A Flexible Interface for Security Issues in Cloud Computing

B. Chandrasekhar, Derick Mathew, and K. A. Sumithra Devi

***Abstract*—Cloud computing is a steadily growing technology. It brings advantages and vulnerabilities with it. A vendor has to consider that a smart customer will ask tough questions especially with regard to the security issues. Changes will have to be made such that these changes will not stunt the growth of the cloud. A way of bringing normalization while allowing a free hand to the vendor has to be considered and in this paper we are discussing a flexible interface for the various cloud services that are available.**

***Index Terms*—Cloud computing, security, flexible interface.**

I. Introduction

The world of computing has seen a large number of changes in past few years but just a few of them have had an impact as huge or as industry moving as the arrival of the cloud computing paradigm. By definition Cloud Computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service. Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Furthermore, cloud computing employs a model for enabling available, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[1].These technologies are not all new most of these have been in use in of themselves but they have come to be presented together to hold allow a greater level of flexibility to the user. Educare in their paper "7 things you should know about cloud computing" put it best when they said the term cloud computing refers to the delivery of scalable IT resources over the Internet, as opposed to hosting and operating those resources locally, such as on a college or university network. Those resources can include applications and services, as well as the infrastructure on which they operate. By deploying IT infrastructure and services over the network, an organization can purchase these resources on an as-needed basis and avoid the capital costs of software and hardware. With cloud computing, IT capacity can be adjusted quickly and easily to accommodate changes in demand. [2]

A. Services Provided by Clouds

The services that cloud computing hosts provide are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) & Software-as-a-Service (SaaS).

Infrastructure-as-a-Service provides virtual server instances or blocks of storage on demand. Customers use the provider's application program interface (API) to start, stop, access and configure their virtual servers and storage.

Platform-as-a-service in the cloud can be defined as a set of software and product development tools hosted on the provider's infrastructure so that developers can create applications on the provider's platform over the Internet. Platform as service providers may use APIs, website portals or gateway software installed on the customer's computer.

Software-as-a-service cloud model has the vendor supplying the hardware infrastructure, the software product and interacting with the user through a front-end portal.

B. Advantages of Cloud Computing

Cloud computing allows the user to reduce his or her cost so that the saved money can be used for other important resources. Clouds also allow organizations to increase their storage capacity as it is easier to store more data on clouds rather than on private computer systems. It does not need IT professionals to maintain and update the softwares as these are responsibilities that are shouldered by the service provider, and allows a greater amount of data mobility. Since the organization no longer has to spend a large time on the hardware and software as of such the organization can spend more energy into other aspects of their business.

Cloud computing allows for scalability and if used efficiently by the user it can bring the organization to pay way less than when they were running on their own systems or servers

II. Solution Proposed

A. Areas of Change

Having seen the structure and working of cloud computing technologies, it seems evident that the only solution that can be found is in the normalization of the standard set by the various vendors. Setting standards that are generally accepted and adopted by the various vendors can bring a greater flexibility to users and also improve the appeal that cloud computing has. Providing standards would also allow users to easily shift or transfer between vendors.

Another aspect that needs consideration is security, the measures of security that has been used to secure data this far within organizational servers will fall short and will not be able to withstand the threat that malicious users of the cloud could pose. Suggesting a single method of security is not feasible for obvious reasons and each cloud vendor or service provider would like to incorporate a different kind and measure of security.

The final aspect that this paper looks at changing is the aspect that the data that is put up on the cloud has to be allowed to interactive with other clouds from other cloud providers. This would imply that a user can buy a storage

Manuscript received September 13, 2012; revised November 18, 2012.

The authors are with Dept of Mca, Rvce, Bangalore, India (e-mail: bchandra72@gmail.com, derick.j.mathew@gmail.com, sumithraka@gmail.com).

cloud from one cloud vendor and a certain set of services and applications from another vendor.

B. Need for Normalization

The cloud is still in an early stage of development and normalization on large scales will stunt growth for this technology There is a need for normalization that will include openness of certain details such as the area / country where the data is being stored as well as the license that is being followed by the vendor and these may be varied to provide a standard that will not impose on the growth rate of this technology.

C. Need for Security Changes

Smart customers will ask tough questions and consider getting a security assessment from a neutral third party before committing to a cloud vendor. [3]

D. Vulnerabilities in Cloud Computing

The cloud has had much vulnerability that is yet to be worked on, most of these problems are not relatively new but are by products and vulnerabilities that have been carried forward with the technologies that have helped in implementing cloud computing. The most prominent of these vulnerabilities include Web application vulnerabilities, such as cross-site scripting and sql injection. 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 "unfixable flaws" such as "trusted 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.

Privacy and control issues stemming from third parties having physical control of a data is an issue for all outsourced networked applications and storage, but cloud architectures have some specific issues that are distinct from the usual issues.

