South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 81–86

ISSN No: 2454-9614

Featuring New Methods for Security of Data in Cloud

E. Pavithra, J.K. Keerthana*, A. Chandrasekar

Department of Computer Science & Engineering, SNS College of Technology, Coimbatore, Tamil nadu, India.

*Corresponding Author: E. Pavithra

E-mail: Pavibvn95@gmail.com

Received: 10/11/2015, Revised: 14/12/2015 and Accepted: 03/03/2016

Abstract

Cloud computing is used to reduce the expense of the users and the man power they use vastly for maintaining the servers that is mostly needed only for some particular days for important publishes or updates. Cloud can be regularly used for any purpose related to networks. There is a drawn back with this technique. The main issues nowadays are that the need of network facility to transfer data to cloud and related security problems during transfer of data. In this paper we feature the new idea to provide some better way for the data transfer in cloud.

Keywords:-security, encryption, keys, finger prints, RSA, blowfish, AES.

Reviewed by* **ICETSET'16 *organizing committee*

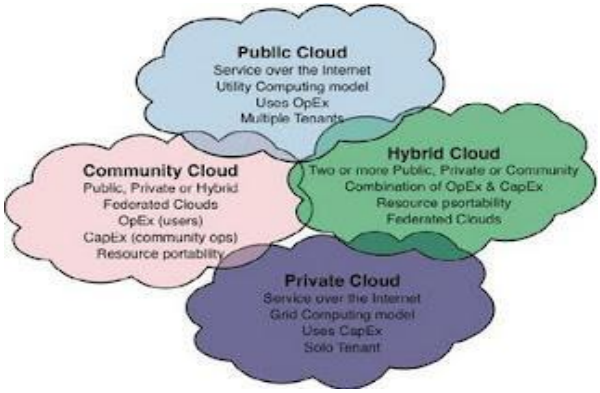
1. Introduction

1.1Cloud Computing

Cloud computing is defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud computing is comparable to grid computing, a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machine.

1.2 Cloud Computing Works

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive online computer games. To do this, cloud computing uses networks of large groups of server's typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them.



This sharedIT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

1.3 Infrastructure

In the most basic cloud-service model - and according to the IETF (Internet Engineering Task Force) - providers of IaaS offer computers – physical or (more often) virtual machines – and other resources. (A hypervisor, such as Xen, Oracle Virtual Box, KVM, VMware ESX/ESXi, or Hyper V runs the virtual machines as guests. Pools of hypervisors within the cloud operational system can support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements. IaaS clouds often offer additional resources such as a virtual-machine disk-image library, raw block storage, file or object storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles.IaaS-cloud providers supply these resources on-demand from their large pools of equipment installed in datacenters. For wide-area connectivity, customers can use either the Internet or carrier clouds (dedicated virtual private networks).

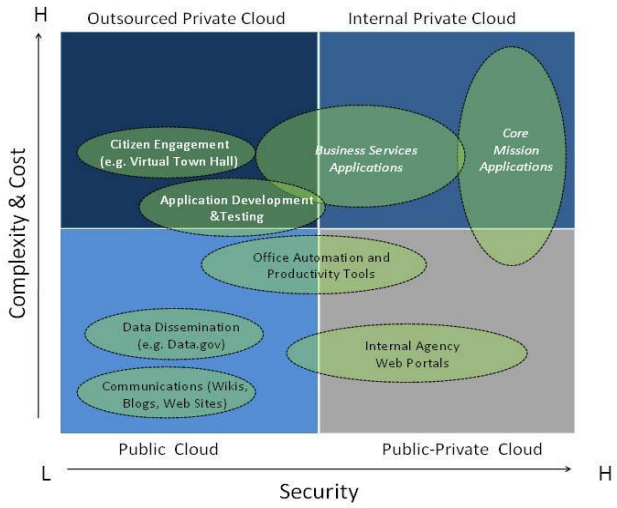
1.4 Architecture

Cloud architecture

The systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue. Elastic provision implies intelligence in the use of tight or loose coupling as applied to mechanisms such as these and others.

