**IOSR Journal of Engineering (IOSRJEN)** **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 04, Issue 02 (February. 2014), ||V1|| PP 26-31

# A Survey on mitigations in Secured Cloud Environments

Mohammed Younus[1], Fahmida Begum[2], Ahmad A.Alhamed[3]
[1]*Lecturer at College of Computer and Information Sciences, KING SAUD UNIVERSITY. (AL-MUZAHIMIYAH BRANCH)*
[2]*Asso.Professor, Dept. of MCA, Dr. K.V. Subba Reddy college of MCA, Kurnool.(Dt),A.P,*
[3]*Director of College of Computer and Information Sciences at KING SAUD UNIVERSITY (AL-MUZAHIMIYAH BRANCH)*

***Abstract: -*** Cloud computing now remains as a hot research topic in IT industry because of its mannerism that provides us to make use of various computing resources. Cloud computing mechanism has been proven as an On-Demand paradigm. To create trustiness and belief on cloud to a customers or organizations we need to consider various security aspects. *The concept of cloud computing creates new challenges for security, because sensitive data may no longer reside on dedicated hardware.* Assuring the security of a software system in terms of testing nowadays still is a quite tricky task to conduct. If considering today's emerging trend in the adoption of cloud computing, This paper mainly focuses on the TaaS in cloud platform and also explains importance of security in cloud platform and also provides few methods to overcome limitations in security aspects of the cloud.

***Key words:*** *- cloud computing, security and privacy, information Technology, security concerns in cloud.*

## I. INTRODUCTION

Cloud computing received significant attention recently as it provides a different approach of utilizing various computing resources. In comparison cloud services are better than in traditional sense. Security is the most important factor to be considered all the time in cloud environment. Cloud computing mainly focus on three service layers namely SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a service). Cloud computing has been recognized as a business service model that provides Xaas (Everything as a Service). Today leading cloud vendors are Google, Amazon, IBM, Microsoft etc; cloud computing changes the way we deliver and use software and managing them effectively when compared to traditional way of approach.

In 2010, Gartner research predicted that 20% of business would have a zero ownership of IT assets by 2013 & instead seek to acquire and make best use of cloud. Merrill Lynck estimation have shown that within next five years, the annual global market for cloud computing will surge to $95 billion. According to consulting firm Zinnov, India's cloud computing market is expected to reach $ 4.5 billion by 2015. Public IT cloud services revenue is expected to hit $55.5 billion in 2014, up from $16 billion in 2009-annual growth rate of 27.4 %. Traditional IT product growth is expected to be 5 %. Cloud Computing to Grow 1200% by 2015.[1]

In order to make use of cloud services one should have trust, belief on cloud. Here to make customers and organizations create trust on cloud and services provided by it we need to provide assurance on cloud by testing cloud considering various parameters. In order to provide more security we have to answer few questions like:

- What are current practice, tools and major providers of cloud services?
- How and up to what extent your data is secured in cloud platform?
- Security in cloud environments and views of security?

Organizations should have a well defined methodology before migrating to cloud computing. Moving the application to the cloud depends on the security objectives of an organization, cloud computing should be approached carefully with due consideration of the sensitivity of data that the organization is planning to move beyond their firewall. The less control you have for your data means more you have to trust the providers' security policies. Security and privacy issues have to be addressed from the initial phase, considering after the deployment will be more complicated, expensive and risky. Every organization should thoroughly study the safety measures and policies followed by the provider and should make sure that it is aligned with the privacy and security requirements of the organization.

In the past the cloud services that faced security breach was never expected to succumb to vulnerabilities and it's evident that cloud providers also face the security concerns faced by other organizations. The usual security norm in public cloud is service level agreements (SLAs) which talks about the expected level of services provided by the cloud provider to the cloud consumer. Consumers should make sure that the contract they sign have reference to the security measures that the provider have in mind and also make sure that the

contract meet the expected security norms from their business perspective. SLAs are usually of two types, off-the-shelf non negotiable contracts and customized negotiable agreements. Public clouds usually follow non negotiable SLA's which may not be acceptable for business that have crucial data. Organizations who want to deploy critical applications can think about private clouds over public clouds which offer better insight and control over security and privacy.

