

# Cloud Computing Security Issues, Challenges and Solution: A Review

Sulender<sup>1</sup>, Mrs. Neeraj Chauhan<sup>2</sup>

<sup>1</sup>Student, College of Computing Sciences and Information Technology, Teerthanker Mahaveer University, Moradabad  
College of Computing Sciences and Information Technology, Teerthanker Mahaveer University, Moradabad

[1sulenderraj1911@gmail.com](mailto:sulenderraj1911@gmail.com)

[2neeraj.computers@tmu.ac.in](mailto:2neeraj.computers@tmu.ac.in)

**Abstract**— this paper explores the concept of cloud computing security issues, challenges and also defines the solution of these issues. Cloud computing is an Internet-based computing, where shared resources, software and information, are provided to computers and devices on-demand. We describe various service and deployment models of cloud computing and identify major challenges. In particular, we discuss three critical challenges: regulatory, security and privacy issues in cloud computing. Some solutions to mitigate these challenges are also proposed along with a brief presentation on the future trends in cloud computing deployment. Cloud Computing is a new operational model which is providing very easy and cost effective for hosting and delivering the services e.g. Platform as a Service (PaaS), Software as a Service (SaaS), Infrastructure as a Service (IaaS).

**Keywords**— Cloud computing, Platform as a Service, Software as a Service, Infrastructure as a Service, Software as a Service

## I. INTRODUCTION

Cloud Computing is the combination of a technology, platform that provides hosting and storage service on the Internet. Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels. In the increasingly prevalent cloud computing, datacentre play a fundamental role as the major cloud infrastructure providers, such as Amazon, Google, and Microsoft Azure. Cloud computing is sharing of resources on a larger Scale which is cost effective and location independent. Mobile cloud computing is simply defined as combining the cloud computing services into the mobile ecosystem that brings the wireless network and cloud computing, which provides outstanding services to the users? Mobile devices access centralized applications over the wireless

connection based on a web browser or a thin native client.

## II. LITERATURE REVIEW

Yandong and Yongsheng (2012) compared security challenges in public and private cloud and argued that private cloud is more secure as compared to public cloud, though its deployment cost is very high and only large enterprises can invest in it. Security threats due to flexibility and more open access interface, vulnerability of virtualisation technology, privacy of data, are the security challenges. However, these security challenges of public cloud are unsatisfactory to justify that public cloud can be preferred over private cloud.

Data integrity and authentication was the focus of (Mace et al., 2011) research and it shows that resources sharing, availability of data and resources, data and privacy breaches and digital forensics are the security risks in CC, which highly affect the trust and security of CSUs in CC. Data and privacy breaches were conducted to change data in virtualisation layer using Virtual Machine Introspection (VMI).

Almulla and Yeun (2010) explain that Confidentiality, Integrity and Availability (CIA triad) are the major concerns of CSUs while Identity and Access Management (IAM) protocols must be protected by CSPs in order to maintain the authentication, authorisation and auditing of CSUs. Access control management technique ensures access to cloud data and resources by authorised

users only and allow CSUs to maintain rules and policies by enforcing login and passwords for legitimate users (Zhou et al., 2010).

Integrity and availability of data and resources are other challenges in CC. Service Level Agreement (SLA) and multi-model based solutions specified by CSPs provide data and resources integrity and availability assurance to CSUs (Kaur and Kaushal, 2011) to which (Almulla and Yeun (2010) propose a solution of using IAM protocols smartly and protecting them. Isolation, availability and cryptography are the main features in multi-model based approach (Kumar et al., 2010) to address these security challenges.

### III. CLOUD COMPUTING SERVICE MODELS

There are three different broad service models for cloud computing:

a) Software as a Service (SaaS), where applications are hosted and delivered online via a web browser offering traditional desktop functionality for example Google Docs, Gmail and MySAP.

b) Platform as a Service (PaaS), where the cloud provides the software platform for systems (as opposed to just software), the best current example being the Google App Engine.

c) Infrastructure as a Service (IaaS), where a set of virtualized computing resources, such as storage and computing capacity, are hosted in the cloud; customers deploy and run their own software stacks to obtain services. Current examples are Amazon Elastic Compute Cloud (EC2), Simple Storage Service (S3) and Simple DB.

Cloud computing technology is also differentiated by scope. In private clouds; services are provided exclusively to trusted users via a single-tenant operating environment. Essentially, an organization's data centre delivers cloud computing services to clients who may or may not be in the premises. Public clouds are the opposite: services

are offered to individuals and organizations who want to retain elasticity and accountability without absorbing the full costs of in-house infrastructures. Public cloud users are by default treated as untrustworthy. There are also hybrid clouds combining both private and public cloud service offerings.

