Security Challenges & Resolutions in Cloud Computing

Sandeep Jain
Component Engineering Group
Tata Consultancy Services Ltd.
Ahmedabad, India

***Abstract*— Cloud computing is a model to provide on-demand network, software and hardware resources to customers. It provides the infrastructure, storage and virtualization environment to end-users without vendor's interventions. The purpose of cloud computing is to provide as-a-service model to users.**

Usually Cloud suffers from various levels of risks because essential services are normally outsourced to third party. This makes very difficult for cloud vendors to maintain data privacy and providing failure free service availability. Cloud network requires a major review on security challenges. Inside cloud, it is difficult to locate the original data and sometimes the security processes are hidden behind the layers. The end user is not capable to see the ill effects of clouds while using its services.

This paper presents the various scenarios of breaching the cloud security, its impact for the real world users, challenges & resolutions in cloud network. The paper discusses the risks involved during communication of various components inside cloud and suggest algorithm to resolve them.

***Keywords*- Cloud Security Framework, Cloud Models, Data Center, Private/Public/Hybrid clouds**

I. INTRODUCTION

Cloud Computing is a flexible on demand network to provide services to users on pay as per use basis. The clouds contain vast description on virtualized platform and it's on demand scalability. Cloud computing increases its presence in global market by deploying and managing its models. Cloud models may be distributed in terms of Software-as-a-service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). These models may be further divided into public, private and hybrid clouds. On base of cloud requirement of users, the vendor can isolate the cloud infrastructure from rest of the platform using its models.

Enterprise applications running on the clouds may cause hazards to the organization. Often the data kept somewhere on the cloud storage is a cause of concern for the users. The level of cloud attacks increases as soon as the vendor decides to move the data from primary data centre to the backup data centre. The data confidentiality may be breached, if the user vacates the storage bundle but the data is not erased by the vendor from physical storage.

Many cloud products and vendors are available in market which guarantees to secure your data. Amazon cloud is one of them [1]. Another attempt to secure the clouds is by Trend Micro. "As a global leader in content security, Trend Micro has pioneered SecureCloud – a next-generation advancement that enables enterprises and other organizations to operate safely and securely in the cloud." [2]

As per the IDC (International Data Corporation) survey on clouds in 2008 to rate the challenges/issues for the on-demand model of cloud, the surprising figures come as seen below as in Figure 1.

As per the statistics, we can see that 74.6% people regarded security as the main cause of concern for clouds while the lowest percentage goes to the lower number of major suppliers. The graph simply states that security in cloud is the major challenge which causes both the architecture builder of cloud and its users to think over it before they go for real implementation.

Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering
Editor In Chief Sahil Seth. Copyright © 2012 Universal Association of Computer and Electronics Engineers. All rights reserved.
ISBN: 978-981-07-1403-1

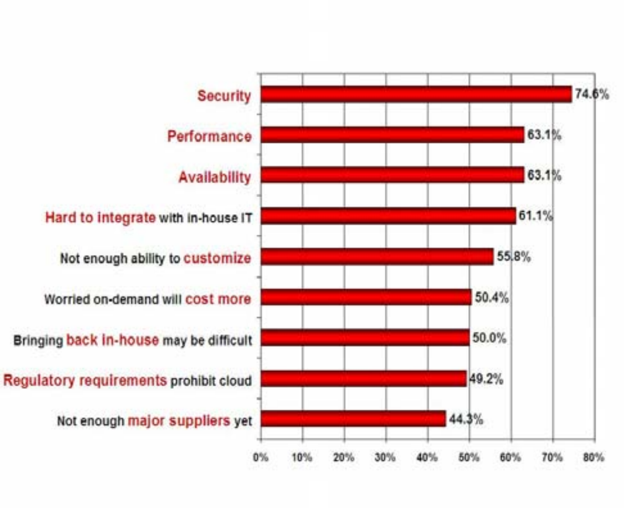


Figure 1 Rating the challenges/issues for the on-demand model of cloud [3]

We are going to discuss the various cloud models available in market and the security breaches in those models. The objectives of paper can be explained as below:

- Study the security management in clouds.
- Research on private/public/hybrid clouds and their security breaches.
- Analysis of migrating traditional platform into cloud enabled architecture and services.
- Study the authentication of users and virtual machines framework.
- Develop full proof algorithm to mitigate risk during communication of components in cloud network.

