International Journal of Scientific Research in Computer Science and Engineering
Review Paper Volume-2, Issue-3 ISSN: 2320-7639

# Analysis of Cloud Computing Security Issues in Software as a Service

Vishnu Patidar[1*], Makhan Kumbhkar[2]

[1*,2] *Department of Computer Science and Electronics,*
*Christian Eminent College Indore, M.P. - INDIA*

**Available online at www.isroset.org**

Received: 10 Mar 2014 Revised: 28 Mar 2014 Accepted: 12 May 2014 Published: 30 Jun 2014

***Abstract-*** Cloud computing is current buzzword in the market. It is standard in which the assets can be leveraged on per use basis thus reducing the cost and complexity of service providers. Cloud computing promises to cut operational and capital costs and more importantly let IT departments focus on strategic projects instead of keeping datacenters running. It is much more than simple internet. It is a construct that allows user to access applications that actually reside at location other than user's own computer or other Internet-connected devices. There are numerous benefits of this construct. For instance other company hosts user application[1]. This implies that they handle cost of servers, they manage software updates and depending on the contract user pays less i.e. for the service only. Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well. Software as a Service (SaaS) serves as the foundation layer for the other delivery models, and a lack of security in this layer will certainly affect the other delivery models, i.e., PaaS, and SaaS that are built upon IaaS layer. This paper presents an elaborated study of SaaS components' security and determines vulnerabilities and countermeasures. Service Level Agreement should be Considered very much importance [1].

***Keywords***— Computing, Cloud Computing Security, Service Level Agreement (SLA), Software as a Service (SaaS)

## I. INTRODUCTION

Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture (SOA) mature and new developmental approaches, such as Ajax, become popular. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world. SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. IDC identifies two slightly different delivery models for SaaS. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth[2].

## II. CLOUD COMPUTNG SERVICES

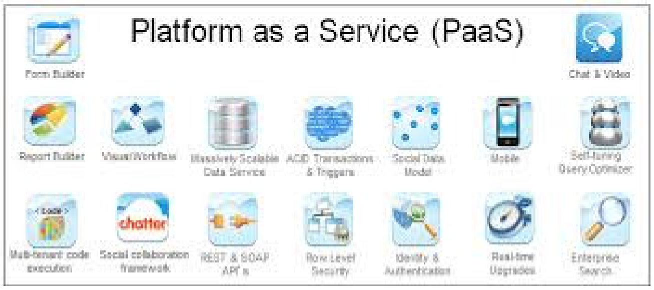
### *A. Infrastructure-as-a-Service*

Fig(1): Iaas Service

The Infrastructure as a Service is a provision model in which an organization outsourcers the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it through as Hardware as a Service (HaaS)[3].

### *B. Plateform-As-A-Service*

Platform as a Service (PaaS) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones. Platform as a Service (PaaS) is an outgrowth of Software as a Service (SaaS), a software distribution model in which hosted software applications are made available to customers over the Internet.


Platform as a Service (PaaS)
Form Builder
Chat & Video
Report Builder
Visual Workflow
Massively Scalable Data Service
ACID Transactions & Triggers
Social Data Model
Mobile
Self-tuning Query Optimizer
Multi-tenant code execution
Social collaboration framework
REST & SOAP API's
Row Level Security
Identity & Authentication
Real-time Upgrades
Enterprise Search
chatter

Fig(2): Paas Service

### *C. Software-As-A-Service*

No Software as a service sometimes referred to as "software on demand," is software that is deployed over the internet and/or is deployed to run behind a firewall on a local area network or personal computer. With SaaS, a provider licenses an application to customers either as a service on demand, through a subscription, in a "pay-as-you-go" model, or at no charge. This approach to application delivery is part of the utility computing model where all of the technology is in the "cloud" accessed over the Internet as a service. SaaS was initially widely deployed for sales force automation and Customer Relationship Management (CRM). Now it has become commonplace for many business tasks, including computerized billing, invoicing, human resource management, financials, content management, collaboration, document management, and service desk management.

Fig(3): Saas Service

## III. CLOUD COMPUTING SECURITY ISSUES

In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is[1].