1.4.1 Private Cloud

Private cloud is the phrase used to describe a cloud computing platform that is implemented within the corporate firewall, under the control of the IT department. A private cloud is designed to offer the same features and benefits of public cloud systems, but removes a number of objections to the cloud computing model including control over enterprise and customer data, worries about security, and issues connected to regulatory compliance.



1.4.2 Private Cloud Security

A private cloud implementation aims to avoid many of the objections regarding cloud computing security. Because a private cloud setup is implemented safely within the corporate firewall, a private cloud provides more control over the company's data, and it ensures security, albeit with greater potential risk for data loss due to natural disaster.

A form of cloud storage where the enterprise and storage service provider are separate and the data is stored outside of the enterprise's datacenter.

1.4.3 Public Cloud

The cloud infrastructure is made available to the general public or a large industry group and is owned by an Organization selling cloud services and the comparison of private and public cloud.

1.4.4 Hybrid Cloud

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources.

Hybrid cloud service as a cloud computing service that is composed of some combination of private, public and community cloud services, from different service providers. A hybrid cloud service crosses isolation and provider boundaries so that it can't be simply put in one category of private, public, or community cloud service. It allows one to extend either the capacity or the capability of a cloud service, by aggregation, integration or customization with another cloud service.

Varied use cases for hybrid cloud composition exist. For example, an organization may store sensitive client data in house on a private cloud application, but interconnect that application to a business intelligence application provided on a public cloud as a software service. This example of hybrid cloud extends the capabilities of the enterprise to deliver a specific business service through the addition of externally available public cloud services.

2. Security and Privacy

Cloud computing poses privacy concerns because the service provider can access the data that is on the cloud at any time. It could accidentally or deliberately alter or even delete information. Many cloud providers can share information with third parties if necessary for purposes of law and order even without a warrant. That is permitted in their privacy policies which users have to agree to before they start using cloud services. Solutions to privacy include policy and legislation as well as end users' choices for how data is stored. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access.

According to the Cloud Security Alliance, the top three threats in the cloud are "Insecure Interfaces and API's", "Data Loss & Leakage", and "Hardware Failure" which accounted for 29%, 25% and 10% of all cloud security outages respectively - together these form shared technology vulnerabilities. In a cloud provider platform being shared by different users there may be a possibility that information belonging to different customers resides on same data server. Therefore, Information leakage may arise by mistake when information for one customer is given to other. "There are some real Achilles' heels in the cloud infrastructure that are making big holes for the bad guys to get into". Because data from hundreds or thousands of companies can be stored on large cloud servers, hackers can theoretically gain control of huge stores of information through a single attack a process he called "hyperjacking".

There is the problem of legal ownership of the data (If a user stores some data in the cloud, can the cloud provider profit from it?). Many Terms of Service agreements are silent on the question of ownership.

Physical control of the computer equipment (private cloud) is more secure than having the equipment off site and under someone else's control (public cloud). This delivers great incentive to public cloud computing service providers to prioritize building and maintaining strong management of secure services. Some small businesses that don't have expertise in IT security could find that it's more secure for them to use a public cloud.

There is the risk that end users don't understand the issues involved when signing on to a cloud service (persons sometimes don't read the many pages of the terms of service agreement, and just click "Accept" without reading). This is important now that cloud computing is becoming popular and required for some services to work, for example for an intelligent personal assistant (Apple's Siri or GoogleNow).

Fundamentally private cloud is seen as more secure with higher levels of control for the owner; however public cloud is seen to be more flexible and requires less time and money investment from the user.

2.1 Encryption

Encryption is an interesting piece of technology that works by scrambling data so it is unreadable by unintended parties.

2.2 Existing Algorithms for Cloud Security:

1. Triple DES
2. RSA
3. Blowfish
4. Two fish
5. AES

2.2.1 Triple DES

Triple DES was designed to replace the original Data Encryption Standard (DES) algorithm, which hackers eventually learned to defeat with relative ease. Triple DES uses three individual keys with 56 bits each. The total key length adds up to 168 bits, but experts would argue that 112-bits in key strength is more like it.

