International Journal of Research (IJR) Vol-1, Issue-6, July 2014 **ISSN 2348-6848**

Critique of Cloud Integral's and it's Security Schema

Swati N. Sonune[1]

Abstract:

Cloud is an emerging technology in which the research community and industries have recently embarked. However, the infrastructures of most cloud computing systems today are invisible to the research community, or are not explicitly designed to the researchers interested in cloud computing systems. Cloud computing represents a significant shift in the way that IT resources are managed, operated, and consumed. This change exposes several benefits to enterprises, promoting greater IT efficiency and agility. Cloud is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet .Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud. When a Cloud is made available in a pay-as-you-go manner to the general public, we call it a Public Cloud; the service being sold is Utility Computing. We use the term Private Cloud to refer to internal datacenters of a business or other organization, not made available to the general public. Thus, Cloud Computing is the sum of SaaS and Utility Computing, but does not include Private Clouds. This paper is intended to depict a architecture of cloud computing, benefits of a cloud based system and security framework of enterprise systems on cloud and also we depict the Cloud paradigm from a variety of aspects, such as definitions, features, and technologies.

Keywords: Cloud, SAAS, PAAS, IAAS, Public Cloud, Private Cloud

[1] M.E., Department of Computer Science & Engg.
Shri Ram Institute of Technology. Jabalpur.
RGPV University, Bhopal, India
swatisonune@gmail.com

1. Introduction

CLOUDs are environments which provide resources and services to the user in a highly available and quality-assured fashion, thereby keeping the total cost for usage and administration minimal and adjusted to the actual level of consumption. The resources and services should be accessible for a principally unlimited number of customers from different locations and with different devices with minimal effort and minimal impact on quality. The environment should thereby adhere to security and privacy regulations of the end-user, in so far as they can be met by the internet of services. Cloud is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet .Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud. When a Cloud is made available in a pay-as-you-go manner to the general public, we call it a Public Cloud; the service being sold is Utility Computing. We use the term Private Cloud to refer to internal datacenters of a business or other organization, not made available to the general public. Thus, Cloud Computing is the sum of SaaS and Utility Computing, but does not include Private Clouds. People can be users or providers of SaaS, or users or providers of Utility Computing. We focus on SaaS Providers (Cloud Users) and Cloud Providers, which have received less attention than SaaS Users.

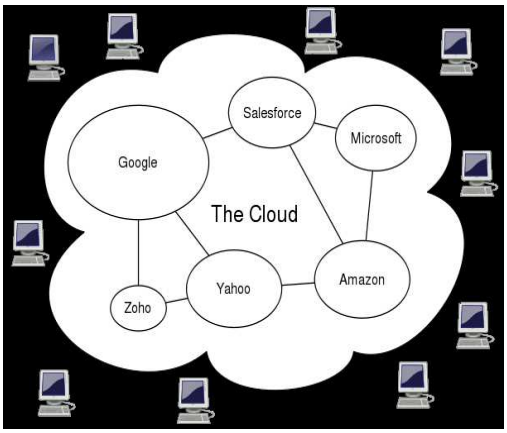

Fig. 1. Architecture of Cloud Computing

The concept generally incorporates combinations of the following:

1.1 Infrastructure As A Service (IAAS)

IaaS typically supports the user to specify the number of machines and provides different images of different operating systems. We believe that current support is too low level and does not encourage CSE researchers to use cloud computing. Infrastructure-as-a-Service like Amazon Web Services provides virtual server instances with unique IP addresses and 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. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and bring more online as soon as required. Because this pay-for-what-you-use model resembles the way electricity, fuel and water are consumed, it's sometimes referred to as utility computing.

1.2 Platform As A Service (PAAS)

PaaS provides existing tools for the developer to write and deploy cloud applications. Examples of PaaS are the Aptana , the Appirio Cloud Connectors Cloud computing for small research groups in CSE , and the Bommi integration components . Typically, a PaaS will provide a Web programming portal, a set of available components that can be composed, and libraries/tools that can be used easily. Providing PaaS for CSE means that cloud providers should support ready-to-use platforms for scientists to develop and test their applications. Platform-as-a-service in the cloud is defined as a set of software and product development tools hosted on the provider's infrastructure. Developers create applications on the provider's platform over the Internet. PaaS providers may use APIs, website portal or gateway software installed on the customer's computer. Force.com, (an outgrowth of Salesforce.com) and GoogleApps are examples of PaaS. Developers need to know that currently, there are not standards for interoperability or data portability in the cloud. Some providers will not allow software created by their customers to be moved off the provider's platform.

1.3 Software As a Service (SAAS)

Providing SaaS is especially interesting for many domains. For example, sharing application capabilities using Web services and Web portal is very fine when scientists do not want to share the application's source code and when their applications are computation-intensive and non-interactive with simple input data.

