A Technique to Enhance the Privacy Issues

in

Cloud Computing

A Dissertation Report Submitted

By

PROMILA DEVI (Regd. No. 41200433)

to

Department of Computer Science & Engineering

In partial fulfillment of the Requirement

For the

Award of the Degree of

Master of Technology in Computer Science & Engineering

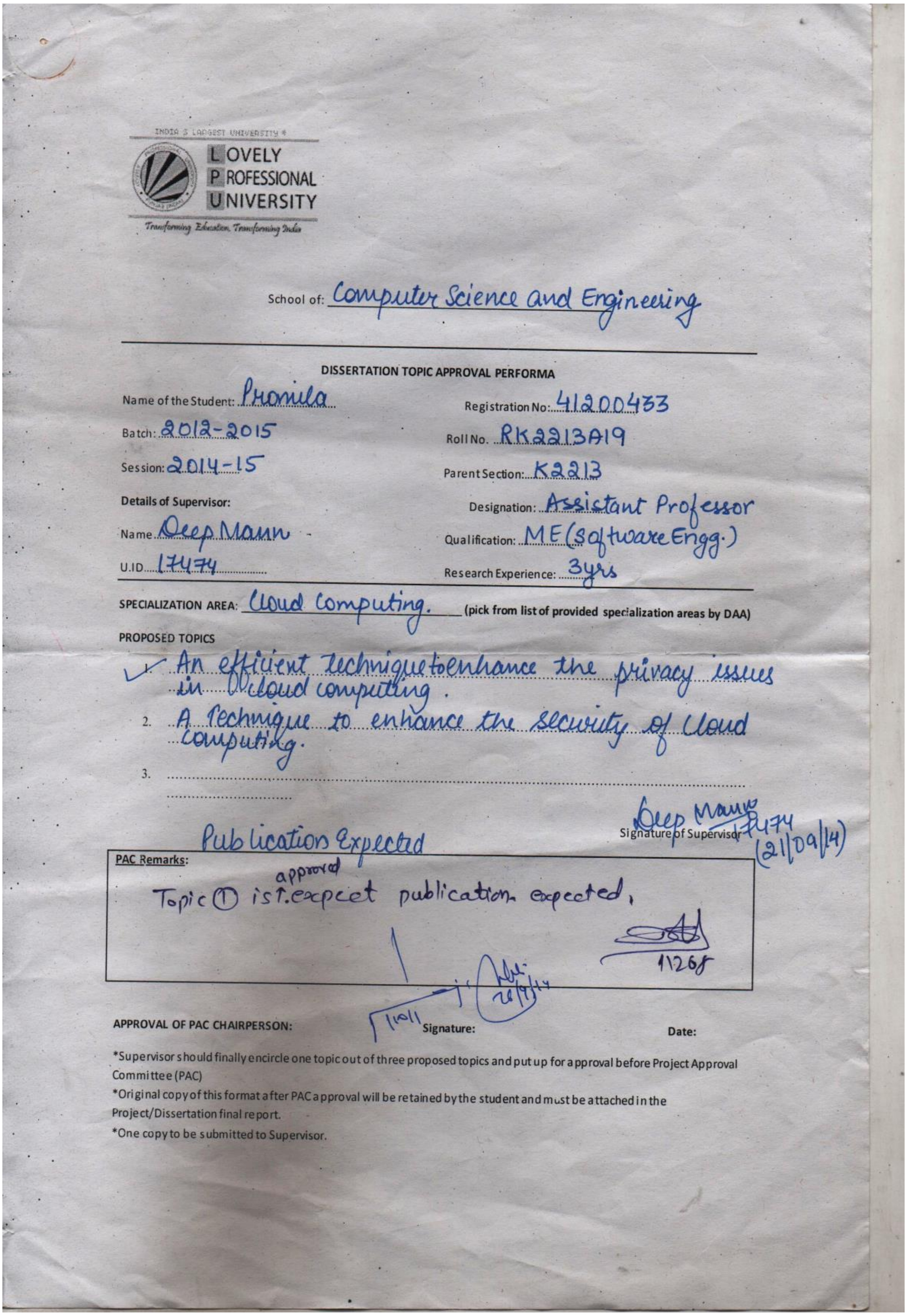
Under the guidance of

MS. DEEP MANN

(Assistant Professor, Dept. Of CSE)

(June, 2015)

PAC Approval



INDIA'S LARGEST UNIVERSITY

LOVELY PROFESSIONAL UNIVERSITY

Transforming Education, Transforming India

School of: Computer Science and Engineering

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Promila Registration No: 41200433

Batch: 2012-2015 Roll No. RK2213A19

Session: 2014-15 Parent Section: K2213

Details of Supervisor: Designation: Assistant Professor

Name: Deep Mann Qualification: ME (software Engg.)

U.ID: 17474 Research Experience: 3yrs

SPECIALIZATION AREA: Cloud Computing. (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

✓ 1. An efficient technique to enhance the privacy issues in cloud computing.

2. A Technique to enhance the security of cloud computing.

3. ....

Publication Expected

Signature of Supervisor: Deep Mann 17474 (21/09/14)

PAC Remarks:

Topic ① is approved excpcet publication expected,

11265

APPROVAL OF PAC CHAIRPERSON: 11011 Signature: 26/9/14 Date:

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)

*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.

*One copy to be submitted to Supervisor.

CERTIFICATE

This is to certify that Ms. Promila Devi has completed M. Tech dissertation report titled "A Technique to Enhance the Privacy Issues in Cloud Computing" under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation report has ever been submitted for any other degree or diploma.

The dissertation report is fit for the submission and the partial fulfillment of the conditions for the award of M. Tech Computer Science & Engineering.

Date: 01 June, 2015

Signature of Advisor

Name: Ms. Deep Mann

UID: 17474

ABSTRACT

With every passing day as the businesses are growing, the computational needs and usage is getting bigger and bigger. Organizations are moving their data over cloud very rapidly to get benefit from the cloud services. But security and privacy of user’s data are still very important issue that needs more attention. The architecture of the cloud is implemented in such a way that it provides flexibility to the users to share their applications over cloud as well as they may request to expand or contract the resources. The increasing popularity of IaaS has created many new problems and challenges in managing the physical resources of large data centers as well as in managing the growth of VM images. There is a need to keep the VM images updated to secure them from malwares but as the image sizes are larger, it becomes necessary to pay attention to the cost of deployment and capturing of images. With the increasing acceptance of virtualization in cloud, a number of inactive VM images are growing which are still a threat to the security and privacy of cloud computing. The large deployment of the VM images is not purely benefitted by the existing patching system as they still suffering from unpredictability, performance challenges and high computational costs. The aim of this research work was to enhance the VM image library and the speed of VM deployment by improving the cost of mirage translations and the speed of translation algorithm.

The Structure-aware Content Address Base technique of translating disk images to virtual images in Mirage Library is modified to decrease the cost and enhance the speed of Mirage Library. The QEMU and KVM tools are used to create the raw virtual images whose indexed version is picked up while searching and deploying the virtual images. Data selection from raw images ignores the additional contents to make the storage, searching and deployment process of virtual images fast. Hence translation cost is automatically reduced and Image library is improved.

ACKNOWLEDGEMENT

It is a great pleasure for me to acknowledge the assistance and contribution of number of individuals who helped me in my dissertation report titled “A Technique to Enhance the Privacy Issues in Cloud Computing.” First and foremost I would like to express my deepest gratitude to my Guide Ms. Deep Mann who has encouraged, supported and guided me during every step of my dissertation report. Without her valuable advice completion of this work would not be possible. I take this opportunity to thank our Head of Department Mr. Dalwinder Singh for his able guidance and for providing the necessary facilities. I am also thankful to the faculty of Computer Science & Engineering of LPU for their invaluable suggestions and advice.

Last, but not the least, I am also grateful to my family for their consistent assistance, encouragement and love.

DECLARATION

I hereby declare that the dissertation report entitled “A Technique to enhance the Privacy Issues in Cloud Computing,” submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: 01 June, 2015

(Promila Devi)

Regd. No. 41200433

CONTENTS

List of Figures

List of Tables

Chapter 1
INTRODUCTION

This chapter gives the overview of basic introduction of Cloud computing as a new computing paradigm including the usage of cloud computing in current scenario, prediction table for growth, basic definition, service models, deployment models, essential traits, benefits, drawbacks, application and major service providers of cloud computing in the IT market.

1.1 Review of Cloud Computing

Over the last decade, the rapid penetration of the internet and information technologies into all spheres of society and individuals lives' has led to a sharp increase in Internet users: in 2011[1], their number exceeded 2 billion in the world and in 2014, their number exceeds … In the world. These facts tell us that to increase the efficiency of a business it is good to prepare specialists who are well oriented in modern innovative technologies, including the connection to the Internet.

In the present scenario, almost every aspect of our professional and personal life is moving towards the availability of resources online. With the understanding of this trend, the herculean web-based organizations like Amazon, Google and IBM came with a new paradigm of computing named ad Cloud Computing which provides the sharing of web based infrastructure. Cloud Computing is a new computing prototype, also be named as an online service model which provides the computer resources to the users as an Internet services depending on their requirement and pay as an operating expense. The uses have access to their own data.

Since the 1960s, researchers Douglas Park hill and John McCarthy have focused their efforts on the development of a computing model names "Utility Computing" aims to provide users with services on the Internet that are similar to traditional utilities. Nowadays, Utility Computing is named Cloud Computing which has rapidly changed the dynamics of IT [5, 18, 23].

Cloud computing is different from conventional computing. In conventional computing the organizations needs to setup a lot of equipment like ample servers and storage devices in support of their business. It does not require large capital investments but also requires a lot of efforts for the maintenance and up gradation of technology being used. Continual power supply, cooling mechanism, spacious server rooms and a team of experts were of course the additional requirements whereas Cloud computing creates the new perspectives of opportunity for organizations. Cloud computing is introduced as a new business model which allow its customers to pay only for that what they use. [19]

In 2007, with the accelerated development of network communication and growing furtherance of the needs force business and private users to expand their information system which support cloud computing to gain the lionization. According to the survey of IDCI 2009-2013 report, Figure1 represents revenues for five major IT segments: Application software, Application development and deployment software, Systems Infrastructure software and Disk Storage delivered via cloud services model.

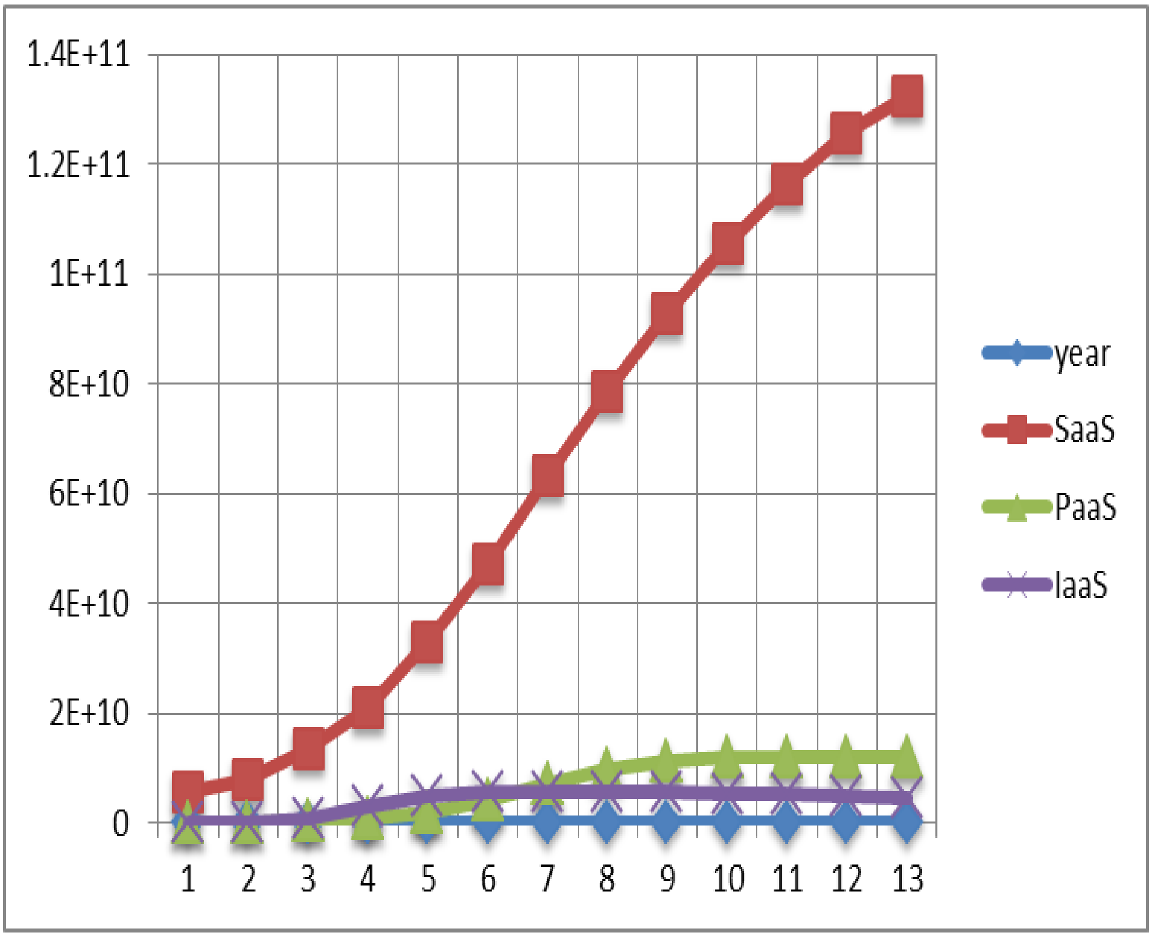


Figure1: Worldwide growth of cloud products/services Source: IDC, 2014

According to the survey of Forbes, CISCO predicts the global cloud index showing the global Data Centre traffic in Exabyte for 2011 to 2016.Table 1 shows the global cloud Data Centre IP traffic by Type and by Segment of a Data Centre.

