A Study on Cloud Computing and its Security Issues

[1]Mr. Venkata Sreedhar Ventrapragada, [2]Daniel Ravuri, [3]G Jyothi

[1, 2, 3] Department of Information Technology, Vignan's Institute Of Information Technology, Duvvada, Visakhapatnam- 530049, A.P., INDIA.

Abstract

"Cloud computing" was coined for what happens when services and applications are propelled into the internet "cloud." Cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the devices used to access these services and applications do not require any special applications. Advances in service oriented architecture (SOA) have brought the world close to the once imaginary vision of establishing and running a virtual business, a business in which most or all of its business functions are outsourced to online services. Cloud computing offers a realization of SOA in which IT resources are offered as services that are more affordable, flexible and attractive to businesses. Secure delivery of data to and from the cloud is however a serious issue that needs to be addressed. This paper illustrates Cloud Computing architecture, working and service models and exemplifies homomorphic encryption as a solution for dealing with these serious security concerns for accessing the cloud data.

Keywords: *Internet cloud, service oriented architecture (SOA), homomorphic encryption.*

1. Introduction

Cloud computing is the ability to rent a server or a thousand servers and run a geophysical modeling application on the most powerful systems available anywhere [10]. It can be the ability to rent a virtual server, load software on it, turn it on and off at will, or clone it ten times to meet a sudden workload demand. It can be storing and securing immense amounts of data that is accessible only by authorized applications and users. It can be supported by a cloud provider that sets up a platform that includes the OS, Apache, a MySQL™ database, Perl, Python, and PHP with the ability to scale automatically in response to changing workloads. Cloud computing can be the ability to use applications on the Internet that store and protect data while providing a service. It can be using a storage cloud to hold application, business, and personal data. Cloud Computing, the long-held dream [4] of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Ironically, the recent global economic recession served as a booster for interest in cloud computing technologies as organizations sought for ways to reduce their IT budget, while keeping up with performance and profits. The cloud computing buzz began in 2006 with the launch of Amazon EC2, gaining traction in 2007 as seen in the figure (1).

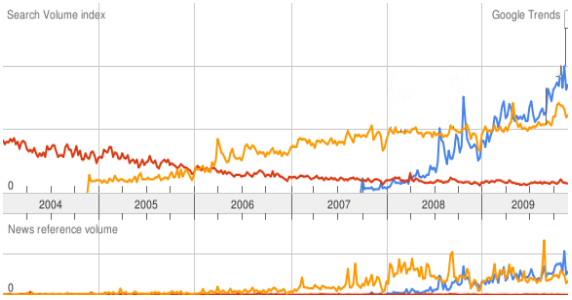

Figure (1): Search & News Volume for Cloud Computing- April 2011.

Cloud computing is represented by blue line the Red and Orange lines represents Grid computing and Virtualization. Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud. And it can be the ability to use a handful [5] of Web services to integrate photos, maps, and GPS information to create a mash up in customer Web browsers.

2. Architecture

Cloud computing architecture, just like any other system, is categorized into two main sections.

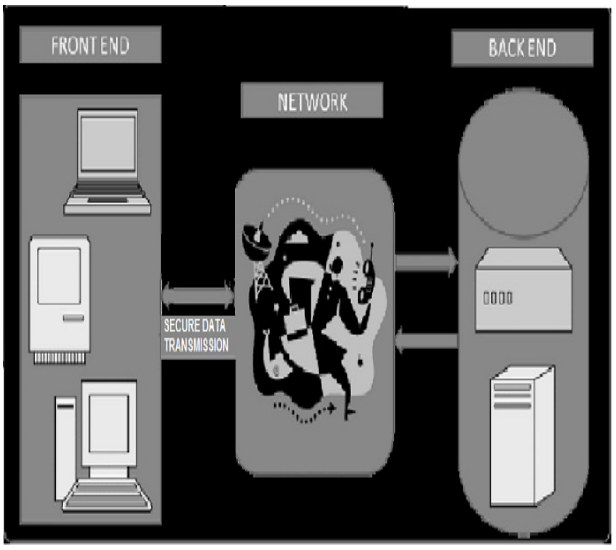

Figure (2): Cloud Computing Architecture

Front end, which can be end user/ client/ application which use's cloud services as shown in figure(2). Back End, which is the network of servers with any data storage system and computer program [1]. Cloud contains infinite storage capacity and it has different applications that are hosted on their own dedicated server farms.

