Addressing Trust Issues in Cloud Computing

Manoj Prabhakar Darsi[#1], Vinay Babu D*[2], Gayathri Darsi[#3]

[1]*Assistant Professor &CSE&JNTUK, Chalapathi Institute of Technology, Mothadaka Guntur – 522016, India*
[2]*Assistant Professor&CSE&JNTUK, Chalapathi Institute of Technology, Mothadaka Guntur – 522016, India*
[3]*PG Scholar&CSE&JNTUK, KITS, Vinjanampadu, Guntur-522017, India*

Abstract: *Cloud computing is an evolving paradigm with tremendous momentum, but its unique aspects exacerbate trust issues in cloud computing. Data is the most valuable of clients (or) company's asset; it must be protected with much vigilance than any other. Data Security in the cloud is one of the big issue which acts as obstacle in the implementation of cloud computing. This article explores about different trust issues in cloud computing for trustworthy cloud computing environment.*
Keywords: SAS,PaaS,IaaS,SaaS.

I. INTRODUCTION

Cloud computing is an Internet based computing, where resources are shared, software and information are provided to computers and devices on-demand. It provides to people the way to share distributed resources and services that belong to different organization. Since cloud computing uses the distributed resources in open environment, thus it is important to provide the trust and security to shared data for developing cloud computing applications.

Cloud computing is now days as emerging field because of its performance, high availability and low cost. In cloud many services are provided to the client by cloud. Data store is main function that cloud service provides to the companies to store huge amount of storage capacity.

1. RIGHT TO AUDIT CONSIDERATIONS
Auditors need to be involved with their organization cloud computing plans right from the idea conception stage to help ensure the identification and mitigation of risks. So many aspects should be considered by auditors while reviewing a cloud computing project.

The criticality of the application being sent to cloud. While is it less risky to start with, sending non-critical applications to the cloud (for example, budgeting and expense tracking tools), significant applications such as business-to-business (B2B) or business-to-consumer (B2C) web site should be moved to the cloud only after careful consideration.

Country or regional regulations that affect the organization's business and requires the specific safeguards. The Industry regulations such as the Gramm-Leach-Bliley Act (GLBA) in the US require the safeguards to protect the client's nonpublic personal information, depend up on how the organization collects, stores and use the information. Under US model of privacy, consumers have the choice to opt out of the information being shared with affiliated parties. In European Union, Canada and some other countries, the privacy laws are stringent and require specific opt in by consumers.

Auditor examining the cloud vendor's policy on vulnerability management and reporting (beyond basic "contact us" web site links), commitment's to following up on potential security incidents, and ability to respond promptly to the reports of

Cloud user experience with the service level agreements (SLAs) and vendor management.

Auditors gaining independent assurance about the controls at the cloud service provider, whether an independent auditor's report or through audit rights in the agreement. The independent auditor's reports could be a Statement on Auditing Standards (SAS) No. 70 or Trust Services report, depending on the type of processes and application outsourced.

2. SECURITY

Cloud computing security (cloud security) is an evolving sub-domain of network security ,computer security and more broadly information security. It refers to a broad set of the technologies, policies, and controls deployed to protect applications, data and

the associated infrastructure of cloud computing. The Cloud security is not to be confused with security of software offered as "cloud based" (security-as-a-service).

There are so many of security issues or concerns associated with the cloud computing but these issues fall into two broad categories: 1.Security issues faced by cloud providers and 2.Security issues faced by their customers.[1] In most cases, provider must ensure that the infrastructure is secured ,their client's data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.

3. THE ROLE OF STANDARDS IN CLOUD COMPUTING ENVIRONMENTS

Cloud users would particularly welcome standards that address the workload migration and data migration use cases because such standards would mitigate to vendor lock-in concerns. This requires the Standardization of virtual machine image file formats and APIs for cloud storage.

Standardization for the user-authentication use case has the advantage that user identities based on OpenID or authentication protocols based on OAuth, for example, could be used across multiple providers that support these standards.

Similarly, the standardization to support the work load-management use case would leverage any existing efforts related to the construction of workload management clients and scripts that could be used across multiple providers more from standardization than others. The remaining section looks at how PaaS ,IaaS and SaaS would benefit from standardization.