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]

III. The Interface Explained

To incorporate these changes and to apply them successfully, an interface that would allow modules that are standardized can be built, similar to a web browser but one that is customized to fit the requirements of the cloud computing environment. The cloud interface should have standards that let the user access the various clouds that have been bought by the user and also be able to transfer data safely between each of these clouds. The various cloud vendors having set various security measures have to be taken into account and the cloud interface should allow the connection to be made directly from one cloud to the other or through a third system, namely the users system. The second method may increase the time taken but may very well decrease the number of security issues that may rise with sharing clouds [5].

The normalization has to be across the wide range of vendors that will not only allow the users of the cloud but the vendors as well, as the availability of normalized clouds would allow cloud computing a larger base by removing a few of the hurdles that are posed by cloud vendors. The availability of normalized clouds can allow various levels of security for the various kinds of clouds. One of the major setback of security standards being set for the cloud includes a lack of set standards for the various types of clouds the standardization of the clouds will allow the vendors to work with greater ease as the architecture of the various clouds can be standardized and a known limit can be set as the area to be worked on thus allowing measures to be placed [6].

The security measures that have been implemented thus far will not be as effective as it has been over the past for the web as the cloud also provides infrastructure and services at a much larger scale. The various security measures that can be incorporated vary over time but the changes are not always readily accepted by the vendors and normalizing the cloud just for every algorithm or method is not feasible but it is accepted to let the basic interface have a set security measure and the vendor choose a second security module to be incorporated or applied over the basic module. This method of security modules will allow a user (here seen as an organization) to access the cloud from various systems with various permissions to access the cloud and work on the same. The various access levels for the data, services, etc. will be helpful in giving the authorization of access to the same for the members of the organization with greater ease and also security. Since the log of all users logging in will be stored, a user will allow the user The will also allow a normal view of the cloud to be shown as presented by a normal folder with various clouds to be accessed as subdirectories within the interface once the cloud has been signed into. The implementation of clouds can also allow the user to have a clearer idea of how much time was actually used by the user over various interfaces and will also log when multiple users log in and access the same cloud [7]. Hence the administrators can request for and view the list of users who have logged and accessed the cloud. This will allow the administrator to grant or revoke permission to various interfaces thereby restricting disgruntled employees from accessing the cloud if and when they are fired which a major issue was before.

IV. Conclusion

There is a need to provide a standard for the various vulnerabilities that are found as well as introduced into cloud computing but these need to be flexible that allow vendors to implement their own methods of security and encryption but need to give the user a easy to use and clear understanding of the technology that they are using.

The largest gaps between cloud-security practice and cloud-security research lies in the fact that the assumptions in the research leave out some very important differences between cloud security and virtual machine security. One of

the way is to monitor the cloud's management software, and another might be development of isolated processing for specific clients' applications. Having a way to tell whether the virtual machines in the cloud are patched properly would also be a useful part of the framework. People's behavior can be tracked and monitored; for instance whether people allow the automated patching software to run, or updating anti-virus software definitions (on virtual machines running operating systems that are susceptible to viruses, worms and other such malware), or whether people understand how to harden their virtual machines in the cloud.

ACKNOWLEDGMENT

I thank RSST, Principal R. V. College of engineering, Director of Dept., of MCA, for providing me this great opportunity to take up this work and encouraging me to complete it.

I thank IJMLC for providing me this great opportunity and publishing in the International Journal

I thank all my colleague, friends and family for their constant support and encouragement.

REFERENCES

[1] F5 Networks "Cloud computing survey results June-July 2009," pp. 6.
[2] E. Mills, "Cloud computing security forecast: clear skies," *CNET News*, 2009.
[3] *EDUCARE*, "7 things you should know about cloud computing," pp. 1. [Online].Available: www.educause.edu.
[4] Assessing the security risks of cloud computing. *Gartner's.* [Online].Available: www.gartner.com, June 2008.
[5] N. Wienberg. Cloudy picture for cloud computing. [Online]. Available: http://www.networkworld.com/news/, 2008.
[6] M. Miller, "Cloud computing: web-based applications that change the way you work and collaborate online," [Online]. Available: www.Amazon.com, August 2008.
[7] A. Basta and W. Halton, "Security issues and solutions in cloud computing," Wolf, *Cloud Computing Tech Security*, June2010.

B. Chandarashekhar has 10 years of experience in teaching and 3 years of industry. Currently working as Asst. Professor at R.V. College of Engineering, Bangalore from July 2005 to till date, Worked as lecturer at KLES's S. Nijalingappa College, Bangalore, from Aug 2000 to June 2005. Worked as member of technical staff at BBS, Bangalore from Oct 1997 to Nov 1998. Worked as Software Engineer at Aeronautical Development Establishment, Bangalore from August 1996 to Sept 1997