

# Securing Software as a Service (SaaS) Model of Cloud Computing: Issues and Solutions

Mr. Suryakant E. Madane

[suryakantmadane91@rediffmail.com](mailto:suryakantmadane91@rediffmail.com)

Mrs. Ashwini Brahme

[ashwinibrahme@sinhgad.edu](mailto:ashwinibrahme@sinhgad.edu)

*Abstract-This paper provides an insightful analysis of the existing status on cloud computing security issues based on a detailed survey carried by the author. When we access cloud Applications or Software what security problems or errors occurs and how to resolve it. It also makes an attempt to describe the security challenges in Software as a Service (SaaS) model of cloud computing and also endeavours to provide future security research directions. While it is important to take advantages of cloud based computing by means of deploying it in diversified sectors, the security aspects in a cloud based computing environment remains at the core of interest. Keywords- Cloud Computing, Service Delivery Models, Software as a Service, Security Challenges, Privacy.*

## I. INTRODUCTION

Cloud computing allows application software to be operated using internet-enabled devices. Cloud computing exhibits the following key characteristics:

Agility improves with users' ability to re-provision technological infrastructure resources.

Cost reductions claimed by cloud providers.

Device and location independence enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone)

Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

Multitenancy enables sharing of resources and costs across a large pool of users thus allowing for:

Centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)

Peak-load capacity increases (users need not engineer for highest possible load-levels)

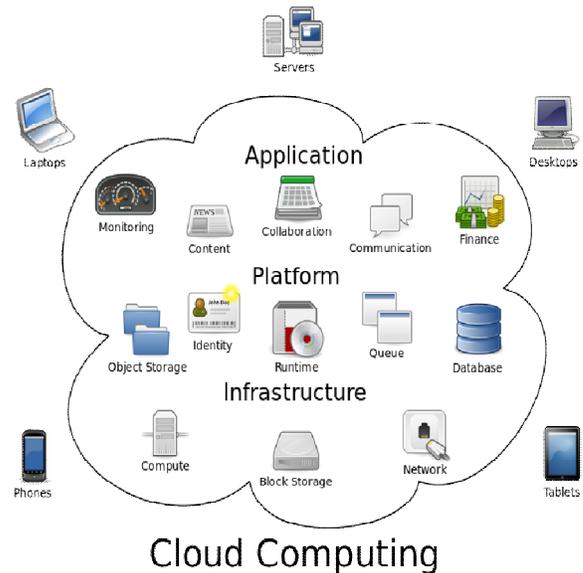
Utilization and efficiency improvements for systems that are often only 10–20% utilised.

Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.

Productivity may be increased when multiple users can work on the same data simultaneously.

Security can improve due to centralization of data, increased security-focused resources etc.

Reliability improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for business continuity and disaster recovery.



## Service Models-

Cloud computing providers offer their services according to several fundamental models.

Infrastructure as a service (IaaS)

Platform as a service (PaaS)

Software as a service (SaaS)

## 2.SecurityIssues in SaaS/Existing System

In Software as a Service (SaaS) model, the client has to depend on the service provider for proper security measures. The provider must ensure that the multiple users don't get to see each other's data.

### 2.1 Traditional Security Challenges

1. Authentication and authorization
2. Availability
3. Data confidentiality
4. Virtual Machine Security

### 2.2 Cloud Specific Security Challenges

1. Information Security
2. Network Security
3. Resource Locality
4. Cloud standards
5. Data Segregation
6. Data Access
7. Web application security
8. Data breaches
9. Backup
10. Identity management and sign-on process

#### 1. Efficient SaaS With API Integration

Software-as-a-service (SaaS) is a contemporary cloud computing trend emerging in the IT industry which is getting better day by day and a preferred choice of service delivery model for cloud providers. Biggest advantage of SaaS cloud computing service delivery model is the more meaningful, powerful and efficient integration of Application Programming Interface (API). Now a days Business needs or demands are evolving day by day, in order to meet these demands from their customers or end users, cloud providers need to maintain & utilize their resources efficiently for providing services they are confined with. In order to meet these challenges businesses needs to update their applications & services with the pace of the new technology.

#### 3. Hypothesis

Securing Software as a Service (SaaS) Model of Cloud Computing: Issues and Solutions.

#### 4. Objective Hypothesis

1. User Satisfaction
2. Easy to Access data
3. Cost Effective
4. Time Saving

5. Well Resource Utilization
6. Improve Flexibility
7. Improve Accessibility
8. Disaster recovery
9. Security
10. Work from Anywhere.

### 5. Current solutions available for securing SaaS

S.no.	Security Areas	Current /Possible Solutions
1	Backup	• Method for data Backup and Recovery
2	Availability	• Data Dispersion
3	Data confidentiality	• Attribute based Proxy Re-Encryption
4	Virtual Machine	• Survey on Virtual machine Security
5	Information Security	• Information Security Risk Management
6	Network Security	• Network Security for virtual machines • Network Security Sandbox
7	Cloud standards	• IEEE Cloud Computing Standard Study • ITU Cloud Computing Focus Group • Cloud Security Alliance (CSA)
8	Data Access	• Multi-user access policies • Data Access Management
9	Web application	• Web Application Scanners
10	Authentication and authorization	• Open Authorization • Two Factor Authentication

### 6. Conclusion-

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. 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.

**6. References-**

- <http://www.cs.indiana.edu/mit.research.how.to/mit.research.how.to.html>
- <http://www-2.cs.cmu.edu/afs/cs.cmu.edu/user/mleone/web/how-to.html>