3.1 Infrastructure as a Service (IaaS)

IaaS is the service model that would benefit from standardization because of main building blocks of IaaS are workloads represented as virtual-machine images and storage units that vary from typed data to raw data .

For workload migration, standards efforts such as OVF and VHD would allow users to extract an image from one provider and upload it to another provider. Given that most IaaS providers allow to consumers to install and run in any operating system, a manual and time-consuming form of migration would be retrieve the image from the current provider, create a new image on a new provider, and reinstall software. This manual migration would not require standards as long as there is a way to retrieve the application state (e.g., application data, files, running processes) from the source image and move it to a new image. The cloud will offer the advantages of ease of development and tool availability.

For data migration, standards efforts such as CDMI and the Amazon S3 API, which multiple providers support, would enable users to extract data from one provider and upload it to a different provider. If a provider implements these standard interfaces using SOAP- or REST-based protocols, the cloud will offer the advantages of ease of development and tool availability.

3.2 Platform as a Service (PaaS)

The PaaS service model benefits less from standardization than IaaS. Organizations that buy into PaaS do it for the perceived advantages of the development platform. The platform provides number of capabilities out of the box, such as user authentication, managed application environments, data storage, reliable messaging and other functionality in the form of libraries that can be integrated into applications. The functionality is tied to a specific language and runtime environment. For example, Google App Engine supports applications written in Java, Python, and Go. Microsoft Azure supports applications written in .NET, and more recently applications written in Java, PHP, and Node.js

3.3 Software as a Service (SaaS)

SaaS is a somewhat different from the IaaS and PaaS because it is a licensing agreement to third-party software instead of a different deployment model for existing resources that range from data storage to applications .Benefits of standardization for SaaS are even more limited than PaaS. For SaaS offeres such as Salesforce.com and CRM. However, there are other SaaS offerings such as Google Maps or Yahoo Social in which the user can be a developer who is

integrating functionality from these services into other applications [Google 2012c, Yahoo! 2012]. In the latter case standardized APIs are useful because they facilitate the development process [Linthicum 2010a] However, unless the APIs are identical from a functional perspective, this standardization helps little with migration.

4. PERFORMANCE ISSUES

The system can effectively provide a service. From the user point of view, poor performance and non-availability of service are the same. Users will not accept slow performance regardless of where the problem is. Poor application performance causes companies to lose the customers reduce employee productivity deal with the service outage reduce bottom line revenues deal with general lost productivity.

Application performance can vary significantly based on delivery environment. Businesses must ensure that the application performance is optimized when it is moved from a data center to a cloud computing infrastructure or it is written to take advantage of the benefits of the cloud. You keep in mind that ensuring the minimum performance level across the cloud could be challenging.

5. IAM AND DATA MANAGEMENT

Cloud security is a topic that enjoys coverage by thousands of voices and nearly as many vendors offering services and products aimed at taking the pain out of moving data and applications to the cloud. Perhaps no more onerous is the topic of trust placed in individuals. When you move to the cloud the people who you are asked to trust grows exponentially and there are those who say this is indeed the most difficult of security concerns.

Managing identities and access control for enterprise applications remains one of the greatest challenges facing IT today. While an enterprise may be able to leverage several Cloud Computing services without a good identity and access management strategy, in the long run extending an organization's identity services into the cloud is a necessary precursor towards strategic use of on-demand computing services

So you not only have to ensure the people YOU trust are trustworthy, but ultimately you have to extend that person's ability to manage your data into the cloud along with an identity and access management (IAM) scheme that is bullet proof. Along the way you will inevitably be extending trust to the people who the cloud vendor hires and has placed its trust in. With so much at stake you really can't assume the person you are trusting today with the keys to the kingdom will remain trustworthy. To complicate things you will want to leverage investments already made in IAM at the enterprise level, but they may be difficult to extend to the cloud.

For Identity Provisioning the CSA says those functions offered by cloud vendors are not currently adequate for enterprise requirements and you should resist vendor proprietary solutions like custom connectors and insist instead on standard connectors that use the SPML schema.

