Authentication in Cloud Computing

Mr. Amey Hawal[#1], Mr. Rahul Mirajkar[#2], Mr. Sagar Lad[#3]

Miss.Pouravi Kadam [#4,] Miss.Sayali Jamadade [#5]

Department of Computer Science & Engineering,
Bharati Vidyapeeth's College of Engineering, Kolhapur, India
[1]amey_hawal@yahoo.com
[2]rahulmirajkar982@gmail.com
[3]sagarlad930@gmail.com
[4]pouravikdm10@gmail.com
[5]sayalijamadade@gmail.com

Abstract— **Cloud computing security (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing**.

Index Terms— ***Cloud issues, Security issues, Data issues***

I.INTRODUCTION

Cloud computing provides computational software applications ,data access, data management and storage resources without requiring cloud users to know the location and other details of computing Infrastructure [1], [2].

There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers [3], [4], [5]. 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.

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. For example, a breach in the administrator workstation with the management software of virtualization software can cause whole datacenter to go down or reconfigured to attacker's liking.

II. CLOUD SECURITY CONTROLS

Cloud security architecture is only effective if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management [6], [7]. The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind cloud security architecture. They can usually be found in one of the following categories:

1) Deterrent Controls:

These controls are set in place to prevent any purposeful attack on a cloud system. Much like a warning sign on a fence or a property, these controls do not reduce the actual vulnerability of a system.

2) Preventative Controls:

These controls upgrade the strength of the system by managing the vulnerabilities. The preventative control will safeguard vulnerabilities of the system. If an attack were to occur, the preventative controls are in place to cover the attack and reduce the damage and violation to the system's security.

3) Corrective Controls:

Corrective controls are used to reduce the effect of an attack. Unlike the preventative controls, the corrective controls take action as an attack is occurring.

4) Detective Controls:

Detective controls are used to detect any attacks that may be occurring to the system. In the event of an attack, the detective control will signal the preventative or corrective controls to address the issue.

5) Dimensions of cloud security:

Correct security controls should be implemented according to asset, threat, and vulnerability risk assessment matrices. While cloud security concerns can be grouped into any number of dimensions (Gartner names seven while the Cloud Security Alliance identifies fourteen areas of concern these dimensions have been aggregated into three general areas: Security and Privacy, Compliance, and Legal or Contractual Issues.

III. SECURITY ISSUES IN CLOUD COMPUTING

Cloud Deployments Models:

In the cloud deployment model, networking, platform, storage and software infrastructure are provided as services that scale up or down depending on the demand as depicted in figure 2. The Cloud Computing model has three main deployment models which are:

a. Private cloud:

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality.

b. Public cloud :

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis.

c. Hybrid cloud :

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure.

Fig. 1 shows different types of cloud computing.

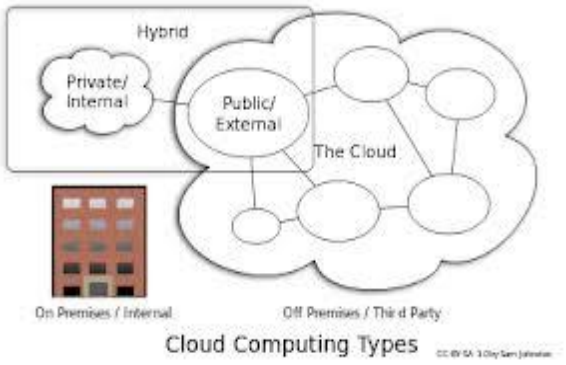


Fig. 1 Cloud Computing Types

IV. EXPERIMENTAL RESULTS

Windows Azure:

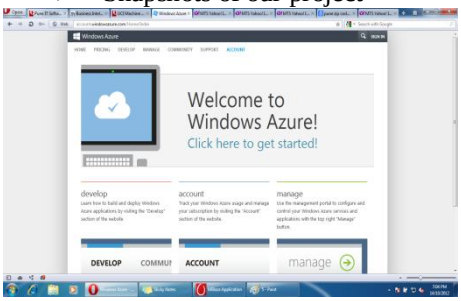
Windows Azure is a cloud computing platform and infrastructure created by Microsoft for building, deploying and managing applications and services through a global network of Microsoft-managed datacenters. It provides both platform as a service (PaaS) and infrastructure as a service (IaaS) services and supports many different programming languages, tools and frameworks, including both Microsoft-specific and third-party software and systems. Windows Azure is Microsoft's competing product to Amazon's AWS cloud computing platform.