Software as a Service (SaaS) has the potential to transform the way information-technology (IT) departments relate to and even think about their role as providers of computing services to the rest of the enterprise. The emergence of SaaS as an effective software-delivery mechanism creates an opportunity for IT departments to change their focus from deploying and supporting applications to managing the services that those applications provide. A successful service-centric IT, in turn, directly produces more value for the business by providing services that draw from both internal and external sources and align closely with business goals.

SAAS as a concept is often associated with the application service providers (ASPs) of the 1990s, which provided "shrink-wrap" applications to business users over the Internet. These early attempts at Internet-delivered software had more in common with traditional on-premise applications than with modern SaaS applications in some ways, such as licensing and architecture. Because these applications were originally built as single-tenant applications, their ability to share data and processes with other applications was limited, and they tended to offer few economic benefits over their locally installed counterparts.

Today, SAAS applications are expected to take advantage of the benefits of centralization through a single-instance, multi-user (tenent) architecture, and to provide a feature-rich experience competitive with comparable on-premise applications. A typical SAAS application is offered either directly by the vendor or by an intermediary party called an aggregator, which bundles SAAS offerings from different vendors and offers them as part of a unified application platform.

SAAS model can add efficiency and cost savings for the both the vendor and customer. Customers save time and money since they do not have to install and maintain programs. The customers do not have to hire staff, or use existing staff to maintain the software. They also generally

do not have to buy any new hardware. This allows a customer to focus more resources on growing the business.

Shifting the burden of software hosting and development to the vendor can also speed up the time it takes for the customer to see a return on the software investment. Using the SAAS model, the number of seats can be increased as the business grows. This is usually faster and cheaper than purchasing another license and adding to another computer, as with traditional software. Vendors usually only have to update and maintain the software on the network, versus updating different copies of the software on different computers. This allows the vendor to provide the latest updates and technology to each customer in a timely manner. The drawback for the customer is that they do not control the software, and customization of programs may be limited.

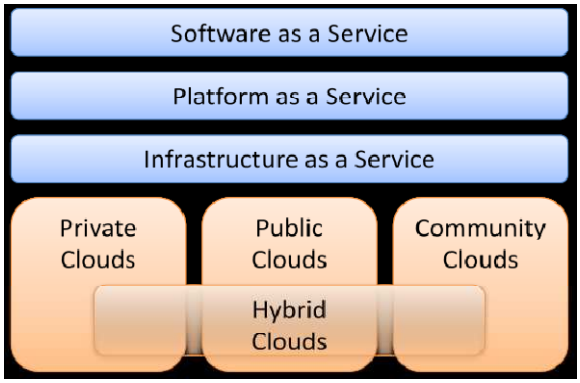

Figure 2: Cloud computing deployment and service models

2. Benefits Of Cloud Based Systems

- **Reduced Cost:** The business model of Cloud computing is pay-per-use and hence the customers only need to pay on the basis of the usage of a particular service.
- **Unrestrained Access:** Any user can access the system based upon the roles assigned to them. Since Cloud supports Ubiquitous network access, the system can be accessed using various devices of their choice and through any wired or wireless protocols.
- **Uptime:** The system is always up and running, which guarantees a zero down time.
- **Human Resources:** Maintenance of the system is done by the service provider. Hence no additional skilled man power needs to be employed by the organization.
- **Increased performance Requirements:** Expanding the system, handling peak load performance issues etc. become very simple for the organization.
- **Customization:** The customer has got the freedom to choose from among the modules and the services offered by the cloud service provider.
- **Group Organization:** All the different branches of an organization can access the same cloud based system in real time through the web.
- **Speedy Implementation:** Cloud ERP typically takes 3-6 months compared to the 12 months that it typically takes to implement an on-premise solution.

- **Scalability:** Cloud based enterprise systems gives the organization the flexibility to add more users as the business grows. In the case of on-site ERP solutions it is often necessary to provide additional hardware.

3. SECURITY FRAMEWORK COMPONENTS OF CLOUD

Literature reveals that many organizations are adopting cloud–based enterprise systems in the present scenario. But at the same time the enterprises should be convinced that security is not a threat for their implementation. Hence this study has been under taken to propose a framework to enhance the security. Figure 1 represents the components of the proposed security frame work for cloud-based enterprise systems.