### *A.* Identity management in the cloud is immature

Cloud providers themselves aren't always sophisticated about integrating their platforms with identity services that exist behind the enterprise firewall, says Forrester analyst Chenxi Wang. There are some third-party technologies that let IT extend role-based access controls into the cloud with single sign-on, from Ping Identity and Symplified, Wang says. But overall, "this is a field that is still in the early stage,"

We know that Google has a "Secure Data Connector" that forms an encrypted connection between a customer's data and Google's business applications, while letting the customer control which employees may access Google Apps resources. Salesforce provides a similar tool[2].

### *B.* Cloud standards are weak

We know that any cloud vendor touting its security credentials. SAS 70 is an auditing standard designed to show that service providers have sufficient control over data. The standard wasn't crafted with cloud computing in mind, but it's become stand-in benchmark in the absence of cloud-specific standards. On the other hand, users may leak hidden information when they accessing cloud computing services. There's no guarantee that your data will be safe with an ISO 27001-compliant vendor, however. One survey of IT managers commissioned by CA found numerous companies that claim to be compliant with ISO 27001 yet "admit to bad practices with regard to privileged user management," including sharing of administrator accounts between users and granting broader privileges to users than is necessary[2].

### *C.* Secrecy

Cloud vendors argue that they are more able to secure data than a typical customer, and that SaaS security is actually better than most people think. But some customers find this hard to believe because SaaS vendors tend to be rather secretive about their security processes.In particular, many cloud service providers release very few details about their data centers and operations, claiming it would compromise security. However customers and industry analysts are getting fed up with all the unanswered questions and hush-hush nondisclosure agreements.

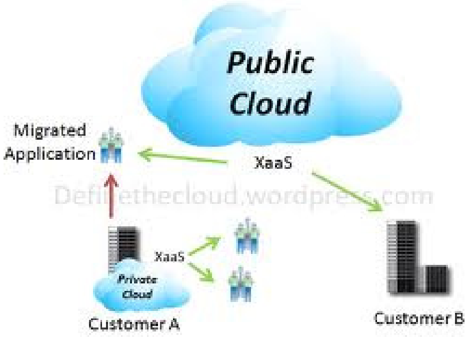
## IV. CLOUD COMPUTNG MODELS

### A. *Public Cloud*

A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model[1].

The main benefits of using a public cloud service are:

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



Fig(4): Public Clouds

### B. *Community Cloud*

Private cloud (also called internal cloud or corporate cloud) is a marketing term for a proprietary computing architecture that provides hosted services to a limited number of people behind a firewall. Advances in virtualization and distributed computing have allowed corporate network and datacenter administrators to effectively become service providers that meet the needs of their "customers" within the corporation. Marketing media that uses the words "private cloud" is designed to appeal to an organization that needs or wants more control over their data than they can get by using a third-party hosted service such as Amazon's Elastic Compute Cloud (EC2) or Simple Storage Service (S3)[4].

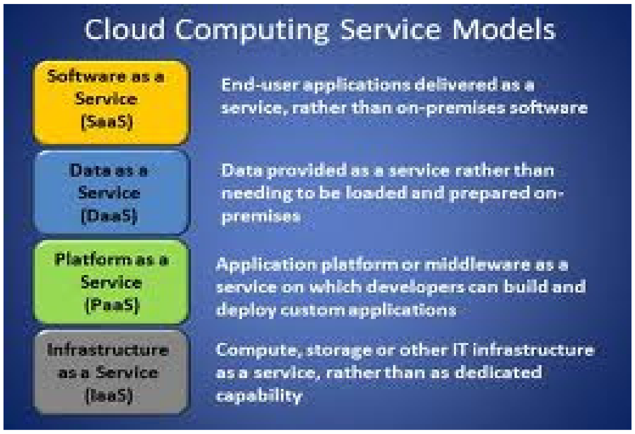
### *C. **Hybrid Cloud***

A hybrid cloud is a Cloud Computing environment in which an organization provides and manages some resources in-house and has others provided externally. For example, an organization might use a public cloud service, such as Amazon Simple Storage Service (Amazon S3) for archived data but continue to maintain in-house storage for operational customer data. Ideally, the hybrid approach allows a business to take advantage of the scalability and cost-effectiveness that a public cloud computing environment offers without exposing mission-critical applications and data to third-party vulnerabilities[4].

