A Review on Practical Compute Capacity Management for Virtualized Data Centers

Anil Kumar Raghuwanshi1, Priya Bharti2
1M. Tech. Scholar, Oriental College of Technology, Bhopal, M.P., India
2Assistant Professor, Department of CSE, Oriental College of Technology, Bhopal, M.P., India

Abstract — Cloud computing is an emerging technology that is enriched with variety of services few of them are dynamic scalability, Cloud storage, security, data integrity etc. dynamic scalability used to handle growing numerous application data in a flexible manner or to be readily enlarged. Security plays a vital during the transmission of data from the sender to the receiver in any environment. Cloud storage offers remotely accessed memory space. Data integrity is the storing of data from many nodes to a particular place. In this paper we are presenting survey of cloud storage, cloud security, public verifiability, virtualization techniques offered by numerous researchers.

Keywords— Cloud Computing, Public Varifiability, Cloud Storage, Cloud Security, Virtualisation.

I. INTRODUCTION

With growing Internet scenario cloud computing is novel technique to serve better and secure services. Recently e-business is progressively more conducted over the Internet. Cloud computing is the hottest emerging computing technology where data storage, platform, and IT services are offered over the internet. Due to immense availability of resources and numerous tasks being submitted to the task management becomes important for optimal scheduling which affects the efficiency of the whole cloud computing environment. The use of Cloud Computing is ahead reputation due to its mobility and massive availability in minimum cost. The Cloud Computing provides its users benefit of extraordinary access to expensive data that can be turned into valuable insight that can help them achieve their business objectives.

Efficient cloud computing can be capable to manage different data centers. These data centers are able to run diverse workload with time just because of running virtual machines (VMs) inside them. This will lead high and low recourse utilization. To deal with this problem enhanced virtualization mechanism were developed and recent researches still going on in this era [1]. Cloud computing has been visualized as the next generation information technology (IT). It is mainly constructed for enterprises to offer unusual advantages like; location independent resource pooling, everywhere network access, on-demand self-service, usage-based pricing, transference of risk and quick resource elasticity.

Cloud computing generally provides three types of services: Infrastructure as a service, Software as a service and Platform as a service shortly known as IaaS, SaaS and PaaS respectively. IaaS is a single tenant cloud layer where the cloud computing vendor’s devoted resources are only shared with clients at a pay-per-use payment. SaaS operates on the virtualized and pay-per-use costing mold whereby software applications are leased out to contracted organizations by specialized SaaS vendors. Clients use PaaS services to transfer even more costs from capital investment to operational expenses but must acknowledge the additional constraints and possibly some scale of lock-in posed by the additional functionality layers. Apart from services cloud computing also provides four types of cloud models. They are public, private, hybrid and community cloud. A public cloud allows users’ access to the cloud via interfaces using mainstream web browsers. A private cloud is set up within an organization’s internal enterprise datacenter. The composition of more than one cloud is called Hybrid. The community cloud is reserved for exclusive utilize by a specific community of customers from organizations that have public apprehensions.

The cloud computing provides on demand self service methodology that authorizes users to request resources dynamically as a best benefit. Data can be stored and retrieved remotely and due to this conventional cryptographic algorithm is not used for security. Once the data has been stored on cloud data storage security should be maintained by cloud service provider. To preserve data safety measures, publicly auditable cloud storage space providers trusted third party auditor (TPA) to verify the data integrity of sourced data to make certain security. To ensure cloud data storage security, TPA calculates the service quality from an objective and autonomous perspective. Public audit capability also permits clients to delegate the integrity verification tasks to TPA in case they are not being able to commit necessary computation resources performing continuous verifications [4]. The privacy-preserving public auditing is uniquely integrating the homomorphic non-linear authenticator with random masking technique. The entity auditing of TPA can be dreary and extremely inefficient.
In the cloud environment, the customers themselves are variable or cannot afford the overhead of performing frequent truthfulness verifies. Thus, for practical use, it seems more balanced to prepare the verification protocol with public verifiability that is conventional to play a major role in achieving economies of degree for Cloud Computing. Verifiability is kind of authentication mechanism. This will used to authenticate or validate the party or sometimes used to authenticate TPA. There are two types of Verifiability one is private Verifiability and another is public Verifiability. Second one is more secure. Public Verifiability is forced user to do not upload personal data in cloud storage and stored records should be properly stored.

Virtualization is capacity to hide physical resources that is used in cloud computing environment. Virtualization software offers facility to use multiple operating systems or application in a same computer at same time. Virtualization also capable to hide local and global resources attached with any system. It also makes server, workstation storage and other systems independent from physical hardware layer. Virtualization is having some benefits over traditional systems. It can reduce the number of physical system availability. It provides facility to use multiple system environments within a single system. Cloud security refers to the security of data, networking and other resources from viruses, worms, hackers, intruders etc. as far as security issues are concerned its is of two types: first one is category of cloud service providers while another one is users of it. Different points should be discovered which states that how secure cloud services are achieved? Some common parameter that are essential for cloud securities are: authentication, privacy, personal and physical security, availability and application security.

