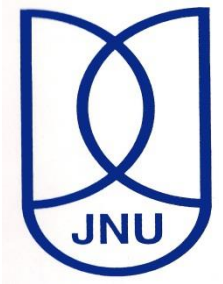
A HEURISTIC FOR SECURITY PRIORITIZED RESOURCE PROVISIONING IN CLOUD COMPUTING

A Dissertation submitted to Jawaharlal Nehru University
in partial fulfilment of the requirements
for the award of the degree of

Master of Technology
in
Computer Science & Technology

Submitted
By
Devki Nandan Jha

Under the Supervision
of
Prof. D. P. Vidyarthi



School of Computer and Systems Sciences
Jawaharlal Nehru University
New Delhi -110067, India
June-2015

जवाहरलाल नेहरु विश्वविद्यालय
SCHOOL OF COMPUTER & SYSTEMS SCIENCES
JAWAHARLAL NEHRU UNIVERSITY
NEW DELHI-110067
INDIA

Certificate

This is to certify that dissertation entitled **"A Heuristic for Security Prioritized Resource Provisioning in Cloud Computing"** is being submitted by **Mr. Devki Nandan Jha** to the **School of Computer & Systems Sciences, Jawaharlal Nehru University, New Delhi-110067, India**, in the partial fulfilment of the requirements for the award of the degree of **"Master of Technology"** in **"Computer Science & Technology"**. This work is carried out by himself in the School of Computer & Systems Sciences under the supervision of **Prof. D. P. Vidyarthi**. The matter personified in the dissertation has not been submitted for the award of any other degree or diploma.

Dean

Prof. C. P. Katti

School of Computer and Systems Sciences
Jawaharlal Nehru University
New Delhi-110067

Dean
School of Computer & Systems Sciences
Jawaharlal Nehru University
New Delhi-110067

Supervisor

18.6.15

Prof. D. P. Vidyarthi

School of Computer and Systems Sciences
Jawaharlal Nehru University
New Delhi-110067

i

जवाहरलाल नेहरु विश्वविद्यालय
SCHOOL OF COMPUTER & SYSTEMS SCIENCES
JAWAHARLAL NEHRU UNIVERSITY
NEW DELHI-110067
INDIA

Declaration

I hereby declare that the dissertation work entitled **"A Heuristic for Security Prioritized Resource Provisioning in Cloud Computing"** in partial fulfilment of the requirements for the award of degree of **"Master of Technology"** in **"Computer Science & Technology"** and submitted to the School of Computer & Systems Sciences, Jawaharlal Nehru University, New Delhi-110067, India is the authentic record of my own work carried out during the time of Master of Technology under the supervision of **Prof. D. P. Vidyarthi**. This dissertation comprises only my own work. This dissertation is less than 14,000 words in length, exclusive tables, figures and references. The matter personified in the dissertation has not been submitted for the award of any other degree or diploma.

Devki Nandan Jha.

Devki Nandan Jha
M.Tech (2013-2015)
School of Computer and Systems Sciences
Jawaharlal Nehru University
New Delhi-110067
India

Dedicated to my parents…

the world is nothing without them.

…∫…

Acknowledgement

Without the generous support of many people this dissertation would not have been possible. I owe my gratitude to all those peoples who have made this dissertation possible. First of all I thank god almighty for giving me enough powers to pursue this first research. I am eternally grateful to my parents who has supported and helped me along the course of this dissertation by encouraging me and providing emotional and moral support that I needed to complete my work.

I acknowledge the contribution of my supervisor, Prof D. P. Vidyarthi, who guided me into the research area of cloud computing and security, discussed about my ideas, challenged me with sharping questions, gave suggestions about the structure of the paper and did proofreading with great patience. I appreciate the insightful suggestions given by him and the strong belief he has put in me. His hard work and passion for research also set an example that I would like to follow.

I thank Prof C. P. Katti, Dean, School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, for the academic support and facilities provided to carry out the research work at center.

It is very important to have a nice social environment outside the lab. My friends (Priyanka, Bindu, Dhirendra, Ashish, Satyam and Gaurav) supported me everytime and never make me feel alone. My sincere gratitude further goes to my seniors including Achal Kaushik, Dr. Shiv Prakash, Pawan K Tiwari, Isha P Tripathi, Bharti Rana, Neetesh Kumar, Sunil Kumar, Jyoti Sahni, Gaurav Baranwal and Atul Tripathi for their invaluable suggestions and support. I would like to thank many more persons whose name is not mentioned here for creating a wonderful social environment.

(**Devki Nandan Jha)**

Abstract

Cloud Computing is a technological shift which presents computing in the form of utility service. It provides an ability to utilize the enormous power of astonishing computing resources without having the burden of buying, setting, securing and maintaining the resources. One only needs to pay for the manipulated resources. There are many benefits of cloud computing on the overall system (individual, small and large enterprises, etc.) like low cost, pooled resource availability, elasticity, easy access, etc.

The increasing dependency on cloud computing also increases the risks associated with it which affects the entire IT industry. Security is one of the most important issues which prevents the complete utilization of cloud services. A number of organizations like CSA (Cloud Security Alliance), OSA (Open Security Alliance), etc. are involved in handling these problems. Resource provisioning is also considered as an important research issue for the researchers. The requirements of users are varying; even for one user different job demands different requirements. The cloud resources are also of varying specifications and so the provisioning of resources to the user's job is monotonous. The problem becomes more complex when the number of requirement is more than one i.e. multiple criteria are there. A plenty of research, all over the world, is going on in this particular field.

Analytical Hierarchy Process (AHP) is one of the techniques that solve the problem when there are many options with multiple criteria and one has to choose the best among them. The criteria are considered to be independent from each other. AHP forms a comparison matrix of criteria on the basis of priority assigned by the user and the normalized eigen value gives the final priority of the criterion. Comparison matrix of options is also constructed based on the criteria, it satisfies or not. The problem with AHP is its complexity which is very high as it works on matrix manipulation. If the number of criteria or options is too many the AHP does not give efficient results. There exist some methods which are used for shortlisting of the options like L_p metric method. The L_p metric method forms an ideal case by collecting the best value of all the parameters and

all the options are compared from this case. The rank is calculated for each options on the basis of comparison. The options with minimum rank i.e. deviation is minimum from the ideal case is considered for the next step i.e. applying AHP. This way the number of options are shortened before applying AHP.

In this dissertation, an AHP-L_p metric based framework is proposed which is used to find the appropriate cloud service provider for each job. The proposed framework takes the advantages of both AHP and L_p method and generates a resource provisioning model which considers qualitative attributes like security along with quantitative attributes such as execution time, cost, availability, etc. The problem of high complexity with AHP is vanished by the use of L_p metric method. The applicability of the proposed model is shown by a case study which justifies the proposal.