Table1: Global Data Centre IP Traffic, 2011-2020

Year	IP Traffic (EB)	Percentage Change
2011	1755	-
2012	2551	45.35
2013	3251	27.44
2014	4124	26.85
2015	5246	27.2
2016	6649	26.74
2017	7300	9.79
2018	8254	13.06
2019	9209	11.57
2020	10164	10.37

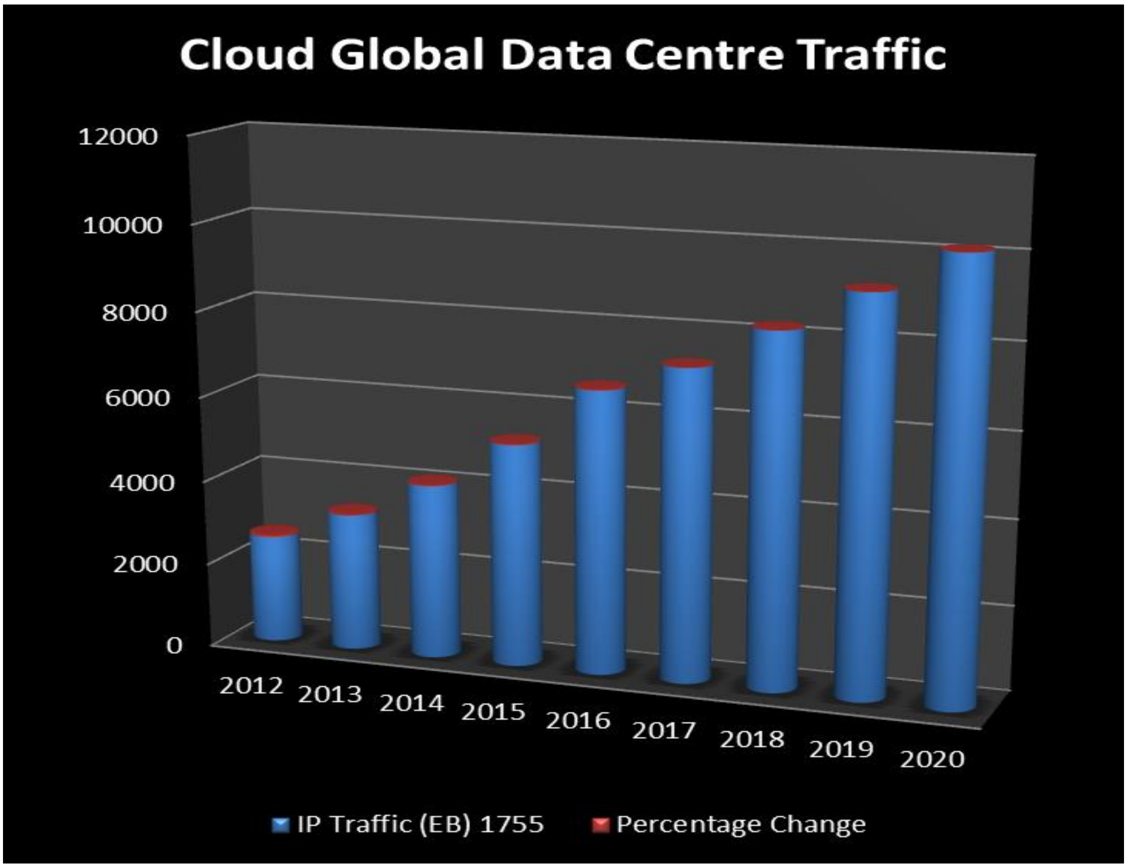


Figure 2: Cloud Data Centre Traffic Source: Cisco Global Cloud Index, 2012

Today many organizations are shifting their businesses over cloud as they realize that with the help of cloud they can achieve quick entry to outstanding business applications and expand their framework at trivial cost. A cloud has several benefits like:

- Rapid stationing
- Metered Service
- Minor costs
- scalability
- Accelerated provisioning
- Adaptability
- Pervasive Network Access
- Prominent elasticity
- Hypervisor security
- Low-cost catastrophe restoration and data storage solutions
- On-demand security management
- Real-time detection of system tampering
- Fast reconstruction of services

Despite being a jargon, several convincing factors are allied with the security issues in cloud. According to an IDCI survey in 2009, 74% of entrepreneurs are still not sure about shifting to the cloud, alleged data security as the top most risk prohibiting their acceptance to cloud service model [82].

Analogue of Cloud Computing

The review of the paper by NIST [20, 21], IASA [37] and Barkley [29] tells that the definition of cloud computing as:

“Cloud computing is a web-based model of computing, provides the scalable and elastic information technology resources to multiple users at the same time. The user has no need to own and manage his own IT resources as it provides necessary amount of virtualized resources through Internet."

Table 2: NIST definition of Cloud Computing

Key Characteristics	Deployment Models	Service Delivery Models
On-demand Self- service	Public Cloud	Software as a Service (SaaS)
Broad Network Access	Private Cloud	Platform as a Service (PaaS)
Resource Pooling	Community Cloud	Infrastructure as a Service (IaaS)
Rapid Elasticity	Hybrid Cloud	
Measured Service		

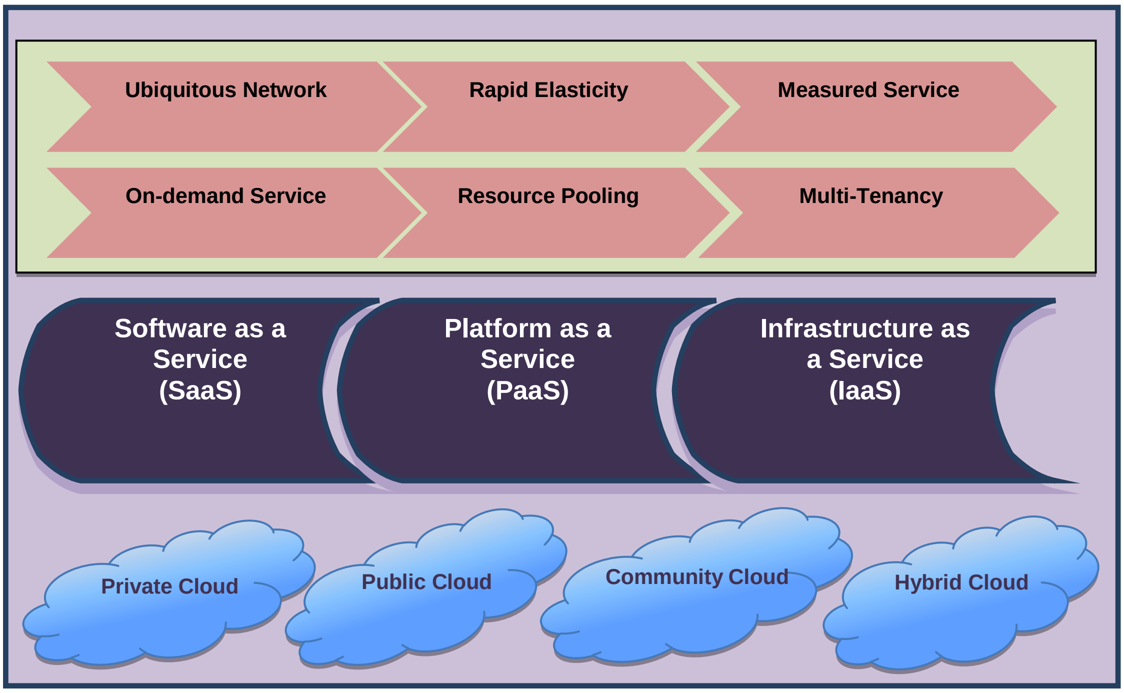


Figure 3: NIST architecture of Cloud Computing

Service Models

❖ **Software as a Service**: SaaS provides application developers services which run on cloud infrastructure of the provider. In SaaS, application is not owned by the user.

They are control and management by the cloud providers and user has to pay for the amount of time he wants to use it. There are several SaaS applications such as CRM applications and HR solutions. Google Apps are the example of SaaS.

❖ **Platform as a Service**: PaaS provides platforms include the tools for creating, testing and implementing the applications such as DBMS, Middleware and the programming environment. It also provides the development and deployment tools which are needed to develop applications. Force.com is an example of PaaS.

❖ **Infrastructure as a Service:** IaaS serves the infrastructure to users to develop and deploy software within the bared infrastructure. IaaS also offers Virtual machine disk storage, VLANs, Load balancers and IP addresses. Typical examples of IaaS are Amazons Dynamo and Google Big table

Deployment Models

❖ **Private cloud:** Private cloud structure can be used only within a single organization where resources are handled by a third party or by their own. It is an intranet system or email system used by the users within the organization.

❖ **Public Cloud:** The public cloud structures can be used by the public with some payable option or for free. The service is provided by Government agencies. It may be in the ownership of a commercial, academic or government organization. Dropbox is an example of public storage service.

❖ **Community Cloud:** The Community cloud is used by specific communities to serve the society. It may be possessed by a specific community or third parties. It is accessible to a group of organizations.

❖ **Hybrid Cloud:** It is the interfusion of public and private cloud. It enables the data and applications portability for balancing the load between clouds.

It is a provision of computing resources via Internet such as SaaS, PaaS and IaaS on the same physical server. The cloud resource-exposure models are highlighted as: Software as a Service (SaaS), Where user buys subscription to on-line applications/software, Platform as a Service (PaaS), offering development support tools to develop software products, Infrastructure as a Service (IaaS), offering fast and easy scalability of storage, computation and network capabilities to grow and shrink the number of virtual machines according to workloads [7, 12]. Cloud computing is quickly becoming the center of attention for its various strengths such as cost saving of IT and flexible use of resources.

Essential traits of Cloud Computing

The NIST proposed architecture is more reliable and universally accepted architecture of cloud computing which fixed some essential traits of this computing paradigm. [31]

❖ **On-demand Service:** It provides the resources or services only when user demands for them. A user has the freedom to customize and personalize his computing adequacy such as software installation, the speed of data access and processing, amount of data stored and network configuration.

❖ **Resource Pooling:** It provides a pool of resources which serves multiple users with different resources being allocated and reallocated dynamically as per their demand. Users only control the basic parameters of service such as access speed and amount of data storage.

❖ **Rapid Elasticity and Scalability:** Elasticity and scalability are two important features of the cloud computing. Elasticity is referred as the ability of a provider to grow and shrink the amount of resources to meet demand of customers. This is a cloud-key feature which reduces the organizational overhead or space. Scalability is referred as the ability of a service provider to instantly and automatically scale their computing resources whenever they deem it necessary.

❖ **Measurable Service:** It provides an automatic mechanism to optimize the essential resources according to the demands of users and the services required by them. These services are completely measurable and transparent to both, provider and users.

1.2 Related Technologies

In order to make easy and clear understanding of this approach, we need to compare cloud computing with its two contemporary and universally accepted computing paradigms known as Cluster computing paradigm and Grid computing paradigm. [11]

❖ **Grid Computing:** The Grid computing paradigm was derived in 1990 from an electrical power grid. The objective behind this computing approach was to affirm the power grid characteristics such as pervasiveness, simplicity and reliability, typically used to run bulky computational tasks inside an organization. It is like a parallel and distributed system which enables the sharing of geographically distributed resources dynamically, rely upon their availability, performance and cost. Foster says that grid computing is the decentralization of resources.

❖ **Cluster Computing:** In computer networking, cluster is defined as altered implementation of shared resources. It was developed in 1960 by IBM. The objective behind this computing approach was to facilitate an alternate to link mainframe computers in such a way that a cost effective approach of parallelism can be provided. [1]

1.3 Merits of Cloud Computing

The Table 3 shows the merits of cloud computing [14].

Table 3: Merits of cloud computing

S.No.	**Benefit**	**Description**
1.	Reduced Cost	A user has to pay per use for availing a service. Thus, it is easy to control and reduce the cost.
2.	Storage space	A user can avail more space as storage space is provided through the cloud.
3.	Mobility	The users connected to the cloud can gain the access to data where ever they are by using different sources like tablets, smart phones and laptops.
4.	Flexibility	Cloud makes the resources flexible which can be easily obtained.

1.4 Drawbacks of Cloud Computing

The table 4 shows the basic drawbacks found in cloud computing [14].

Table 4: Drawbacks of cloud computing

S.No.	Drawback	Description

1.	Security and Privacy	Many organizations hesitate to utilize the services provided by cloud because data is handled by external sources. [35]
2.	Large Dataset	It is very difficult to shift large amount of data over clouds.
3.	Internet Connectivity	Internet connection is mandatory for the cloud to work
4.	Reliability	There is a probability of performance issues if provide is not reliable.

1.5 Applications of Cloud Computing

The Table 5 shows the various application areas where cloud services are mostly used [25]

Table 5: Applications of cloud computing

S.No.	Application Area	Applications
1.	Business	Mail Chimp, Google Applications for business.
2.	Storage and Backup	Box.com, and Mozy
3.	Management	Time tracking, organizing notes.
4.	Social	Facebook, Twitter, etc.
5.	Entertainment	Audiobox.fm
6.	Fine Arts	Moo

1.6 Cloud Service Providers

❖ **Amazon:** AWS is known as a leader in field of cloud storage service.

❖ **Microsoft:** Microsoft's Windows Azure is also the most broadly used cloud storage service [26].

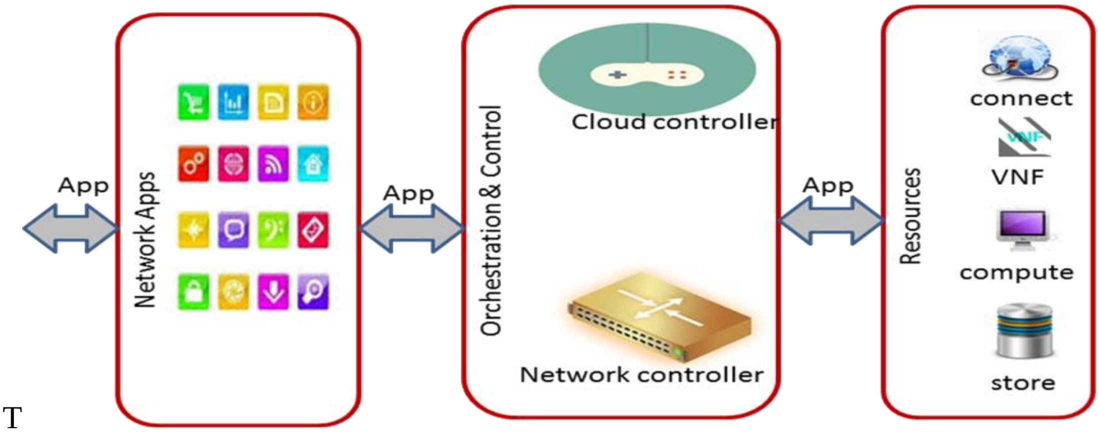
❖ **Google:** Google Cloud was launched in 2010 includes cloud-based virtual machines and used as a big data dissection tool.

