*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727,*
*PP 40-44*
*www.iosrjournals.org*

# Issues & Solution of SAAS Model in Cloud Computing

Ms. Pushpa B. Rajegore[1], Ms. Swapna G. kadam[2]
[1.] *Dept. of Computer Science and Information Technology ,MGM Dr. G.Y.Pathrikar college of C.S. & I.T, Aurangabad. India*
[2.] *Dept. of Computer Science and Information Technology ,MGM Dr. G.Y.Pathrikar college of C.S. & I.T, Aurangabad. India*

***Abstract:*** *Cloud computing of is an Internet-based computing, where shared resources, software and information, are provided to computers and devices on-demand. It provides people the way to share distributed resources and services that belong to different organization. Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. Security is one of the major issues which hamper the growth of cloud. in This paper we introduce what is cloud computing in saas model. And also provide the security issues & solution of cloud computing. And detail description of what are the security issues & Solution in SAAS model. And also define the Solution on that issue.*

***Keywords:*** *Cloud Computing, Software as a Service, Challenges, Issues, solution.*

## I. Introduction

A lot has been written and spoken about Cloud Computing technology, by IT experts, industry and business leaders and independent experts. While some believe it is a disruptive trend representing the next stage in the evolution of the Internet, others believe it is hype, as it uses earlier established computing technologies. So, what exactly is cloud computing? From a user perspective, cloud computing provides a means for acquiring computing services without any need for deep understanding of the underlying technology being used from an organization.[1]

Our main area of concern in this paper is the Software as a service (SaaS). model This best-known branch of cloud computing , is a delivery model in which applications are hosted and managed in a service provider's datacenter, paid for on a subscription basis and accessed via a browser over an internet connection. It basically deals with licensing of an application to the customers for use as a service on demand. Perspective, cloud computing delivers services for consumer and business needs in a simplified way, providing unbounded scale and differentiated quality of service to foster rapid innovation and decision making. This paper focuses on the issues related to the service delivery model of cloud computing.

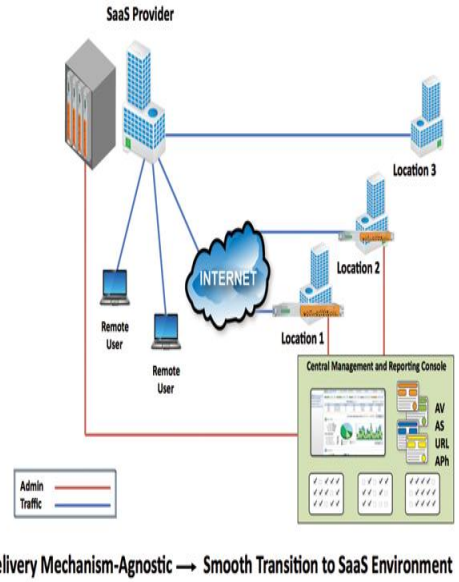


**Fig.1** Delivery Mechanism-Agnostic Smooth Transition to saas Environment

**1.1 Software as a Service (SaaS) :**

SAAS is a software licensing and delivery model. It provides software services on demand. The use of single instance of the application runs on the cloud services and multiple end users or client organizations. SAAS is used as strategies of nearly all leading enterprise software companies. The most widely known example of SaaS is salesforce.com, though many other examples have come to market, including the Google Apps offering of basic business services including email and word processing. Although salesforce.com preceded the definition of cloud computing by a few years, it now operates by leveraging its companion force.com, which can be defined as a platform as a service.

**1.2. Challenges of SAAS model:**

There are varies challenges while adopting cloud computing in Saas, because users are still worried about it's authenticity. The major challenges that prevent Cloud Computing from being adopted are recognized by organizations are as follows:

**A. Security:** It is clear that the security issue is most important in Cloud computing acceptance. Without doubt, putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. Some of the security issues are data loss, phishing, botnet pose serious threats to organization's data and software. For example, hackers can use Cloud to organize botnet as Cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start an attack.[2]

**B. Costing Model:** Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. While migrating to the Cloud can significantly reduce the infrastructure cost, it causes raise in the cost of data communication, i.e. the cost of transferring an organization's data to and from the public and community Cloud and the cost per unit of computing resource used is likely to be higher.