Cloud has server follows protocols, commonly known as middleware. Centralized server balances client supply, monitors traffic, avoids congestion, adjusts demand and administers the system. Middleware controls the communication of cloud network among them. Data security is the top most priority in all the data operations of cloud [7]. Here, all the data are backed up at multiple locations which increases the data storage to multiple times in cloud compared with a regular system. Redundancy of data is a must-have attribute of cloud computing which is very crucial and important.

3. Working

In a large corporation it is the responsibility of that firm to make sure that all of its employees have the right hardware and software they need to do their jobs. Buying computers for everyone isn't enough there is a necessity to purchase software/ software licenses to provide the tools they require [3]. There is also a necessity to make sure that the current software license allows another user whenever there is a new hire, which is very expensive. Instead of installing a suite of software for each computer there is an alternative this, you'd only have to load one application. That application would allow workers to log into a Web-based service which hosts all the programs the user would need for his or her job. Remote machines owned by another company would run everything from e-mail to word processing to complex data analysis programs. It's called cloud computing, and it could change the entire computer industry. There are different characteristic features [6] like, On-demand self-service, Rapid elasticity, Pay per use associated with this working.

4. Service Models

Cloud computing providers offer their services according to three fundamental models as shown in figure(3).

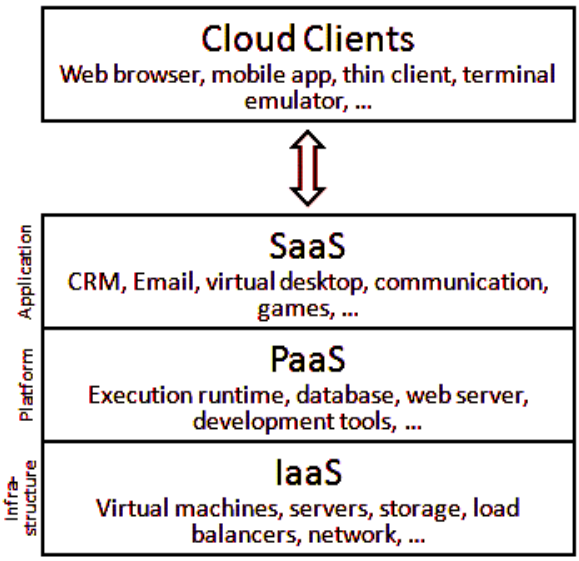

Figure (3): Service Models- Block diagram

4.1 Infrastructure as a service (IaaS)

In this most basic cloud service model, providers offer computers, as physical or more often as virtual machines, and other resources. The virtual machines are run as guests by a hypervisor which are managed by the cloud operational support system leads to the ability to scale to support a large number of virtual machines. Other resources in IaaS clouds include images in a virtual machine image library, raw and file-based storage, firewalls, load balancers, IP addresses, VLANs, and software bundles. STaaS - STorage As A Service. Amazon EC2 [12] is the best example for IaaS.

4.2 Platform as a service (PaaS)

In the PaaS model, cloud providers deliver a computing platform typically including operating system, programming centralized server administration system and this language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing [8] the underlying hardware and software layers. For example- Windows Azure Compute[11].

4.3 Software as a service (SaaS)

In this model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients [2]. The cloud users do not manage the cloud infrastructure and platform on which the application is running. This eliminates the need to install and run the application on the cloud user's own computers simplifying maintenance and support. For example like Google apps.

5. Security Issues

Security has always been the main issue for IT Executives when it comes to cloud adoption. In two surveys carried out by IDC in 2008 [13] and 2009 [14] respectively, security came top on the list (see Figure 4).

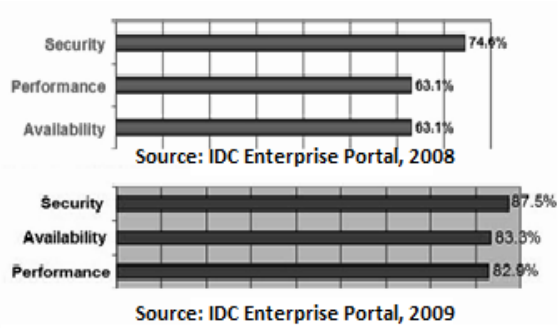

Figure (4): Top 3 issues with the cloud/on-demand model

Cloud computing is a collection of technologies, operating systems, storage, networking, virtualization, each fraught with inherent security issues. As denial of service attacks, browser based attacks, and network intrusion become carry over risks into cloud computing. There are potentials for a new wave of large-scale attacks via the virtualization platform. Chow et al. described the "Fear of the Cloud" by categorizing security concerns into three traditional concerns, data security, availability and third party data control. Cloud companies are also able to afford a dedicated security team and invest more in security infrastructure. Other benefits noted in include rapid smart scaling of resources, standardized security interfaces and an overall benefit of scale.