## II. BACKGROUND AND RELATED WORK

***Background:***

One has to know where the term "Cloud Computing" originated? When did the hype around cloud start? The evolution can be split into 3 phases:

1. The Idea Phase – this started in the 1960s and stretched to the pre internet bubble era. The core idea of computing as a utility computing and grid computing developed.
2. The Pre Cloud Phase – this started around 1999 and lasted till 2006. In this phase internet as the mechanism to provide Application as Service got developed.
3. The Cloud Phase – this phase started in 2007 when the term cloud computing term became popular and the sub classification of IaaS, PaaS & SaaS got formalized.

1960s – Evolution of the core concept of Cloud Computing:-

"J.C.R. Licklider": He is considered by many to be the person who brought the idea of cloud computing to the forefront.

We need to know the leading vendors of cloud today. On some gap, cloud computing came back with the arrival of Salesforce.com in 1999, which was with the idea of delivering enterprise applications using a simple website. This was the first attempt of SaaS (Software-as-a-Service).

After Salesforce.com next major development was Amazon web services in 2002, which provided a suit of cloud-based services such as storage, computation and even human intelligence via Amazon Mechanical Turk. After the success of Amazon web services, in 2006 Amazon launched Elastic Compute cloud (EC2) as a web service to rent computers for small-scale companies to run their own application stack.

"Amazon EC2/S3 was the first widely accessible cloud computing infrastructure service," – (Jeremy Allaire, CEO of Brightcove) which provides its SaaS online video platform to UK TV stations and newspapers.

Amazon was the only major cloud service provider until Google and others started browser-based enterprise solutions. In 2009 Google introduced its cloud service named Google Apps. Cloud computing has been emerged with many cloud apps from leading technology giants such as VMware, Oracle and Google. Other key factors that have enabled cloud computing to evolve include the maturing of virtualization technology, the development of universal high-speed bandwidth, and universal software interoperability standards. Many IT professionals recognize the benefits cloud computing offers in terms of increased storage, flexibility and cost reduction etc.

There are some who see cloud computing as a fad. Those who share that view tend to look at the Cloud as if it's an all or nothing proposition; if you can't move your entire infrastructure to the Cloud it must certainly be a passing fancy.

But the Cloud is here to stay. There are many applications, like compute intensive statistical analysis, business intelligence and testing, that are incredibly well-suited for cloud computing.

Cloud computing in terms of security has evolved because there are more number of customers and organizations turning towards cloud platform. So security aspects in cloud can be considered such that in most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. Various issues, challenges regarding security in cloud should be evaluated very often to make the cloud environment secured.

***Related work:***

We need to understand what's cloud computing and security importance in cloud environment?

Security is an important factor to be considered in the cloud environment today so, we need to be cared about the security in cloud platform both from client and server side. Special kind of testing intended to check the level of security and protection offered by an application to the users against unfortunate incidences. This incidences could be loss of privacy, loss of data etc. the application is checked for possible perpetrators which can affect the system adversely, by peeping inside the system, and the points of penetration where system can be broken by these penetrators. There are always some weak points in a system, which are vulnerable to outside attacks/ unauthorized entry in system. Since security and its services becomes major concern inside clouds, it should focus on the issues, challenges in security validation for clouds.

Here are some few related issues regarding security in cloud:

- How can we assure the security of cloud based application?
- What are QOS standards to be followed to assure security?
- Will data and ownership matter in cloud?
- How can we assure and assess user privacy in cloud infrastructure?

To all the above related works few questions are really a challenging task. So, we can come through few solutions in methods section.