**C. Charging Model:** The elastic resource pool has made the cost analysis a lot more complicated than regular data centers, which often calculates their cost based on consumptions of static computing. Moreover, an instantiated virtual machine has become the unit of cost analysis rather than the underlying physical server. The cost of developing Multi tenancy within their offering can be very substantial for SaaS cloud providers. Consequently, SaaS providers need to weigh up the trade-off between the provision of multi tenancy and the cost-savings yielded by multi-tenancy such as reduced overhead through amortization, reduced number of on-site software licenses, etc. Therefore, a strategic and viable charging model for SaaS provider is crucial for the profitability and sustainability of SaaS cloud providers.

**D. Service Level Agreement (SLA):** Although cloud consumers do not have control over the Underlying computing resources, they do need to ensure the quality, availability, reliability, and performance of these resources when consumers have migrated their core business functions onto their entrusted cloud. In other words, it is vital for consumers to obtain guarantees from providers on service delivery.[8] Typically, these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers.

**E. Cloud Interoperability Issue:** Currently, each cloud offering has its own way on how cloud Clients/applications/users interact with the cloud, leading to the "Hazy Cloud" phenomenon. This severely hinders the development of cloud ecosystems by forcing vendor locking, which prohibits the ability of users to choose from alternative vendors/offering simultaneously in order to optimize resources at different levels within an organization.The primary goal of interoperability is to realize the seamless fluid data across clouds and between cloud and local applications. There are a number of levels that interoperability is essential for cloud computing.

## II. Security Issues In SAAS:

In Software as a Service (SaaS) model, the client has to depend on the service provider for proper security measures. It becomes important to the user to ensure that right security measures are in place and also difficult to get an assurance that the application will be available when needed. While using SaaS model, the cloud customer will, be substituting new software applications for old ones. Therefore, the focus is on preserving or enhancing the security functionality provided by the legacy application and achieving a successful data migration instead of portability of applications. The SaaS software vendor may host the application on his own private server or deploy it on a cloud computing infrastructure service provided by a third-party provider (e.g. Amazon, Google, etc.). Enterprises today view data and business transactions as strategic and guard them with access control and compliance policies. However, in the SaaS model, enterprise data is stored at the SaaS provider's data center, along with the data of other enterprises. Moreover, if the SaaS provider is leveraging a

public cloud computing service, the enterprise data might be stored along with the data of other unrelated SaaS applications. The cloud provider might, additionally, replicate the data at multiple locations across countries for the purposes of maintaining high availability. The SaaS security issues have been categorized as traditional and new cloud specific security challenges, for sake of convenience.

**2.1. Availability:**

The availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. The availability of cloud service providers is also a big concern, since if the cloud service is disrupted; it affects more customers than in the traditional model. [4]The SaaS application providers are required to ensure that the systems are running properly when needed and enterprises are provided with services around the clock. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. Resiliency to hardware/software failures, as well as to denial of service attacks, needs to be built from the ground up within the application.

**2.2. Data confidentiality:**

Confidentiality is refered as the prevention of intentional or unintentional unauthorized disclosure of information. Confidentiality area in cloud system includes the areas of intellectual property rights, covert channels, traffic analysis, encryption, and inference. Cloud computing involves the sharing or storage of information on remote servers owned or operated by others, while accessing through the Internet or any other connections. There are differences in cloud computing services. it includes data storage sites, video sites, tax preparation sites, personal health record websites and many more. [5]All the contents of a user's storage device may be stored with a single cloud provider or with many cloud providers. Privacy and confidentiality is important whenever an individual, a business, a government agency, or any other entity shares information in the cloud.