Features of windows Azure:

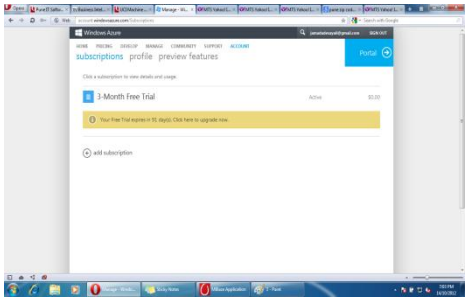
- Websites allows developers to build sites using ASP.NET, PHP, or Node.js and can be deployed using FTP, Git, or Team Foundation Server.
- Cloud services - Microsoft's Platform as a Service (PaaS) environment that is used to create scalable applications and services. Supports multi-tier scenarios and automated deployments.
- Data management - SQL Database, formerly known as SQL Azure Database, works to create, scale and extend applications into the cloud using Microsoft SQL Server technology.

Integrates with Active Directory and Microsoft System Center and Hadoop.

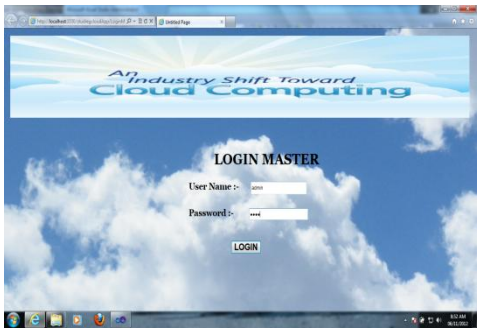
- We are providing url here of windows azure for free trial i.e. http://www.windowsazure.com/en-us/pricing/free-trial/
- Snapshots of our project-



Snapshot 1. Welcome window of Windows Azure



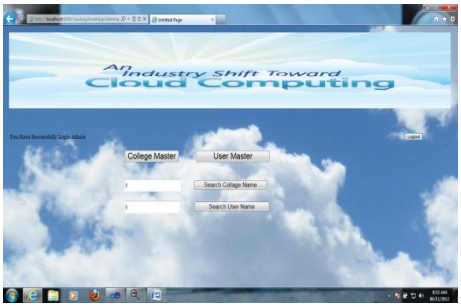
Snapshot 2. After registration window



Snapshot 3. Login window for Admin

We have used Windows Azure Cloud for our project. For that purpose we did registeration online on website.http://www.windowsazure.com/en-us/pricing/free-trial/. We have done this procedure using credit card.

We have used login master page providing username and password for authentication and security purpose and user master page for adding records of particular college including staff and students.



Snapshot 4. After login window of Admin

V. CONCLUSION

"Authentication in Cloud computing" represents different security issues which occur in cloud computing and how to make data secure from unauthorized users and check data integrity during transmission of data from cloud to users and vice versa and how to secure private data over Server.

Thus, in our work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and get back the original data from it. Hence forth, data security is provided by implementing RSA Algorithm and digital certificate.

REFERENCES

[1] Monaco, Ania (7 June 2012 [last update]). "A View Inside the Cloud". *theinstitute.ieee.org* (IEEE). Retrieved August 21, 2012.

[2] "Baburajan, Rajani, "The Rising Cloud Storage Market Opportunity Strengthens Vendors," infoTECH, August 24, 2011". It.tmcnet.com. 2011-08-24.Retrieved 2011-12-02.

[3] "The NIST Definition of Cloud Computing". National Institute of Standards and Technology.Retrieved 24 July 2011.

[4] Gruman, Galen (2008-04-07). "What cloud computing really means". *InfoWorld*.Retrieved 2009-06-02.

[5] "Jeff Bezos' Risky Bet". *Business Week*

[6] P.Kalpana, "Cloud Computing – Wave of the Future", *International Journal of Electronics Communication and Computer Engineering, Vol 3, Issue 3, ISSN 2249–071X, June 2012.*

[7] Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila et al, / (IJCSIT) *International Journal of Computer Science and Information Technologies, Vol. 2, 1836-1840, 2011.*