❖ **IBM**: IBM has also become a prime player in the large enterprises of cloud market [24]

1.7 Open Security Architecture of Cloud Computing

The OSA is the manifest of the internal functioning of core cloud beyond various organizations and also includes the controls that acquire special attention.

Figure 4:



T

he OSA of Cloud

The figure 4 contains three types of controls in this architecture as shown in the following table.

Table 6: OSA Controls

S.No.	Control Type	Description
1	SA-I/4/5	It is a control of system possession which ensures that acquired services is managed in a correct manner.

2	CP-I	It is a contingency planning control ensures the way how to respond on occurrence of interruption to service delivery.
3	Risk Assessment Control	It assists to recognize the threats associated with services.

The OSA is also consisting of the patterns which prepare a view of activities shared by security architects and business managers like how to translate these into a framework of the providers and deciding the risks mitigating controls.

1.8 MIRAGE Image Management System

MIRAGE is an image library management system, states various security threats concerned with the sharing of VM image [1]. MIRAGE image library addresses various issues associated with the secured management of the VM images that encapsulates all applications of the cloud. MIRAGE transfer disk images into Mirage and store contents with indexes of image in a structured file system instead of the opaque images. Mirage image library impart features for capturing and deploying virtual machine images. It conserves a derivational tree that indicates how an image was derived from existing images in terms of patching and scanning of images. Generally it requires a VM entity to run off-line and enable image analysis.

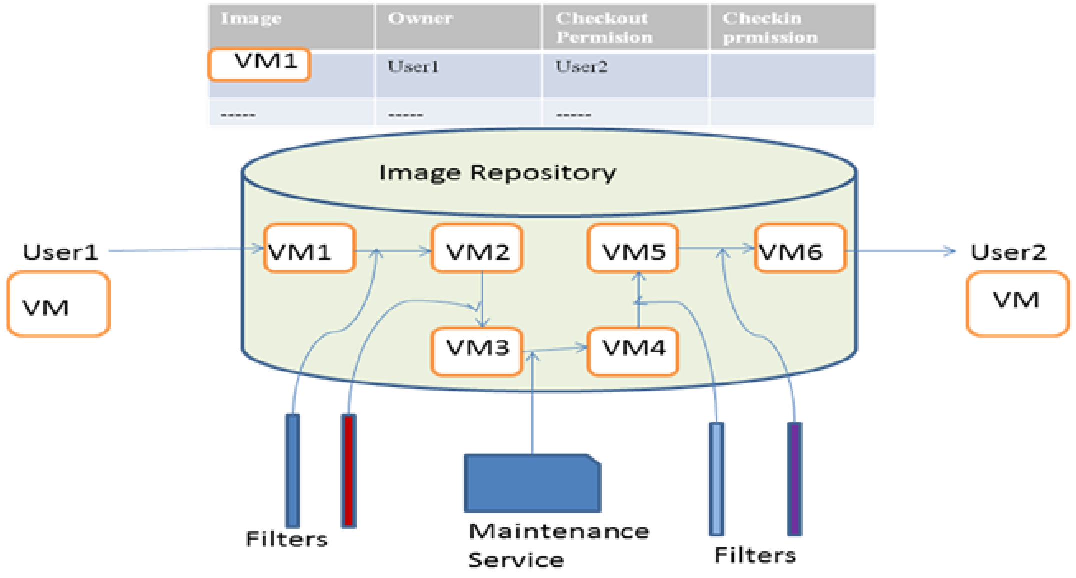


Figure 5: Mirage Image Architecture

The Figure 5 depicts four types of components of MIRAGE system.

- **Access Control:** It controls the framework that governs the allocation of virtual machine images. Every image in the data warehouse has a solo owner, authorized to share the images only with authorized users by authorizing access rights for an image.

- **Filters:** They transform the images at publish time by removing the unwanted data or hiding the sensitive data from publisher's original image. Storage specific filters are system-wide filters, out of which few are compulsory and few are arbitrary. The user-specific filters encapsulate user's confidential information with help of images.

- **Provenance Tracking:** It keeps a record of the derivation history of an image at the time of the submission of a new image is submitted in the repository. This information can be used by audit system to find out the presence of crooked or malign data.

- **Image Maintenance:** Repository system has a set of maintenance utilities implemented over entire repository to find and fix malware exposed after the publishing of images.

With the rise of IaaS, both public and private clouds has suffered from the problem of managing huge collection of VM images as VM images need to be updated with security chunks and regularly scanned for malware. As Mirage's image format is different from the format that a hypervisor requires, hence, Mirage imposes translation costs. IBM Research [25] recommended three algorithms to reduce translation/ Runtime cost and the development cost as:

- **A Structure-Aware Content Address Store:** CAS provides the storage to arbitrary data of users where each item is identified by a secure identifier that is created by using SHA1. The semantics of CAS are always write-once which means that no image can be stored without altering its existing identifier. It will produce a new item which exploits the write-once rule of CAS. Each item in CAS is stored as a separate item where contents of file are known as leaves, interior nodes as partition manifests, disk image as disk manifest and VM image as image manifest. To reference the nodes, manifest use their CAS identifier also known as a sequence number for the image. The image indexer uses a standard hypervisor to convert images in both directions between a disk image and the Mirage image but make it harder to implement file level operations on disk images fastly. The catalog manager in CAS records the Meta data for each image in form of a relational database. It also record version image data for each named image. User-level services and administrator level services are offered by library services of CAS.

Mirage stores large volumes of indexed images in CAS where each item on disk index can be mapped by its content identifier. Content identifier is also known as location of image in a volume. Volumes are the sparse files where on-disk index is similar to a directory structure. The structure permits the CAS to optimize the items randomly but it very costly for on-disk index. It associates the lookup index tables with raw content volumes instead of with items. Thus, it becomes more robust when image retrieval processes do not follow the structure closely.

- **Virtual Mount Mechanism:** There are many situations are observed when offline patching do not need disk images. In that case, image writes are placed on scrape area in disk from where new datafile manifest system is created with a new identifier and this attribute automatically replace the file contents. It speeds up the offline patching.

- **Delta Deployment:** It reduces the disk recreation cost by computing file-level deltas for similar disk images. Generally, Mirage consults cache when a disk image is retrieved. If image is not found in cache, it is reconstructed otherwise it is cloned. In case of Delta deployment, if disk image does not exist in cache, its source image is searched, a delta is computed to get image. On getting image, the image is cloned and delta is applied on the clone. Mirage employs delta only when a user has the privilege to read the source image as well as the target image.

These algorithms are purposely recommended to mitigate the translation cost involved in storage and transfer of mirage virtual images. Mirage uses a standard hypervisor to translate disk image to mirage library and from mirage to disk manifest. For few technical weaknesses in the architecture of cloud computing, it is sensitive to several privacy and security risks as the management of data and services associated with the application and databases migration from cloud to large data centers is not trustworthy. It poses many security challenges [53]. All the possible security and privacy risks are studied under review of literature in chapter 2.

1.9 Organization of Report

The overall organization of this Dissertation Report is as:

Chapter 2: This chapter is a descriptive study of all the possible research issues concerned with Cloud Computing, Barriers to Cloud Computing, Virtualization and Hypervisor role in Cloud Computing, Existing schemes associated with security of Cloud Computing and detailed description of Mirage Image Management System.

Chapter 3: This chapter describes the scope and significance of reduced translation costs of VM images to IT organizations and Data Centers.

Chapter 4: This chapter describes the objectives for which this report is prepared.

Chapter 5: This chapter describes the research methodology chosen for accomplishing this study includes internal structure of CAS, steps to achieve the objectives, inputs to system and expected outcomes.

Chapter 6: This chapter describes the implementation process of structure- aware CAS, required libraries and the approximated results of existing and enhanced library are compared to analyze the improvement in the new system.

Chapter 7: This chapter describes the concluding observations and the future recommendations.

Chapter -2

REVIEW OF LITERATURE

The objective of performing literature review is to identify the ontology of cloud computing as a new computing paradigm and the challenges for cloud computing.

Cloud computing is a new paradigm of computing in the business community, therefore many definitions are available. The NIST [1, 2] imparts a universally accepted definition of cloud computing inclusive of its traits, service and deployments models. In all available documents, various facets of cloud computing are investigated, along with its advantages, threats involved, and suggestions for securing the Cloud.

2.1 Research Issues in Cloud Computing

The scope of security of the information residing on cloud will depend on the cloud delivery models used by the cloud-user organizations. According to CIA security models, security threats are categorized into three categories.

Table 7: Threats to Security model of Cloud

Security Threat	**Description**
Loss of Confidentiality	Confidentiality ensures that the message sent over cloud should be kept secret or not readable to others. A loss of confidentiality is the unauthorized disclosure of information. The insider threats to confidentiality of data are malicious cloud provider users, customer users and third party users and external threats are the threats of hardware attacks and supply chain attacks by dedicated attackers.
Loss of Integrity	Integrity ensures that the data presented are true, valid and includes escorting against any kind of discrepancy in information and also ensures its authenticity. A loss of integrity is the unauthorized alteration or destruction of information. Integrity threats are related with the data segregation, user access and data quality.

Loss of Availability	Availability ensures that the committed resources will perform its designated function upon the demand of its users to provide cloud services. The availability threats are concerned with the availability of data residing on the cloud. Any change in cloud delivery service model could introduce negative effect. Denial of service, physical disruption is the threats to the availability of data.

2.2 Barriers to Cloud Computing

❖ **Security and Privacy Risks:** The success of any computing language can be determined from the level of security it provides to ensure how much secure it is [12, 21, 68]. Almost all the service providers assert that information sides in their servers is more secure and abundantly guarded from any kind of invasions and thefts than the data stored on innumerable personal computers or Laptops. But there have been many cases observed when the security provided by these providers is violated and the complete system has been interrupted for several hours. Moreover, several security rifts found that bring crucial breaches in the security model of leading service providers (CSPs).

Privacy is the capability of an object to control the information that it acknowledge about itself to the service provider. It has also the ability to regulate the approach to its information means that who has the privilege to use that information. R. Gellman [65] altercate the various guidelines concerned with the collection, sustenance and revelation of personal details of an object. Information requiring privacy needs the specific treatment as discussed in [9, 23].

In case of deployment models, multiple security issues have been observed that also need to be inscribed in contrast of a public cloud to private cloud. Public clouds perform as a moderator for a myriad of VMs, VM auditors and supportive middleware [44]. The protection of a public cloud depends on the behavior of all the entities and relationships between them. A public cloud provides distributive multi-tenant environment in which a group of users share a common software instance with specific privileges. As the users accumulate, security threats are assimilating more intensive and assorted. Thus it is essential to recognize the areas which are decumbent to security attacks and the necessary devices to ensure the protection of client-side as well as the server-side [81]. The existence of diverse security concerns in public cloud, idea of affirming a private cloud is safer with option to choose the public cloud in future only if required [35].

Evolution of cloud computing be obligated to mash-up. A mash-up is a code, integrates data or functions from different web sources to create a new service. It uses the data or functions of multiple web sources in relation to a specific application by which security challenges become more multifarious and acute. On the basis of this conviction of mash-up, a secure component model has been proposed in [17].

❖ Risks to the Performance, Reliability and Latency

It is discovered that virtual machines are sharing CPUs and main memory more efficiently as compare to Network and Disk I/O. One way to improve the performance of an I/O is to refine the architecture and operating system so that it may virtualizes the interrupts and I/O channels more effectively and efficiently. Another possibility to improve its performance is the usage of flash memory that conserves the information even when the system is powered off. It has no moving part, thus it accelerates the accessing speed and sustains more I/O operations than a disk. Latency [55, 62] is also a sensitive affair in cloud computing which deals with the flow of data throughout the different clouds. Some latency influencing determinants are: Data encryption and decryption when it switches over unsecured networks, Congestion, Windowing.

Congestion leads to blockage when the amount of data flows through network channel are high and there are numerous requests that need concurrent access. The conduct of system is a key element that should be taken into consideration, but, several times service providers face shortage either by permitting many VMs to access or getting its maximum throughput threshold, which hurts the performance of the system and increases the latency of the system.

❖ Portability and Interoperability Risks

Several scenarios have been noticed when organizations need to move their data and applications from existing cloud platform to some other cloud platform which is better than the existing one. When a customer is trying to migrate from one cloud platform to other cloud platform, faces many challenges which implicates multiple risks and disintegrate the system if it is not executed properly[48]. Sometimes, multiple platforms are needed for a specific solution for which platforms communication is required for the successful completion of a task. For smooth running of such tasks, the internal structure of the organization should be capable to manage the interoperability between multi cloud platforms [49]. Cloud security model proposed in [48] act like a guideline principle in constructing security tools for clouds. The multi-folded feature provided by cloud is still an issue that is needed to be solved for a better functioning.

❖ **Risk of Data Breaching:** During the last few years, many security issues in data transitioning have been observed. Data transitioning includes multiple data centers and cloud deployment models. Leaving from one datacenter to other datacenter is major security issue as it has been infringed several times. Data transitioning through Fiber-Optic cables was advised a secure mode to transfer data until an illegal fibre wiretap device was detected by US security forces in Telco Verizon's optical network implanted at a Mutual Fund company [33]. It can tap the information without creating any disturbance and can easily access fibre. Hence, it also becomes security issue concerned with data transitioning over networks.

❖ **Risks with Data Storage**

On-line data storage is becoming quite fashionable as it permits organizations to keep extensive blocks of data without mounting up the needed architecture. In spite of many benefits of on-line data storage, still, there is a threat of data leakage. Some problems are noticed very frequently in dynamic data storage that remains continuous in the cloud. Depending on the level and category of storage provided, multiple risks are attached to them have been described in [12, 53]. To avoid these barriers, quality scanners and malware protection software are to be initiated.