Table of Contents

List of Figures

List of Tables

Abbreviations & Acronyms

AHP- Analytical Hierarchical Process

ANP- Analytic Network Process

API- Application Program Interface

BWM- Best Worst Method

CAIQ- Consensus Assessment Initiative Questionnaire

CCBKE- Cloud Computing Background Key Exchange

CI- Consistency Index

CR- Consistency Ratio

CSA- Cloud Security Alliance

CSP- Cloud Service Provider

DoS- Denial of Service

EC2- Elastic Compute Cloud

ENISA- European Network and Information Security Agency

EU- European Union

GFLOPS- Giga FLOating point instructions Per Second

GI- Giga floating point Instructions

GP- Goal Programming

GRA- Grey Relational Analysis

HTTP- Hypertext Transfer Protocol

IaaS- Infrastructure as a Service

IBM- International Business Machines

IDC- International Data Corporation

IKE- Internet Key Exchange

MCDM- Multi Criteria Decision Making

MS- Microsoft

NIST- National Institute of Standards and Technology

OSA- Open Security Alliance

PaaS- Platform as a Service

QoS- Quality of Service

RI- Random Index

S3- Simple Storage Service

SaaS- Software as a Service

SIR- Superiority and Inferiority Ranking

SLA- Service Level Agreement

STAR- Security, Trust and Assurance Registry

VM- Virtual Machine

VPC- Virtual Private CLoud

WPM- Weighted Product Model

XML- EXtensible Markup Language

Chapter 1

INTRODUCTION

Cloud computing, in recent, has emerged as a most promising service providing platform for number of hardware/software services. With the help of the Internet backbone, the Cloud services can be extracted from the Cloud service providers located at various parts of the globe. As the service providers are located at many places, to ensure security of such systems becomes an important issue. The security issue is one of the important issues which is being addressed in this dissertation work.

1.1 Cloud Computing

Cloud computing is a recent shift in the way of technological trend in the direction of computing. Now computing is considered as fifth prominent utility service after water, fuel, electricity and communication. Cloud computing contributes a lot in making computing as a utility. Almost all the Internet savvy citizen uses cloud knowingly or being unaware. Cloud enables its user to focus on various business activities rather than thinking about the technical requirements, specifications and advancements. All these requirements are satisfied by the cloud providers. Cloud takes the advantages of all the previously defined technologies like grid computing, service computing, utility computing, web 2.0, service oriented architecture, distributed computing, virtualization technology, broadband networks, autonomic systems, web as a frameworks, etc. without having good knowledge about any of them.

There is no particular definition of cloud computing, various organizations define cloud computing according to their own interest. Some of the famous definitions are presented here.

NIST (National Institute of Standards and Technology) defines Cloud Computing as "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers,*

storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1].

European Union (EU) defines cloud as "A Cloud is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality of service" [2].

According to Berkeley view of Cloud Computing "Cloud Computing refers to both the applications delivered as services over the Internet and the hardware & systems software in the datacenters that provide those services" [3].

The utility oriented definition of Cloud Computing given by Buyya et.al is "A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers" [4].

The reference model of Cloud, given by NIST is presented in fig 1.1. According to the NIST, cloud computing is comprised of four deployment models, three service models and five essential characteristics as shown in the fig 1.1.

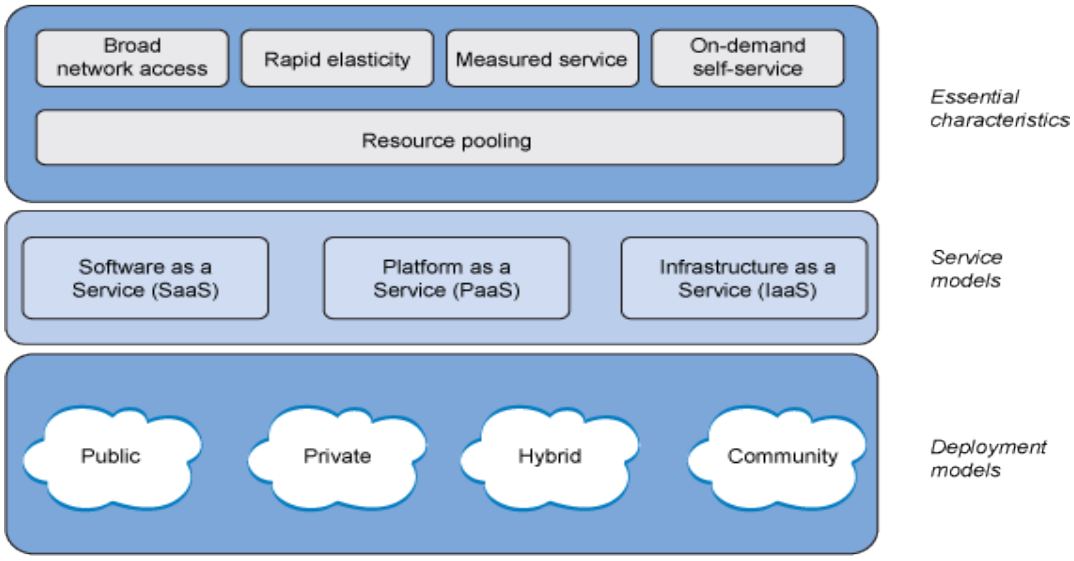


Fig 1.1: NIST Cloud Computing Reference Model [1]

1.2 Characteristics of Cloud Computing

There are some distinct characteristics of cloud computing which makes it different from other types of computing. The five essential characteristics, defined by NIST, are as follows [1].

1. On-demand self-service,
2. Broad network access,
3. Resource pooling,
4. Rapid elasticity and
5. Measured service

Along with these, two additional characteristics are usually defined for cloud computing [2] as given below.

6. Virtualization and
7. Multi-tenancy

1.2.1 On Demand Self Service

Cloud computing enables the cloud users to perceive the requested resources automatically in a flexible manner without any interaction with the third party. The user can request for the resources at run-time as per their requirement. It is closely associated with underlying architecture, resource availability and elasticity property.

1.2.2 Broad Network Access

The resources, hosted by the cloud network, can be retrieved by various types of devices viz. laptops, personal computers, smartphones, tablets, etc. The devices are distributed anywhere in the network and access the resources being unaware about the platform supporting the resources. The resources are accessed through internet using standard protocols such as HTTP, XML, Java, etc.

1.2.3 Resource Pooling

The cloud provider can create a virtual infinite pool of resources and impart it to the users as per their fluctuating demand. This property is exhibited by the application of multi-tenancy. The cloud provider hides the location information of the resource abstracting the user from these information. The location independence makes the cloud an abstract model for various cloud resources like memory, storage, bandwidth, etc.

