisioning and automatic deprovisioning, application programming interfaces (APIs), billing and metering of service usage in a pay-as-you-go model. (Cloud Computing Characteristics discusses these elements in detail.) This flexibility is what is attracting individuals and businesses to move to the cloud.

These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

- **Infrastructure-as-a-Service** like Amazon Web Services provides virtual server instanceAPI) to start, stop access and configure their virtual servers and storage. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and bring more online as soon as required.
- **Platform-as-a-service** in the cloud is defined as a set of software and product development tools hosted on the provider's infrastructure. Developers create applications on the provider's platform over the Internet. PaaS providers may use APIs, website portals or gateway software installed on the customer's computer. Force.com, (an outgrowth of Salesforce.com) and GoogleApps are examples of PaaS.
- **Software-as-a-service** cloud model, the vendor supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal. SaaS is a very broad market. Services can be anything from Web-based email to inventory control and database processing.

2. Virtualization

2.1 Virtualization:

Virtualization is the creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device or network resources.

You probably know a little about virtualization if you have ever divided your hard drive into different partitions. A partition is the logical division of a hard disk drive to create, in effect, two separate hard drives.

Operating system virtualization is the use of software to allow a piece of hardware to run multiple operating system images at the same time [2]. The technology got its start on mainframes decades ago, allowing administrators to avoid wasting expensive processing power.

There are three areas of IT where virtualization is making head roads, network virtualization, storage virtualization and server virtualization:

2.2 Virtual Machine:

A virtual machine is a tightly isolated software container that can run its own operating systems and applications as if it were a physical computer. A virtual machine behaves exactly like a physical computer and contains it own virtual (i.e, software-based) CPU, RAM hard disk and network interface card (NIC).

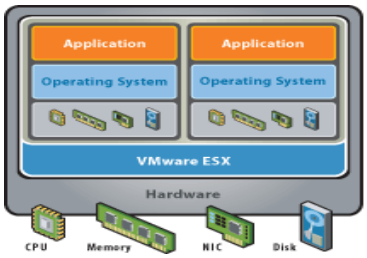

Figure 1

An operating system can't tell the difference between a virtual machine and a physical machine, nor can applications or other computers on a network. Even the virtual machine thinks it is a "real" computer.

Nevertheless, a virtual machine composed entirely of software and contains no hardware components whatsoever. As a result, virtual machines offer a number of distinct advantages over physical hardware.

3. Security Issues Of Cloud Computing:

When it comes to Security, cloud really suffers a lot. The vendor for Cloud must make sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud thus affecting many customers who are sharing the infected cloud. Some of the problem which is faced by the Cloud computing [4],

- Data Integrity
- Data Theft
- Privacy issues
- Infected Application
- Data loss
- Data Location
- Security on Vendor level
- Security on user level

One of the issues that become apparent with more users choosing to work from mobile phones and tablets is the issue of security. Sometimes these devices can end up in the wrong hands and when that happens it is reasonable to take precautions about how can open and gain access to files you have stored in the Cloud.

The secondary security concern can be with Cloud the Providers themselves. Users often want to protect certain files on the actual Cloud where they reside, and to that end they can want to use encryption independent of the Cloud Provider.

This particular use case can be solved by using the Cloud encryption service that SME Storage provides. This feature is provided to free, personal, and Cloud File Server users.

I have studied so many research papers on security for files and get some of the new issues of regards missing files from server and any unauthorized end user can read the content of your files, loss of confidential information. There is some more issue that can occur in the cloud and it's more unprotected for communication and affects our environment of cloud.

In many of research papers that has so much issue of security in eucalyptus cloud. It is very complex problem in the cloud environment.

End user is sending many confidential data but its lost. So Almost need some protection from the unauthenticated user whom breach security and most research paper there is lot of security related issues occurred in the cloud computing.

In the File level Encryption in which there is some issues:

- There is inconsistency occurred when two user that can access same file at the time in the virtual machine.
- In second problem, If any instance have its own rights as a owner that can access all files but other

user of the owner's team that can access something in that instance. Owner is giving access rights to that user and that can access the owner's confidential file. It's also big issues in the private cloud of the organization.

There is kind of security issues are occurs eucalyptus cloud.

- All Eucalyptus components use WS-security for authentication.
- SSH keys provide root level access. The cloud controller generates the public/private SSH key pairs and installs them on each instance.
- Admin can invite users to their cloud by providing them with a private token. Users can enter the token in a dialog box to register and gain access to the cloud.
- Admin can add/remove users
- The basic areas of cloud vulnerability are similar to the standard issues that surround networking and networked applications. The issues specific to cloud architectures include network control being in the hands of third parties and and a potential for sensitive data to be available to a much larger selection of third-parties, both on the staff of the cloud providers, and among the other clients of the cloud. Cloud computing shares in common with other network-based application, Storage and communication platforms certain vulnerabilities in broad areas:
- Web application vulnerabilities, such as cross-site scripting and SQL injection (which are symptomatic of poor field input validation, buffer overflow; as well as default configurations or mis-configured applications.
- Accessibility vulnerabilities, which are vulnerabilities inherent to the TCP/IP stack and the operating systems, such as denial of service and distributed denial of services.
- Authentication of the respondent device or devices. IP spoofing RIP attacks, ARP poisoning (spoofing), and DNS poisoning are all too common on the Internet. TCP/IP has some flaws such as untrusted machine status of machines that have been in contact with each other, and tacit assumption that routing tables on routers will not be maliciously altered.
- Data Verification, tampering, loss and theft, while on a local machine, while in transit, while at rest at the unknown third-party device, or devices, and during remote back-ups.
- Physical access issues, both the issue of an organization's staff not having physical access to the machines storing and processing a data, and the issue of unknown third parties having physical access to the machines.