2.3 Security Levels of Cloud Computing

The main objective of cloud computing is to arrange a secure environment over multi-tenancy and isolation [70]. It is necessary to secure the cloud model at all the levels i.e. at Network, Host and Application Level to retain the cloud up. In conformation to these levels, various security rifts may occur.

❖ **Security at Network Level**

Network systems are categorized in various categories as communal and Non-communal Networks, Public and Private Networks, restricted spaced and large size Networks. Every category of these networks has been victimized by a number of attacks. To assure the security at network level, one should consider some factors like confidentiality and integrity of data in network, proper data and network access controls and security maintenance mechanisms across third-party threats. Threats associated with network level security are:

DNS attacks: DNS is a key building block of Internet which allows users to access websites and exchange emails. Domain Name System is a network (Internet) service that renders a domain name into IP address. DNS attack is a type of attack in which the client has been wiped off to some nefarious cloud rather than to the server called by user. Undoubtedly Domain Name System Security Extension (DNSSE) minimizes the domain risks, but still many cases have been observed when these measures prove to be inadequate [15].

Sniffer attacks: Sniffer attacks are placed by attackers to hack sensitive network information. A sniffer is a piece of code that grabs the packets flowing in a network. Sniffers are the real network troubleshooting tools. If the network packets are not encrypted, intruder can read their data through sniffer [84].

Reusability of IP Addresses: Every node on the network has assigned an IP address and when a specific user exits from network then same IP address is reassigned to a novel user. It takes some time to changes IP address in DNS. During this lag time, there is a probability that the data may be accessed by some hacker reason being the address quietly resides in the domain name space cache that can violates the privacy of the previous user [61].

BGP Prefix Hijacking: In BGP attack, a wrong declaration to an IP address of Autonomous System (AS) is made which allows hijackers to trace the untraceable IP addresses and obtain control over them. ASs communicates via the Border Gateway Protocol (BGP) model. Sometimes a faulty autonomous system may announce wrongly about the IP address affiliated to it, which routed the traffic to some other IP than the destined one. As a result data is leaked and reaches to some unwanted source. Security system for autonomous system is proposed in [37].

- **Security at Application Level**

Security at application level is concerned with customization of applications and physical resources to protect all software so that intruders cannot capture the control over them. Attacks at application level are launched by attackers as they appear to the system as a trusted user to obtain access and the system gets victimized. Thus, it is necessary to implement security checks to minimize the risks at this level. The threats to application level security are:

Denial of Service Attacks: DoS reroute the services assigned to authorized users. It causes the congestion by overloading the server by numerous requests that raise bandwidth utilization to make some portions unapproachable to its users. Intrusion Detection System (IDS) is proposed to guard against DoS [3, 41].

Cookie Poisoning: It alters cookie elements to provide crooked access to an application. Cookie basically includes the personal information of user. Once the cookie is available, its contents can be forged. This situation can be escaped either by carrying out the regular cookie clean-up or encoding the data of cookie [14].

Invisible Field Manipulation: On web pages, we find that some properties are invisible as they have some information relating to page only for the use of its developers. These fields are extremely prostrate to attacks as they are modifiable. This is a severe security breach [3].

Backdoor and Debug Options: The reason behind enabling the debug option is only to make developmental changes in the code. Sometimes, the debug options are unknowingly left enabled which may allow an attacker to make changes in code [66].

Distributed Denial of Service Attacks: DDoS targets the substantial services active on server. It overloads the server with numerous of packets so that it fails to handle them and obtain the control of information flowing at certain times [3]. Prevention treatment suggested against DDoS is to install IDS on all the machines [66].

CAPTCHA Breaking: CAPACHAs was introduced to control spam and exploitation of the attached network components by bots. Recently, it has been observed that the spammers discovered a way to crack CAPACHA, favored by the service providers of Hotmail and Gmail as they introduces the audio systems to read CAPACHA characters for the visually busted people [1].

Google Hacking: Google has appeared as the most widely used search engine to search any information on Internet. It is a hacking technique in which intruder uses Google search engine to locate sensitive information from user’s account. A Google hacking case was observed in 2010 in China when log on information of millions of gmail users were abducted by a body of Chinese attackers [42].

❖ Host Level Security

From the perspective of security, the information regarding the host platforms, operating systems and process are publically not shared .The host level security problems are related with hypervisor and virtual servers as:

Hypervisor Security- Virtualization is the most important element in the formation of cloud computing. Leading virtualization vendors are VMware, Xen and Microsoft. Virtual Machines and the hypervisor are two levels of virtualization. Virtual machine refers to a logical computer that runs on operating system and applications like a physical computer. A hypervisor virtualization approach permits different OS to run simultaneously on a host machine. It becomes available at boot time of the machine and act as a controlling agent of all the resources across the host machine, so they do not intersect each other. With increase of VMs, the security issues associated with them needs to be considered because it becomes difficult to maintain all systems.

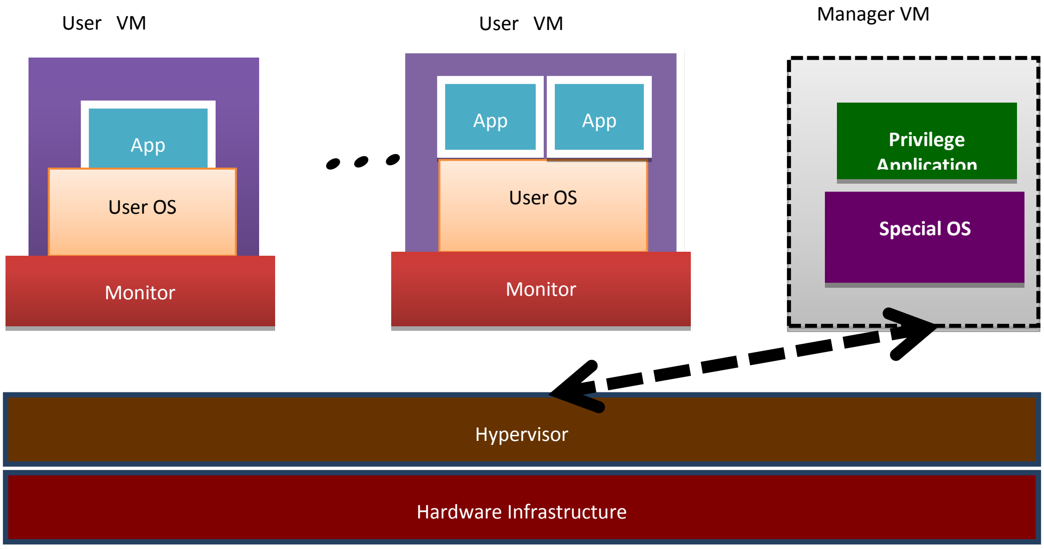


Figure 6: Hypervisor Based Virtualization

Undoubtedly, there are many security zones but all exists within the same physical infrastructure. In case hypervisor crashes or the attacker obtains full control over hypervisor, all the systems and virtual machines gets affected.

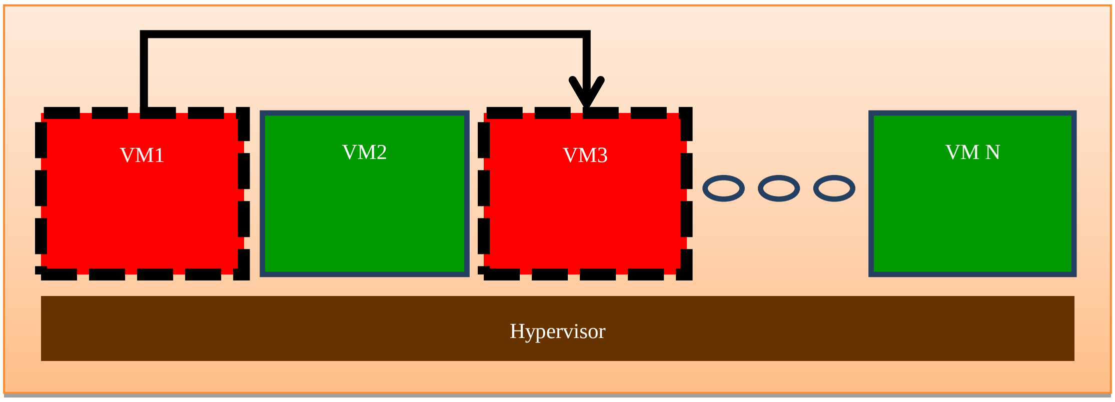


Figure 7: Attack scenario within hypervisor

There is a need of more secure APIs and careful network planning to minimize the hypervisor risks. By understanding the type, behavior and association between the components of hypervisor architecture, cloud systems can be developed [18].

Virtual Server Security: When a user is running his sensitive data on virtualized platforms, a lot of changes occurred like location, physical server, thus sensitive assets need to be secured all the time. IaaS users have full access to the guest virtual machine which is hosted and isolated by hypervisor technology. Virtual servers are approachable on the Internet, thus the process of protecting the virtual server in cloud environment demands very strong security operations.

Some suggestions for virtual server security are given as:

1. Guard the integrity of images from unauthorized users.

2. Avoid password based access.

3. Allow Role based access password

4. Keep the decoding key away from the cloud.

5. Facilitates system auditing and event logging.

6. Cloud Data Storage and Security

It is a revolutionary storage method that service providers use to bring storage as a service. From music files to pictures to sensitive data, they take the backup of the user's data and store them on the large data centers. It allows the users to access synchronize and access his data across multiple devices as long as Internet is available. The flow of data between the user, server and its storage in cloud is shown as figure 7

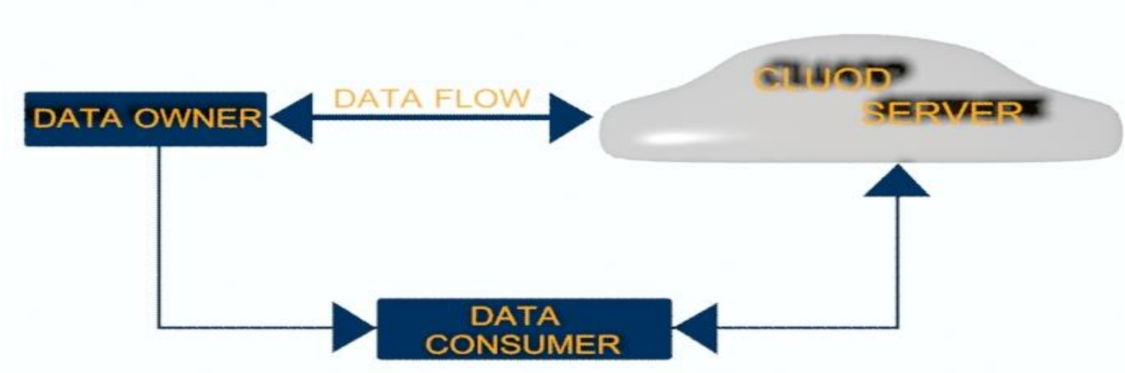


Figure 8: Data flow between user and cloud server

Although, providers commit that their cloud is highly secure but many cases has been identified when their clouds have been modified and data leaked or lost due to security cracks or due to user mistakes. No doubt, service providers are trying various technologies to ensure security of their cloud against any kind of security breach. Whether to store the data in cloud is secure or not is still a question for organizations.

The traditional environment of virtualized cloud storage is not suitable for controlling the security issues. The service providers’ use various encryption and homo-morphic token techniques to secure the data resides in their cloud [11]. Domain-based trust model is useful to handle cross clouds where each domain has a specific actor dedicated for the purpose of trust management.

Neglected Data-Remanence is other major issue relates with the data storage security. Data-Remanence is the lingering representation of data which allow data reconstruction when data is removed, may cause minimal threat in case of private clouds and severe security threats in public types [31].

2.4 Virtualization

In virtualized cloud environments, workloads can be deployed and scaled-out easily through the rapid trapping of virtual machines. Consequently, cloud computing has become very attractive computing technique which provides reliable and customized computing environment for widespread Internet users. In spite of many advantages, it also brings many challenges such as security and privacy that should be taken under consideration [6, 8].

IaaS is the well-established service model of cloud, presents ample variety of products and competence. It is necessary to investigate the various security and privacy issues concerned with each one of six components of IaaS. Security challenge to SLA to monitor and enforce Q0S attributes, , Utility Computing issue as multilayers makes system more complex, Cloud Software issues against XML and web services, threat of DDoS, MITM to network and Internet connectivity, issues against physical infrastructure and issues related to secure virtualization of VM [10, 12, 31].

Virtualization is act like a key enablers in foundation of cloud computing. Virtualization technology helps organizations to reduce the operational cost and ensuring improved efficiency. Virtual machine is a soft computer that runs both OS and applications. In virtualized environment, Virtual Machine Manager (VMM) creates and controls all the virtual machines. Two major benefits offered by virtualization are the Resource Sharing and Isolation. In virtualized environment, the virtual machines share the physical resources like disk, memory and network devices of the underlying host where Hypervisor plays an important role. All the virtual machines are isolated means all the running virtual machines on the same physical hardware cannot see each other. Virtualization also provides an isolated environment to test new applications and to debug malicious programs [18, 19, 30].

The cloud users can hire the computational time and the storage space of large data centers via IaaS. For leasing the computational time, IaaS allow the users to deploy virtual machine environment on the resources of the data center. The increasing popularity of IaaS has created many new problems and challenges in the managing the physical resources of large data centers as well as in managing the growing collection of VM images. Many critical responsibilities are closely related with VM images like a stable storage of images, inferior latency regeneration of images for instantiating to user requests, capturing of VM images from running objects and fast transfer of VM images across cloud servers [1, 15, 29].

There are different ways to virtualize the environment and different technologies are available in the market to do this. An organization can opt any of the techniques on the basis of its need and objectives. The approaches followed to virtualize an environment are Full-Virtualization and Para-Virtualization. In full-virtualization, hypervisor stimulates several logical instances of VMs so that a VM may run on any operating system without any modification [2, 26]. In Para-virtualization, the running VMs can be altered in order to be operated in a virtual environment.