When it comes to SaaS and PaaS the authentication, authenticated users with your identity provider and used for trust with the SaaS vendor. The CSA recommends enabling the use of a single set of credentials valid across multiple sites for individual users and to avoid vendor proprietary methods. The alliance says using a dedicated VPN for IT personnel will help them leverage existing investments.

As with most things in life, nothing is really guaranteed and that's probably the Andy Grove, the CEO of Intel once quipped "only paranoid survive." When it comes to the people the trust is like to think is well placed and in most cases it probably. There is always a "but" though.

The Essentials of Managing The Data in Cloud Computing

The issues surrounding the data in the cloud environment is a big and complicated topic. The reality is that data is the life of an organizations. Therefore how you are going to manage data, regardless of where it stores, is critical to the health of your business. Data has a lifecycle, It's created, changed, stored (or destroyed), secured, and governed. Although this is the normal process within data storage center, forgetting

management elements is easy, when an outside service manages the data.

- Comparing the Traditional Data Center with Cloud Data Center Operating Costs: Ultimately Cloud computing services are attractive because of cost is likely to be far lower than providing the same service from your traditional data center, so it helps to understand.

- How to Scale the Cloud in Cloud Computing: From the cloud provider's point of view, the whole cloud computing is to achieve the economies of scale by managing a very large collection of computing resources in a highly economic and efficient fashion.

- How to Locate the Data in Cloud Computing : After data goes into the cloud, you do not have any control over where your company's data is stored in data center. Consider these may issues connected with cloud computing services.

- How to Control Data in Cloud Computing: Control of data in the cloud computing environment includes the governance policies set in place to make sure that your data can be trusted and maintaining integrity, reliability, and confidentiality of your data.

- How to Secure the Data Transport in Cloud Computing: When transferring data in the cloud computing environment, keep two things in mind: Make sure that no one can intercept your data as it moves from point A to point B in the cloud, and make sure that no data loss.

- How to Talk to Cloud Computing Vendor about Data: You're thinking about using some of the data services available for cloud computing. Before taking a contract, remember that data (especially your company's data) is a precious asset and you need it.

6. AVAILABILITY

The infrastructure-as-a-service (IaaS) of a company that completely reengineered the delivery of cloud computing, today announced that general availability of true High Availability (HA) virtual data centers for business-critical cloud deployments. This new feature enables an easy-to-use implementation and offers the dynamic routing of IPv4 addresses to virtual machines (VMs) through the industry's first support of Address Resolution Protocol (ARP). ProfitBricks' own network stack can dynamically assign the address to any VM in the network and provides the industry's first implementation of high availability functionality, the same as can be configured in the on premise data center. ProfitBricks dynamic routing provides the maximum reliability of the virtual infrastructure and which is different from standard networks where the IPv4 address is assigned to a specific virtual machine.

Linux distributions like Ubuntu and Debian can be implemented with Linux-HA and deployed on the ProfitBricks cloud without any special configuration in the Linux high availability environment. ProfitBricks network support the gratuitous ARP enables an out-of-the-box high availability VM environment.

7. DATA MIGRATION

Data management is important for any business for its enhanced efficiency. However, with each day your data is bound to increase, which may become difficult for you to manage. Today, data management has been made easy with cloud computing and many enterprises have accepted cloud based services for managing their data. Some who have not, have done so mosly out of fear of security of their data or lack of information. You should note that cloud based services provided by third party vendors have benefited those who have adapted the same. These services are of help to individuals or small scale enterprises to large scale enterprises.

When you adapt the cloud services, your entire data is migrated on the cloud. Data migration to the cloud has a lot of benefits, which are as discussed below:
Once your data is migrated to the cloud, you can access it from anywhere and at any time via the internet. Billing system is another benefit that data migration to the cloud offers. It means that you can pay your service provider based on the resources, used by you or your websites and applications, available under your account. This can compensate the lack of capacity of the data center.

As mentioned earlier, many companies restrain from adopting cloud computing services out of fear of losing their sensitive data or misuse of the same. However, you should note that the third party vendors providing you with cloud services for your data management are only interested in providing you with a service capable and suitable enough for managing your data. The vendor has no interest in using the data you have migrated on the cloud.