1.2.4 Rapid Elasticity

According to the varying demand of the user, the cloud allocates or de-allocates the required resources to fulfill the requirements of the user. The resources can be delivered to the user immediately after the request arises and de-allocated as and when the resource gets free. The resources are provisioned in such a manner that it appear to be infinite for the user. This is achieved by the process of scaling (scale up, scale down and scale out).

1.2.5 Measured Service

There is an outlining capability present in the cloud which measures the amount of resources consumed by the user. Based on this measurement, a user needs to pay only for the resources which are actually utilized by the user. A well-defined mechanism monitors the resources consumed by the user and the resource granted by the provider which helps in the determination of total cost.

1.2.6 Virtualization

Virtualization is a technology which allows the creation of different virtual computing environment. It is one of the key components of cloud computing which creates an infinite resource pool for the user. With the help of the virtualization, the utilization of resources is performed in an efficient manner. The main aim of virtualization is to set up autonomic networks that are virtually isolated from both the fundamental architecture and other virtual machines.

1.2.7 Multi-tenancy

Multi-tenancy refers to a property by which requirements of a number of users can be fulfilled by only one instance of a resource (hardware, software, etc.). The aim of multi-tenancy is to transform the application so that multiple instances can run on a single application. The multiple instances can be allocated to the users in such a manner that every user assumes as they own the resources alone. The resources are shared among different users in a sophisticated manner so that the resources are utilized properly.

1.3 Service Models

According to the requirement of the user, the service provided by the cloud also varies. IBM has categorized the cloud services into three categories that has some similarities and some unique features which makes them distinct. The service provided by one layer may be utilized by the other layer. All the services are virtualized and abstracted from the servers and data storages. These service models are explained as follows.

1.3.1 Software as a Service (SaaS)

This is the topmost layer of the service model architecture. The cloud provider provides the readymade software services to the user which is directly utilized by the user through networking devices without much interaction with the provider. The overall management and control of the services is in the hands of cloud provider except with some configuration settings. The user can only use the software. The services provided by SaaS are shared by various users without any direct interaction with each other. Globus Toolkit, Hadoop, CTERA, Redis, Navajo, Dropbox, Google Apps, Intuit QuickBooks Online, Oracle On Demand, etc. are some examples of SaaS.

1.3.2 Platform as a Service (PaaS)

The cloud provider provides the autonomy to the user to create their applications without worrying about the management of the resources (networks, operating systems, servers, etc.). The customer can develop and manage the application on the platform provided by

the cloud service provider. The user can abstractly change the developed applications by reprogramming. Google App Engine, Aneka, VMforce, MS Azure, Amazon SimpleDB, Apprenda, Force.com, etc. are some examples of PaaS.

1.3.3 Infrastructure as a Service (IaaS)

This layer allows cloud consumer to customize all the hardware resources of the cloud using the principle of virtualization. The provider allocates virtual instances of the hardware to the user according to the request. Cloud provider manages only the physical resources and the user has overall control of the allocated resources. Scalr, Rackspace Cloud Files, CloudSwitch, Amazon S3, EC2VPC, CloudWatch, etc. are example of IaaS.

The control of various cloud architecture layers by user varies according to the service models as shown in fig 1.2. There is minimal control in case of SaaS and maximal control in case of IaaS. The physical resources are always under the control of Cloud Service Provider as shown in the figure below.

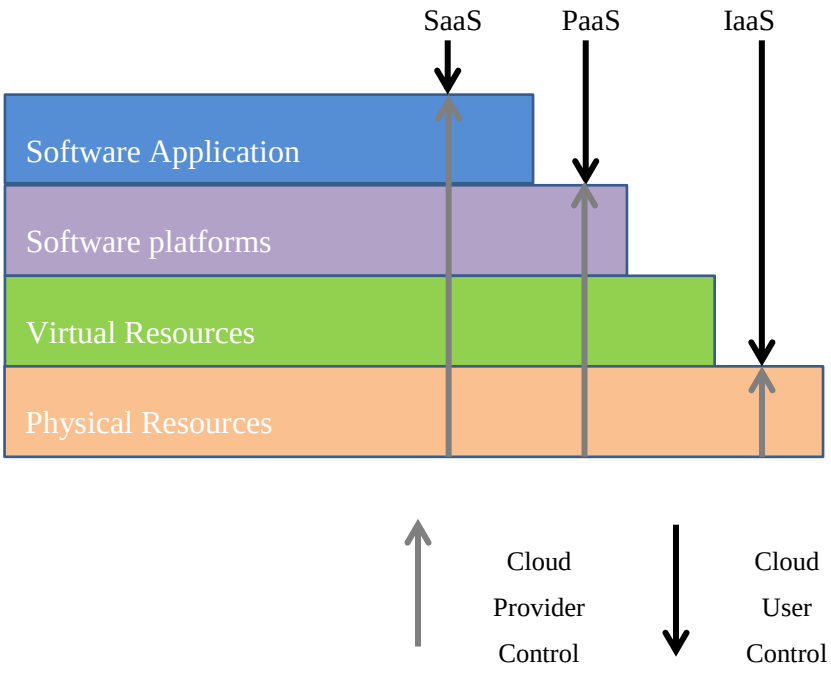


Fig 1.2: Controls in Cloud Service Model [5]

1.4 Deployment Models

According to NIST [1], there are four deployment models defined for cloud computing corresponding to the services provided by the cloud. The organization of various deployment models is briefly explained in fig 1.3.

1.4.1 Private Cloud

Private Cloud is a cloud that is available only for a particular organization and cannot be used by other organizations. Before using the services of the cloud, the user needs to be registered to the cloud. After successful registration, the cloud manager would provide the authentication to use the services. The services are managed by either a member of the organization or a third party. This is the most secured and trusted form of cloud as only the authorized person can access the services provided by the cloud belonging to an specific organization.

