

# A Survey on Scalable Data Security and Load Balancing in Multi Cloud Environment

**Mr. Avinash R. Dhok**  
*Department of Computer Engineering*  
*B.D. College of Engineering, Sewagram, Wardha,*  
*Maharashtra.*

**Ms. Ashwini P. Kolhe**  
*Department of Computer Engineering*  
*B.D. College of Engineering, Sewagram, Wardha,*  
*Maharashtra*

**Ms. Neha V. Lutade**  
*Department of Computer Engineering*  
*B.D. College of Engineering, Sewagram, Wardha, Maharashtra*

## Abstract

Internet and network application are growing very fast and use of cloud computing has increased rapidly in today's world. Cloud computing provides many advantages such as low cost, on-line, on-demand services pay per use basis and accessibility of data. Security in cloud computing is major issue, as user often store sensitive information in cloud storage provider but these providers may be untrusted. Encryption algorithms play a main role in information security systems. Several issues as scalability, security, performance, integrity etc. are discussed so far. This paper surveys recent research related to multi cloud security and address possible solution. This paper introduces a better load balance technique for public cloud based on data distribution system over the database server. It is found in research that use of multi-cloud providers to maintain security has received less attention than single clouds. This work aims to promote the use of multi cloud due to its ability to reduce security risks that affect the cloud computing user. The way to secure the data using different compression and encryption algorithms and to hide its location from the users that stores and retrieves it.

**Keywords:** Cloud computing, single cloud, multi cloud, load balancing, data security, Data distribution

## I. INTRODUCTION

The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN.

Cloud computing is architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc.

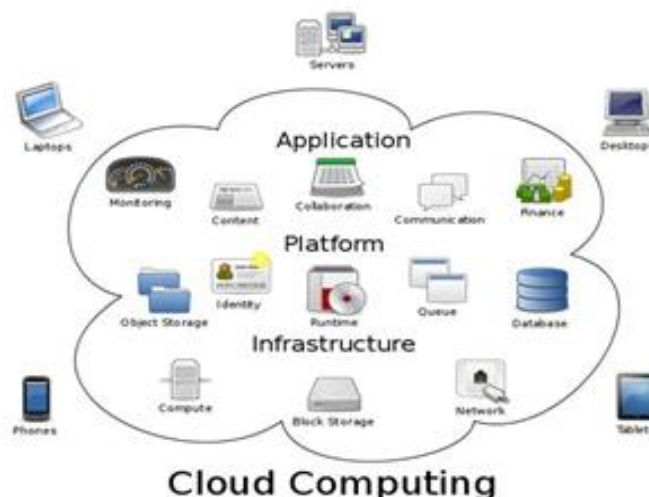


Fig. 1: Cloud Computing

**Public Cloud:** Public cloud makes services (such as computing, storage, application, etc.) available to general public. These services may be free or offered as payment as per usage. Major public cloud providers are Amazon, Google, Microsoft, etc.

**Private Cloud:** Private cloud is a cloud infrastructure operated only for a single organization. It is not available to general public.

**Community Cloud:** Community cloud shared infrastructure between several organization with common concerns such as compliance, jurisdiction, etc.

**Hybrid Cloud:** Hybrid cloud is a combination of two or more clouds (public, private, or community). the Taxonomy in which the service models of the cloud are stated and the technologies related to cloud computing are described.

#### **A. Deployment Models of Cloud Computing:**

Generally cloud services can be divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

##### **1) Software as a Service:**

Software as a Service describes any cloud service where consumers are able to access software applications over the internet. The applications are hosted in “the cloud” and can be used for a wide range of tasks for both individuals and organizations. Google, Twitter, Facebook and Flickr are all examples of SaaS, with users able to access the services via any internet enabled device.

##### **2) Platform as a Service:**

PaaS, is a category of cloud computing that provides a platform and environment to allow developers to build applications and services over the internet. PaaS services are hosted in the cloud and accessed by users simply via their web browser. 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.