II. Cloud Models

The cloud network can be distributed on base of its deployment models. Majorly 3 models are available public, private and hybrid. We are going to discuss on public and private models. Hybrid model is the combination of private and public clouds.

A. Public Cloud

The concept of cloud computing is based on sharing of resources among many users. The cloud environment may sometimes cause privacy, performance, security and sustainability issues. Some of these issues are discussed and the most suitable solutions are designed by J. Wayne & G. Timothy for public cloud models. [4]

A public cloud offers services to users through interaction of third party service provider. It may or may not be free. The features of public cloud include providing enough elasticity and robustness to its customers. Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform. [5]

The main benefits of using a public cloud service are:

- Easy and inexpensive set-up because hardware, application and bandwidth costs are covered by the provider.
- Scalability to meet needs.
- No wasted resources because you pay for what you use.

IDC estimates the market for public cloud products and services at $16B in 2010, growing to $56B by 2014. Gartner more optimistically estimates the cloud market at $150B by 2013 while Merrill Lynch estimates the market at $160B by 2011. SMB (Small and Medium Business) cloud spending alone will reach $100B by 2014. As per these statistics it seems that the market for public cloud infrastructure, platforms and applications is large and growing much more quickly than any other type of IT spending [6].

Now we are going to discuss various security breaches and loopholes available in public clouds:

1) *Cloud Complexity*: Public cloud often offers large surface of security attack to the criminals. It contains the large infrastructure, the applications deployed by various users, data storage in dispersed format and the middle ware. As explained by J. Wayne and G. Timothy [4] in Security Guidelines "Public cloud Security depends not only on the correctness and effectiveness of many components, but also on the interactions among them."
2) *Multi-Shared Architecture*: As soon as more users adopt the practice of using the cloud and its infrastructure for its own use, the gaps in the security increase as well. Public cloud one way

provides the flexibility in managing the centralized platform for its users; on the other side it may give chance to attackers to behave their applications to misuse the network and its resources. For ex: An attacker may pose himself as the cloud subscriber and can increase the risk of over-loaded network resources.

3) *Service offering by Public Clouds*: Previously the organizations managed to restrict the users to use the applications and playing with data inside their own premises. Now the conditions are changed and migrating applications to public clouds offers services to its clients through internet. Managing clouds through outside data centre increases the risk compared with traditional data centres.

4) *Loss of Control:* Previously the organizations managed to control the applications and its data inside their own premises. Now the conditions are changed and migrating applications to public clouds offers loss of control to its administrators.

An example can be shown here for the public cloud malicious attack:

Mechanism cracking [4]: WiFi Protected Access (WPA) Cracker, a cloud service ostensibly for penetration testers, is an example of harnessing cloud resources on demand to determine the encrypted password used to protect a wireless network. With cloud computing, a task that would take five days to run on a single computer takes only 20 minutes to accomplish on a cluster of 400 virtual machines [Rag09]. Because cryptography is used widely in authentication, data confidentiality and integrity, and other security mechanisms, these mechanisms become, in effect, less effective with the availability of cryptographic key cracking cloud services. Both cloud-based and traditional types of systems are possible targets. CAPTCHA cracking is another area where cloud services could be applied to bypass verification meant to thwart abusive use of Internet services by automated software.

B. *Private Clouds*

The public cloud refers primarily to third-party providers who deliver services—often in a self-service model—through the Internet. Because of this open environment, there are understandable concerns about security, privacy and service reliability. Private clouds, on the other hand, are gated communities connected to the internet where access, security, disaster recovery processes and almost everything else can be more easily controlled. Nevertheless, they can still offer significant economies of scale as well as best in class technology.

Few challenges for the private clouds may be discussed here [7]:

1) Physical Security: Often there is concern over the security requirements upon which data centre employees and contractors are there. Automate authorization for access and authentication for certain safeguards is must to resolve the issues in physical security.