Now that you know of the benefits of migrating your data on the cloud, you can take advantage of this fast growing technology and take your business to great heights.

Data migration challenges: The key challenge involved in data migration to cloud environments is matching the incoming data to the particular storage protocol and infrastructure being used. The enterprise may have data stored on an iSCSI SAN, for example, but the cloud environment may be Fibre Channel. The cloud infrastructure and protocol translations are a requirement for the migration to be successful.

Another challenge is to perform the data migration with reasonable performance. Stretching out a migration over days or even weeks becomes the data center dilemma. The migration solution has to increase the efficiency to allow for business change and allowing for agility to decrease the likelihood of errors in the process and confining precious IT administrative resources. The IT administrator has to insure flexibility and meet the requirement to migrate data while applications continue to remain "online," as well as minimize the number of times an application needs to be stopped and restarted.

The complexity of enterprise data centers means administrators must rely on a single solution to perform local or remote data migration across multiple network fabrics (SAN, WAN, LAN). The key is remote migrations of data, which provide the capability of the cloud as part of infrastructure as a service (IaaS). IaaS provides, as part of a simple method, the capability to support remote applications deployment, remote infrastructure changes and remote site moves. It is important in the cloud infrastructure the data migration solutions must include flexibility, availability and performance.

A data migration solution (DMS) is an appliance that provides a simple and effective way to provide multi-protocol translation and allow migration of all of the Fibre Channel-based (2Gb, 4Gb, or 8Gb) or iSCSI-based (1Gb or 10Gb) data that supported for applications to be run in the cloud. Without a DMS, users can implement alternatives to bridge between the data center and the cloud, but they are still without a way to translation between Fibre Channel and iSCSI or vice versa. It is possible to implement the translation of a server, but the process requires installing multiple components and is fraught with the potential for errors.

8. CLOUD TRANSPARENCY

The topic of cloud computing data transparency, Amazon, Google, Microsoft and many other top-tier cloud computing service providers are getting a bad rap, according to John Howie , chief operating officer at the Cloud Security Alliance (CSA). Oddly enough, it's reached the point where cloud providers now offer too much information.
"It's not really consumable by your average IT pro or procurement department who is looking to make a decision on which cloud provider to go with," Howie said. "So what the [CSA] has do, in conjunction with the major cloud service providers, is come up with a means by which they can document how they operate their services in a fashion that is easily consumable and comparable to other cloud providers."

Transparency is not a simple thing. It’s not just about honest communications. In the world of cloud computing environment, the transparency has three dimensions: security, design or architecture and communication. Most cloud service providers offer one dimension of transparency. Some offer two. Few offer all three. You need all three to minimize your risk and maximize your ROI.

8.1 Transparency in Security:

Because of the most important dimension for many organizations, and the one nearly every provider gets wrong. Every cloud service provider, with varying degrees of sophistication and success, monitors its services and data centers for security risks and incidents. But not all use independent, specialized third-parties to augment the security monitoring of

the environment to ensure the highest level of responsiveness and preparedness. And almost no cloud providers in the market today are extends critical information and alerting relating to the security of their infrastructure to the customers who depends upon the infrastructure to supported for business applications and protect corporate data.

8.2 Transparency Issue in Design & Architecture**:**
Many service providers are unwilling to share the technical details of their cloud environment. Some cite security and others cite propriety. We cite the customer's need to know and, as such, encourage for open discussion of the cloud architecture, service design, and the impact those have on your applications and data of the cloud users. .

If we were evaluating a cloud services provider, we want to know what kind of storage, servers and network hardware they used. We want to understand how the network is designed and how we connect to my virtual infrastructure to the cloud. We want to know how the virtual infrastructure is designed and optimized. we want to know how maintenance is performed and its impact on cloud services.

8.3 Transparency Issue in Communications: The clouds more appropriately are called as customer friendly SLAs. This is an easiest dimension of transparency for a cloud services provider to deliver the SLAs that are understandable and measurable yet it's the area so many vendors overlook.