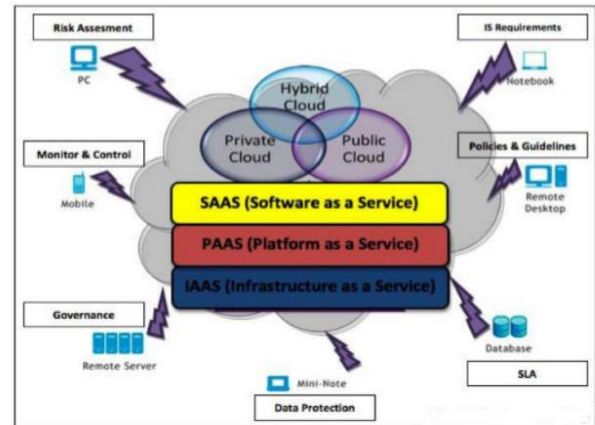


FIG. 1 CLOUD COMPUTING MODELS

### IV. CLOUD COMPUTING ARCHITECTURE

There are several major cloud computing providers including Amazon, Google, Sales force, Yahoo, Microsoft and others that are providing cloud computing services. Cloud computing providers provide a variety of services to the customers and these services include e-mails, storage, platform-as-a-services, software-as-a-services, infrastructure-as-a-services etc.

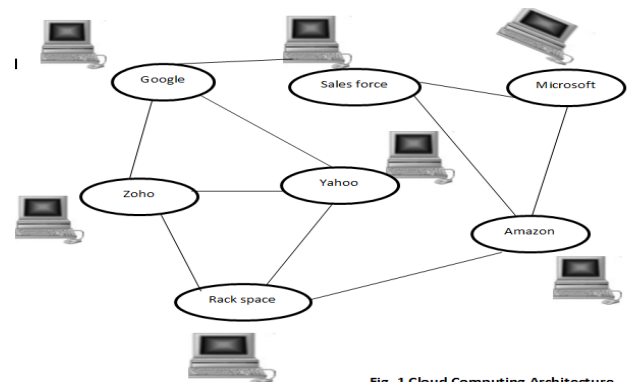


Fig. 1 Cloud Computing Architecture

In practice, cloud service providers tend to offer services that can be grouped into three categories: software as a service, platform as a service, and infrastructure as a service.

#### A. Software as a Service (SaaS)

This service is commonly used by business users. This service provides the complete applications to the user which is customizable within the limits. It is mainly used for achieving specific business task with the focus on end- user requirements.

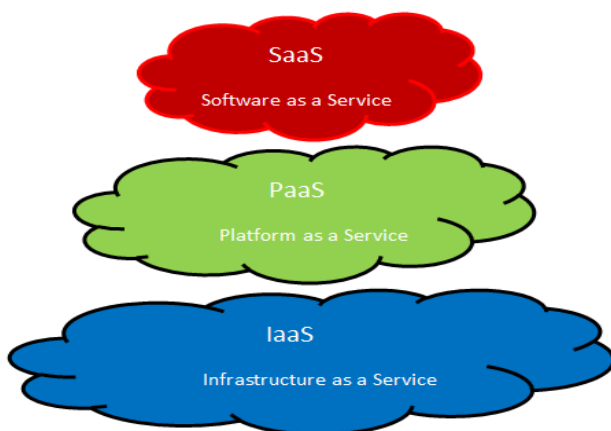


Fig. 2 Cloud Services and Application

#### B. Platform as a service (PaaS)

Platform as a Service is similar to SaaS, but the service is an entire application development environment, not just the use of an application. Its solutions differ from SaaS solutions in that they provide a cloud-hosted virtual development platform, accessible via a Web browser. Platform as a service encapsulates a layer of software and provides it as a service that can be used to build higher level services.

#### C. Infrastructure as a service (IaaS)

Infrastructure as a service delivers basic storage and compute capabilities as standardized services over the network. Servers, storage systems, switches,

routers, and other systems are pooled and made available to handle workloads that range from application components to high performance computing applications. This service is mainly used by the system managers. The main advantage is that there is no need to purchase a server or manage physical data centre equipment such as storage, networking, etc.

### V. TYPES OF CLOUDS AND ISSUES

Cloud environment we can class into different types, each with its own benefits and drawbacks:

#### A. Public clouds

In this service providers offer their resources as services to the general public. In public cloud computing there will not be initial amount on infrastructure. However public clouds have drawback that does not have control over the data, network and security settings, which hampers their effectiveness in many business scenarios.

#### B. Private clouds

These are internal clouds and are used by a single organization. It has the advantage of highest degree of control over performance, reliability and security. The drawback of private clouds it is being similar to traditional proprietary server farms and does not provides benefits such as no up-front capital costs.

#### C. Hybrid clouds

This is the combination of public and private cloud models and it will tries to overcome the limitations of both private and public clouds. These are more flexible than private and public clouds and it will provide more control and security over the system and data.