Despite slowly being phased out, Triple DES still manages to make a dependable hardware encryption solution for financial services and other industries.

2.2.2 RSA

RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet. It also happens to be one of the methods used in our PGP and GPG programs.

Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. You've got your public key, which is what we use to encrypt our message, and a private key to decrypt it. The result of RSA encryption is a huge batch of mumbo jumbo that takes attackers quite a bit of time and processing power to break.

2.2.3 Blowfish

Blowfish is yet another algorithm designed to replace DES. This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually.

Blowfish is known for both its tremendous speed and overall effectiveness as many claim that it has never been defeated. Meanwhile, vendors have taken full advantage of its free availability in the public domain.

Blowfish can be found in software categories ranging from e-commerce platforms for securing payments to password management tools, where it used to protect passwords. It's definitely one of the more flexible encryption methods available.

2.2.4 Two-Fish

Computer security expert Bruce Schneider is the mastermind behind Blowfish and its successor two fish. Keys used in this algorithm may be up to 256 bits in length and as a symmetric technique, only one key is needed.

Two-fish is regarded as one of the fastest of its kind, and ideal for use in both hardware and software environments. Like Blowfish, Two fish is freely available to anyone who wants to use it. As a result, you'll find it bundled in encryption programs such as Photo Encrypt, GPG, and the popular open source software True-Crypt.

2.2.5 AES: AES- Advanced Encryption Standard

A symmetric -key encryption standard. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. AES algorithm ensures that the hash code is encrypted in a highly secure manner. AES has a fixed block size of 128 bits and uses a key size of 128 in this paper.

1. Key Expansion
2. Initial Round
3. Add Round Key
4. Rounds

5. Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
6. Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
7. Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column
8. Add Round Key—each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.
9. Final Round (no Mix Columns)
10. Sub Bytes
11. Shift Rows
12. Add Round Key

3. Main Theme of the Paper

So for the techniques used for security purpose is based on the keys. As seen in encryption techniques the keys are used to encrypt and decrypt the data in cloud .And there is vulnerability during the data transfer in cloud network.

The suggested technique is, encrypt your data and compress your data during transfer and lock them using the **finger prints** of the clients. And also, transfer them by rearranging the packets. The sequence of the packets may be placed on any one of the packet as to support for recovery of data. This helps the unauthorized access of data during transfer in cloud. This is more secured because the finger prints are used to access the data.

4. Conclusion

The important thing that should be taken into account is security issues. The above specified approach will make some efficient security for the data that is being transferred in cloud in cloud.

Reference

[1] Q Chen,Q Deng, “Cloud and its Key Techniques”,Journal of Computer Applications,2009.
[2] F Dong,AB Song, “Architecture”Journal of China Institute,2011.
[3] Mipro, “Security Issues”,2010 Proceedings of the 33rd International Convention.
[4] R Basmadjan,”Issues of Cloud Computing”,2012, Springer.
[5] Gartner “7 Cloud Computing Security Risks”,July 2008.
[6] Cloud Security Allience, Security Guidence for Crital areas of focus in Cloud Computing,December 2009.
[7] I. Foster, Ian; Y. Zhao, I. Raicu, and S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared," Grid Computing Environments Workshop, 12-16 Nov. 2008.
[8] B. Sotomayor, et al, "Virtual Infrastructure Management in Private and Hybrid Clouds", IEEE Internet Computing, Sept. 2009.
[9] R. He, J. Niu, M. Yuan, and J. Hu, "A Noval Cloud-Based Trust Model for Pervasive Computing", The Fourth International Conference on Computer and Information Technology,Sept. 14-16 2004, pp. 693-700.
[10] A. Cavoukian, "Privacy in The Clouds",http://www.ipc.on.ca/ image/Resources%5Cprivacyintheclouds.pdf.
[11] C. Hoffa, et al., "On the Use of Cloud Computing for Scientific Workflows," IEEE Fourth Int'l Conf. on eScience,Dec. 2008.