4. Proposed Design And Implementation:

4.1. Proposed Design:

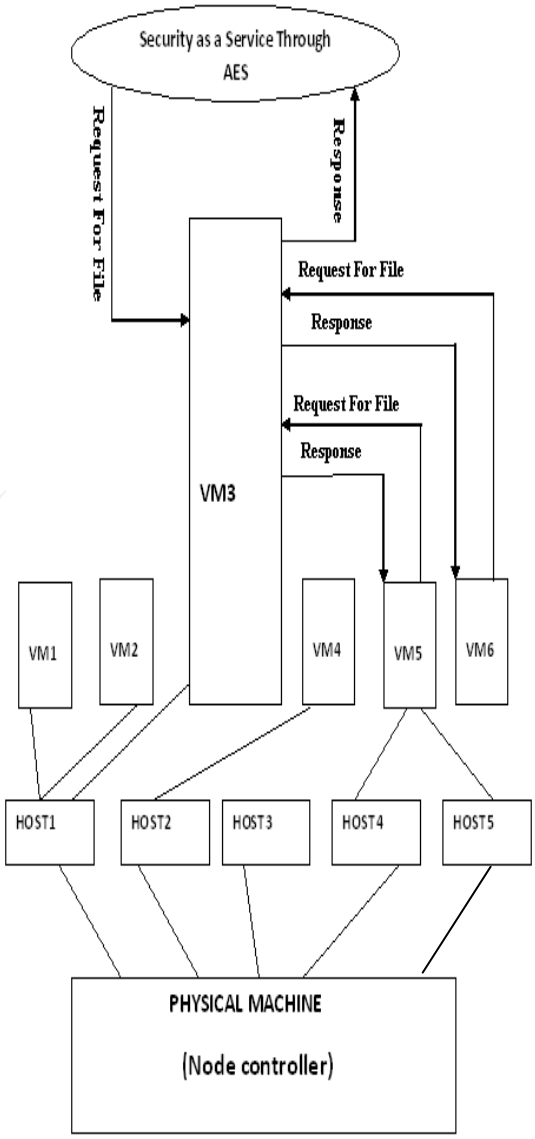

Figure 2

The above design is proposed for the file encryption problem for the end user in cloud environment.

In the above architecture, we have to make one virtual machine as security as a services provider and another one take security from security service provider through AES algorithm. With use of above design, main concern is to resolve the issues of security.

Better way to solve our security purpose regards file encryption and can more securely transfer the file.

4.2. Implementation

With the use of eucalyptus tool, we can make the cloud and through it, we have to develop one application and run that application in the cloud environment.

In the First step virtual machine; there is one virtual machine that can send the request for security of file to the security services provider virtual machine. Client can easily upload their file and encrypt it. So, any unauthorized person can't access file and can't read the content. If any client that can need that original file then it can decrypt with the key and get the file.

Security is main concern in the cloud environment where we can send some important files or data securely through encryption. The flows can easily be seen in this architecture and give wide ideas how one security as service provider machine accept the request from the user.

Through the AES Encryption, response can be send back to it and it is the easy way to give the response to the virtual machine. We have been using the lamp server to make one Graphical User Interface in which the client can easily upload files and use the encryption services from security service provider. Client can download that file and decrypt it.

5. Future work and conclusion

In my work, I have used AES and provided the file level security to end users of Cloud. To open secure file, user must need securely their confidential file in storage in secure manner or user can securely transfer their confidential files across the network. By this key, all data will be in encrypted manner. This approach is quite useful because it enables user to keep away the unauthorized person such that he cannot be able to read user files.

In my work I have provided the service for file level encryption. There is no inbuilt mechanism in Eucalyptus to initiate the file level encryption. So, it can be added in Eucalyptus. I have to resolve some more security related issues that can occur in cloud computing.

6. References

[1] Margaret Rouse, “cloud computing”, December 2010

[2] Margaret Rouse, “Virtualization”, December 2010

[3] Michael Adams, “Virtualization Basics”,Octomber 2011

[4] Lord CrusAd3r,"Cloud Computing Diffulties", Septermber 2010

[5] Wolf Halton Opensources & Security,” Security Issues and Solutions in Cloud Computing “, June25, 2010

[6]Farzd Sabahi, “Virtualization-Level Security in cloud computing”, 2011

[7]P.Sysam kumar R. Subramania and D.Thamizh Selvam,”Ensuring data storage security in cloud computing”, 2010