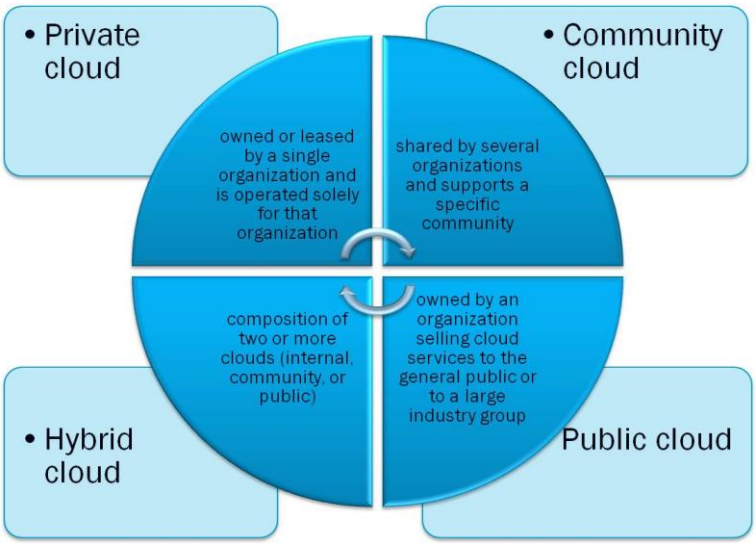


Fig 1.3: Cloud Deployment Model [6]

1.4.2 Community Cloud

Community cloud is an extension of private cloud where more than one organization having some common concerns/objectives (security, timeliness, etc.) can access the

services provided by the cloud. The management of cloud is done by either a member or some other trusted party.

1.4.3 Public Cloud

The cloud service which is purveyed for general public and can be easily accessed using internet is public cloud. It is the most common and well known service. The services are completely under the control of Cloud Service Provider (CSP). Unfortunately, it is the most untrusted form of cloud as anyone can access it. Social networking sites are the most common examples of public cloud.

1.4.3 Hybrid Cloud

Sometimes, for some of the services, a private cloud may hire the services of a public or community cloud or vice-versa. The cloud services lying between public cloud, private cloud and community cloud is called as hybrid cloud. It possesses the characteristics of all; public cloud, private cloud and community cloud. It has flexibility and versatility of public cloud and at the same time it has comfortability of the private cloud. However, it may have the disadvantages of these cloud services as well. M-Cloud and Aneka are examples of hybrid cloud.

1.5 Why should one move to Cloud?

There are immense advantages of cloud computing. Some of the important merits of cloud computing are as follows.

- Reduction in Cost
- Easily Scalable
- Automatic Up-gradation
- Less Energy Consumption
- Reliable and Fault tolerance

- Remote Access

1.5.1 Reduction in Cost

In general, to perform some computational work the computing resources must be owned by the user. It involves large investment at the time of establishment along with its operational and management costs. Thus, the overall investment is huge to avail the computing services. Cloud computing provides a pay-per-use model in which a user needs to pay only for the deployed resources. Using the cloud require to pay only for operational cost thus reducing the other cost incurred [3].

1.5.2 Easily Scalable

As the demand of the user changes (increases or decreases), the cloud is able to handle the requirements making user oblivious about the realization of resources. This is done by applying some specific mechanisms like 'scale up' i.e. making hardware stronger or 'scale out' i.e. adding additional nodes for expanding requirements and scale down i.e. taking resource back from the user for shrinking requirements [7]. The scaling is performed by the cloud provider to integrate new customized hardware into the existing systems without making user aware about any modification in the hardware. The fastness of scale up and scale down is very important in case of cloud computing as the speed gap may lead to the reduction of performance.

1.5.3 Automatic Up-gradation

The user uses the services of the cloud without being involved in any hardware oriented service generation. User completely depends on the cloud provider for the contentment of the request without worrying about any hardware or software required for providing the service so when there is any technology change, user doesn't need to be bother about. The cloud provider is solely responsible for any up-gradation and enhancement.

1.5.4 Low Energy Consumption

The cloud computing approach leads to energy efficient use of computing power of the available resources. It is because the services are pooled and maintenance costs lowers. This leads to low carbon emissions as some systems not being utilized are turned off (Server Consolidation) [8].

1.5.5 Reliable and Fault Tolerant

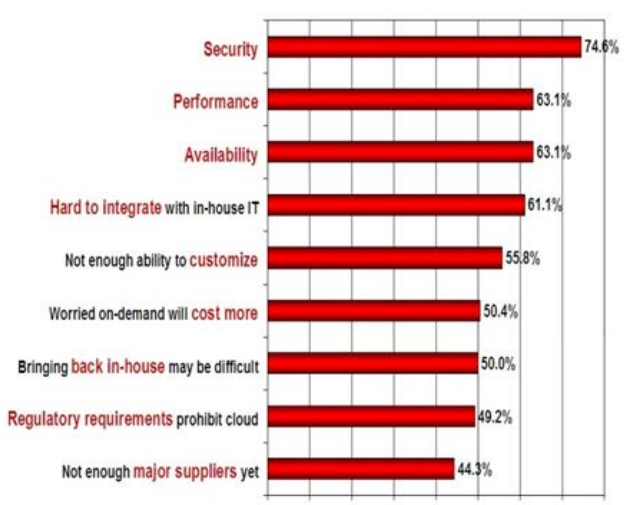
The cloud computing system is more reliable than other centralized systems as here if there is any failure in the underlying virtual machine, the entire service will not stop rather the service is migrated to some other virtual machine without any interruption and delay.

1.5.6 Remote Access

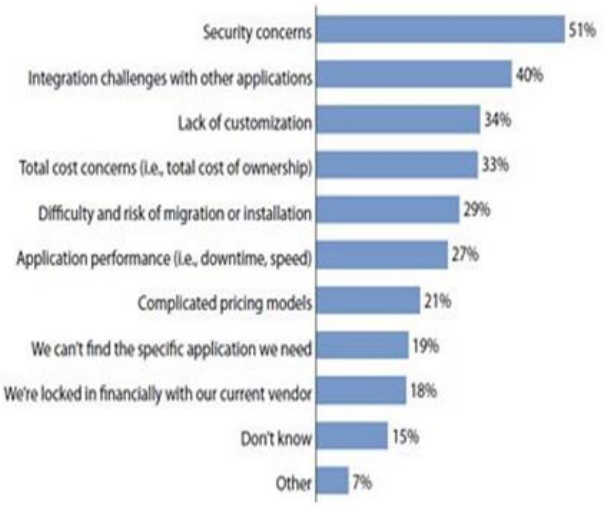
The accessing of the services provided by the cloud is incognizant about the location of the user. The requester can access the cloud services from any device present anywhere through the internet.