2) Network Security: The attackers normally interact with the network and involve in passive attacks without knowledge of the organization handling clouds. To resolve this many layers of security are necessary to data centre devices and network connections. Specialized hardware such as load balancers, firewalls, and intrusion prevention devices, should be in place to manage volume-based denial of service (DoS) attacks.

3) Data Security: The attackers may directly attach to the data centre and may steal confidential information. They may design their own applications to attack the data servers. The resolver must classify the assets to determine the strength of security controls to apply.

III. ADDRESSING CLOUD SECURITY- A CHALLENGE

It is always necessary for cloud vendor to delivers a highly scalable cloud computing platform with high availability and dependability, and the flexibility to enable customers to build a wide range of applications. The issues of end-to-end security and end-to-end privacy within the cloud computing world are more sophisticated than within a single data centre not facing the internet. The whole network must ensure the confidentiality, integrity, and availability of customer's systems and data with the utmost importance. This paper is intended to answer user's questions such as "*How does the framework help me ensure my data is secure?*"

A. *Categorising Types of Attacks on Clouds*

Without security measures and controls in place, user credentials data might be subjected to an attack. Some attacks are passive, meaning information is monitored; others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself. Following are the common types of attack as listed in Table I.

TABLE I
TYPES OF ATTACKS IN CLOUD FRAMEWORK

S.No.	Type of Attack	Description
1	Eavesdropping	Allows an attacker to listen in or interpret (read) the traffic.
2	Data Modification	Attacker can modify the data in the packet
3	Identity Spoofing	Attacker can use special programs to construct IP packets that appear to originate from valid addresses.
4	Password-Based Attacks	Allow an eavesdropper to gain access to the network by posing as a valid user.
5	Denial-of-Service Attack	Prevents normal use of your computer or network by valid users.
6	Man-in-the-Middle Attack	Someone between sender and receiver is actively monitoring, capturing, and controlling your communication transparently.
7	Compromised-Key Attack	Attacker obtains a key and uses it to gain access to a secured communication.
8	Sniffer Attack	Analyse your network and gain information to eventually cause your network to crash.
9	Application-Layer Attack	Targets application servers by deliberately causing a fault in a server's operating system or applications.

B. *Security Resolution in Public Clouds*

1) *Governance of Cloud Framework:* It is necessary to follow the proper organization practices throughout the system lifecycle. It will include the policies, standards and service provisioning in clouds.[9]

2) *Regulatory Compliance:* Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements.

3) *Risk Management Program:* Ensure visibility into the security and privacy processes employed by the cloud provider. Institute a risk management program that is flexible enough to adapt to the continuously evolving and shifting risk landscape.

4) *Cloud Architecture:* Understand the underlying technologies the cloud provider uses to provision services.

5) *Access Management:* Involve the secure authentication, authorization, and other identity and access management functions.

6) *Software Isolation:* Understanding the virtualization and other software isolation techniques that the cloud provider employs.

7) *Data Protection:* Evaluate the various data centres in place for the primary as well as the backup purpose.

8) *Availability of critical operations:* Ensure that the critical operations can be immediately resumed in time bound manner.

9) *Incident Response:* Understand and negotiate the contract provisions and procedures for incident response required by the organization.

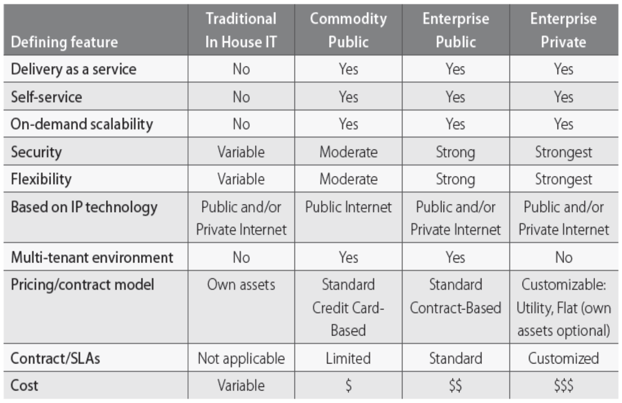
C. *Security Resolution in Private Clouds*