**2.3. Virtual Machine Security:**

Although the global adoption of virtualization is a relatively a recent phenomena, threats to the virtualized infrastructure are evolving just as quickly. [6]The hypervisor and virtual machines used in cloud providers may also have vulnerabilities, as exemplified by Such vulnerabilities represent an even more serious problem in multi-tenant environments, where compromise of even a single virtual machine can affect all users on the same physical server. Virtualization is one of the main components of a cloud. But this poses major security risks ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization which is not met completely in today's scenario. The other issue is the control of administrator on host and guest operating systems.

**2.4. User Access:**

Users ask providers for specific information on the hiring and oversight of privileged administrators and the controls over their access to information.[3] Major Companies should demand and enforce their own hiring criteria for personnel that will operate heir cloud computing environments.

**2.5. Regulatory Compliance:**

Make sure your provider is willing to submit to external Audits and security certifications.

**2.6. Data location:**

Enterprises should require that the cloud computing provider store and process data in specific jurisdictions and should obey the privacy rules of those Jurisdictions.[3]

**2.7. Data Segregation:**

Find out what is done to segregate your data, and ask for proof that encryption schemes are deployed and are effective.

**2.8. Disaster Recovery Verification:**

Know what will happen if disaster strikes by asking whether your provider will be able to completely restore your data and service, and find out how long it will take.

**2.9. Disaster Recovery:**

Ask the provider for a contractual commitment to support specific types of investigations, such as the research involved in the discovery phase of a lawsuit, and verify that the provider has successfully supported such activities in the past. Without evidence, don't assume that it can do so.[4]

**2.10. Long-term Viability:**

Ask prospective providers how you would get your data back if they were to fail or be acquired, and find out if the data would be in a format that you could easily import into a replacement application.

## III. Solution of Security Issues

The increase in malicious attacks, whether email, Web based, or across the Network, is impacting individuals and organizations in many ways. Threats are rapidly evolving, increasing the complexity of managing on site security solutions with finite resources. For optimal protection, threats must be managed in the cloud, before they reach users' systems and compromise information security.

Trend Micro Software as a Service (SaaS) Security Solutions provide industry leading Internet content security for individual users, small, medium and enterprise businesses, as well as service provider partners. These hosted service offerings influence the strength of the Trend Micro Smart Protection Network to immediately and automatically protect customers' information and resources against the latest threats wherever they connect. Moreover, all SaaS solutions are hosted and maintained by Trend Micro security experts, ensuring easy deployment and 24x7 availability.

This also allows Service Providers to focus on quick application delivery with no capital expenditure (CAPEX) and therefore minimum financial exposure.

**1. Find Key Cloud Provider:**

The very First solution is to find the right cloud provider. Different vendors have different cloud IT security and data management. A cloud vendor should be well established, have experience, standards and regulation. So there is not any chance of cloud vendor closing.

**2. Clear Contract:**

Contract with cloud vendor should be clear. So if cloud vendor closes before contract, enterprise can claim.

**3. Recovery Facilities:**

Cloud vendors should provide very good recovery facilities. So, if data are fragmented or lost due to certain issues, they can be recovered and continuity of data can be managed.

**4. Better Enterprise Infrastructure:**

For betterment of enterprise, it must have infrastructure which facilitates installation and configuration of hardware components such as firewalls, routers, servers, proxy servers and software such as operating system, thin clients, etc. Also should have infrastructure which prevents from cyber attacks.

**5. Use of Data Encryption for security purpose:**

Developers should develop the application which provides encrypted data for the security. So additional security from enterprise is not required and all security burdens are placed on cloud vendor.

IT leaders must define strategy and key security elements to know where the data encryption is needed.

**6. Prepare chart regarding data flow :**

There should be a chart regarding the flow of data. So the IT managers can have idea where the data is for all the times, where it is being stored and where it is being shared. There should be total analysis of data.

**7. WorryFree Business Security Services**:

Designed primarily for small business customers but also suitable for larger companies,it protects desktops and laptops wherever they are connected in the office, at home, or on the road.