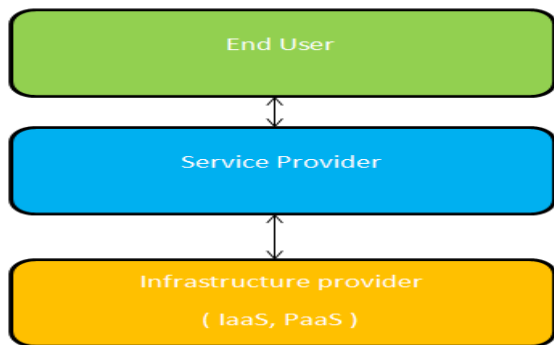


Fig. 3 Business model of cloud computing

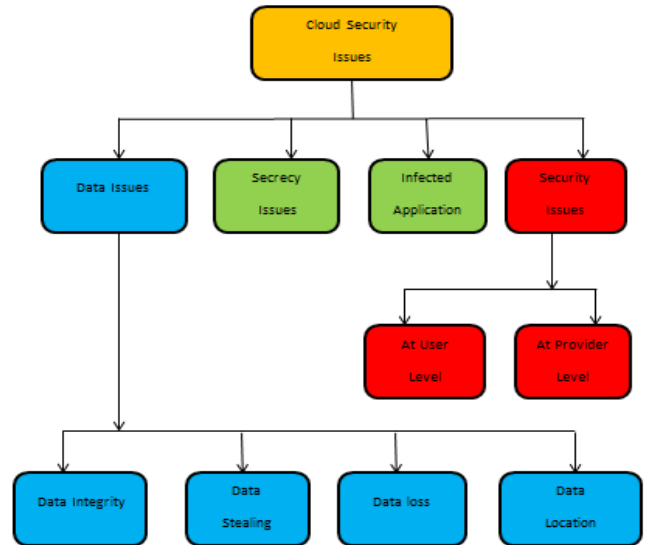


Fig 4: Cloud Security Issues

## VI. SECURITY ISSUES

There are four types of issues raise while discussing security of a cloud.

- A. Data Issues
- B. Privacy Issues
- C. Infected Application
- D. Security Issues

A. **Data Issues:** There are major issues of the data as:

(a) **Data Integrity:** whenever a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data maybe common, private and sensitive data in a cloud. So at the same time, many cloud computing service consumer and provider accesses and modify data. Thus there is a need of some data integrity method in cloud computing.

(b) **Data Stealing:** Data stealing is a one of serious issue in a cloud computing environment. Many cloud service provider do not provide their own server instead they acquire server from other service providers due to it is cost affective and flexible for operation and cloud provider. So there is a much probability of data can be stolen from the external server.

(c) **Data Loss:** Data loss is a common problem in cloud computing. If the cloud computing service provider shut down his services due some financial or legal problem then there will be a loss of data for the user. Moreover,

data can be lost or damage or corrupted due V. to miss happening, natural disaster, and fire. Due to above condition, data may not be accessible to users.

- (d) **Data Location:** data location is one of the issues what requires focus in a cloud computing environment. Physical location of data storage is very important. It should be transparent to user and customer. Vendor does not reveal where all the data's are stored.
- B. **Secrecy Issues:** The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintaining the server so that it enable the provider to protect the customer's personal information.
- C. **Infected Application:** cloud computing service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server. So this will prevent any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.
- D. **Security issues:** cloud computing security must be done on two levels. One is on provider level and another is on user level. Cloud computing service provider should make sure that the server is well secured from all the external threats it may come across. Even though the cloud computing service provider has provided a good security layer for the customer and user, the user should make sure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action. A cloud is good only when there is a good security provided by the service provider to the user.

## V. CHALLENGES

The following are some of the notable challenges associated with cloud computing.

- A. **Security and Privacy:** In general, Cloud computing have several customers from an ordinary users, academia and enterprises who have different motivation to move to cloud. If cloud clients are academia security effect on performance of computing and for them cloud providers have to find a way to combine security and performance. These issues are generally attributed to slowing the deployment of cloud services. These challenges can be addressed, for example, by storing the information internal to the organization, but allowing it to be used in the cloud.
- B. **Lack of Standards:** Clouds have documented interfaces; however, no standards are associated with these, and thus it is unlikely that most clouds will be interoperable. The Open Grid Forum is developing an Open Cloud Computing Interface to resolve this issue and the Open Cloud Consortium is working on cloud computing standards and practices. The findings of these groups will need to mature, but it is not known whether they will address the needs of the people deploying the services and the specific interfaces these services need. However, keeping up to date on the latest standards as they evolve will allow them to be leveraged, if applicable.
- C. **Continuously Evolving:** User requirements are continuously evolving, as are the requirements for interfaces, networking, and storage. This means that a "cloud," especially a public one, does not remain static and is also continuously evolving.
- D. **Access:** It has the threat of access sensitive information. The risk of data theft from machine has more chances in cloud environment data

stored in cloud a long time duration any hacker can access this data.