***Security in the Cloud:***

Conventional infrastructure security controls designed for dedicated hardware do not always map well to the cloud environment. Cloud architectures must have well-defined security policies and procedures in place. Realizing full interoperability with existing dedicated security controls is unlikely; there has to be some degree of compatibility between the newer security protections specifically designed for cloud environments and traditional security controls.

**Major issues in cloud Computing:**

1. Every breached security system was once thought infallible
2. Understand the risks of cloud computing
3. How cloud hosting companies have approached security
4. Local law and jurisdiction where data is held
5. Best practice for companies in the cloud[3]

## III. METHODS

Understanding the essential requirements, actual needs regarding the cloud testing we can come up with new test models and frameworks and accurate approaches which will become more helpful in making the cloud and it's services trusted before using it. Thus, her we shall discuss few issues, future works in regard to security in cloud.

***Client side security:***

Cloud computing encompasses a client and a server .Client side security is always over looked. As first step towards secure data management business should strengthen the client side security. To provide physical and logical safety to client machine is a big challenge. Built in security measures can be eluded by an erudite person without much difficulty. To maintain secure client, organizations should review existing security practices and employ additional ones to ensure the security of its data. Clients must consider secure VPN to connect to the provider.

Web browsers are majorly used in client side to access cloud computing services. Cloud providers usually provide the consumers with APIs which is used by the latter to control, monitor the cloud services. It is vital to ensure the security of these APIs to protect against both accidental and malicious attempts to evade the security. The various plug-ins and applications available in the web browsers also causes a serious threat to the client systems used to access the provider. Many of the web browsers do not allow automatic updates which will append to the security concerns. To ensure secure cloud organizations should work on the existing internal policies and improvise its security strategies if necessary.

***Security Concerns from Cloud Service Vendor's:***

There exist many security concerns in server side. To adopt cloud computing it is necessary to ensure providers security measures. To enhance the trust factor providers can get their system verified by external organizations or by security auditors. Aside from the security factor other issues that needs attention is about the data in the cloud, if at the provider goes bankrupt or being acquired by another business.

Traditional data centers used to have regular security audit and mandatory security certifications which ensure the data security. Cloud providers should also incorporate these measures to assure secure transaction among its customers.

***Lack of Control over the data:***

Two recent events have exposed the dark sides of cloud computing for both businesses and consumers. These incidents—the partial outage of Amazon's EC2 cloud service and the security breach of Sony's PlayStation Network and Qriocity music service—underscore a key issue of the cloud computing model: customers 'lack of control over their data. Non cloud services also have security concerns but cloud has

additional risk of external party involvement and exposure of critical and confidential data outside organizations control. Modifying security measures or introducing pristine best practices relevant to one particular organization is also unattainable. Cloud provider stores the data in providers side and maintenance is exclusively done by the providers hence clients have no means to check on the providers security practices, providers employees, their skills specializations etc. Insider threats go beyond those posed by former employees to include contractors, organizational affiliates, and other parties that have received access to an organization‘s networks, systems, and data to carry out or facilitate[4].

***Data recovery in cloud computing:***

Usually cloud users do not know their data location and the vital query of data recovery in all circumstances may not be possible. Providers should be able to tell the users what will happen in case of any natural disaster, how much of data they will be able to recover and the stipulated time for the recovery should also be mentioned.

We have discussed about the different security vulnerabilities of cloud computing and the question arises about the measures that has to be taken to secure data over the cloud.

***Securing data in cloud:***

A secure infrastructure ensures and builds confidence that the data stored is secure in providers’ side. Proper implementation of security measures is mandatory in cloud computing. The fact that application is launched over the internet makes it susceptible for security risks. Cloud providers should think beyond the customary security practices like restricted user access, Password protection etc. Physical location of stored data is also vital and it‘s the responsibility of the provider to choose the right location of storage.

