

# Analysis of Cloud Security, Performance, Scalability and Availability (SPSA)

Shailja Sharma<sup>1</sup>, Sheeba Khan<sup>2\*</sup>

<sup>1</sup> Department of Computer Science & Engineering, RNTU University, Bhopal

<sup>2</sup> IPER college, Bhopal

Received: 20/Feb/2019, Accepted: 27/Feb/2019, Published: 10/Mar/2019

**Abstract:** Present trends and advancement in technology have increase to the success and admire of computing in cloud. Computing in cloud provides services on demand. Computing of the cloud formulate make use of complicated remote network sites and servers that are associated with the internet for storing, managing and data processing of data, rather than a server of (LAN) Local Area Network or a single computer. Now a day, computing of cloud is extremely demanded service because of the advantages like powerful computing, low cost of services, high performance, scalability, reliability, accessibility and availability. This investigation of research discusses the performance, issues in security and challenges in environment of cloud data. This survey provides insights to study recent cloud issues and cloud challenges.

**Keywords—** Cloud Storage, Cloud Performance, Cloud Scalability, Cloud Availability, Cloud Security, Cloud Access Control, Document Sharing.

## I. INTRODUCTION

The Computing of cloud paradigm has bulged as an dexterous technique which enables omnipresent, access on demand to a common pool of flexibly reconfigurable computing resources by the elevation of the same time as networks, servers, storage space, applications, and services with the intend of quickly deployed with least management efforts and service provider interactions. A very popular and simplest definition of cloud is, “a solution of network for provided that economical, trustworthy, uncomplicated and straightforward permission to IT resources” [3]. The service oriented approach of Computing in cloud is not merely reduces the operating cost of infrastructure and ownership cost furthermore provides improved performance and flexibility to the customer [4]. NIST has defined the apparatus that are used in computing of cloud with essential features and two models these models are[5] :

- a) Deployment Model.
- b) Service Model

Deployment Model are classified as :

- a) Public
- b) Private
- c) Hybrid
- d) Community

Basically depends upon on demand of the organization.

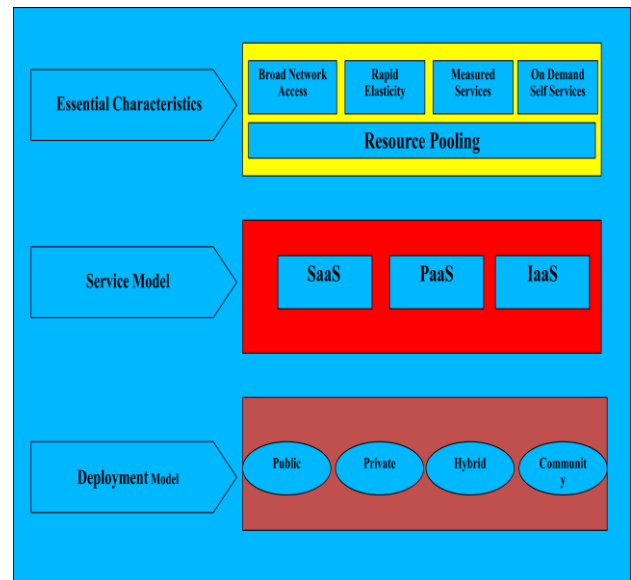


Fig 1.1 A conceptual view of computing in cloud

Computing of cloud Service models being classified as [6]:

**Software as a Service (SaaS):** Providing Software’s as a service for the patrons according to their necessities, enable patrons to utilize the services that are available on

the servers of cloud.

**Platform as a Service (PaaS):** Clients are provided platforms access, which enables them to put their own customized software's and other applications on the clouds.

**Infrastructure as a Service (IaaS):** Rent processing, storage, network capacity, and other basic computing resources are granted, enables patrons to deal with the operating systems, applications, storage, and network connectivity.

Performance, availability, scalability, and Security of data are the biggest challenges in adaptation of cloud [7]. Data integrity, privacy and protection are some of the mandatory issues for the services of cloud. For this reason, numerous service providers are using variant policies, techniques and methods that depend upon the following parameters:

- Size of data.
- Nature of data.
- What Types of data.
- Size of data.

## II. Literature Review

So as to comprehend the fundamental concepts of Computing in the cloud and storing secure data on the cloud, diverse wherewithal have been consulted. This segment is for literature review to locate an underpinning of discussing different aspects of Computing in the cloud environment.

Previous study provides that how to improve performance in the computing of cloud and how many parameters effected performance of cloud? The endeavor of this research was depends in the lead of the following factors [1].

- a. How can performance with in Cloud Computing be improved?
- b. Workload analysis and innovative cloud resource management?

Previous study adopted the resource allocation technique to increasing the cloud performance and applies encryption process to the files. By using these existing methods decrease the downloading and uploading time of file on cloud to enhance the performance [1].

Previous study also provides the concept of Scalability means that when increase the load lying on the workstation then performance of the system ought to be constant in every environment without the harm the customer requirements. According to study various scaling techniques are available for improve scalability in the

computing of cloud [1].

- a. Vertical Scaling.
- b. Horizontal scaling.
- c. Diagonal scaling.

Another meaning of Scalability is that various user can share their data simultaneously without any collision.