E. **Lack of user control:** In SAAS environment service provider is responsible to control data. Now how customer can retain its control on data when information is processed or stored.

F. **Trust:** Trust is very necessary aspect in business. Still cloud is failed to make trust between customer and provider. So the vendor uses this application should make trust. Weak trust relationship and lack of customer trust cause many problems during deployment of cloud service.

Accountability	<ul style="list-style-type: none"> <li>For businesses having data lost, leakage or privacy violation is catastrophic</li> <li>Accountability needs in legal and technical.</li> <li>Audit is need in every step to increase trust</li> <li>All CSP make contractual agreements</li> </ul>
Mechanism for rising trust	<ul style="list-style-type: none"> <li>Social and technological method to raise trust.</li> <li>Joining individual personal rights, preferences and conditions straightforwardly to uniqueness of data.</li> <li>Devices connected should be under control by CSP.</li> <li>Use intelligent software.</li> </ul>

## VI. SOLUTIONS

There are some solutions of these issues as:

**TABLE 1: SOLUTION**

Solutions	Description
Data Handling Mechanism	<ul style="list-style-type: none"> <li>Classify the confidential Data.</li> <li>Define the geographical region of data.</li> <li>Define policies for data destruction.</li> </ul>
Data Security Mitigation	<ul style="list-style-type: none"> <li>Encrypting personal data.</li> <li>Avoid putting sensitive data in cloud.</li> </ul>
Design for Policy	<ul style="list-style-type: none"> <li>Fair information principles are applicable.</li> </ul>
Standardization	<ul style="list-style-type: none"> <li>CSP should follow standardization in data tracking and handling.</li> </ul>

## VII. CONCLUSIONS

This paper discussed the architecture and popular services of cloud computing. It also addressed challenges and issues of cloud computing in detail. Cloud computing is latest development that provides easy access to high performance computing resources and storage infrastructure through web services. Cloud computing delivers the potential for efficiency, cost savings and improved performance to governments, organizations, private and individual users. This research effort will provide a better understanding of the design challenges of cloud computing, and pave the way for further research in this area.

### References

- [1] Object Management Group. Homepage URL: <http://www.omg.org>.
- [2] Open Cloud Computing Interface. Homepage URL: <http://occi-wg.org>.
- [3] Open Cloud Consortium. Homepage URL: <http://opencloudconsortium.org>



- [4] RNewsire.org,://www.reportlinker.com/,2012.
- [5] Preston A. Coz, "Mobile Cloud Computing: Devices, trends, issues & enabling technologies", 2012.
- [6] Schneider, "Essential characteristics of Mobile Cloud Computing", Marquette University, United States, 2012.
- [7] Itani et al, "Towards secure mobile cloud: A survey", Proceedings of Analyses paper, 2012.
- [8] Robert Lemos, "Cloud's Future Security Depends on Mobile", Proceedings of RSA Conference, February 2012.
- [9] Janakiram MSV Cloud Computing Strategist; (2010), "Demystifying the Cloud An introduction to Cloud Computing", Version 1.0 – March.
- [10] Adamov, A ; Erguvan, M.; (2009), "The Truth about Cloud Computing as new Paradigm in IT", IEEE International Conference on Application of Information and communication Technologies, AICT 2009.
- [11] Dikaiakos, M.D; Katsaros, D.; Mehra, P.; Pallis, G.; Vakali, A.; (2010), "Cloud Computing Distributed Internet Computing for IT and Scientific Research". Vol.13 ,pp 10, Sept.-Oct. 2009.
- [12] Joachim Schaper, 2010, "Cloud Services", 4th IEEE International Conference on DEST, Germany.
- [13] Tackle your client's security issues with cloud computing in 10 steps, <http://searchsecuritychannel.techtarget.com/tip/Tackle-your-clients-security-issues-withcloud-computing-in-10-steps>.
- [14] Problems Faced by Cloud Computing, Lord CrusAd3r, dl.packetstormsecurity.net/.../ProblemsFacedbyCloudComputing.pdf.
- [15] [Erickson08]Jonathan Erickson, "Best Practices for Protecting Data in the Cloud", 2008 <http://www.ddj.com/security/210602698>
- [16] [Brodkin08] Jon Brodtkin, "Seven Cloud-Computing Security Risks", 2008 <http://www.networkworld.com/news/2008/070208-cloud.html>
- [17] [Mills09] Elinor Mills, "Cloud Computing Security Forecast: Clear Skies", 2009 [http://news.zdnet.com/2100-9595\\_22-264312.html](http://news.zdnet.com/2100-9595_22-264312.html)