### *D. **Private Cloud***

A community cloud may be established where several organizations have similar requirements and seek to share infrastructure so as to realize some of the benefits of cloud computing. With the costs spread over fewer users than a public cloud (but more than a single tenant) this option is more expensive but may offer a higher level of privacy, security and/or policy compliance. Examples of community cloud include Google's "Gov Cloud"[5].

## V. ALL CLOUD MODELS ARE NOT THE SAME



Cloud Computing Service Models

Software as a Service (SaaS) — End-user applications delivered as a service, rather than on-premises software

Data as a Service (DaaS) — Data provided as a service rather than needing to be loaded and prepared on-premises

Platform as a Service (PaaS) — Application platform or middleware as a service on which developers can build and deploy custom applications

Infrastructure as a Service (IaaS) — Compute, storage or other IT infrastructure as a service, rather than as dedicated capability

Fig(5) Cloud Computing Models

Although the term Cloud Computing is widely used, it is important to note that all Cloud Models are not the same. As such, it is critical that organizations don't apply a broad brush one-size fits all approach to security across all models. Cloud Models can be segmented into Software as a Service (Saas), Platform as a service (PaaS) and Integration as a Service (IaaS). When an organization is considering Cloud Security it should consider both the differences and similarities between these three segments of Cloud Models.

## VI. SAAS COMPONENTS

SaaS delivery model consists of several components that have been developed through past years, nevertheless, employing those components together in a shared and outsourced environment carries multiple challenges. Security and Privacy are the most significant challenges that may impede the Cloud Computing adoption. Breaching the security of any component impact the other components' security, consequently, the security of the entire system will collapse. In this section we study the security issue of each component and discuss the proposed solutions and recommendations.

### ***A. Service Level Agreement (SLA)***

Cloud Computing emerges a set of IT management complexities, and using SLA in cloud is the solution to guarantee acceptable level of QoS. SLA encompasses SLA contract definition, SLA negotiation, SLA monitoring, and SLA enforcement. SLA contract definition and negotiation stage is important to determine the benefits and responsibilities of each party, any misunderstanding will affect the systems security and leave the client exposure to vulnerabilities. On the other hand, monitoring and enforcing SLA stage is crucial to build the trust between the provider and the client. To enforce SLA in a dynamic environment such Cloud, it is necessary to monitor QoS attributes continuously. Web Service Level Agreement (WSLA) framework developed for SLA monitoring and enforcement in SOA. Using WSLA for managing SLA in Cloud Computing environment was proposed in by delegating SLA monitoring and enforcement tasks to a third party to solve the trust problem. Currently, cloud clients have to trust providers' SLA monitoring until standardizing Cloud Computing systems and delegating third-parties to mediate SLA monitoring and enforcement.

### ***B. Utility Computing***

Utility computing refers to the ability to meter the offered services and charge customers for exact usage. It is interesting to note that the term originates from public utility services such as electricity.

Utility computing is very often connected to cloud computing as it is one of the options for its accounting. As explained in Cloud computing infrastructure, Utility computing is a good choice for less resource demanding applications where peak usage is expected to be sporadic and rare.

Still, Utility computing does not require Cloud computing and it can be done in any server environment. Also, it is unreasonable to meter smaller usage and economically inefficient when applied on a smaller scale. That is why it is most often applied on cloud hosting where large resources are being managed. The provider is the main responsible to keep the system healthy and well functioning, but the client's practice also affects the system.

***C. Cloud Software***

The one caveat for its findings, is that although the survey had 785 executive level respondents, 65% of these were providers, 35% were customers, and their responses were combined in the data. It would have been nice if all of the results were available separately for each of these groups, but having been both a customer and a provider, I know that providers often have much better visibility into the aggregate situation for a market. Hence, the providers' perspectives into such findings as the key drivers, inhibitors and trends for Cloud Computing adoption, actually represent experiences across their entire customer base. Additionally, even with the mixed respondents, the sheer magnitude of some of the data points, as well as their percent year-over-year change, serve as another proof point of the rapid escalation of adoption and market perceptions around Cloud.