Previous study also provides Cloud availability is the another issue in the computing of cloud .It means that when any user want anything in case he is using cloud I should be available. Availability is directly proportional to reliability. Everyone is familiar with this term if system is reliable then user will work more on such kind of system. There are choices of factors which will effect on availability of cloud these are [1]:

- a. Human error
- b. Software Failure
- c. Hardware failure
- d. Migration of machine from one server to another.

Previous study provides the concept in cloud computing according to these Security has a major role in computing of cloud .It means that users data safe form attackers and hackers. Every user worried about the security, privacy and confidentiality of their data. If any system which provides this feature strongly which will the success system for the future aspect? Any of the unauthorized users will not be admittance to the system this will be another security aspects for the system. Security parameters which are required for the successful system [2].

- a. Privacy
  - b. Confidentiality
  - c. Unauthorized Access
  - d. Safe for attacker
  - e. Safe for hackers etc.

Every aspects in the computing of cloud is mandatory for this researcher have various security algorithms over and above rules as they can implement for the security point of view.

Previous study endow with a commendable approaching into the basic concepts of cloud computing. In this paper, numerous key concepts are explored that examples of applications that can be developed using Computing of cloud and how they can help the developing world in getting benefit from this emerging technology [3].

Previous study Cloud computing provides highly scalable resources accessed via Internet. Since Computing in cloud is growing quickly day by day used by individuals and

companies throughout the world, data protection problems in the Computing of cloud have not been tackled currently. In the cloud, cloud services users have serious threat of losing confidential data. To take in hand data privacy issues of users, they have proposed data protection framework. The proposed data protection framework addresses the challenges throughout the cloud services life cycle. Their proposed framework comprises of three key components: policy ranking, policy integration and policy enforcement. For each component, they have presented various models and analyzed properties of each component. This paper includes a discussion on general guidelines for weighing up designed systems based on such kind of framework. This study also accessible numerous models of data protection and defined cost functions [8].

Previous method provided a standard to secure data-in-transit within the cloud. A yardstick for encryption technique has been discussed for guarding information for the duration of immigration. Other standard of encryption is required for stout security although it involves superfluous computation. The yardstick discussed in their study presents equilibrium for the security and encryption overhead [9].

### III. CONCLUSION

In this study different security and privacy related research papers were studied briefly. Services of cloud are used by both bigger and slighter scale organizations. Computing of cloud is affliction from brutal threats of security as of user standpoint, some cloud user mentioned that be short of security is the merely significance disadvantage of computing in the cloud. Both the Service providers and the clients must work together to ensure safety and security of computing in cloud along with data on clouds. Here researches conclude that security is prevalent stumbling block in extensive recognition of computing of cloud. Another problem with users of cloud services are in trepidation of information hammering and privacy. Researchers and experts of IT security are required to come forward and accomplish more to make sure security and privacy to users. Another aspect of present study is to find out top security concerns of computing in cloud, these concerns are slaughter of data, outflow of Data, Client's trust, Authentication of user, spiteful users handling, erroneous usage of computing in cloud and its services, Hijacking of sessions whilst accessing data.

### REFERENCES

- [1] Shoaib Hassan, Asim Abbas kamboh, Dr. Farooque Azam "Analysis of Cloud Computing Performance, Scalability, Availability & Security", In the Proceedings of the 2014 International Conference on Information Science & Applications (ICISA), Seoul, South Korea, 978-1-4799-4441-5/14/\$31.00 ©2014 IEEE.
- [2] Chao YANG, Weiwei LIN, Mingqi LIU "A Novel Triple Encryption Scheme for Hadoop-based Cloud Data Security", In the Proceedings of the 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies, Xi'an, China, pp.437-442, 2013, 978-0-7695-5044-2/13 \$26.00 © 2013 IEEE.
- [3] J. Srinivas, K. Reddy, and A. Qyser, "Cloud Computing Basics", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue. 5, pp. 3–22, 2012.
- [4] M. A. Vouk, "Cloud computing - Issues, research and implementations", In Proceeding of the 2008 30<sup>th</sup> International Conference. On Information Technology Interfaces(ITI), Cavtat, Croatia, pp. 31–40, 2008.
- [5] P. S. Wooley, "Identifying Cloud Computing Security Risks," University of Oregon, pp.1-88 February, 2011.
- [6] F. B. Shaikh, S. Haider, "Security Threats in Cloud Computing", In Proceeding of the 2011 International Conference on Internet Technology and Secured Transactions, Abu Dhabi, 2011, pp. 11-14, 978-1-908320-00-1/11/\$26.00 ©2011 IEEE..
- [7] Abdulrahman, Alharthi, Fara Yahya, Robert J. Walters and Gary B. Wills, "An Overview of Cloud Services Adoption Challenges in Higher Education Institutions ", In Proceedings of the 2nd International Workshop on Emerging Software as a Service and Analytics (ESaaS-2015), pp.102–109.
- [8] Dan Lin and Anna Squicciarini, "Data Protection Models for Service Provisioning in the Cloud", In Proceedings of ACM Symposium on Access Control Models and Technologies (SACMAT, 2010), Pittsburgh, Pennsylvania, USA.
- [9] J. Hu and A. Klein, "A benchmark of transparent data encryption for migration of web applications in the cloud," In Proceeding of 2009 8th International conference on Dependable, Autonomic and Secure Computing, Chengdu, China., pp. 735–740, 2009.