1.6 Research Issues in Cloud Computing

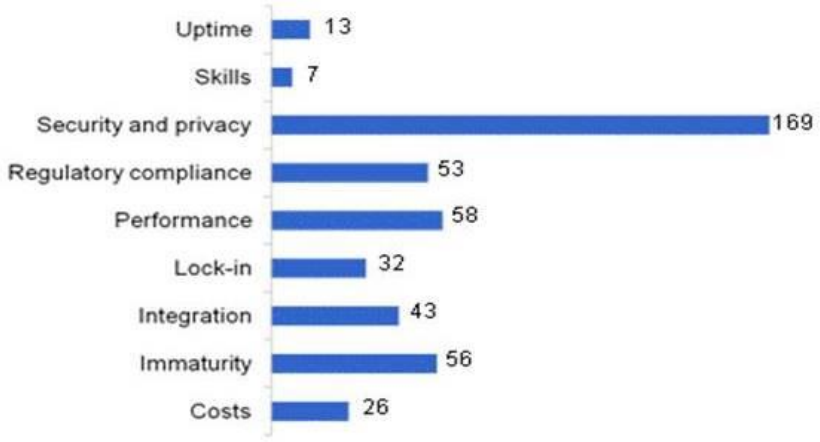
With every new technology, some barriers are also associated which creates problem in its complete adoption. The same exists for cloud computing. As cloud is in its infancy, there are number of issues which needed to be tackled properly. Various international organizations like IDC, Gartner research; Forrester, etc. are engaged in identifying these issues. The issues noted by these organizations are shown in fig 1.4.



Source: IDC Enterprise Panel Survey, August 2009, n=244
1=not significant, 5=very significant



Source: Enterprise and SMB Software Survey, North America and Europe, Q4 2009, Forrester



Source: Gartner Data Center Conference Poll, Dec 2009, n=94

Fig 1.4: Survey on Issues of Cloud Computing by Various Organizations

The figures obtained, from the survey by various organizations, shows the similar result leading to a common point that security, performance, availability, etc. are some common issues that are to be resolved for the overall spread of cloud computing. Without resolving these issues, the cloud computing cannot be utilized perfectly. Some of the most important issues which hinder the evolution of cloud computing [2], [3], [9], [10] are discussed as follows.

- Security
- Resource Provisioning
- Availability
- Costing
- Service Level Agreement (SLA)
- Interoperability

1.6.1 Security

Security is considered as the most important issue because the service providing organizations are not controlled by the user. The user does not know where the data is residing (which server) and what would happen with it. No one wants to compromise with the privacy of their data. Some organizations are completely focusing on the security issues of cloud computing such as CSA (Cloud Security Alliance), OSA (Open Security Architecture) and ENISA (European Network and Information Security Agency). These organizations are completely focused on determining and managing the security issues.

1.6.2 Resource Provisioning

User requires resources (storage, processing power, bandwidth etc.) for the execution of the job, and the same are provided by the cloud provider. The job must be finished within time, cost and without any SLA (Service Level Agreement) violation. One cloud provider satisfies a number of users having multiple jobs. To fulfill this, there must be some mechanisms which allow the users to use the services of cloud simultaneously without violating SLA. The resources should be provisioned in such a way that the Quality of Service (QoS) must be satisfied.

1.6.3 Availability

Availability is one of the key requirements in cloud computing. Unavailability of a service will create a lot of problem for a user. If a user wants to access a cloud service

and if the service is unavailable at that particular time, the user may switch to some other service and the trust to the earlier service will be decreased. In the recent past, many instances for service unavailability in big organizations such as google, facebook, amazon, etc. lead to a big loss. So, there must be some mechanism which ensures the availability of the services and resources.

1.6.4 Costing

There should be a tradeoff among computation, communication and integration (merging various services provided by different CSPs) cost attained by cloud consumer [11]. Cloud computing is a pay-per-use model so user needs to pay only for the used resources yielding reduced infrastructure cost. As there is communication between user and cloud, it increases the overall communication cost. A consumer can use the services of more than one cloud provider so it also adds integration cost. Cost analysis becomes more complicated due to elastic resource pooling and multi-tenancy.

1.6.5 Service Level Agreement

The requirement of the user and the service provided by the cloud provider varies in different aspects. There must be some common level on which both user and cloud provider negotiate. The conditions of this common level are converted into an agreement known as service level agreement. With the changing demand of different user, the requirements also vary and accordingly the SLA should also be complex and varying. There must be some mechanism which ensures that the SLA should be well contrived and well followed by both cloud user and provider. What happens if the SLA is violated? All these issues needed to be managed very carefully.

1.6.6 Interoperability

This is one of the open issue posing serious hurdle for the development in cloud computing. Today each cloud has its own architecture and the way in which it interacts with the user. It creates many problems like user is not comfortable to compare which cloud is best suitable for the particular requirement and other is difficulty in integration of

cloud services with organizations existing legacy system. Interoperability refers to the linkage among different clouds as well as within cloud to realize smooth data flow within clouds and between cloud and users.

1.7 Conclusion

Cloud is transforming the computing paradigm in the form of utility which can be accessed by any user on demand without any obligation to handle it. Even with a lot of advantages it cannot be fully implemented due to some implementation hindrance. This chapter identifies various issues needed to be resolved. Security is one of the most important issues resisting the fast implication of cloud by most of the organizations. The dissertation work addresses the security issue of Cloud computing.

Chapter 2

THE PROBLEM

Cloud computing is an emerging computing platform to store, manipulate, access and share data among internet connected devices according to some specific rules. The problem, addressed in this dissertation work, is of Security in Cloud which has been presented and deliberated in this chapter.

2.1 Security Aspects in Cloud Computing

Security is considered as the most important issue desisting many users to join the cloud and thus resisting the growth of cloud computing. The user transfers his/her data to the cloud being incognizant about the location and any other activity on that data. A number of organizations are completely involved in the identification and evaluation of security problems invoked by the cloud user's data. Some of the common agencies among them are ENISA (European Network and Information Security Agency), CSA (Cloud Security Alliance), OSA (Open Security Architecture), etc. The security concerns, notified by all the organizations, can be divided into seven groups [12], [13], [14] as described below.

1. Network Security

2. Interface

3. Data Security

4. Virtualization

5. Compliance

6. Legal Issue

7. Ethical Issue

2.1.1 Network Security

It deals with all the issues related to the configuration and communication of network related to the cloud computing infrastructure. The user considers cloud network as an extension of the local network following the same measures for security and privacy, but this is not the case as the cloud network is very complex as well as it is shared among a number of users. Various factors affecting the network security are as follows.

Transfer Security

Due to distributed architecture and immense resource sharing, a lot of data is in conveyance which may be accessed by the attackers. The data should be kept secured from various attacks like spoofing, sniffing, man in middle attack and side channel attack, etc.

Denial of Service (DoS)

This is a phenomenon in which the resources are made unavailable to deliberate users due to malicious requestors which consume all the resources by sending fake requests [12], [14]. Various security means viz. firewalling is done to protect the resources.

Security Configuration

It is important to know the configuration of security protocols and technologies provided by the cloud provider before taking their services.

2.1.2 Interfaces

The user and services provided by the cloud are directly connected through the interface. It should be necessary that the interface should be much secured so that unauthorized users cannot access the services. The various security issues, related to the interface, are discussed as follows.