##### **3) Infrastructure as a Service:**

As with all cloud computing services Infrastructure as a Service (IaaS) provides access to computing resource in a virtualized environment, “the Cloud”, across a public connection, usually the internet. In the case of IaaS the computing resource provided is specifically that of virtualized hardware, in other words, computing infrastructure. The definition includes such offerings as virtual server space, network connections, bandwidth, IP addresses and load balancers. Physically, the pool of hardware resource is pulled from a multitude of servers and networks usually distributed across numerous data centers, all of which the cloud provider is responsible for maintaining. The client, on the other hand, is given access to the virtualized components in order to build their own IT platforms. We now discuss the main issue in IAAS i.e. Security.

Characteristics and components of IaaS include:

- 1) Utility computing service and billing model.
- 2) Automation of administrative tasks.
- 3) Dynamic scaling.
- 4) Desktop virtualization.
- 5) Policy-based services.
- 6) Internet connective

Where is your data more secure, on your local hard driver or on high security servers in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security.

This project solves the security issues in cloud IaaS (i.e. Infrastructure as a Service) which mainly includes use of cloud request processors and database servers. This project mainly includes securing the data by encrypting it using symmetric Encryption algorithm and splitting the data in multiple parts and stores it in different database servers.

#### **B. Load Balancing:**

“The load balancing technique used to make sure that none of the node is in idle state while other nodes are being utilized”. In order to balance the lode among multiple nodes you can distribute the load to another node which has lightly loaded. Thus distributing the load during runtime is known as Dynamic Load Balancing technique. Load balancing algorithm can be divided into two categories as 1) Static and 2) Dynamic. In static load balancing algorithm, all the information about the system is known in advance, and the load balancing strategy has been made by load balancing algorithm at compile time. This load balancing strategy will be kept constantly during runtime of the system [8].

##### **1) Goals of Load balancing:**

The goals of load balancing are [10]:

- To improve the performance substantially.
- To have a backup plan in case the system fails even partially.
- To maintain the system stability.
- To accommodate future modification in the system.

## II. ISSUES IN CLOUD COMPUTING

In single storage cloud system each cloud customer's data is stored on single higher configuration server. Even if that server has huge amount resources such as RAM, Hard disk, processing power, it has certain limit. If it crosses that limit then particular resource performance slows down. It may loss the data or does not provide the services. Cloud computing is efficient and scalable but maintaining the stability of processing so many jobs in the cloud computing environment is a very complex problem with load balancing receiving much attention for researchers.

- Security: Where is your data more secure, on your local hard driver or on high security servers in the cloud? Customer data is more secure either when managed internally, or cloud providers have a strong motive to maintain trust and as such customer a higher level of security. However, in the cloud, your data will be distributed over these individual computers regardless of where your base repository of data is ultimately stored.
- Privacy: Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users.
- Reliability: Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSPs service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk.
- Legal Issues: Regardless of efforts to bring into line the lawful situation, as of 2009, supplier such as Amazon Web Services provide to major markets by developing restricted road and rail network and letting users to choose availability zones. On the other hand, worries stick with safety measures and confidentiality from individual all the way through legislative levels.
- Open Standard: Open standards are critical to the growth of cloud computing. Many cloud providers exposes Application Program Interface (APIs) which are well-documented and unique to their implementation and thus not interoperable. To develop agreement on cloud computing standards, the Open Cloud Consortium (OCC) is used.
- Freedom: Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers. Customers will contend that this is pretty fundamental and affords them the ability to retain their own copies of data in a form that retains their freedom of choice and protects them against certain issues out of their control whilst realizing the tremendous benefits cloud computing can bring .
- Long-term Viability: One should be sure that the data in the cloud will never become invalid or disable even your cloud computing provider go broke or get acquired and swallowed up by a larger company.

As cloud computing is in its evolving stage, so there are many problems prevalent in cloud computing

- Ensuring proper access control (authentication, authorization, and auditing)
- Network level migration, so that it requires minimum cost and time to move a job
- To provide proper security to the data in transit and to the data at rest
- Data availability issues in cloud