Figure 8 gives idea of a VM environment in which three different guest machines are running on hardware. Every VM is isolated to process its own OS and applications. Hypervisor is a host layer that always lies between physical infrastructure and the guest machines that enable the interoperability between different operating systems on a single physical infrastructure.

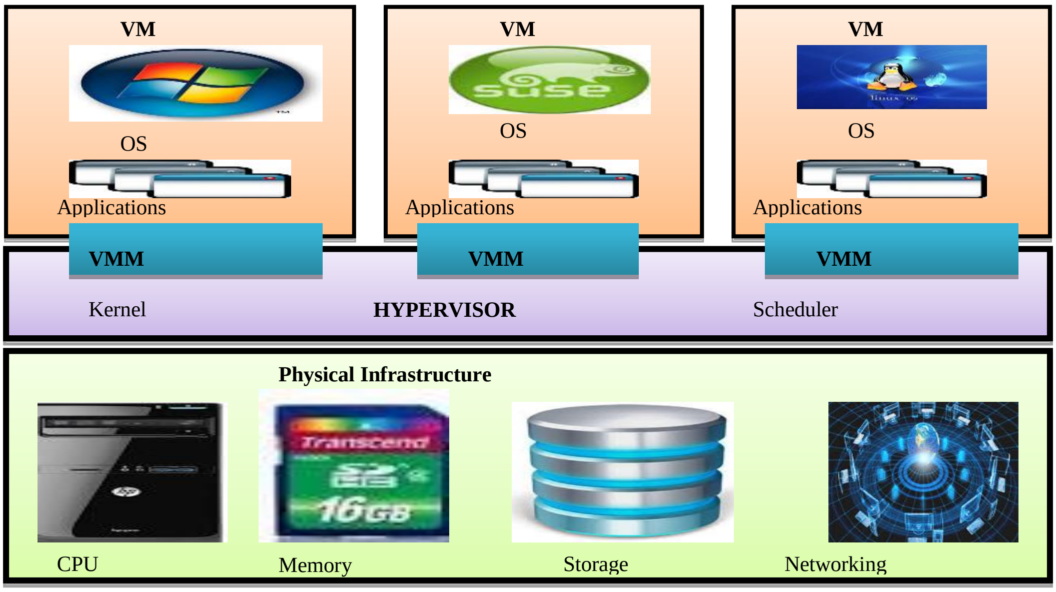


Figure 9: Virtual machine Environment

In latest years, we observe a lot of improvements in cloud computing as well as in virtualization. With a rise in the popularity of cloud, malicious hackers are also finding the ways to get sensitive information resided in cloud by manipulating safeguards. The user have no clues about storage location of information [27, 28].Table 9 shows the

possible attacks for which we need to take some steps to provide secure virtualization in cloud computing.

Table 8: common virtualization attacks

Attack	**Description**
Resource Attacks	In this kind of attacks cloud providers are targeted via manipulating the available resources.
Denial of Service	It has the ability to shut down the hypervisor and get the control of VMs underneath the hypervisor.
VM Jumping	In case of any security notch in hypervisor, active user of one VM can skip to other and gain its access.
Data Attacks	These includes unauthorized modification of confidential data of cloud providers and users at nodes
Host Traffic Interception	Vulnerabilities in the hypervisor allow tracking the system calls, memory and disk activities.

2.5 Orchestration

Cloud computing automatically orchestrates utilities from different sources to design a transparent service flow to its users; it also offers a set of templates on demand, which could be composed by services inside the computing cloud. [14, 30]

2.6 Web Services and SOA

Open-source software and merchandise hardware are major drivers of cloud computing. Linux has become a prime building block of largest cloud environments. Cloud computing services are generally bared web services managed in a Service Oriented Architecture.

2.7 Existing solutions to security of Cloud Computing

To provide a safeguard against security and privacy threats to cloud computing, various solutions are suggested [70].

Table 9: Existing Solution to Cloud Computing Security Issues

S.No.	Solution	Description	Advantages	Limitations
1	MIRAGE Image Management System [25]	MIRAGE is an image library that where disk images are stored in form of indexes associated with the content of file system structure of customers. It addresses the security risks concerned with the sharing of VM images.	VM image security risks are treated in a very systematic and efficient way.	Extensive performance overheads both in time and space Filters mitigate the risk but not entirely
2	Client Based Privacy Manager	It is concerned to meet all the requirements came from privacy legalization.	Decrease the risk of data leakage when it is processed in cloud.	Needs trustworthy cooperation of the service provider.
3	Transparent Cloud Protection System	TCPS is purely a host side scheme that maintains transparency of guest machines.	Custom-made solution that protect guest VMs from attacks and keeps record of the integrity of cloud components.	Only trace attacks guest machine attacks
4	Secured and efficient access to outsourced	It provides access to large scaled data outsourcing in a secure and efficient	Handles user revocation without affecting	Not a generic solution.

	data	manner.	service provider.	

In the present scenario, the most demanding aspect of any organization is its physical security [13, 14]. To enhance the physical security, there is a need to closely monitor the traffic between VMs, enforce well configured gateways when VM is reconfigured, migrated or added and use third-party validation checks in accordance with security standards [22, 24, 25].

2.8 Virtual Images

The formation of an image is described in terms of three layers named as Core, Base and Image. The Core is a mini operational layer demanding a minimum set of software requirements to run images on VMM. Base is the top layer of core that demand some additional software in order to satisfy requirements of Virtual Appliance where virtual appliance is a subclass of image and Image is also the top layer accommodate user-defined software.

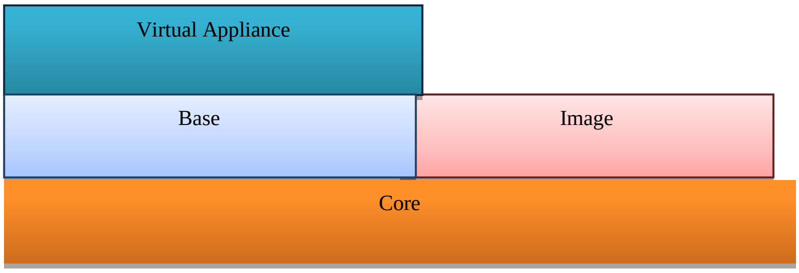


Figure 10: Generation layers of an Image

The core layer is shared between images but base can only be shared by the virtual appliances. To speed up the formation process of images, core and base both layers are cached in logical Volume Manager (LVM|), first time, they are generated. Images are cached and tagged in such a manner that if any image call matches with the cached image, the requested image is returned promptly. If an image has identical configuration parameter which already exist in cache, the image is returned and a time-out value is set on each cache entry to restrict its sessional validity. In case of time-out, same cache entry is regenerated. The cache also works as image repository from where images can be browsed and downloaded immediately.

❖ Content- based transfer of Virtual Images

Content-based transfer is a mechanism of transferring VM images from the source to destined host machine. It yields the benefit of insight to structure of image contents to fetch only communal data, need to be transmitted. Most of the file systems are coordinated on a fixed boundary. Basically, Content Addressable Storage (CAS) exploits identity in order to decrease storage load of images.

Chapter-3

SCOPE OF THE STUDY

Virtual Machine images enclose each application of the cloud and secure management of VM images is one of the issues concerned with security of cloud computing. Cloud focus on three resources associated with VM images as- collection of VM images, Servers on which virtual images are running and the repository to store persistent user data. VM images are designed for distributive environments, can be shared by many unknown users. Thus the integrity and security of VM images is the base for complete security of clouds, but sharing of virtual images is still an unpinning issue. Sharing of virtual images come out with many security threats to its owner, consumer and administrator.

From the perspective of owner of an image, he is concerned about the confidentiality of his original image in the repository. The consumer who retrieves the images from repository and run them is concerned about the safety of image. The administrator is concerned about the integrity of images as he is assumed to be responsible for potential damage caused by malicious and illegal content in the repository.

The cloud users can hire the computational time and the storage space of large data centers via IaaS. For leasing the computational time, IaaS allow the users to deploy virtual machine environment on the resources of the data center. The increasing popularity of IaaS has created many new problems and challenges in the managing the physical resources of large data centers as well as in managing the growing collection of VM images. This study refined the various factors that will affect the efficient management of virtual images using MIRAGE image library to deploy the environment of virtualization at large data centers. It reveals the impact of cost and security of images of organizations.

Mirage is a centralized image library, easily injectable into hypervisor platforms already available to the customers in their data centers.

Few principal inferences of this study are delimited here.

❖ Findings of this study indicate that the study is completely informative and useful for service providers as well as for the organizations obliged in cloud technologies.

- Findings of this study help in understanding factors reflecting benefits and threats of cloud computing and its impact on general public and business organizations.

- It will be worthwhile for the providers and organizations to take a note of the results obtained and their analysis before going to actual implementation of cloud computing technology.

Chapter-4

OBJECTIVES OF THE STUDY

Cloud computing is defined as Internet-based model of computing which provides the simultaneous scalable and elastic IT resources to concurrent users. The user has no need to own and manage his own IT resources as it provides necessary amount of virtualized IT resources through Internet. Cloud computing is quickly becoming the center of attention for its various strengths such as cost saving of IT and flexible use of resources. John McCarthy is known as the founder of cloud computing who recommended that in the coming times calculations would be borne through the public utilities.

MIRAGE is a library to manage VM images for virtual environment. As VM images grow, the risk and cost of its maintenance also increases. There is a strong need to reduce the translation cost of mirage image but cost reduction can be achieved only by knowing the process to manage the resources via VM images. Reduction in the cost of translation will increase the running cost of the virtual systems. I will work on reducing the translation cost, hence improving the running cost of the system. My objectives behind this study are as follows:

- To implement and study MIRAGE image library
- To improve cost of MIRAGE translations by improving translation algorithm
- To enhance VM image library and speed of VM deployment

Chapter-5

RESEARCH METHODOLOGY

Mirage provides image transformation filters, checkin and checkout as interfaces to transfer disk image to and fro Mirage system. In CAS technique, each item is identified in store by a cryptographically secured digest of its content and the semantics of CAS are write-once. The process of modified item creates new item for same image which exploits the write-once rule of CAS. Image indexer converts in both directions by a standard hypervisor. Catalog manager keep Meta data about images in a relational database including CAS identifier, state of image, creation time, parent identifier, image version number etc.

The architecture of content based transfer of disk image to virtual image in Mirage library is shown in Figure 11 as:

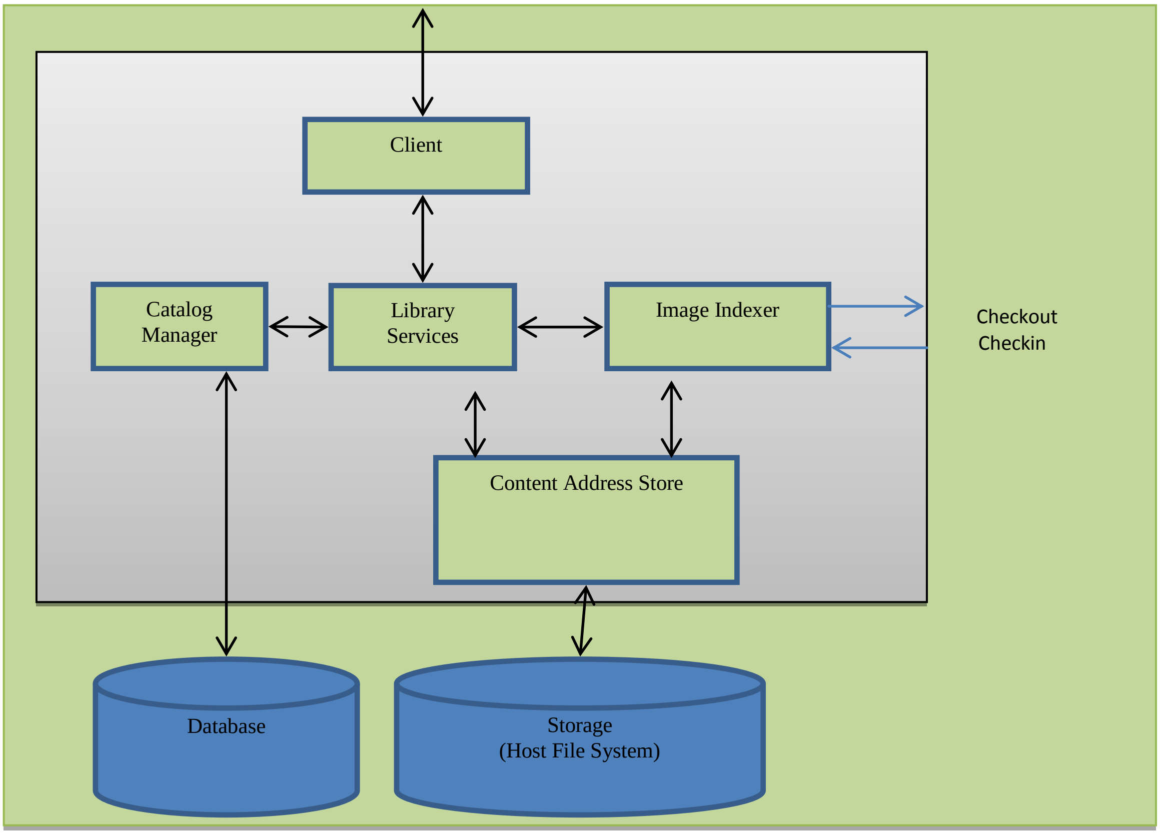


Figure11: CAS Architecture

The methodology that I choose to achieve my objectives is consisting of five steps.

- Set up existing Mirage image library
- Improve binary translation algorithm and increase its efficiency
- Integrate improved translation algorithm into mirage library
- Compare existing mirage with enhanced mirage library system
- Present the result analysis

5.1 Inputs:

Different disk images are saved in *.img format which are managed by KVM. A sample of 10 virtual machine images is considered during this study and the size of items varies in range from 1GB to 10 GB. In this study, we write the Java Code in Eclipse and use KVM and VMware workstation as tools where a sample of 10 virtual images is tested ranging in size from 1GB to 10 GB and our process of managing VM images in the cloud repository reduces the translation cost and as a development cost of the system. The mean costs obtained from existing structure-aware CAS Mirage library and enhanced Mirage library is shown in table 10 and table 11.A paired t-test is used to compare the existing system to enhanced system.