Application Program Interface (API)

API is a source code based interface used to access various applications/services provided by the cloud provider. It must be protected to keep the applications safe from malicious users [14].

Authentication

Authentication is a technique used for validation of a cloud user. Any mistake may increase the probability of attack. Password is the most common method of authentication but not always secured as loss or misuse of password again creates more dangerous situations.

2.1.3 Data Security

Data is the most important entity to be managed by the cloud provider. User uploads their data to the cloud believing that the cloud provider will take care of it and provide access whenever required [15]. Various issues related to the management of data security, are as follows:

Redundancy

It is the most common method of securing data from any unknown damage or loss e.g. machine crash, earthquake, system failure, etc. But sometimes it may lead to increase vulnerability as due to redundancy one needs to protect data at all the places using different methods which is a tedious task.

Cryptography

It is the most common method to secure sensitive data from being accessed by any unauthorized user. Various encryption methods are there which are based on keys (public key, private key, shared key, etc.). Keys are given only to the authorized users. Loss or stealing of encryption key may again create the security problems.

2.1.4 Virtualization

Virtualization is one of the key characteristic of cloud computing. It can complicate the security requirement of cloud as many users can independently access the cloud resources without knowing each other. Some of the factors, affecting this issue, are as follows.

Isolation

The resources provided to the cloud users are virtually isolated but they may share the same resources physically. Isolation is the solution of many security problems but the cloud provider never ensures that the resources provided are isolated.

Hypervisor Vulnerabilities

Hypervisors are also vulnerable to various attacks like cross VM (Virtual Machine) attacks in which data and network capability of one VM is stolen by some other VM. This reduces the overall capabilities of a VM which is not desirable.

Data Leakage

Due to hypervisor vulnerability and lack of isolation data becomes vulnerable. One may take advantage of this data and access the confidential data.

VM identification

Some VMs are designed for some specific purposes. There is no any provision to identify a VM for specific purposes (storage, processing, transfer, etc.). This leads to underutilization of specific VMs.

2.1.5 Compliance

Compliance refers to the method of complying with the rules or regulations required for proper issuing of service. It is necessary for building trust of a user towards a cloud provider. There are various methods which facilitates in building compliance.

Service Level Agreement (SLA)

It is necessary for the consumer to obtain guarantee over quality, availability and performance of the services provided by the provider. There is a point at which both user and cloud provider negotiate, the set of rules are called SLA. SLA is a bilateral agreement stating conditions, constraints and agreed Quality of Service (QoS) in form of a matrix. The main objective of the provider is to maximize profit and user satisfaction whereas a user looks for better services in least cost. Sometimes, a penalty is imposed for the violation of agreement.

Audit

The auditing of security and other aspects of cloud computing is done by a third party. It is believed that the auditor is independent and does transparent auditing. But imagine, what happens if the auditor becomes biased? It completely changes the view. Some suggested solutions involve transparency of the auditor to both user as well as provider.

2.1.6 Legal Issues

The cloud provider needs to follow the rules and regulations of the country where it is located. The rules vary from country to country though a cloud provider offers service to the users located anywhere in the world. The user needs to understand all these regulation before taking any service from the cloud provider because if there is any misunderstanding the provider runs according to their country's rule and user may not follow that. The main issues regarding legislation [12], [16] are as follows.

Data Location

Cloud data stored in multiple locations may get affected by the local legislation of that geographic area. Any issues associated with that data management will follow the rules of data storing location not the data user's location.

Warranty

It is important to know about the warranty provided by the cloud provider in case of any compromise on the issued service. The warranty will increase the trust on that particular cloud provider.

E-Discovery

Any complain by a user about enforcement of law leads to seize of particular hardware to investigate about the issues related to the complaint. This will affect all other users of that particular hardware to access their data. This leads to a critical situation where cloud provider is unable to serve any user which leads to decreased trust.

2.1.7 Ethical Issues

As cloud computing is an emerging technology, we don't know the legal, ethical and social relevance of cloud computing in future. It is important to take some measures for the general issues before they become undesirable. Various ethical issues[16], [17], need to be addressed, are discussed below.

Accountability Control

The user does not have any control over the data after sending it to the cloud. It is difficult to find the reason of occurrence of any risk (resource failure, unauthorized access, etc.). In absence of any evidence, it is impossible that any entity accept the responsibility of the risk. Proper accountability is one of the solutions but it is tough to implement.

Ownership

The most important question in cloud is; who is the owner of data? In cloud along with many users' data, it contains its own data for the purpose of control and management. All the data need to be isolated and protected properly. User can access the data by following identity based mechanisms though it may lead to identity fraud and theft.

Monopoly & Lock-in

Due to legal issues, the number of cloud provider may be limited in the near future. This leads to the dominance and monopolization of a provider resulting in many problems like monopolized cost, reduced quality of services, etc.

2.2 Cloud Architecture

No any precise architecture has been defined for cloud computing as it is a business model and every cloud user manipulate the architecture according to their expectation. There are different architectures of cloud computing proposed by various organizations e.g. NIST [1], IBM [18], CSA [19], etc. which presents cloud computing as a layered architecture where different layers are involved in performing unique functionality. Buyya et.al [4] proposed a high level market oriented architecture for cloud computing which presents a global market oriented resource management strategy required for service and risk management for customer services to satisfy SLA. There exists a cloud market which facilitates the communication between user and hardware. The architecture contains four layers as explained in fig 2.1.

2.2.1 User/Broker

This entity basically represents the resource requester which is the main focus of the whole cloud business. User either directly sends their request to the cloud market or sends it to the brokers which collects requests from various users and communicate with the cloud.

2.2.2 SLA Resource Allocator

This is the identifying feature of this architecture. The user requests are not directly entertained by the cloud provider rather these are tackled by a mediator known as SLA Resource Allocator. This layer is involved in making proper connection between cloud user and provider by negotiating between user and provider at a common point. The

common point is converted in an agreement followed by both user and provider. Any violation leads to penalty. There are multiple functions of this layer as noted below.