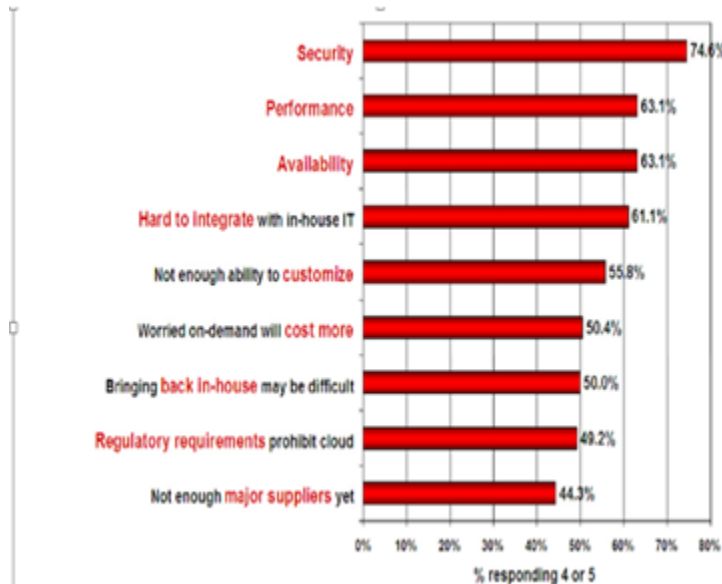


Fig. 2: Issues in Cloud Computing

### III. OBJECTIVES

The main objectives of the study are listed below

- 1) To provide security in cloud IAAS database servers.
- 2) Splitting the data into multiple parts after encryption and store it in different database servers.
- 3) Provide data Hosting services i.e. upload and download.

### IV. ORGANIZATION OF PAPER

This paper is organized as follows:

- Section I gives Introduction about domain as well as about our project work.
- Section II describe Issues in cloud computing
- Section III illustrate objectives of our proposed system
- Section V provides literature survey.
- Section VI introduces our proposed systems which recovers issues or solve the problem in existing system.
- Section VII finally has conclusion of project.

### V. BRIEF LITERATURE SURVEY

[A. AL Zain et al., 2012] [1] Cloud Computing Security: From Single to Multi-Clouds 45th Hawaii International Conference on System Sciences. The author in this paper proposed that the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. Their work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user.

[Olfa Nasraoui et al., IEEE, 2013][2] VOL. 20, No. 2 Ensuring Data Integrity and Security in Cloud Storage, This paper proposed security architecture for Cloud to secure the system using client side encryption and compression. Their application allowed them to upload and download files which are encrypted and decrypted at client side. Encryption algorithm used is AES 128.

[Qin Liu et al., IEEE, 2011][3] Reliable Re-encryption in Unreliable Clouds, They proposed a time based re-encryption scheme, which enables the cloud servers to automatically re-encrypt data based on their internal clocks. Their solutions are built on top of a new encryption scheme, attribute based encryption, to allow fine-grain access control, and does not require perfect clock synchronization for correctness.

[Wei-Tek Tsai et al., 2010][4] Service-Oriented Cloud Computing Architecture Seventh International Conference on Information Technology. They proposed a fully distributed load rebalancing algorithm is presented to cope with the load imbalance problem. Their algorithm is compared against a centralized approach in a production system and a competing distributed solution presented in the literature. The simulation results indicate that our proposal is comparable with the existing centralized approach and considerably outperforms the prior distributed algorithm in terms of load imbalance factor, movement cost, and algorithmic overhead.

[Cheng-Kang Chu, et al., 2014][5] Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage They describe new public-key cryptosystems which produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts are possible.

[Divya Thazhathethil, et al., 2014][6] volume 4 , issues 2014 A Model for load balancing by Partitioning the Public Cloud, Comp Engg,TCOER India, This paper introduces a system which has main controller, balancers and servers. The main controller selects the appropriate balancer for a particular job. The balancer further selects the server having minimum load.

Hence, this system will help dynamically allocate jobs (data) to the least loaded server which will result in an efficiently balanced cloud system.

[Rabi Prasad Padhy, et al., 2011][7] vol. 1 No. 2 “Cloud Computing: Security Issues and Research Challenges” This research paper outlines what cloud computing is, the various cloud models and the main

Security risks and issues that are currently present within the cloud computing industry. This research paper also analyzes the key research and challenges that presents in cloud computing and Offers best practices to service providers as well as enterprises hoping to leverage cloud service to improve their bottom line in this severe economic climate.

[Mangal Nath Tiwari et al., 2014][8] Volume 4, Issue 2, “Analysis of Public Cloud Load Balancing using Partitioning Method and Game Theory” This paper introduces a better approach for public cloud load distribution using partitioning and game theory concept to increase the performance of the system.