5.2 Hypothesis

H0 : There is a significant improvement in the translation cost and development cost of VM images in the improved Structured Aware CAS.

5.3 Step-wise Diagrammatic Representation

To achieve the predefined objectives of this study, we need to follow some steps. Figure 12 represent the step-wise diagrammatic representation of the proposed system.

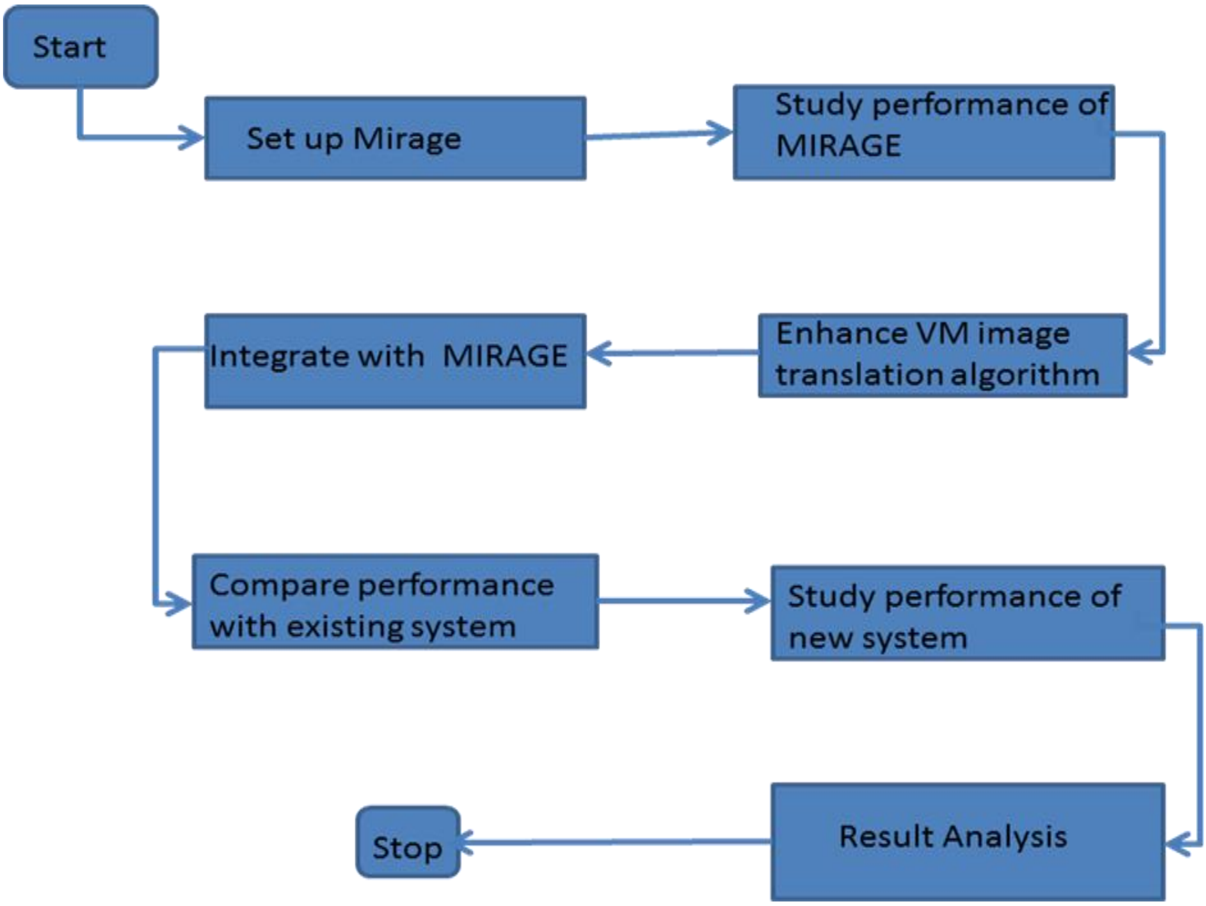

Start
Set up Mirage
Study performance of MIRAGE
Enhance VM image translation algorithm
Integrate with MIRAGE
Compare performance with existing system
Study performance of new system
Result Analysis
Stop

Figure 12: Diagrammatic representation of Proposed System

5.4 Expected outcomes

Improving performance of the Virtual Machine Management System will decrease the cost of managing virtual machines. This will yield the following benefits:

- Reduced VM management cost
- Effective VM systems
- Lesser setup cost and time.

Chapter-6

IMPLEMENTATION AND RESULT ANALYSIS

Indexed images are stored in CAS by Mirage which is variably sized in form of large volumes. In actual these volumes are the sparse files. On-disk images are stored also indexed in form of a directory structured tree whose leaves hold location of items. As the indexed images are purely structured, follows a hierarchy. Image manifests referencing the disk manifests, disk manifest references partition manifests which further references data files contains file-content items.

The format of a Structure aware CAS is shown in figure 13

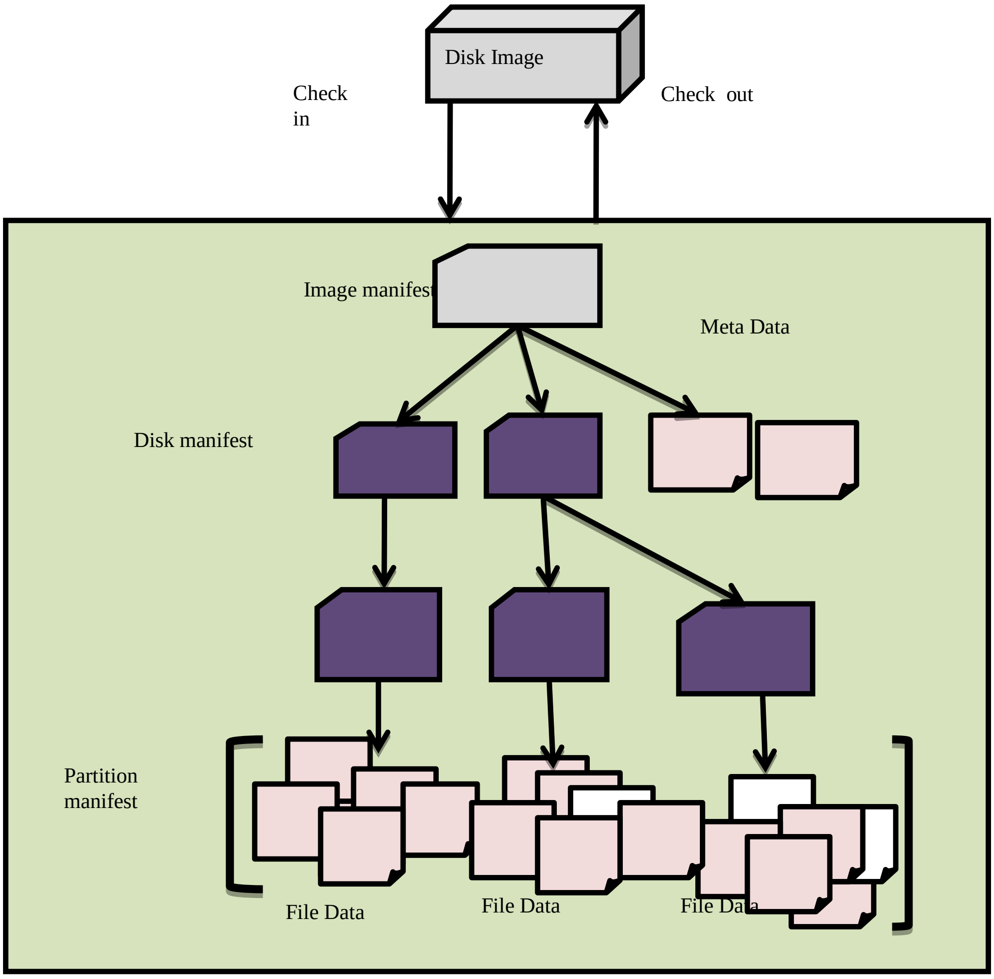


Figure 13: Structure Aware CAS

When a file data is stored in CAS, it also receives file-content items by the file manifest. If a new item is added that references other item in CAS, CAS creates a location table to get references of stored items. Whenever a user fetched an item from CAS, it reads the item's lookup table and cache the location of all referenced items cached in the memory. This modified CAS associates lookup tables with raw items instead of with their content volumes. The advantage of this alteration is that it reduces the translation cost as compare to the existing optimization method of CAS.

6.1 Tools

Implementation of Structure-aware CAS uses Eclipse Juno for Java developers as a good pact between adaptability and accessibility.

❖ Kernel-Based Virtual Machine (KVM)

KVM is a Linux kernel module developed by RedHat as a free, open-source technology. It provides a set of APIs to accelerate virtualization. In KVM, I/O part is handled by QEMU and used to create and deploy images. KVM is also used as a hypervisor. The simple way to create a virtual disk file is as:

Qemu-img create –f qcow2 vdisk.img 10G

Kvm is also named as "qemu-system-x86_64 on some distributions.

❖ JAVA

Java is the most popular programming language used to create web applications and new platforms. It was released by Sun Microsystems in 1995. Java is a platform independent, object oriented, secure and reliable language.

❖ Libraries

KVM API Support: The kvm API is a set of input/output controls (ioctls) that are issued to control various virtual machine specific input/output operations which do not work with regular system calls. The ioctls has three classes –system ioctls is a set of global attributes used to create VMs. VM ioctls are set of attributes used to create virtual cpus. Vcpu ioctls are set of attributes that control the operations of a single vcpu.

Libvirt: Libvirt is an open source API tool used for managing platform virtualization. It is used to manage kvm, Xen, VMware, QEMU and many more virtualization. It is used in the orchestration layer of hypervisors to develop cloud-based solutions.

6.2 Implementation

The implementation process contains three phases.

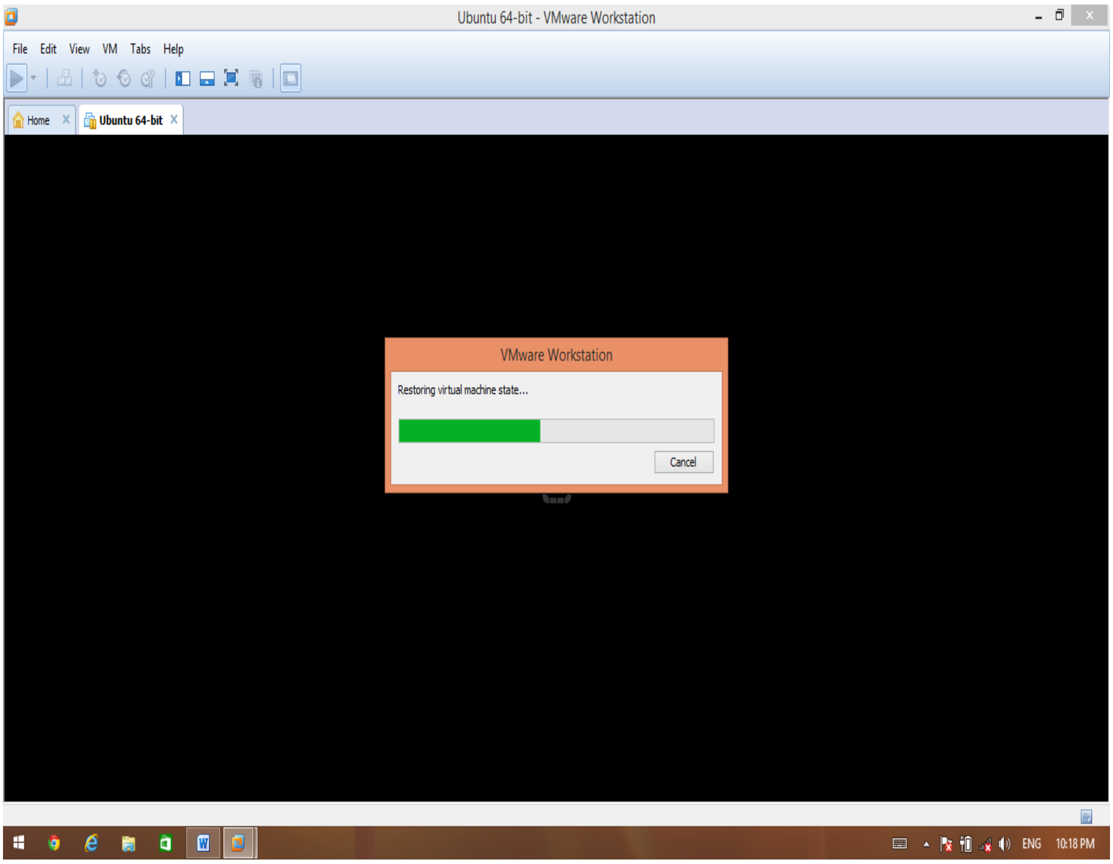
❖ **Implementation of KVM hypervisor:** The minimum hardware requirement to install kvm is that the processor and OS should be 64bit, 6GB HDD and 2GB of RAM. KVM is installed as a normal user with the following command:

Sudo yum install qemu-kvm virt-install virt-manager

To check whether libvirtd service is started, type command: sudo service libvirtd start

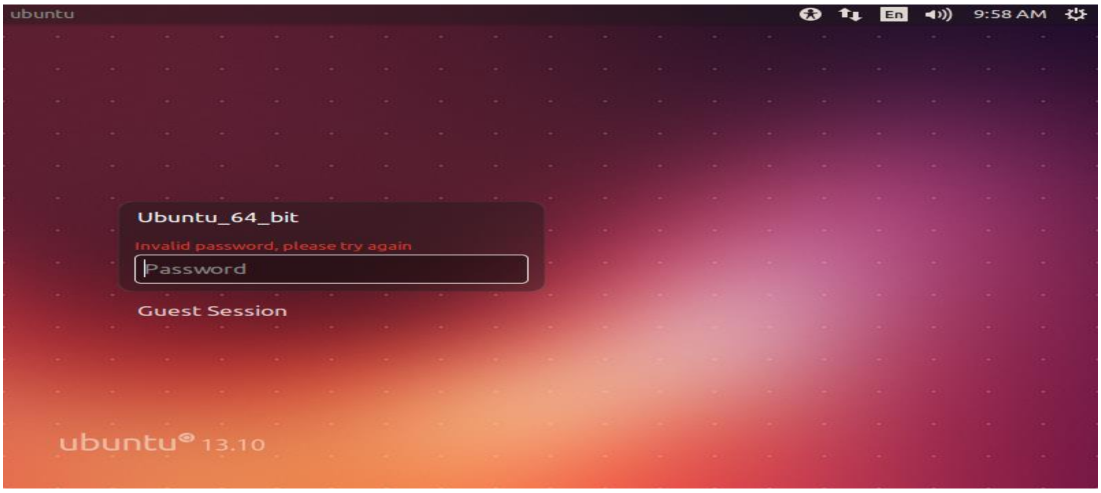
Now run virtual manager as: virt-manager

❖ **Implementation of Virtual Image Manager**



Restoring virtual machine state...