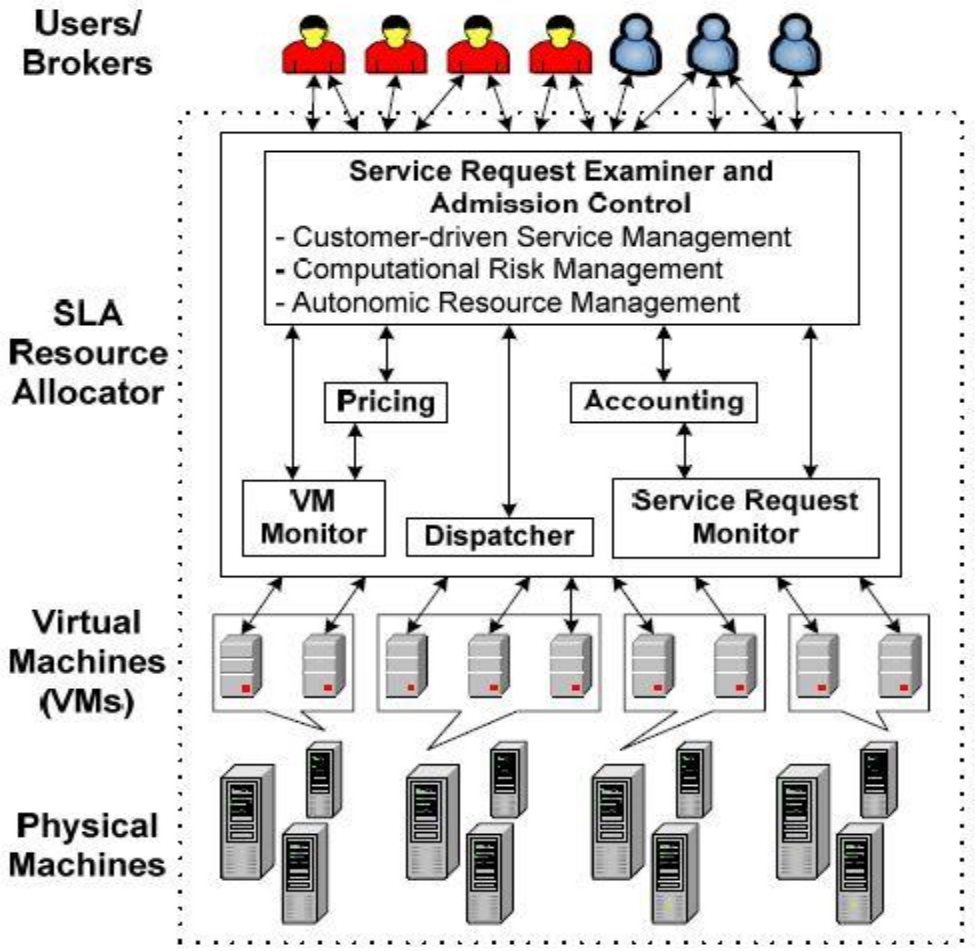


Fig 2.1: Market Oriented Cloud Architecture [4]

Service Request Examiner and Admission Control

It involves the function associated to accept or reject a request when arrived first time. The decision is based on the QoS requirement and availability of the requested resource. It also manages all the resource (available or occupied) and users' job information.

Pricing

The pricing rate of the services provided by the cloud is also decided by the SLA resource allocator. The decision is based on various parameters like number of requests, available instances, price of the competitor, etc.

Accounting

The services, provided by the cloud, vary according to the changing requirement of the user's job. This layer is involved in proper metering of the provided service so that the costing can be done appropriately.

VM Monitor

The monitoring of virtual machines i.e. list of free VMs, resource contained by the VM is done by this layer.

Dispatcher

It is involved in the management of how to execute the requested service of selected user on allocated virtual machine without any interruption.

Service Request Monitor

This component is involved in tracking the execution process of requested service. Based on the information collected by the Service Request Monitor, the performance of the system is analyzed and a feedback is forwarded to the cloud provider about the capability to satisfying the user's requests.

2.2.3 Virtual Machine

Any number of virtual machines can be created and destroyed based on the user's request. It enables to utilize the limited space on physical machines in an efficient manner. One Virtual machine can run in isolation from other virtual machine on same physical machine.

2.2.4 Physical Machine

This is completely under the control of the cloud provider. The cloud provider uses the resources to form virtual machines according to the users' request. The physical resources are shared among various users without any information to the user.

2.3 Security Prioritized Resource Provisioning: The Problem

The quality of service requirements of various job is different depending on the type of job viz. military job requires high security, scientific tasks requires quick response, normal job requires reduced cost, etc. Even for a single job, the requirements of various tasks may be different which is not so easy to estimate. If all the tasks are provided with the resource required by the largest task, some resources are not utilized by the smaller tasks leading to wastage of some resources. If we satisfy the requirements of only smaller jobs the larger jobs can't get executed as the requirements are not satisfied. It is very important to know the requirements of each and every task a-priori so that only required resources can be allocated to that task. The resource provisioning to the jobs are done to satisfy some of the quality of service requirements as listed below.

- Security,
- Deadline,
- Cost,
- Availability,
- Reliability,
- Bandwidth Requirement, etc.

There are enormous cloud providers available in the market, which satisfies the user's requirements. Each CSP (Cloud Service Provider) has some unique characteristics. The resources are provisioned in such a way that all the requirement of user's job is satisfied in cost efficient manner. Security is the most affecting barrier for the complete adoption of cloud computing but most of the existing work doesn't take security as a prime issue in

consideration. Only few works considers security as an issue but the given solutions are not so efficient.

The work, in this dissertation, proposes a model for efficient provisioning of cloud services to the user. The model considers security as a main parameter along with other Quality of Service (QoS) parameters used to find an appropriate CSP (Cloud Service Provider) for each user's job in an efficient way.

2.4 State of the Art

Some of the related work done in the field of Cloud resource provisioning is discussed below.

Ye Hu et.al in [20] discussed about the resource provisioning of interactive jobs in cloud computing with autonomic resource management. In this, a two level architecture is presented; the upper layer is used to provide abstraction for shared computing environments while the lower layer is involved in providing the desired service. The SLA's are constructed on the basis of probability distribution of response time.

In [21] Saurabh et.al explained the resource allocation problem for varying workload (interactive, non-interactive, etc.) application. A concept of admission control is presented here which helps in scheduling the resources with maximizing resource utilization and profit along with assurance to satisfy the SLA requirements. The mechanism is based on proper monitoring of the resource demand at particular interval and allocating resources to a task based on the type of task, resource status and reserved capacity.

In [22] Qian Zhu et.al proposed a feedback control based automatic and dynamic resource provisioning algorithm which satisfies the quality of service parameters of adaptive applications in the dynamically changing environment within fixed deadline and limited budget.

Buyya et.al in [23] proposed a market-based provisioning and virtualization policy for easy resource allocation to applications. The proposed method satisfies the quality of service requirements incorporating some extra features like customer handled service control, easy resource and risk management in dynamically changing cloud environment.

In [24], Shuai Ding et.al proposed an ideal resource recommendation method for the multi-criteria attribute matching between provider and consumer. The model consists of two modules one is resource matching algorithm which analyzes all the user requirements either functional or non-functional and the other is resource recommendation part which analyze the cloud resource based on customer evaluation and various attributes.