A private cloud offers services which are restricted to particular user and cloud provider. User has greater control over the infrastructure and support of enhanced security. The restriction of bandwidth and security protocols is not there as in public clouds. Following are the breaches that can be taken care [9]:

1) *Integration of Private cloud:* Private clouds are concentrated towards maturity to achieve the hybrid model. Hybrid model are the combination of public and private clouds. There must be a secure solution and encryption methodology to secure data when migrating from private to hybrid model.
2) *Mitigating the Hypervisor vulnerabilities [10]:* Certain times the hypervisor vulnerability allow a guest OS (Operating System) to run processes on other host machines. Strong updates must be applied of hypervisor to avoid this.
3) *Network Access Control:* Access list should be properly maintained to diversify the access controls of external users. For Ex: Data on payroll management should be available only for the employees of payroll department and not to the marketing department people.
4) *Dipartite the Internal and External Users:* The most deleterious security breaches come from inside the organization and therefore you should treat the traffic inside the internet perimeter with as much security as the traffic outside.
5) *Network level authentication*: It is possible that virtual machines will be able to communicate with each other even if they are not allowed to do so. Ensure that the network level authentication and encryption mechanisms are used, such as those provided by IPsec.
6) *Host OS Isolation:* The host operating system should be isolated from all virtual machines contained within it. Assure that there are no back-channels that enable guest virtual machines from communicating with the host operating system over either virtual or physical network connections. Dedicate physical NICs (Network Interface Card) to virtual machines, or dedicate VLANs (Virtual LAN) to the virtual machines. The host operating system must be free from malware, and mechanisms, such as anti-malware software, must be in place to detect potential compromise.
7) *Security Zones:* In a private cloud environment, guest virtual machines belonging to different security zones should not be hosted on the same virtual server. For example, if the private cloud virtual server is hosting internet facing resources, such as virtual firewalls or internet-facing front-end applications, these internet-facing guest virtual machines should not be hosted on the same virtual server as non-Internet facing guest virtual machines, such as those hosting internal database and collaboration information.

D. *Spectrum of Delivery Models from traditional IT to private cloud*

All cloud services are not equal in terms of the control that they offer over security, performance and host commercial considerations. We can see the spectrum of Delivery Models in As per the statistics, we can see that 74.6% people regarded security as the main cause of concern for clouds while the lowest percentage goes to the lower number of major suppliers. The graph simply states that security in cloud is the major challenge which causes both the architecture builder of cloud and its users to think over it before they go for real implementation [11].



Defining feature	Traditional In House IT	Commodity Public	Enterprise Public	Enterprise Private
Delivery as a service	No	Yes	Yes	Yes
Self-service	No	Yes	Yes	Yes
On-demand scalability	No	Yes	Yes	Yes
Security	Variable	Moderate	Strong	Strongest
Flexibility	Variable	Moderate	Strong	Strongest
Based on IP technology	Public and/or Private Internet	Public Internet	Public and/or Private Internet	Public and/or Private Internet
Multi-tenant environment	No	Yes	Yes	No
Pricing/contract model	Own assets	Standard Credit Card-Based	Standard Contract-Based	Customizable: Utility, Flat (own assets optional)
Contract/SLAs	Not applicable	Limited	Standard	Customized
Cost	Variable	$	$$	$$$

Figure 2 Difference in Service provided by Private and Public Clouds

E. *PHPS Algorithm and Prototype to enhance Security*

PHPS here means Private, Hybrid, and Public Secured Algorithm for clouds. The algorithms will address risk which can be broadly categorised as:

Risk 1: Resource Exhaustion
Risk 2: Interception of Data in Transmission

Risk 3: Authentication of user credentials
Risk 4: Virtual Machine Identification
Risk 5: Loss or Compromise of Encryption Keys
Risk 6: Handling of Storage data once cloud ends
Risk 7: Dynamic authentication within department
Risk 8: Dependence on secure hypervisors
Risk 9: Security of virtual OSs in the cloud

We are going to discuss the cloud deployment model as stated in Figure 3.