Internet supported online service provides huge amounts of storage space and customizable computing resources, such computing stage shift, although is removing the liability of local machines for data maintenance at the similar time. Due to this users are at the mercy of their cloud service providers for the availability and integrity of their data. So the security of data is a significant aspect of service quality. The rest of paper is organized as follows. In Section II describes about background of cloud environment. Section III describes about related work in public verifiability, cloud security, virtualization. Section IV describes the proposed methodology and section V describes about expected outcome.

II. BACKGROUND

Cloud Computing is continuously evolving and showing consistent growth in the field of computing.

Excluding, the security issues and threats linked with it still stay as a cumbersome. Cloud data storage can be affected by two different sources. The cloud data storage provider itself is untrusted and possibly malicious. Preserving the privacy of user, his identity and data in the cloud is very mandatory. When large data is downloaded, it does not give guarantee about accuracy of data. To store valid data should be dependent on user and the type of data we are using. Sometimes private data also uploaded and shared among users. So it is important, that the privacy has to be preserved anytime and anywhere. Although security of data also a critical issues in cloud computing. Day by day new techniques were suggested by numerous researchers, and still there is a flaws in it.

III. RELATED WORK

This section describes about related work in fields of cloud storage, cloud security, virtualization and public verifiability.

A system based on cloud capacity management (CCM) was presented in [1]. This is on demand CCM enriched with various low-overhead techniques. Self motivated by practical on-field observations and to achieve scalability allocation for thousands of machines. CCM architecture is divided in to three levels that are top-level cloud manager, midlevel super cluster managers, and finally cluster managers at the lowest level. According to the figure 1, hosts are logically grouped into clusters tight with capacity manager (VMware DRS) and these clusters are monitored by super cluster. These super clusters are known as corresponding capacity manager. All these super clusters come under collection of super clusters known as cloud-level capacity manager.

![Figure 1: Architecture of Cloud Capacity Management System [1].](Image)

Capacity manager is used to monitor and aggregate black-box VM CPU and memory usage information.
After that use this aggregated data to make independent and localized capacity allocation decisions. The use of black-box monitoring and allocation enables CCM to perform capacity allocation for a broad class of applications including those that do not typically scale out horizontally. The core concept embodied in CCM’s capacity multiplexing is the on-demand balancing of load, across logical host-groups, at each level in the hierarchy. Reductions in management cost are obtained by having monitoring and resource changes occur at progressively less frequent intervals when moving up the hierarchy. At super cluster and cloud level CCM computes the total estimated demand of a cluster and super cluster respectively. This total demand estimate is then used to determine the amount of capacity required by a cluster or super cluster, and to perform coarse-grain facility changes as per demand. The capacity changes are realized by logically re-associating hosts between cluster and super cluster managers. The monitoring and resource changes in this system occur at progressively less frequent intervals when moving up the hierarchy [1].

In [3] they proposed publicly auditable cloud storage providers where data owners can rely on third party auditor to verify the data integrity of sourced data to make sure security. To considerably diminish the arbitrarily large communication overhead for public auditability without commencing any online burden on the data owner, they resort to the homomorphic authenticator technique. Homomorphic authenticators are extraordinary metadata generated from individual data blocks that can be securely aggregated in such a way to guarantee a verifier that a linear combination of data blocks is properly computed by verifying only the aggregated authenticator. Unauthorized data leakage still remains a problem due to the potential exposure of encryption keys. To address this concern, a proper approach is to combine the homomorphic authenticator with random masking. This way, the linear combination of sampled blocks in the server’s response is masked with randomness generated by the server. With random masking, the TPA no longer has all the necessary information to build up a correct group of linear equations and therefore cannot derive the owner’s data substance, no issue how many linear combinations of the same set of file blocks can be collected [3].

Meanwhile, due to the algebraic property of the homomorphic authenticator, the exactness validation of the block-authenticator pairs (μ and σ) can still be carried out in a new way, even in the presence of randomness. This improved technique ensures the privacy of owner data content during the auditing process, regardless of whether or not the data is encrypted, which definitely provides more flexibility for different application scenarios of cloud data storage. Besides, with the homomorphic authenticator, the desirable property of constant communication overhead for the server’s response during the audit is still preserved [3].