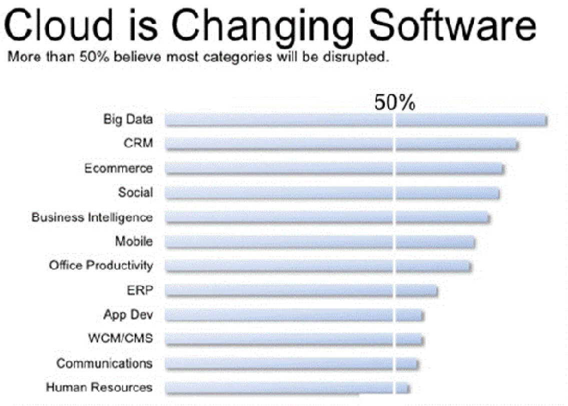


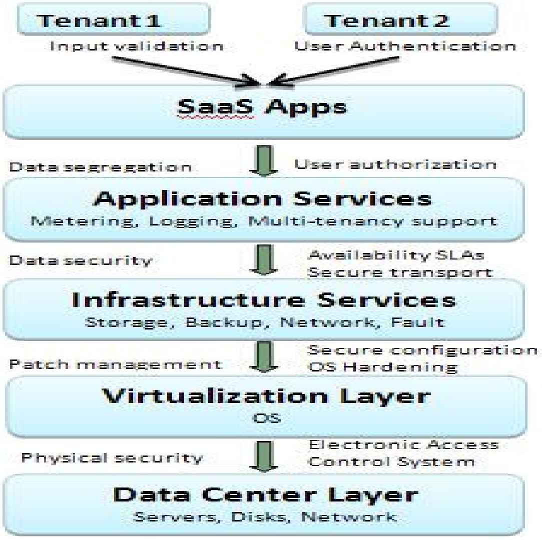
Fig (6): Cloud Is Changing Software

***D. Platform Virtualization***

Virtualization, a fundamental technology platform for Cloud Computing services, facilitates aggregation of multiple standalone systems into a single hardware platform by virtualizing the computing resources (e.g., network, CPUs, memory, and storage). Hardware abstraction hides the complexity of managing the physical computing platform and simplifies the computing resources scalability. Hence, virtualization provides multi tenancy and scalability, and these are two significant characteristics of Cloud Computing As the hypervisor is responsible for VMs isolation, VMs could not be able to directly access others' virtual disks, memory, or applications on the same host. IaaS, a shared environment, demands an accurate configuration to maintain strong isolation. Cloud service providers undertake a substantial effort to secure their systems in order to minimize the threats that result from communication, monitoring, modification, migration, mobility, and DoS. In this section, we discuss virtualization risks and vulnerabilities that affect particularly IaaS delivery model in addition to the recent proposed solutions to guarantee security, privacy, and data integrity for IaaS[17].

## VII. SECURITY MODEL FOR SAAS

As a result of this research, we also discuss a Security Model for SaaS (SMI) as a guide for assessing and enhancing security in each layer of SaaS delivery model as shown below. SMI model consists of three sides: IaaS components, security model, and the restriction level. The security model side includes three vertical entities where each entity covers the entire IaaS components. The first entity is Secure Configuration Policy (SCP) to guarantee a secure configuration for each layer in IaaS Hardware, Software, or SLA configurations; usually, miss-configuration incidents could jeopardize the entire security of the system. Nevertheless, we hope SMI model be a good start for the standardization of IaaS layers. This model indicates the relation between IaaS components and security requirements, and eases security improvement in individual layers to achieve a total secure IaaS system[16].