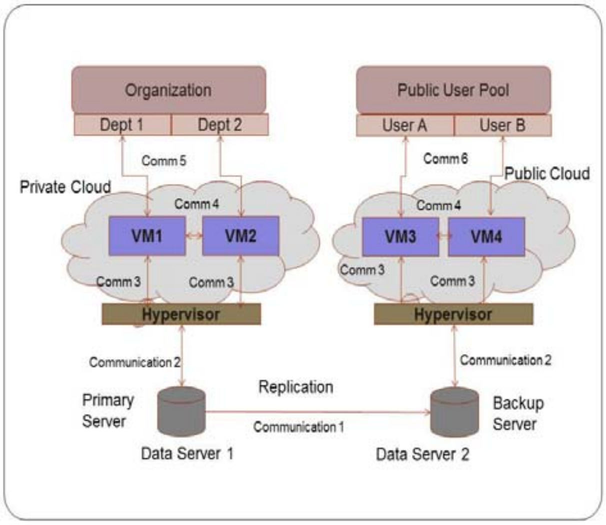


Figure 3 Cloud Deployment Model

Component definition in cloud deployment model in Figure 3:

- Primary Server Data Server 1 (DS1) also called master server is used to generate the response.
- Backup Server Data Server 2 (DS2) also called slave server is used for disaster recovery.
- Hypervisor also called virtual machine manager (VMM) allows multiple operating systems, termed guests, to run concurrently on a host computer.
- Virtual machine (VM1, VM2, VM3 and VM4) is completely isolated guest operating system installation within a normal host operating system.
- Two departments (Dept1, Dept2) in an organization using services offered by private cloud.
- Two Users (User A, User B) in a public user pool using services offered by public cloud.

F. Algorithm to Address the Risk and Issues

The paper presents various algorithm approaches to secure the communications channel among various entities.

Communication 1: Between Primary and Backup Data Server

Step 1: DS1 have the key generation unit. The key generation unit will produce public private key pair. These keys are named as Pu_1 and Pr_1 respectively.

Step 2: DS1 will distribute the Pu_1 across all the secondary data servers. Here in our example, we considered only one backup data server known as DS2. DS1 send the Pu_1 to DS2.

Step 3: Data before transmission to secondary server for replication will be encrypted first at DS1. For encryption DS1 use the Pr_1. After encryption the data is transmitted to DS2.

Step 4: When encrypted data is received by DS2, it will use decryption mechanism using Pu_1 to fetch the original data and store in its storage pool for replication purpose.

Results of implementing the algorithm for communication 1:

As the third party doesn't know about the public key, the risk of "Interception of Data in Transmission" and risk of "Loss or Compromise of Encryption Keys" can be avoided. Data in encrypted form cannot be modified. Even if the intruder fetches the public key during transmission, we can modify the algorithm to be more secure. We can include following step at the end.

Step 5: DS2 will have its own public, private key generator. The keys can be known as Pu_2 and Pr_2 respectively. DS2 will send the double decrypted data (using Pr_2) along with its own public key Pu_2 to DS1. DS1 decrypt it with help of Pu_2 and then by Pr_1 and send the signal to DS2 saying that the data it received is correct and DS2 can proceed with its replication work.

To make the performance better, the data servers can compromise on the size of data to send during handshake.

Communication 2: Between DS1 and Hypervisor

Step 1: DS1 will have hash algorithm unit (Generate hash1). The hash algorithm is applied on data and it is encrypted using DS1 private key.

Step2: The data that hypervisor receive is passed through same hash algorithm that will generate hash2.

Step 3: Also hash3 value is calculated by applying the DS1 public key to the data. If the values of hash2 and hash3 matched, it indicates that the data came from DS1 is valid.

The steps can be elaborated as in Figure 4.