In [4] they explored the problem of providing simultaneous public auditability and data dynamics for remote data integrity check in Cloud Computing. In view of the key role of public auditability and data dynamics for cloud data storage they propose an efficient construction for the seamless integration of these two components in the protocol design. They offered a protocol supporting for fully dynamic data operations principally to support block insertion that is missing in most existing schemes. In the cloud paradigm, by putting the large data files on the remote servers, the clients can be reassured of the burden of storage and calculation. As a client no longer acquires their data locally, it is of vital significance for the clients to ensure that their data are being correctly stored and maintained.
Clients should be equipped with certain security means so that they can periodically verify the correctness of the remote data even without the existence of local copies. In this case clients do not unavoidably have time, feasibility or resources to monitor their data; they can delegate the monitoring task to a trusted TPA. They only consider verification schemes with public auditability: any TPA in possession of the public key can act as a verifier [4].

He tries to utilize the homomorphic non-linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process that not only reduces the burden of cloud user from the tedious and possibly pricey auditing task, but also alleviates the users’ terror of their outsourced data security. Taking into account TPA may concurrently handle multiple audit sessions from dissimilar users for their outsourced data files, he further extend this privacy-preserving public auditing protocol into a multi-user scenario, where the TPA can perform multiple auditing tasks in a batch manner for better effectiveness. Extensive examination shows that this scheme is almost certainly secure and highly efficient [5].

In [6] they suggested efficient provable data possession for hybrid clouds. They focused on the construction of PDP scheme for hybrid clouds, supporting privacy protection and dynamic scalability. They first provide an effective construction of Cooperative Provable Data Possession (CPDP) using Homomorphic Verifiable Responses (HVR) and Hash Index Hierarchy (HIH). This construction uses homomorphic property, such that the responses of the client’s challenge computed from multiple CSPs can be combined into a single response as the final result of hybrid clouds. By using this mechanism, the clients can be convinced of data possession without knowing what machines or in which geographical locations their files reside. More prominently a new hash index hierarchy is proposed for the clients to seamlessly store and manage the resources in hybrid clouds. Their experimental results also validate the effectiveness of their construction.

In CPDP scheme, the client’s communication overhead is not changed in contrast to common PDP scheme, and the interaction among CSPs needs \( c - 1 \) times constant-size communication overheads, where \( c \) is the number of CSPs in hybrid clouds. Therefore, the total of communication overheads is not significantly increased. Next, they evaluated the performance of CPDP scheme in terms of computational overhead. For the sake of comparison, their experiments were executed in the following scenario: a fixed-size file is used to generate the tags and prove data possession under the different number of sectors \( s \). Moreover, there exists an optimal value of \( s \) from 15 to 25. The results indicate that the overheads are reduced when the values of \( s \) are increased. Hence, it is necessary to select the optimal number of sectors in each block to minimize the computation costs of clients and storage service providers [6].

In [7] in 2009 they introduced a new scheme which gives remote data integrity and verifiability means dynamic data operations. The method initially identifies the troubles and potential security problems of direct extensions with fully dynamic data updates.
It achieves efficient data dynamics and improves the Retrieve ability model by manipulating the classic Merkle Hash Tree (MHT) construction used for block tag validation. It is extremely proficient and secure technique [7]. In [8] a concept about warehouse for integrating data from various data sharing services without central authorities is existing with our warehouse, data sharing services can update and control the access and limit the usage of their shared data, as a substitute of submitting data to establishment, and our repository will support data sharing and addition. The main differences between their storehouse and existing central authorities are: 1) repository collects data from data sharing services based on users’ integration requirements rather than all the data from the data sharing services as existing central establishment. 2) While existing central establishment have full control of the collected data, the capability of warehouse is controlled to computing the integration results required by users and cannot get other information about the data or use it for other work. 3) The data composed by warehouse cannot be used to generate other results except that of the specified data addition request, and, hence, the cooperation of warehouse can only reveal the results of the specified data integration demand, while the compromise of central establishment will reveal all data and presented a privacy preserving repository to integrate data from various data distribution services. In contrast to existing data allocation techniques, warehouse only collects the least amount of information [8].

In [9] they presented a survey on cloud computing. They defined basic terminology of cloud. They also compare cloud with other related technologies. They also try to identifying the top technical and non-technical obstacles and opportunities of cloud computing. Virtualization is primary security mechanism of cloud computing. It is a powerful defense scheme. It capable to protects against most attempts by users to attack one another or the underlying cloud infrastructure. One of the common problems is that all recourses are not virtualized. Virtualization software has been known to contain bugs that allow virtualized code to “break loose” to some level. Erroneous network virtualization may consent to user code access to sensitive portions of the provider’s infrastructure, or to the resources of other users. Multiple virtual machines (VMs) can share CPUs and main memory surprisingly well in cloud computing. Virtualization is essential to improve architectures and operating systems to efficiently virtualized interrupts and I/O channels [9].