**8. Hosted Email Security:**

A no maintenance required solution that delivers continuously updated protection to stop spam and email based malware before they reach the customer's network.

**9. Email Security Platform for Service Providers:**

Provides email filtering, antispam , and antivirus within a centrally managed, highly scalable
Architecture complete with a customizable user interface and tiered administration levels.

## IV. Conclusion

Cloud computing is a combination of several key technologies that have evolved and matured over the years. Cloud computing has a potential for cost savings to the enterprises but the security risk are also enormous. Enterprise looking into cloud computing technology as a way to cut down on cost and increase profitability should seriously analyze the security risk of cloud computing.

This security module should cater to all the issues arising from all directions of the cloud. Every element in the cloud should be analyzed at both the macro and micro level and subsequently an integrated solution must be designed and deployed in the cloud to attract and retain the potential consumers. Until then, cloud environment will remain cloudy. In a cloud, where there are heterogeneous systems having a variation in their asset value, a single security system would be too costly for certain applications and if there is less security then the vulnerability factor of some applications like financial and military applications will shoot up.

In this paper an overview of cloud computing service delivery model, SaaS along with the security solution , including both the traditional and cloud specific security challenges ,associated with the model has been presented A number of new solutions 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.

## V. Future Work

Cloud computing in SAAS model is the future of IT industries. It helps the industries to get efficient use of their IT Hardware and Software resources at low cost. This paper totally discuss about the cloud computing security issues and Solution. This paper also analyze cloud computing vulnerabilities, security threats cloud computing faces and presented the security objective that need to be achieved. On one hand, the security-sensitive applications of a Cloud computing of SAAS require high degree of security on the other hand, cloud computing are inherently vulnerable to security attacks. Therefore, there is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The future of cloud computing In SAAS is really appealing, giving the vision of cheap communications. At present, the general trend in cloud computing is toward mesh architecture and large scale. Improvement in bandwidth and capacity is required, which implies the need for a higher frequency and better spatial spectral reuse. Large scale cloud computing of SAAS is another challenging issue in the near future which can be already foreseen.

## References

[1]. ijceronline.com/papers/Vol4_issue06/version-2/J3602068071.pdf ISSN (e): 2250 – 3005 || Vol, 04 || Issue, 6 || June – 2014 || International Journal of Computational Engineering Research (IJCER).
[2]. scribd.com/document/228266788/Survey-on-Security-Issues-and-Solutions-in-Cloud-Computing.International Journal of Computer Trends and Technology (IJCTT) – volume 8 number 3– Feb 2014
[3]. essay.uk.com/essays/computer-science/essay-cloud-computing
[4]. ijetae.com/files/Volume2Issue8/IJETAE_0812_53.pdf. International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 8, August 2012)
[5]. arxiv.org/ftp/arxiv/papers/1309/1309.2426.pdf. International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.4, August 2013
[6]. slideshare.net/dheerajsnegi9/cloud-computing-security-issues-and-challenges-38399521
[7]. Seccombe A.., Hutton A, Meisel A, Windel A, Mohammed A, Licciardi A, (2009). Security guidance for critical areas of focus in cloud computing, v2.1. Cloud Security Alliance, 25 p.
[8]. scribd.com/document/88153949/V2I30030.
[9]. Heiser J.( 2009) What you need to know about cloud computing security and compliance, Gartner,Research, ID Number: G00168345.
[10]. Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online Michael Miller
[11]. Cloud Application Architectures: Building Applications and Infrastructure in the Cloud (Theory in Practice) by George Reese.
[12]. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice) by Tim Mathe
[13]. Choudhary V.(2007). Software as a service: implications for investment in software development.
[14]. International conference on system sciences, 2007.
[15]. B. Hari Krishna, S. Kiran, G. Murali, R. Pradee Kumar Reddy, Security Issues in Service Model of Cloud Computing Environment, Procedia Computer Science, Volume 87, 2016, Pages 246-251, ISSN 1877