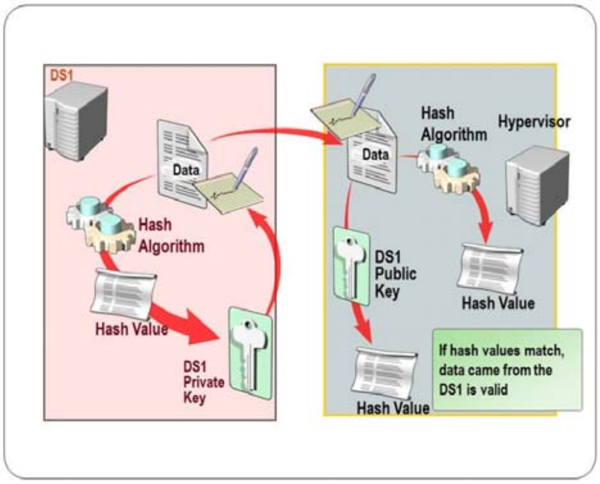


Figure 4 Securing Communication between data server and hypervisor

Results of implementing the algorithm for communication 2:

As the third party doesn't know about the public key, the risk of "Interception of Data in Transmission" and risk of "Loss or Compromise of Encryption Keys" can be avoided.

Communication 3: Between VM and Hypervisor

Step 1: Credentials and identification of each VM are stored in hypervisor managed centralized active directory. This active directory stores all the VM unique identification.

Step 2: Based on the identification, each VM will have restriction to talk only with permitted VM and specific part of operating system.

Step 3: Hypervisor can consult with active directory asking to verify the VM details anytime during communication.

Results of implementing the algorithm for communication 3:

As each and every VM must have to identify itself, they must need to manage the digital certificate duly singed by CA. It is necessary that whenever hypervisor receive the message from VM, it must contain digital certificate. The risk of "Virtual Machine Identification" can be avoided here by using centralized management through CA.

Communication 4: Between VM1 and VM2 in private cloud

Hypervisor will maintain an AD server. AD will store the user credentials and VM instance credentials as well. Prior to communication between VM1 and VM2, these steps can be implemented:

Step 1: Whenever VM1 try to communicate with VM2, VM2 will ask for VM1 credentials.

Step 2: VM1 provide credentials and digital certificate that indicate it is a genuine machine that VM2 want to communicate.

Step 3: VM2 will verify the digital certificate from the CA and VM1 credentials using AD response.

Step 4: Also VM2 ask VM1 to provide OTP generated by third party tool. The same can be verified by VM2.

Step 5: VM2 send the confirmation to VM1 saying that the verification is done.

Step 6: VM1 and VM2 start communicating.

The steps can be elaborated as in Figure 5.

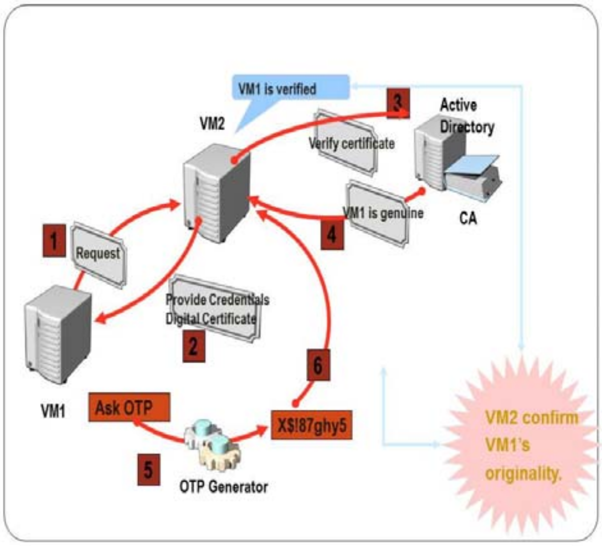


Figure 5 Securing Communication between Virtual Machines

Results of implementing the algorithm for communication 4:

The risk of "Dependence on Secure Hypervisors" and "Authentication of VM" can be address here. VM need not rely on OS or hypervisor as they have their own mechanism to tackle the security.

Communication 5: Between VM1 and Department 1

Step 1: VM ask department1 to show the OTP.

Step 2: OTP is one time password generation unit. Department need to register the associates who are willing to use the VM and show it when ask by VM.

Step 3: VM will have a dynamic authenticity of users of that particular department. Also Company signature and digital signature for all communications is needed.

The algorithm may be extended to support the biometric authentication of users. The algorithm addresses the risk of "Dynamic authentication" within department and "Virtual Machine Identification" security issues.

Communication 6: Between user A and VM3 in public cloud

Step 1: User must be registered and access list is defined along with restriction imposed on users. Users can not directly interact with the database.