Figure 14: Ubuntu 64-bit VMware workstation startup



Invalid password, please try again

Figure 15: image capturing

❖ Improve image translation algorithm

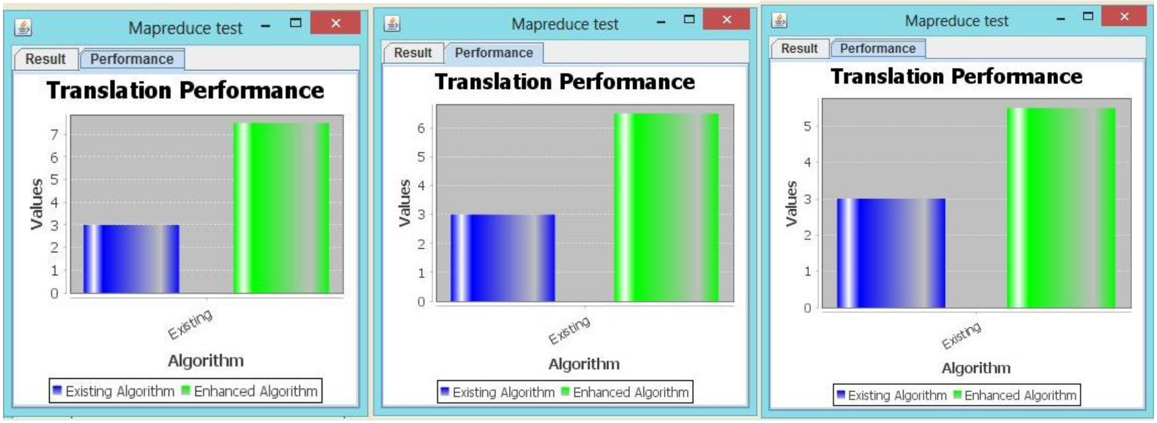
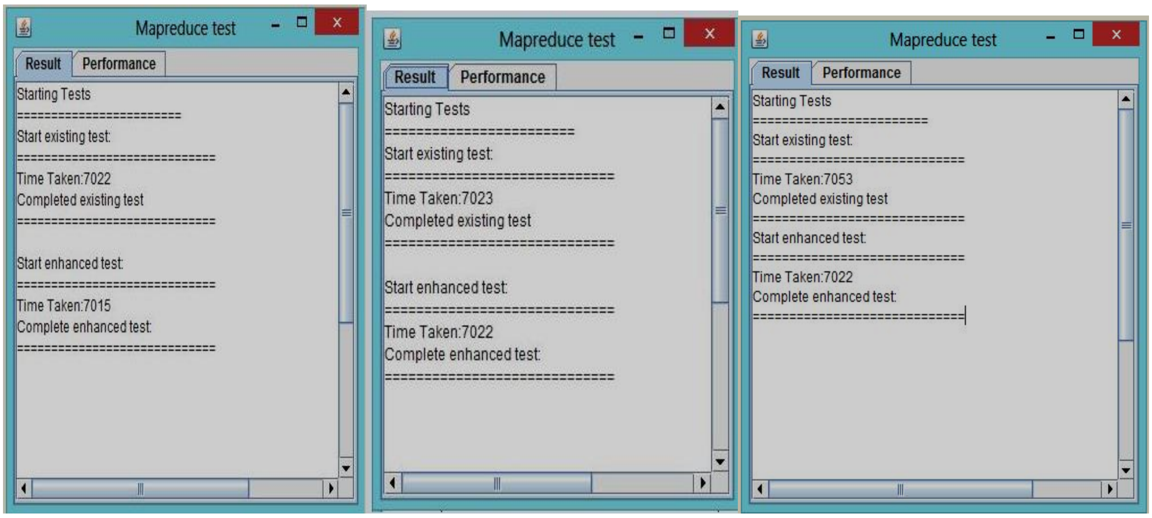


Figure 16: Translation performance Tests



```
Starting Tests
=======================
Start existing test:
============================
Time Taken:7022
Completed existing test
============================

Start enhanced test:
============================
Time Taken:7015
Complete enhanced test:
============================
```

```
Starting Tests
=======================
Start existing test:
============================
Time Taken:7023
Completed existing test
============================

Start enhanced test:
============================
Time Taken:7022
Complete enhanced test:
============================
```

```
Starting Tests
=======================
Start existing test:
============================
Time Taken:7053
Completed existing test
============================
Start enhanced test:
============================
Time Taken:7022
Complete enhanced test:
============================
```

Figure 17: Recorded Test values

6.3 Result Analysis and Interpretation

For running and testing the existing and enhanced algorithms, each images test is performed on different image sizes ranging from1 GB to 10 GB. For each test, Java application calls libvirt API to create, deploy and index that image. Code in KVM starts indexing on getting a new image description from request.

The results show that my implementation achieves an expected cost which closely follows the hypothesis H0.

- **Translation Cost**

The average translation cost is computed by grouping the virtual images on the basis of their sizes. The images are grouped by analyzing their resultant values where there were no significant changes in the translation cost.

Here, we apply paired t-test to compare the performance of existing Mirage image system with new system after integrating Mirage with enhanced translation algorithm of structure-aware CAS.

Table 10: Mean Translation costs of existing and enhanced Mirage library

Image Group by size(GB)	Mean Translation Cost of Existing System(mins)	Mean Translation cost of Improved System(mins)
1-3	12.3	11.8
4-7	22.3	20.8
8-10	27.7	26.3

The value of t is -7.84. The value of p is 2.6. The result is significant at p <= 0.05 level of significance. Hence, we accept the NULL hypothesis and can say that the translation cost of the mirage library is improved from and the existing system is improved.

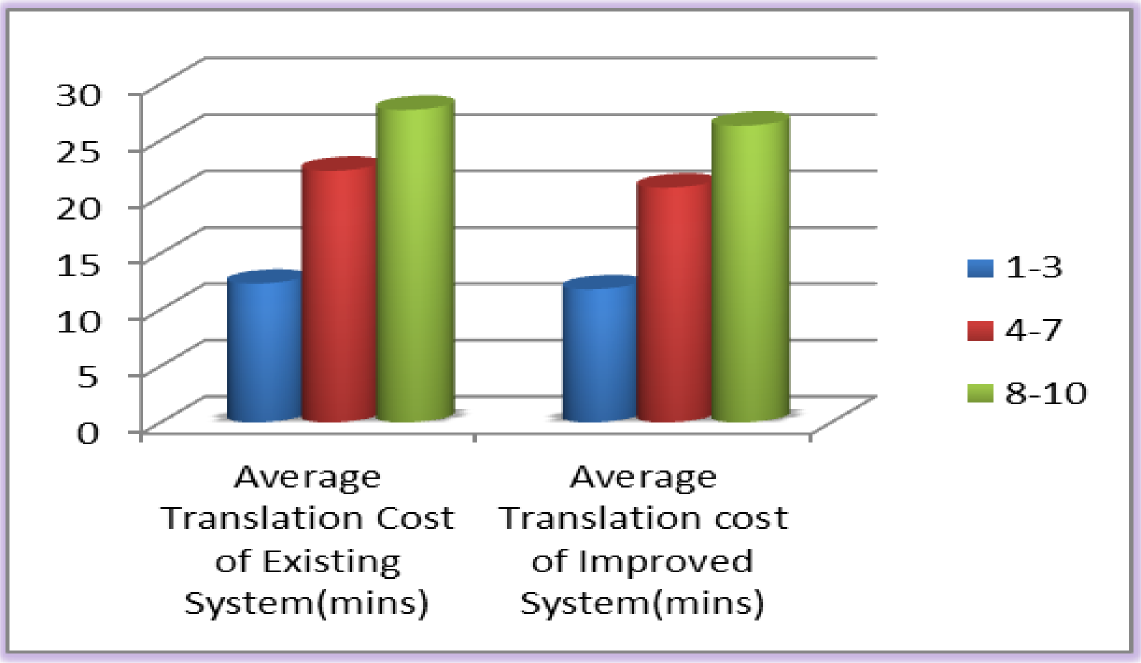


Figure 18: Comparative analysis of translation costs of the system

❖ **Development Cost**

The average development cost is measured by grouping the virtual images on the basis of their sizes. The images are grouped by analyzing their resultant values where there were no significant changes in the development cost. Here, we apply paired t-test to compare the existing and computed values.

Table 11: Mean development cost of existing and enhanced Mirage library

Image Group by size(GB)	Average Development Cost of Existing System(mins)	Average Development cost of Improved System(mins)
1-3	27.9	26.4
4-7	46.5	44.4
8-10	51.3	49.1

The value of t is -18.02. The value of p is less than 0.00001. The result is significant at p <= 0.05 level of significance. Hence, we accept the NULL hypothesis and can say that the development cost of the mirage library is improved from and the existing system is improved.

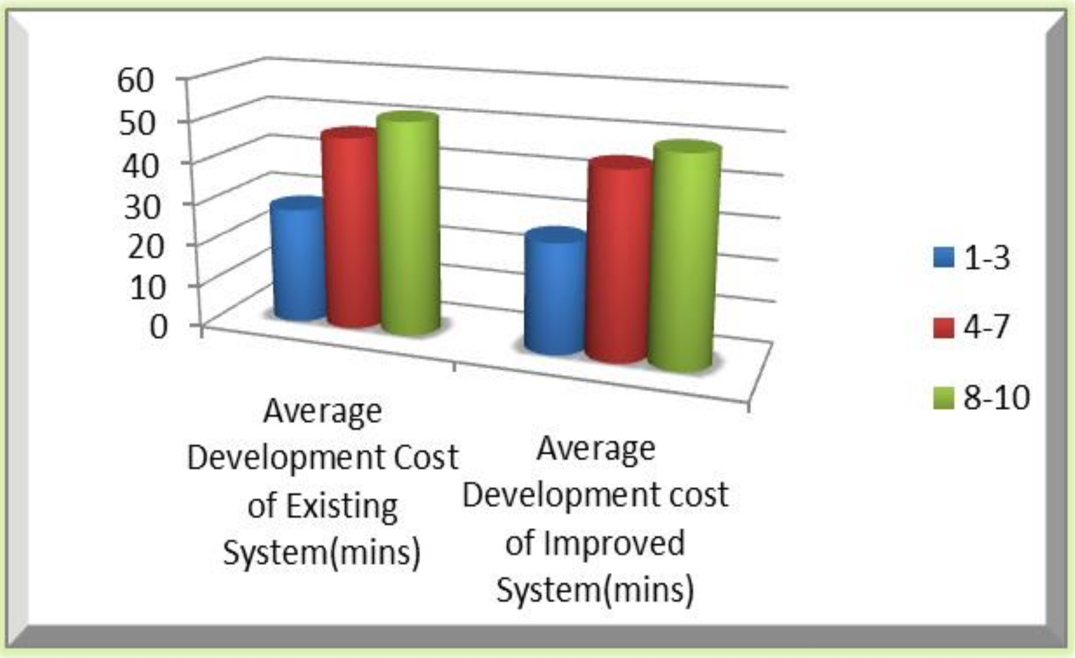


Figure 19: comparative analysis of development cost of the system

Both the figures represent a significant improvement in enhanced system as compared with the existing system and prove that the settled objectives are achieved successfully.

Chapter-7

Conclusion and Future Scope

7.1 Conclusion

The security and integrity of virtual images is the base for complete security of the cloud since they are designed in a distributive manner that can be shared by different and unknown users. MIRAGE is an image library typically used in IaaS clouds that addresses the security issues related with VM images which influence the image publishers, image retrievers and the administrators of the cloud repository. The computational time consumed in deploying the images is a key determinant of the virtual image management in cloud computing which are reduced by creating virtual machine images in raw form through QEMU/KVM. Structure-Aware CAS algorithm is used to select the indexed images from raw content which reduces the translation cost involved in transferring the disk images into and from the Mirage library. The mean translation cost lies in group size 1-3 GB is reduced to 11.8 from 12.3, for 4.7GB images it is reduced to 20.8 from 22.7 and for images lies in size 8-10 GB it reduced to 22.7 from existing cost 26.3. It shows more improvement for images of size 8 to 10 GB. In case of development cost our algorithm shows more improved results for images of size 8-10GB where development cost is reduced to 49.1 from 51.3. Our translation algorithm with raw indexed images shows the improvements at 5% level of significance.

7.2 Future Work

In the computational systems, the amount of resources to be used to complete a process is a prime factor, used to measure the efficiency and effectiveness of that system. To maximize the efficiency, it is necessary to minimize the resource usage described in terms of time and space. Now-a-days, Cloud computing has become an integral part of this rapidly growing computational world where costs involved in development and deployment of such systems will play a major role in its growth and popularity. Hence, there is always a scope to improve the computational costs to make the technology more effective and useful for society. We hope that more improved cost can be achieved by implementing this new scheme of Structure-Aware CAS on the actual cloud environment.

REFERENCES

[1] Abhivan Pandey, Akash Pandey, Ankit Tondon, Brajesh Kr. Maurya, Upender Kushwaha, 2010,Cloud Computing: Exploring the Scope

[2] Aman B, Yogesh B.D., "Securing cloud for DDoS attacks using intrusion Z detection system in VM", ICCSN, pp-260-264, 2010

[3] Amy Shuen, "Web 2.0: A strategy Guide", O'Reilly, ISBN – 13:978-596529963

[4] Antero T, "Mashware: the future of web applications", Technical Report, 2009, DOI: 10.1145/1878537.1878703

[5] Arutyunov V.V., Cloud Computing: Its History of Development, Modern State, and Future Considerations, Seria 1, 2012,Vol. 39, No. 3, pp. 173-178.