In [10] they present a system that uses the blackbox and gray-box information from individual VMs to detect and alleviate resource hotspots using VM migrations. Potentially the most resource is intensive part of a host-move operation due to the need to evict all VMs currently running on the host.

The resource intensity and thus, the duration of the operation is governed by factors that include VM size and active memory dirtying rate [11]. Effective management is archived without demanding expensive fine-grained monitoring of workload VMs at large scales, otherwise required if trying to proactively predict their migration costs [12].

In [13] they presented a cloud database storage architecture that avoids the local administrator in addition to the cloud administrator to study about the outsourced database content. Furthermore, machine readable rights appearances are used in order to limit users of the database that require to recognize source. These limitations are not unpredictable by administrators after the database related application is launched, in view of the fact that a new responsibility of rights editors is defined once an application is get underway. Cloud data must be protected not only against external attackers, but also corrupt insiders. Our proposed system follows the information-centric approach which aims to make cloud data self-intelligent. In this methodology, cloud data are encrypted and packaged with a usage policy. The data after accessed will confer with its policy, create a virtualization and try to review the trustworthiness of the data environment [13].

In [14] author suggested a Privacy Preserving Repository for Securing Data across the Cloud. In this a privacy preserving repository is being presented for acceptance of integration requirements from clients to share data in the cloud and maintain their privacy, collect and integrate the appropriate data from data sharing services, and return the integration results to users. Their key points are: The data sharing services in the cloud possess the ability to update and control the access and usages of their shared data. That is, data can be updated when required and it can be inferred who is using the data and in what way. The sharing of data in the cloud is done based on the need-to-share principle, which states that the dispatched information of the data is adequate to support client’s integration requirements, but carries no extra information of the data. The repository is limited to gathering data from data sharing services and combining the data to satisfy users’ requirements. The repository will contain no other information apart from that required to deliver the results to the user and it cannot use this data for other purposes [14].

In continuing data integration systems, the concept of a central and trusted authority collecting all data from data sharing services and computing the integration results for users based on the data collected is usually not valid for data sharing services across various organizations. As in the Fig. 4 given below, the process of authentication takes place.
Firstly the user will request to the server for their data and then the server or third party will request for its authentication key that should be username and password if this key matches with the data dictionary’s key then process of authentication complete and on next process our repository will collect only that data required for generating users’ requests. It is assumed that our repository will correctly construct the query plans for users’ integration requirements, decompose the query plans, discover and fetch data from distributed data sharing services, assimilate all data together, and, finally, return the final results to users. Further, they assume that this repository is granted the access to the shared data by all data sharing services, and all shared data is well protected. Because the data sharing services use our context-aware data sharing concept, our repository cannot learn any extra information from the inferential relations of the information it obtains during the process. This repository consists of two components: the query plan wrapper and the query plan executor. The query plan wrapper is responsible for scrutinizing integration requirements and constructing query plans for the query plan executor [14].

![Diagram of Basic Authentication Process](image)

**Figure 4. Basic Authentication Process**

**IV. PROPOSED METHODOLOGY**

The proposed methodology works in the following phases:

1. Create a cloud simulation environment.
2. Initialize cloud with number of datacenters, brokers, users and virtual machine.
3. User sends the attribute query to the broker for authentication.
4. As soon as user authenticates brokers maintains dictionary for each query request and allots a virtualized data centers for the user.
5. The user uses his attribute for data encryption and stores into the virtualized allotted data center.

![Diagram of Process Model of Methodology](image)

**Figure 5. Process Model of Methodology**

**V. EXPECTED OUTCOME**

The proposed methodology implemented in future can be compared with the existing techniques on the basis of following parameters:

1. **Resource Management Metrics**: It is the term used for the analyzing of resources stored in the virtual datacenters. A metric denotes the utilization of resources by the user. In our methodology it will perform better as the existing one.
2. **Host Move Latency**: It is defined as the chances of failures or delay during the access of stored data from the datacenters. In our work the chance of failure or delay should be negligible compared to the utilization.
3. **Migration Failures**: It is defined as the chances of failure during the access of the data from the virtualized datacenters. The failure is less when 100% data is access from the datacenters. The method of authentication will definitely reduce it.
4. **Workload**: It is defined as the total load count on each and every virtualized datacenters. Work load can be computed on the basis of total number of data send and stored on the virtualized datacenters.
5. **Accuracy**: It is defined as the total data stored and access from the virtual datacenters. The term denotes the utilization and loss of data packets from the user. In our work accuracy will maintain due to the authentication process.
6. **CPU Utilization**: It is defined as the performance usage of the CPU during the sending and access of data packets from and into the datacenters so that the overhead is less. It will increase in our methodology.
REFERENCES