Some of the pressing security issues in cloud computing include:

5.1 Data Security

This risk stems primarily from loss of physical, personnel and logical control of data. Issues include virtualization and SaaS vulnerabilities [15], potential data breaches and phishing scams [16]. Other data security risks mentioned in include loss of encryption keys, data interception and leakage, economic and distributed denial of service. The inability to fully segregate data or isolate separate users can lead to undesired exposure of confidential data in the investigation of a situation involving co-tenants. Hypervisor vulnerabilities can also be leveraged to launch attacks across tenant accounts.

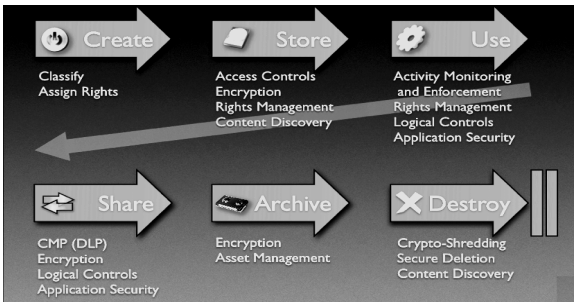

Figure (5): Data Security Lifecycle.

Data containing health data, financial info social and national insurance details raise issues about access controls, authorization and rights management. It is hard to maintain ACID (atomicity, consistency, isolation, durability) properties of during data replication over large geographic zones as pointed out by Abadi. Data persistence or remembrance remains an issue due to distribution and replication of data even after a user has left a cloud provider. Figure (5) shows a data security lifecycle model.

5.2 Availability

This is one of the prime concerns of mission and safety critical organizations. Availability concerns are also need to move to uptime periods of current provider, another provider or long-term viability of the cloud provider as noted in [17]. Table 1 shows some well-known outages of leading cloud providers

Cloud Service	**Outage Duration**	**Dates**
Amazon S3	7 hours	20th Jul , 2008
Google Gmail, Apps	24 hours	11th Aug , 2008
Google Gmail	30 hours	17th Oct, 2008
FlexiScale	18 hours	31st Oct, 2008
Salesforce.com	40 minutes	6th Jan, 2009
Windows Azure	22 hours	13th-14th March, 2009

Table 1: Cloud Service Outrages

5.3 Third-Party Control

As, the value of corporate information is growing the third party access can lead to a potential loss of trade secrets and intellectual property. There is also the issue of a malicious insider who abuses access rights to tenant information. The fear of corporate espionage and data warfare also stems from third party control. Provider compliance with regulations such as those on auditing also raise questions on how that can be effected on site

in a globally distributed multitenant environment [17]. A situation may also arise in which the user can freeze to a particular vendor may be because of the difficulty in migrating data to a new vendor. Risks like prompt disaster recovery may also arise due to third party data control.

5.4 Privacy and Legal Issues

Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Pearson [18] summarized the main privacy issues of cloud computing. Users are made to give away their personal information without knowing where it is stored or what future purpose it might serve. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors who expose sensitive information risk legal liability. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks.

6. Potentials of Homomorphic Encryption

Issues like data security, third-party control and privacy and legal issues could be solved if all data like financial, personal, health etc., stored in the cloud were encrypted. However, a user would be unable to leverage the power of the cloud to carry out computation on data without first decrypting it, or shipping it entirely back to the user for computation. The cloud provider thus has to decrypt the data first, perform the computation then send the result to the user. What if the user could carry out any arbitrary computation on the hosted data without the cloud provider learning about the user's data - computation is done on encrypted data without prior decryption. This is the promise of homomorphic encryption schemes which allow the transformation of ciphertexts *C(m)* of message m, to ciphertexts *C(f(m))* of a computation/function of message m, without disclosing the message. The idea was first suggested by Rivest, Adleman and Dertouzos in 1978, referred to as privacy homomorphisms [19].