Providers love to talk about how many 9's of the availability they provided. You'll hear uptime and availability guaranteed from three to six nines of reliability (so, 99.99 percent would be "four nines"). But when you dig into the contract, you might discover that the devil is in the definition of what constitutes "uptime." It can be quite different from what you consider uptime. For example, one man's uptime is another man's availability. A service can be "up," yet not be available.

9. INTEROPERABILITY BETWEEN THE CLOUD AND THE ENTERPRISE

Organizations need to automatically provision services to manage the VM instances and work with both cloud-based and enterprise-based applications using a single tool set that can function across existing programs and multiple cloud service providers, efforts are under way to solve this problem. For example, the Open Grid Forum (www.ogf.org), an industry group, is working on the Open Cloud Computing Interface, which provides an API for managing different cloud platforms.
The ServePath, a hosting-services provider, has released to its GoGrid API. The API should be easy to adopt because it's based on the existing standards, not on the proprietary technology.

Several vendors that include the Appistry, AppZero, and 3Tera have created the suites for development and deployment platforms that make it easy to write a program once and deploy it on one of many cloud environments. In essence, these suites provide a layer of abstraction between the programmer and the cloud platforms. Developers create applications for the intermediate layer and which then supports and manages the multiple hypervisors or external cloud platforms.

II. CONCLUSION

Cloud computing is promising paradigm for delivering the it services as computing utilities. Clouds are designed to provide the services to the external user. And also provide security to the data at transit and data at rest from cloud to user or vice-versa. We have several security issues addressed above are the main trust issues in the cloud computing environment. These are the main Research Areas in the field of Cloud computing.

REFERENCES

[1] A White Paper on Security and Privacy Challenges in Cloud Computing Environments by Hassan Takabi and James B.D.Joshi University of Pittsburgh Gail-Joon Ahn Arizona State University.
[2] Effective Ways of Secure, Private and Trusted Cloud Computing,by Pardeep Kumar, Vivek Kumar Sehgal , Durg Singh Chauhan, P. K. Gupta and Manoj Diwakar IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011.
[3] CloudSim: A Toolkit for Modeling and Simulation of Cloud Computing Environments and Evaluation of Resource Provisioning Algorithms by Rodrigo N. Calheiros, Rajiv Ranjan, Anton Beloglazov, César A. F. De Rose, and Rajkumar Buyya.

[4] Privacy security and trust issues arising from cloud computing by Pearson, S ,Cloud & Security Res. Lab., HP Labs., Bristol, UK Benameur, A, Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference.
[5] Cloud Security Alliance, "Top Threats to Cloud Computing", v1.0, March 2010.
[6] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing". 2009.
[7] Gellman, R. Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. World Privacy Forum. http://www.worldprivacyforum.org/pdf/ WPF-Cloud-Privacy-Report.pdf, 2009.
[8] An Approach for Data Storage Security in Cloud Computing by Deepanchakaravarthi Purushothaman and Dr.Sunitha Abburu in IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012.
[9] http://www.cloudsecurity.org, accessed on April 10, 2009 .
[10] A New Approach for Providing the Data Security and Secure Data Transfer in Cloud Computing Manoj Prabhakar Darsi , K.Suresh Joseph , Dr. S.K.V.Jayakumar in International Journal of Computer Trends and Technology (IJCTT) - volume4 Issue5–May 2013.

Manoj Prabhakar Darsi[1] ,has completed B.Tech (CSE) from Narayana Engineering College Nellore ,Period from 2007-2011.And Completed M.Tech (CSE) from Pondicherry University, Period from 2011-2013. Presently Working as Assistant Professor in Chalapathi Institute of Technology, Mothadaka in Guntur, from Jun-2013 to till date.

D.Vinay Babu[2], has completed B.Tech (IT) from the Mahatma Gandhi Institute of Technology, Period from
2006-2010. and completed M.Tech (SE) from Karunya University in the year 2010-2012. Presently Working as
Assistant Professor in Chalapathy Institute of Technology, Mothadaka in Guntur from July-2012 to till date.

Gayathri Darsi[3], has completed B.Tech (IT) from the Priyadarsini Institute of Technology Chintalapudi, Period from 2008-2012. And pursuing M.Tech (CSE) in KITS college, Vinjanampadu & JNTUK, period from 2012-2014.