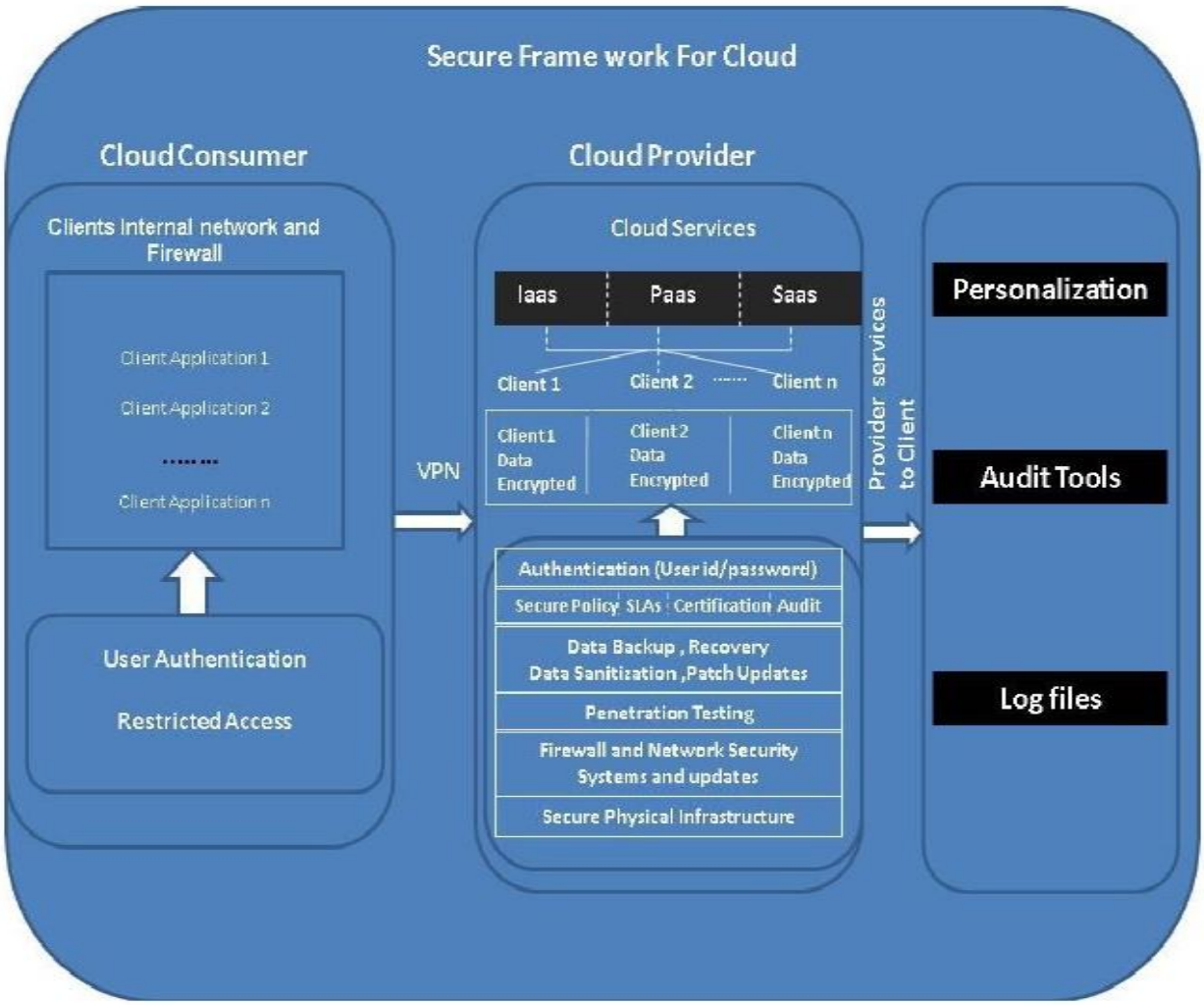


**Fig: Security frame work for cloud**

***Backup and recovery:***

In cloud computing data is stored in distributed location. The cloud customers will never be able to make out the exact storage location of their records and there comes the importance of data back up and recovery. Backup software should include public cloud APIs, enabling simple backup and recovery across major cloud storage vendors, such as Amazon S3, Nirvanix Storage Delivery Network, Rackspace and others, and giving consumers flexibility in choosing a cloud storage vendor to host their data vault.[5] One debatable question is whether to back up the entire data or to backup critical and vital data. If provider agrees to backup crucial data then the question arises on how to determine the priority of data. The easiest and least complicated way is to secure data over the cloud.