An encryption scheme can be said to be fully homomorphic if:

$$E(m_1 \ \Theta \ m_2) \leftarrow E(m_1) \ \Theta \ E(m_2) \ ; \ \forall \ m_1 \ , \ m_2 \ \in \ M \quad (1)$$

Where in equation (1),

M – Plaintexts,

Θ - Any arbitrary function &

$\leftarrow$ - Computation without decryption of plaintexts

The 1st fully homomorphic encryption system was proposed by Craig Gentry using ideal lattices in 2009 [20]. Gentry's approach employed devising a somewhat homomorphic scheme, and then bootstrapping it to get a fully homomorphic scheme. Since then researchers have proposed variants and improvements to Gentry's model.

7. Conclusion

Cloud computing offers a radical way of collaborating, delivering applications and content. So it is easy to see why the enablers are paving the way for massive adoption of the cloud. The strength of cloud computing in information risk management is the ability to manage risk more effectively from a centralize point. The security issues with cloud computing can be avoided by implementing some encryption and decryption scheme's as shown in this study. The enterprises will be better off with a long term vision for technology, people, information, legality and security to leverage capabilities offered by cloud computing. The shift into the cloud computing should be planned and it should be done gradually over a period of time.

References

[1] L. Tang, J. Dong, Y. Zhao and L. Zhang "Enterprise Cloud Service Architecture", 3rd IEEE International Conference on Cloud Computing, Miami, FL, USA, July 5-10,2010.
[2] Software as a service, Wikipedia, http://en.wikipedia.org/wiki/Software_as_a_service.
[3] Wikipedia, http://en.wikipedia.org/wiki/Virtualization
[4] Michael Miller, "Cloud Computing Pros and Cons for End Users", microsoftpartnercommunity.co.uk, 2009.
[5] Wiki, http://en.wikipedia.org/wiki/Cloud_computing
[6] Y. Chen, X. Li and F. Chen, "Overview and Analysis of Cloud Computing Research and Application", International Conference on E -Business and E - Government (ICEE), May 2011.
[7] Y. Luo,"Network I/O Virtualization for Cloud Computing", IEEE Computer Society, Oct. 2010.
[8] K. Chard, S. Caton, O. Rana and K. Bubendorfer, "Social Cloud: Cloud Computing in Social Networks", 3rd IEEE International Conference on Cloud Computing, Miami, FL, USA, July 5-10, 2010.
[9] T. Dillon, C. Wu and E. Chang, "Cloud Computing: Issues and Challenges", 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.
[10] Introduction to Cloud Computing, White Paper,Dialogic Corporation, 2010.
[11] Windows Azure, http://www.windowsazure.com/en-us/
[12] Overview of Amazon Web Services, http://media.amazonwebservices.com/AWS_Overview.pdf
[13] IT Cloud Services User Survey, pt.2: Top Benefits & Challenges. Retrieved April 8, 2011 from http://blogs.idc.com/ie/?p=210.
[14] New IDC IT Cloud Services Survey: Top Benefits and Challenges. Retrieved April 8, 2011 from http://blogs.idc.com/ie/?p=730.
[15] VMware Shared Folder Bug Lets Local Users on the Guest OS Gain Elevated Privileges on the Host OS. Retrieved April 9, 2011 from 69178. ACM, 2009
[16] http://securitytracker.com/alerts/2008/Feb/1019493.html

[17] Salesforce.com Warns Customers of Phishing Scam. Retrieved April 9, 2011 from http://www.pcworld.com/businesscenter/article/139353/salesforcecom_warns_customers_of_phishing_scam.html.

[18] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R.Masuoka, and J. Molina. Controlling data in the cloud: Outsourcing computation without outsourcing control. In ACM Workshop on Cloud Computing Security, 2009.

[19] Gupta, Priyanka, and Ashok Verma. "Establishing a Service Model of Private Elastic VPN for cloud computing cloud computing."

[20] Pearson, S. Taking account of privacy when designing cloud computing services. In ICSE Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, Canada, 2009.

[21] R. Rivest, L. Adleman, and M. Dertouzos. On data banks and privacy homomorphisms. In Foundations of Secure Computation, pp. 169–180, 1978.

[22] C. Gentry. Fully homomorphic encryption using ideal lattices. In Proc. of STOC, pages 1.