Fig(7): Security Model For PaaS

## VIII. CONCLUSION

In This paper we discuss about Various level of Software as a Service examine. Cloud Computing is a term that doesn't describe a single thing – rather it is a universal term that sits over a variety of services from Software as a Service at the base, through Platform as a Service as a development tool and through to infrastructure as a Service replacing on-premise applications.. In this paper an overview of cloud computing service delivery model, SaaS along with the security challenges , including both the traditional and cloud specific security challenges ,associated with the model has been presented A number of new challenges that is inherently connected to the new cloud paradigm has also been deliberated in the paper. As secure data storage in cloud environment is a significant concern which prevents many users from using the cloud, a practical solution to provide security and privacy for user data, when it is located in a public cloud, was also discussed in this paper. The need for further work on various security mechanisms has also been highlighted, in order to provide transparent services that can be trusted by all users .

**REFERENCES**

[1].M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, " *Technical Security Issues in Cloud Computing"*. IEEE, 2009.

[2]. Greg Boss, Padma Malladi, Denis Quan, Linda Legregni, Harold Hall, "Cloud Computing", http://www.ibm.com/developerswork/websphere/zones/hipods/library.html, October 2007, pp. 4-4.

[3]G. Frankova, *Service Level Agreements: Web Services and Security*, ser. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, vol. 4607.

[4]. "Service Level Agreement and Master Service Agreement", http://www.softlayer.com/sla.html, accessed on April 05, 2009.

[5]. S. Berger, R. Caceres, D. Pendarakis, R. Sailer, E. Valdez, R. Perez, W. Schildhauer, and D. Srinivasan, "Security for the cloud infrastrcture: trusted virtual data center (TVDc)." [Online]. Available: www.kiskeya.net/ramon/work/pubs/ibmjrd09.pdf

[6]. http://www.cloudsecurity.org, accessed on April 10, 2009.

[7]. "Sampling issues we are addressing", http://cloudsecurityalliance.org/issues.html#15, accessed on April 09, 2009.

[8]. MikeKavis,"Real time transactions in the cloud", http://www.kavistechnology.com/ blog/?p=789, accessed on April 12, 2009.

[9]. "Secure group addresses cloud computing risks", http://www.secpoint.com/security-group-addresses-cloudcomputing- risks.html, April 25, 2009.

[10]. "Service Level Agreement Definition and contents", http://www.service-level-agreement.net, accessed on March 10, 2009.

[11]"Cloud security alliance: Security guidance for critical areas of focus in cloud computing v2.1," Dec 2009. Available at: www.cloudsecurityalliance.org.

[12]. "Wesam Dawoud, Ibrahim Takouna, Christoph Meinel Infrastructure as a Service Security.

[13]. Dynamic job Scheduling in Cloud Computing based on horizontal load "Mousumi Paul1, Debabrata Samanta2, Goutam Sanyal3 Department of CSE" Vol 2 (5), 1552-1556, ISSN:2229-6093

[14]. V. Vijayalakshmi et al. / International Journal of Engineering Science and Technology (IJEST) "STUDY ON RECENT TRENDS AND OPPORTUNITIES IN CLOUD COMPUTING"

[15]. M.Sudha et. al. / (IJCSE) International Journal on Computer Science and Engineering "Investigation on Efficient Management of workflows in cloud computing Environment", Vol. 02, No. 05, 2010.

[16] S L Saini, Dinesh Kumar Saini, Jabar H. Yousif and Sandhya V Khandage "Cloud Computing and Enterprise Resource Planning Systems" , ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

[17 ] M.Sudha et. al. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 05, 2010, 1841-1845 , "Investigation on Efficient Management of workflows in cloud computing Environment "

[18] SADHANA RANA **. "** RISK ANALYSIS IN WEB APPLICATIONS BY USING CLOUD COMPUTING" , International Journal of Multidisciplinary Research Vol.2 Issue 1, January 2012, ISSN 2231 5780.

[19] Makhan Kumbhkar at el ,"Performance Improvement of Software as a Service and Platform as a Service in Cloud Computing Solution" Vol-1,Issue-6 ISSN: 2320-7639.

**AUTHORS PROFILE:**

I have done M-Phil(Computer Science) Degree The Global (Open) University Nagaland , India as well as MCA form Bhoj (Open) University, BHOPAL ,INDIA .I have more than 15 Years of experience in academics as well as administration. I have attended many conferences and Seminars at National and International Level. I would like to thank my colleagues of the Christian Eminent College, Indore, M.P., INDIA for their contributions, insights, and support.