[Brototi Mondal et al., 2012][9] Elsevier “Load Balancing in Cloud Computing using Stochastic Hill Climbing-A Soft Computing Approach” In this paper, a soft computing based load balancing approach has been proposed. A local optimization approach Stochastic Hill climbing is used for allocation of incoming jobs to the servers or virtual machines (VMs). Performance of the algorithm is analyzed both qualitatively and quantitatively using Cloud Analyst. Cloud Analyst is a Cloud Sim-based Visual Modelers for analyzing cloud computing Environments and applications.

[S. Karthika et al., 2014][10] Volume 2 Issue 2 ISO “Load Balancing and Maintaining the Qos on Cloud Partitioning For the Public Cloud” The main objective of project is to develop a query-based wireless sensor systems, where a user would issue a query and expect a response to be returned within the deadline. They also develop an adaptive fault-tolerant quality of service control methods which is based on hop-by-hop data delivery utilizing “source” and “path” redundancy, with the goal to satisfy application of Qos requirements which prolongs the lifetime of the sensor system.

## VI. PROPOSED WORK

As we mention above, the major requirement is balance work load of database server by which it's easy to interfere with cloud. In our proposed system, all issues are recovered by splitting technique. In our system, firstly user interact with web browser with delegates the servers scripting or servers activities. For storing the data on cloud, it must to have one account on particular cloud therefore we are providing a facility to create one account by which appropriate user will interact with that data.

With the help of login facility user has authority to use cloud. After login, cloud provider provides some space to user on which data are store. But in all that process it's a major issues to store client's data securely for that purpose we are using encryption technique. In encryption technique, we are converting user original data into cypher text form.

In all process firstly clients data are converted into bytes form and then encrypt that and store on database server. This project mainly includes securing the data by encrypting it using symmetric Encryption algorithm and splitting the data in multiple parts and stores it in different database servers.

### A. Problem Defination:

- Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce.com and Microsoft etc.
- Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks.
- There are various research challenges also there for adopting cloud computing such as well managed service level agreement
- (SLA), privacy, interoperability and reliability.

## VII. CONCLUSION

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud.

In this paper we try to solve the security issues in cloud IaaS (i.e. Infrastructure as a Service) which mainly includes use of cloud request processors and database servers. It mainly includes securing the data by encrypting it using symmetric Encryption algorithm and splitting the data in multiple parts and stores it in different database servers.

In this paper, we investigated the security challenges that associated with IaaS implementation and deployment. The security issues presented here concern the security of each IaaS component in addition to recent proposed solutions.

## REFERENCES

- [1] A.AIZain et al., “Cloud Computing Security: From Single to Multi-Clouds” 2012 45th Hawaii International Conference on System Sciences.
- [2] Olfa Nasraoui et al., “Ensuring Data Integrity And Security In Cloud Storage”, IEEE, VOL. 20, No. 2, February 2013.
- [3] Qin Liu et al., “Reliable Re-encryption in Unreliable Clouds” IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2011 proceedings.
- [4] Wei-Tek Tsai et al., “Service-Oriented Cloud Computing Architecture”, 2010 Seventh International Conference on Information Technology.
- [5] Cheng-Kang Chu, et al., “Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage” IEEE Transactions on Parallel and Distributed Systems. Volume: 25, Issue: 2. Year :2014
- [6] Divya Thazhathethil, et al., “A Model for load balancing by Partitioning the Public Cloud” Comp Engg.TCOER ,India volume 4 , issues 2014
- [7] Rabi Prasad Padhy, et al., 2011 vol. 1 No. 2 “Cloud Computing: Security Issues and Research Challenges” IJCSITS conference.
- [8] Mangal Nath Tiwari et al., 2014 Volume 4, Issue 2, “Analysis of Public Cloud Load Balancing using Partitioning Method and Game Theory”
- [9] Brototi Mondal et al., 2012 Elsevier “Load Balancing in Cloud Computing using Stochastic Hill Climbing-A Soft Computing Approach”
- [10] S. Karthika et al., 2014 Volume 2 Issue 2 “Load Balancing and Maintaining the Qos on Cloud Partitioning For the Public Cloud” published ISO