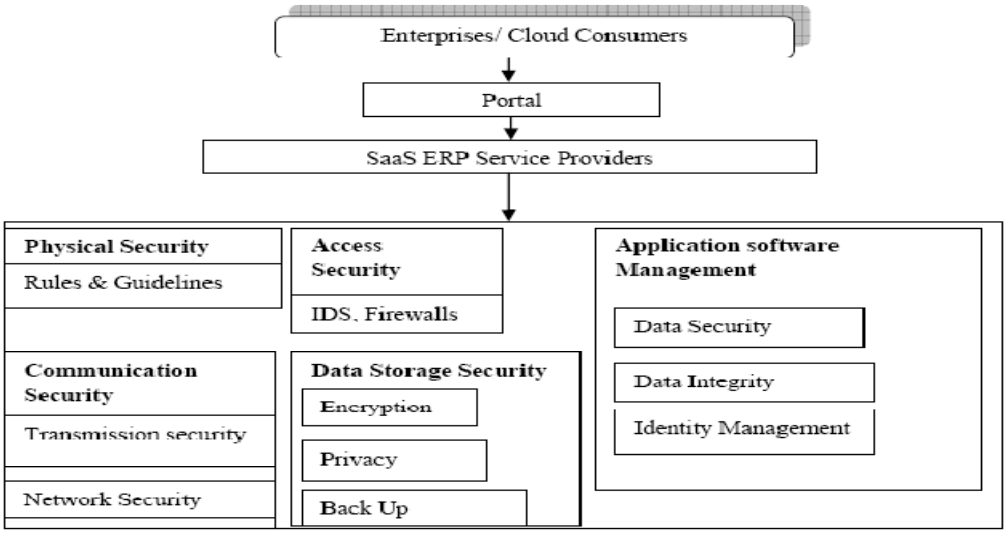

Fig 1. Proposed Security Framework for Cloud Based Enterprise Systems

3.1 Physical Security Management Module:

When an organization has its application running in an external cloud, the physical environment is off premise. A violation to physical security means that an unauthorized user with malicious intent has physical access to the hardware where either the application is running or data is stored. The physical security component must define and enforce rules of conduct and social guidelines for employees and have mechanisms to ensure that the rules are being adhered to. Also the component must include the solutions for disaster recovery.

3.2 Data Storage Security Management Module:

When ERP data is accessed by users, the business logic available in the system must ensure that only authorized

users are able to access the data and that there is clear segregation of data stored by different users. The system

also has a provision for backing up the data to aid in instances of disaster recovery.

3.3 Access Security Management Module:

Access security violations can happen from internal as well as external sources. Internal access Security is required to prevent illegal users from accessing resources and sending unauthorized queries to servers. The lack of proper implementation of access security could impact the availability of an application by authorized users such as in the case of a Denial of Service (DoS) attack. The access security module should have an Intrusion Detection Mechanism (IDS) to guard against such attacks. The module should have various perimeter security devices such as firewalls and must ensure that the various security policies put forward by the organization are incorporated and adhered to.

3.4 Application Software Management Module*:*

This module contains the business logic that ensures the security and integrity of data. The module also includes mechanisms for authenticating the users for providing services. The business logic included in the module also does the task of identity management.

3.5. Communication Management Module:

In a cloud-based enterprise system, the sensitive data is obtained from the enterprises, processed by the SaaS application and stored at the service provider's end. The communication management module assures the security of the information that gets communicated in the cloud environment either within a network or across

networks.

4. Conclusion

In this paper, I have proposed Cloud computing paradigm from a variety of aspects, such as definitions, features, and technologies. Moreover, we have illustrated several representative platforms for the state-of-the-art Cloud computing. Cloud based SaaS enterprise systems are growing in popularity due to its ability to cater to the increasing volume and range of services required by enterprise systems. Security challenges faced by cloud based systems needs to be addressed for the successful implementation of SaaS enterprise systems. A security framework has been designed for providing better security for cloud based enterprise systems. The proposed framework tries to address the security issues faced by SaaS based system.

5. References

1. Above the Clouds: A Berkeley View of Cloud Computing , *Michael Armbrust,Armando Fox, Rean Griffith etc,* February 10, 2009.
2. Research Agenda in Cloud Technologies, Ilango Sriram Department of Computer Science University of Bristol Bristol,

3. Ali Khajeh-Hosseini Cloud Computing Co-laboratory School of Computer Science University of St Andrews St Andrews
4. Cloud computing for small research groups in computational science and engineering: current status and outlook, Hong-Linh Truong · Schahram Dustdar Received: 15 February 2010 / Accepted: 3 September 2010 / Published online: 25 September 2010© Springer-Verlag 2010
5. Advances in Clouds, Research in future cloud computing , Lutz Schburt, Keith Jeffery.
6. ERDOGMUS, H. 2009. Cloud Computing: Does Nirvana Hide behind the Nebula? *Software, IEEE* 26, 2, 4-6.
7. Sun Microsystems, Introduction to Cloud Computing Architecture, 2009
8. VARIA, J.2009. *Cloud Architectures*. Amazon Web Services.
9. Bhadauria et al., ” A survey on Security Issues in Cloud Computing”, arXiv:1109.5388v1