Step 2: The number of applications and processes a particular user can activate is limited. The resource quota for each user is already decided.

Step 3: Strict restructions are imposed on cloud vendor to destroy/remove the date from DS1 & DS2 as soon as the services to particular user ends.

The risk of "Resource Exhaustion" and "Handling of Storage data once cloud ends" are addressed here.

IV. Cloud Security – Market Scenario

Several vendors are now specific to consumer needs and adaptability of cloud platform for their applications. The proposals which are floating in market by organizations purely rely on the cloud platform and its service providers. The number of vendors offering private cloud exploded because of the stronger security it offers compared with other models. Gartner's poll conducted at Data Center Summit in December 2009 showed that over 2/3rd of respondents expect that their investment in cloud will be more oriented towards private cloud than public cloud through 2012.

There are so many products launched in market keeping the cloud security on priority. HP launched Cloudstart, CA acquired Oblicore, 3Tera, Nimsoft, and Hyperformix to boost its private cloud capabilities, Microsoft launched Hyper-V Cloud, IBM expanded its family of Cloudburst appliances, Oracle launched the Exalogic Elastic Cloud, BMC introduced its Cloud LifeCycle Management offering, and even application vendors like SAP announced that its customers will soon have more options and tools for deploying the company’s software on private clouds [12].

V. Conclusion

Cloud computing is the most popular notion in IT today; even an academic report from UC Berkeley says “Cloud Computing is likely to have the same impact on software that foundries have had on the hardware industry.” While many of the predictions may be cloud hype, we believe the new IT procurement model offered by cloud vendors are here to stay. Whether adoption becomes as prevalent and deep as some forecast will depend largely on overcoming fears of the cloud.

Cloud always fears from the perceived loss of control of sensitive data. In my vision, I propose to extend control measures from traditional approach of computing to a long and vast algorithmic secured platform. I believe that the measures listed in the paper will definitely alleviate much of today's fear of cloud computing and have the potential to provide advantages to cloud providers and its consumers.

Acknowledgment

I would like to thank my organization who allowed me to work on cloud computing. I also thank all my team mates for their direct and indirect support.

I would like to mention special thanks to my colleague Shivanand for reviewing the document and verifying the feasibility of algorithms proposed in this paper.

References

[1] *“Amazon Elastic Compute Cloud*” Available: http://aws.amazon.com/ec2/

[2] A Trend Micro White Paper “*Addressing Data Security Challenges in the Cloud,* July 2010, pp 2-4 Available: http://us.trendmicro.com/us/trendwatch/research-and-analysis/white-papers-and-articles/

[3] G. Frank (Jul 2010) IDC Exchange homepage. [Online]. Available: http://blogs.idc.com/ie/

[4] J. Wayne & G. Timothy (Jan 2011), "*Guidelines on Security and Privacy in Public Cloud Computing*" Available: http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

[5] *“Public Cloud Insights”* Available: http://searchcloudcomputing.techtarget.com/definition/public-cloud

[6] *“Cloud Statistics”* Available: http://blogs.computerworld.com/16863/cloud_computing_by_the_numbers_what_do_all_the_statistics_mean

[7] Ballmer, S. *“Seizing the Opportunity of the Cloud”* [Remarks by Steve Ballmer, CEO of Microsoft, Microsoft CEO Summit 2010, Redmond, Wash., May 29,2010]. Available: http://www.microsoft.com/presspass/exec/steve/2010/05-19ceosummit.mspx

[8] *“Microsoft Security Response Center*” Available: http://www.microsoft.com/security/msrc

[9] *“The Microsoft Security Development Lifecycle (SDL)*”. Available: http://msdn.microsoft.com/en-us/security/cc448177.aspx

[10] Meisel A. (2009) *"Hyperguard- Defining a dWAF to secure cloud applications"* Available: www.artofdefence.com/en

[11] Verizon (2010) *"Parting the Clouds: Demystifying: Cloud Computing Options"* Available: verizonbusiness.com/thinkforward/cloud/

[12] *“Private Cloud Insights”* Available: http://www.privatecloud.com/2011/03/09/the-year-of-the-hybrid-cloud/?fbid=P5oFRnrqAEG