[6] B R Kandukuri et. Al., "Cloud Security issues", IEEE, 2009, pp. 517-520

[7] B.P. Rimal, Choi Eunmi, I. Lumb, "A taxonomy and Survey of cloud computing systems", pp44-51, Aug, 2009

[8] Balding C. (2008). Assessing the Security Benefits of Cloud Computing.

[9] Bhaskar Prasad Rimal, Admela Jukan, Dimitrios Katsaros, Yves Goeleven, Architectural requirements for cloud computing systems: An Enterprise Cloud Approach , 2011, pp. 3-26

[10] C Lo, C Huang, J Ku, "A cooperative intrusion detection system framework for cloud computing networks", ICPPW, 2010, ISBN: 978-0-7695-4157-0

[11] C Wang, K Ren, W L J Li, "Towards publicly Auditable secure cloud storage services" IEEE, pp. 19-24, vol. 24, 2010

[12] C Wang, Q Wang, K ren, W Lou, "Ensuring Data Storage Security in cloud computing" IWQoS, 2009, pp. 13-15 ISBN: 978-1-4244-3875-4

[13] C.N.Hofer, G. Karagiannis, Cloud computing services: taxonomy and comparison, Netherland 2011, pp. 81-94

[14] C.W.Hsu, C.W.Wang, Shiuhpyng Shieh, Reliability and Security of Large Scale Data Storage in Cloud Computing, 2010

[15] D Chatteddu, G Hogben, “Cloud computing: Benefits, Risks and Recommendations for Information Security”, ENISA, 2009

[16] David C, “A short introduction to cloud platforms”

[17] Dr Christof Weinhardt, Dr Benjamin Blau, Dr Josen StoBer, Cloud Computing – A Classification, Business Models and Research Directions, DOI 10.1007/s12599-009-0071-2

[18] Dr. Gunter Muller, Dr. Norboru Sonehara, Dr Isao Echizen, Dr Sven Wohlgemuth, Sustainable cloud computing, 2011,10.1007/s12599-011-0159-3

[19] Eugene Gorelik, 2013, Cloud Computing Models, working paper

[20] F.D.Keukelaere, S Bhola, M Steiner, S Chari, S Yoshihama, “Smash: secure component model model cross-domain mashups on unmodified browsers”, ACM,2008 ISBN: 978-1-60558,085-2

[21] Flavio Lombardi and R.D. Pietro, “ Secure Virtualization for Cloud Computing”, JNCA, vol. 34, issue 4, pp. 1113-1122, 2011

[22] Frederico Durao, Jose Fernando S. Varvalho, Anderson Fonseka, Vinicius Cardoso Gracia, “A Systematic Review on Cloud Computing”, Brazil 2014

[23] G.V Hulme, “NIST formalizes cloud computing definition, issues security and privacy guidance”, 2011

[24] Gaoyun Chen, Jun Lu, jian Huang and Zexu Wu, “SaaS- The Mobile Agent Based Service for Cloud Computing in Internet Environment”, IEEE, pp.- 2935-2939, 2010,ISBN: 978-1-4244-5958-2

[25] Glenn Ammons, Vasanth Bala, Todd Mummert, Darrell Reimer, X Zhang, “Virtual machine images as structured data: the Mirage image library”,2011,

[26] Glenn Ammons, Vasanth Bala, Todd Mummert, Darrell Reimer, Xiaolan Zhang, Virtua; machine images as structured data: the Mirage image library, IBM Research(2011)

[27] Hanqian Wu et. Al., "Network Security for Virtual Machines in Cloud Computing", Int. conference on Computer Science and Convergence Information technology, pp 18-21, 2010, ISBN: 978-1-4244-8567-3

[28] Harold C. Lin, Shivnath Babu, Jeffery S. Chase, Sujay S. Parekh, " Automated control in cloud computing: Opportunities and Challenges", pp. 13-18, 2009,ISBN: 978-1-60558-585-7

[29] Hyun-Suk Y, Yvette E. Gelogo, Kyung Jung Kim. Securing Data Storage in Cloud Computing, June 2012

[30] J Marler, " Securing the Cloud: Addressing cloud computing security concerns with private cloud", Rackspace Knowledge Centre, 2011

[31] J Sedayao, S. Su ei. All," A simple technique for securing data at Rest", Lecture notes in computer science, pp. 553-558, 2009

[32] J Wei, X Zhang, G Ammons, Vasanth Bala, P Ning, "managing Security of virtual machine images in a cloud environment", CCSW 2009, ACM workshop on Cloud Computing Security 2009

[33] J Weinman, "The Future of Cloud Computing", IEEE Technology Time Machine Symposium, 2011, DOI: 10.1109/TTM.2011.6005157

[34] James Governer, "web 2.0 architectures: what entrepreneurs and information architects need to know", 2009, O'Reilly, ISBN – 13:978-596514433

[35] Jansen W.A., "Cloud Hooks: Security and Privacy Issues in Cloud Computing", IEEE 2011 HICSS, pp1, 4-7, 2011

[36] Jenni Susan Reuben, "A survey on Virtual Machine Security", Seminar of Network Security, Helsinki University of Technology, 2007

[37] Jessika T, "Connecting Data Centres over public networks", IPEXPO.ONLINE, 2011

[38] Jesus Carretero, Javier Gracia Blas, Introduction to cloud computing: Platforms and Solutions, 2014, DOI 10.1007/s10586-014-0352-5

[39] Jinesh Varia, 2010, Architecting for the cloud: best practices

[40] Jinesh Varia, 2010, Eight Fundamental truths about cloud

[41] Jon Marler, “Securing the Cloud: Addressing Cloud Computing Security Concerns with Private Cloud”, Rackspace Knowledge Centre, 2011, Article id: 1638

[42] Julisch K, Hall M., “Security and control in cloud”, Information Security Journal, vol. 19, pp. 299-309, 2010

[43] K R jayaram et. Al.,” An Emperical Analysis of Similarity in Virtual Machine”, web.cse.ohio-state.edu/~chunyi/pubs/ middleware11-similarity.pdf

[44] Kapil Bakshi, 2009, K: Cisco cloud computing data center strategy, architecture and solution. Points of view white paper for U.S. Public Sector

[45] L M Kaufman, “Data security in the world of cloud computing”, IEEE, pp. 61-64, 2009, ISSN: 1540-7993

[46] L Zhang and Q. Zhou, “CCOA: cloud computing open architecture”, ICWS, 2009, pp. 607-616

[47] L.Wang, Gregor Laszewski, Marcel Kunze, Jie Tao, “Cloud Computing: A Perspective Study”, New Generation Computing- Advances of Distributed Information Processing, pp. 137-146, vol. 28, no. 2, 2008

[48] L.Wang, J Tao, Kunze M. Castellanos A. C., Kramer D, Karl W. ,”Scientific cloud computing” Early definition and experience”, 10th IEEE Int. Conference, pp. 825-830, 2008

[49] Lamia Youseff, Maria Butrico, Dila Da Silva, Toward a Unified Ontology of Cloud Computing, USA,2009

[50] Lizahe WANG, Greogor Von LASZEWSKI, Andrew YOUNGE, XI HE, Cloud Computing: A perspective Study, New Generation Computing, 2010, pp. 137-146

[51] Luis M. Vaquero, Luis Redero- Merino, Caniel Moran, “Locking the Sky: a survey on IaaS cloud security”, Springer-Verlag 2010, DOI 10.1007/s00607-010-0140-x

[52] M . Rajendra Prasad, Cloud computing: Research Issues and Implications, 2013, DOI: 10.11591/closer.v2i2.1963, arXiv: 1005.1904

[53] M Armbrust, A Fox, R Griffith, A. D. Joseph, R Katz, A Konwinski, G Lee, D Petterson, “A view of cloud computing”, ACO, vol. 53, 2010

[54] M Kretzchmar, S Hangik, “Security management interoperability challenges for collaborative clouds”, SVM, 2010, pp. 43-49, ISBN: 1-4244-9181-0

[55] M.D. Dikaiakos, D Katsaros, P Mehra, G Pallis, A Vakali, “Cloud Computing: Distributed Internet computing for IT and scientific research”, IEEE, vol. 13, pp. 10-13, 2009

[56] M.Mulazzani, S Schrittwieser, M Leithner et. All “Dark clouds on the horizon”, USENIX, 2011

[57] M.T. Khorshed, A.B.M Shawket Ali, Saleh A. Wasimi, “Trust issues that create threats for cyber attacks in cloud computing”, IEEE, pp. 900-905, 2011

[58] Madnick S, 1969, Time-Sharing Systems: Virtual machine concept vs conventional approach. J. Modren Data Sys. 2:34-36

[59] Mark Stieninger, Dietmar Nedbal, Characteristics of cloud computing in the business context: A systematic literature review, March 2014, pp. 59-68

[60] McAfee, Whitepaper, “Database Security in Virtualization and Cloud Computing Environment: The three key Technology Challenges in protecting sensitive data in modern IT architectures”, 2015

[61] Mehta HK, Kanungo P, Chandwani M, 2011, Reminiscences on the history of time sharing.

[62] Meiko Jensen et. al, “On technical security issues in cloud computing”, pp. 109-116, CLOUD-II, 2009

[63] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, “On technical security issues in cloud computing”, pp. 109-116, CLOUD-II, 2009

[64] Mell P, Grance T, 2009, The NIST definition of cloud computing(v15). Tech Report, NIST

[65] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz,Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia ,Above the Clouds: A Berkeley View of Cloud Computing. y http://radlab.cs.berkeley.edu

[66] Neal Leavit, "Is cloud computing really ready for prime time?", IEEE, pp. 15-20, 2009

[67] Neal Leavit, "Is cloud computing really ready for prime time?", IEEE, pp. 15-20, 2009

[68] Osama Harfoushi, Bader Alfawwaz, Nazeeh, Ruba Obiedat, Abu Faraj, H. Faris, Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review, Communication and Network, 2014,6, 15-21

[69] Peter Mell, Timothy Grance, "The NIST definition of cloud computing", Jan, 2011

[70] Qi Zhang, L Cheng, R Boutaba, "Cloud computing: State of the art and research chellenges", Journal of Internet services and applications, pp. 7-18, 2010

[71] R A Vasudevan, S Sanyal, "A Novel Multipath approach to security in MANETs", CODEC'04

[72] R Minnear, "Latency: the Achilles heel of cloud computing", Cloud Expo, 2011

[73] R. Maggiani, "Cloud computing is changing How we communicate", 2009, IEEE International Conference, IPCC, pp. 1-4, ISBN: 978-1-4244-4357-4

[74] R.Gellman, "Privacy in the clouds: Risks to privacy and confidentiality from cloud computing", the world privacy forum, 2009

[75] S. Bhardwaj, L. Jain, S.Jain, "Cloud computing: A study of Infrastructure as a service", IJEIT, 2(1):60-63, 2010

[76] S. Pearson, "taking account of privacy when designing cloud computing services", CLOUD'09, pp. 44-52, IEEE, 2009, ISBN: 978-1-4244-3713-9

[77] Sam Murugesan, "understanding web 2.0", IEEE Computer Society, pp. 34-41, 2007

[78] Sangeeta Sen, Rituparna Chaki, “Handlinh write lock assignment in cloud computing environment”, Communications in Computer and Information Science, vol. 245, pp-221-230, 2011

[79] Seny Kamra, Kristen Lauter, “Cryptographic cloud storage”, vol. 245, 2010, DOI: 10.1007/978-3-642-14992-4_13

[80] Shilpashree Srinivasamurthy, David Q. liu, “Survey on Cloud Computing Security”, Department of Computer Science, Indiana University Fort Wayne 2014

[81] Shuai Z, Shufen Z, Xuebin Chen, Xiuzhen H, “Cloud computing research and development treand”, pp. 93-97, China 2010

[82] Tian L.Q, N Y LING, “Evolution of user Behavior Trust in Cloud Computing”, ICCASM 2010, vol 7, pp V7-567, 22-24

[83] Tim M, S Kumaraswamy, S Latif, “Cloud security and privacy: An enterprise edition on risks and compliance”, O’Reilly Media, 2009

[84] Timothy Woodet. al, “The case of enterprise ready Virtual Private clouds”, HotCloud’09, USA, 2009

[85] Vahid Ashktorab, Sayed Reza Taghizadeh, “Security Threats and Countermeasures in Cloud Computing”, IJAIEM 2012, ISSN 2319-4847

[86] W Jansen and T Grance, “NIST guidelines on security and privacy in public cloud computing”, 2011

[87] W Li and X. Pan,” use trust management module to achieve effective security mechanisms in cloud environments”, ICEIE, pp. VI-14, 2010

[88] Yousra Abdul Alsahib S. aladeen, Mohammad Abdur Razzaque, Mazleena Saleh, “A Survey on Security Issue and Its Proposed Solutions in Cloud Environment”, IRICT 2014

[89] Zhou, W., Ning, Zhang, Ammong G, Wang, V Bala, “Always up-to-date: Scalable offline patching of VM images in a compute cloud”, ACSAC 2010, pp 377-386

[90] George Reese (2009), Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, O’Reilly Media Inc.

[91] Golden B.(2008), Virtualization for dummies, Wiley publication Inc.

[92] John Rhoton (2011), Cloud Computing Explained: Implementation Handbook for Enterprises, Recursive Limited

[93] Tim Mather (2009), Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O’Reilly Media Inc.

[94] Rackspace cloud. Http://www.rackspacecloud.com

[95] IBM cloud.http://www.ibm.com/developerworks/websphere/zones/hipods

[96] Tutorials of cloud computing. Http://www.tutorialspoint.com

[97] Microsoft Azure. Http://www.microsoft.com.windowsazure

[98] http://www.gartner.com

[99] http/www.SalesForce.com

[100] Cloud Security Blog at http://cloudsecurity.org/blog/2008/07/21

[101] http://www.davidchappell.com//cloudplatforms

[102] https://www.usenix.org/event/hotcloud11/tech/final_files/Ammons.pdf