***Security Enhancements for Cloud Computing:***

The Following Practices can be followed to improve the Security of Cloud Computing:

- Implement security practices at organizational level and make sure that the providers security plans are in alignment with the business.
- Employ and maintain secure Infrastructure in client side (secure VPN , changing default vendor provided passwords ) and host side (firewalls , patch managements, anti-virus updates )
- Data sanitizations should be done at right time
- Auditing should be done in regular manner
- Frequent data backup policies should be maintained
- User should be intimated in prior before sharing data to third party etc.

***Apart from above we can also follow few Security Best Practices in the Cloud:***

1. Isolate networks
2. Isolation of management networks
3. Isolation of VMware VMotion and IP storage networks
4. Isolation of customer data networks
5. Secure customer access to cloud-based resources
6. Secure, consistent backups and restoration of cloud-based resources
7. Strong authentication, authorization and auditing mechanisms
8. A library of secure and up-to-date templates of base OS and applications
9. Resource management to prevent denial of service (DoS) attacks[6]

## IV. CONCLUSION

Thus we can conclude that this paper we discussed the security issues of cloud computing and have given some measures to limit the vulnerabilities in the cloud. Based on the above discussed proposals i have come up with a framework that will help the cloud consumers and providers to safe guard the data to some extent.

Apart from this all the issues and vulnerabilities should be reviewed regularly and new frame works, security policies, process models and methods can be incorporated in cloud to increase its usage, and efficiency.

## REFERENCES

[1] http://www.futurecloudcomputing.net/survey
[2] http://cloudcomputing.sys-con.com/node/1744132
[3] http://www.computerweekly.com/news/2240089111/Top-five-cloud-computing-security-issues
[4] Wayne Jansen, Timothy Grance The NIST Guidelines on Security and Privacy in Public Cloud Computing
[5] http://www.wwpi.com
[6] http://ebookbrowse.com/savvis-vmw-whitepaper-0809-pdf-d276784800
[7] Richard Chow et al., Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control, ACM Workshop on Cloud Computing Security,Chicago, Illinois, November 2009,<URLhttp://www2.parc.com/csl/members/eshi/docs/ccsw.pdf>.
[8] Wayne Jansen ,Timothy Grance ,The NIST Guidance on security and privacy in public cloud computing ,January 2011.
[9] HP, Yahoo, Intel Launch Cloud Computing Test Bed", www.seekingalpha.com, July 29, 2008.
[10] PC Quest September 2010 issue.
[11] http://www.scribd.com/doc/18172802/Cloud-Computing-Use-Cases-Whitepaper

**AUTHORS PROFILE**

**1) MOHAMMED YOUNUS** did M.S (IT) from University of East London in 2010. I have 3 years of experience in Academics worked as a lecturer in London College of Human Resource and Management At present working as Lecturer at College of Computer and Information Sciences in KING SAUD UNIVERSITY.(AL-MUZAHIMIYAH BRANCH).

**2). FAHMIDA BEGUM** did his MCA from Osmania University, and Completed her Ph.D from MJPRU , U. P. Her interested areas are mobile computing and cloud computing . I have 9 years experience of Teaching in various colleges. At present she is working as an Associate Professor in Dr. K.V Subba Reddy college of MCA, Kurnool.(Dt).

**3) DR.AHMAD A.ALHAMED** is the Director of College of Computer and Information Sciences at KING SAUD UNIVERSITY(AL-MUZAHIMIYAH BRANCH)