Some of the resource provisioning models that addresses the security issue also are as follows.

Chang et.al present a novel authenticated security aware scheduling algorithm named Cloud Computing Background Key Exchange (CCBKE) [25]. The scheme is based on general Internet Key Exchange (IKE) scheme and randomness reuse ratio which reduces the number of standard operations which reduces the load and execution time of the job.

A similar work is done by Garg et.al for ranking of cloud services [26] by measuring various functional and quality attributes. The main aim, of this work, is to find the right cloud provider able to satisfy all the requirements of every user in an efficient manner.

Ahmed et al. explained security as one of the most important parameters of SLA need to be satisfied by the cloud service provider during scheduling [27] i.e. request is scheduled only on those cloud that satisfies the specific security requirements of the job on the basis of weights assigned to various issues.

2.5 Conclusion

Security is the most promising issue resisting the proper spread of cloud computing and is generally unaddressed. Only a few methods considers security as a QoS parameter but the efficiency of such methods are not good i.e. the algorithms do not give better results

when the number of cloud provider is very large. The proposed model, in this dissertation, considers all these issues i.e. security along-with other cloud parameters and also takes care of the efficiency of the working of the methods.

Chapter 3

THE PROPOSED MODEL

In cloud computing, security is an important issue to be addressed for the appropriate provisioning of resources to the user. To provision the resources, the proposed model applies some methods which helps in achieving the goal. This chapter discusses all the methods used and their applications in the proposed model.

3.1 Methods & Techniques

The work considered in the proposed model is security aware resource provisioning in the Cloud for which two methods are employed: L_P metric method and Analytical Hierarchical Process (AHP) method. These methods are explained in the following subsections.

3.1.1 L_P Metric Method

L_P Metric method is the most commonly used method employed for screening purposes i.e. shortlisting few options from the number of available options. A small number of option is easy to handle. The l_P metric for two vectors *X* and *Y* with equal number of attributes and for some real number *p;* $1 \leq p \leq \infty$ is a function metric on real vector space R^n. It is represented as d_{l_p} and is defined as given in equation 3.1 [28].

$$d_{l_p} = \| X - Y \|_P \tag{3.1}$$

Where the function $\| \bullet \|$ is represented as

$$\| Z \| = (\sum_{i=1}^{n} |Z_i|^p)^{1/p} \tag{3.2}$$

Here *Z* is a vector and Z_i is i^{th} attribute of the vector.

The metric space(R^n,d_{l_p}) is abbreviated as l_p^n and is also known as l_p^n space.

L_1, L_2, L_∞ on R^n are the most common metric representations. L_1 and L_∞ are crystalline metrics i.e. metrics with polygonal unit balls. L_2 metric is also known as Euclidean metric. Hilbert metric is special type of L_2 metric for which $\sum_{i=1}^{\infty} |x_i|^2 < \infty$.

The Euclidean metric is also known as Pythagorean distance or Beeline distance and is represented as d_E on vector *X*, *Y* in real space R^n as given in equation 3.3.

$$d_E = \left\| X - Y \right\|_2 = \sqrt{(X_1 - Y_1)^2 + \ \ldots + (X_n - Y_n)^2} \tag{3.3}$$

Here X_i, Y_i represents the i^{th} attribute of vector *X* and *Y* respectively.

3.1.2 Analytical Hierarchical Process (AHP)

There are various situations where we need to take a decision for picking one solution out of a number of present solutions. Sometimes, there is only one condition based on which we find the optimal solution but more often there are more than one conditions. The problem with multiple decisions is known as Multi Criteria Decision Making (MCDM) problem. A number of solutions exists for solving MCDM problem e.g. Analytic Hierarchical Process (AHP) [29], Analytic Network Process (ANP) [30], Goal Programming (GP) [31], Grey Relational Analysis (GRA) [32], Weighted Product Model (WPM) [33], Best Worst Method (BWM) [34], Superiority and Inferiority Ranking Method (SIR method) [35], etc. AHP is the most commonly used method for decision making process because it considers qualitative attributes along with other quantitative attributes for the selection of services. In AHP, the problem is systematically broken into smaller constituent parts and a pairwise comparison is performed on each step to find the respective priority. The whole process is divided into three steps namely decomposition, comparative analysis and prioritization [29]. In decomposition stage, a top-down hierarchical structure is constructed based on similar properties. Each level of hierarchy is used to represent different aspects of the original problem as shown in fig 3.1. There are number of solutions among which one is to be chosen which best satisfies all the requirements. AHP can easily compare the solutions and results out the best available option.

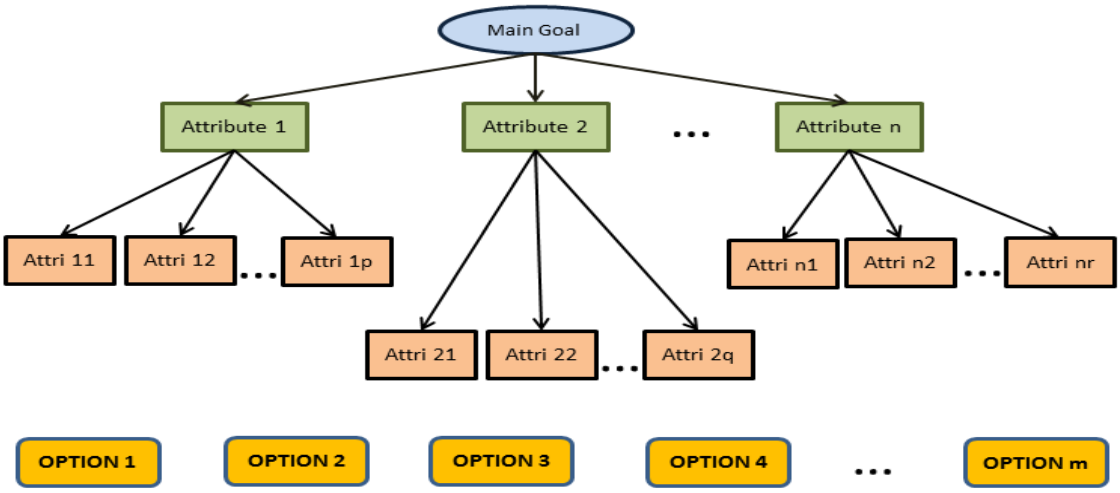


Fig 3.1: Hierarchical Structure for Problem Solving in AHP

A comparison matrix is constructed for each level of hierarchy and the possible alternatives are listed based on a scale defined by Satty [36]. The Satty scale assigns priority at each level as given in table 3.1.

Table 3.1: Satty's Relative Importance Scale for AHP [36]

Intensity of Priority	**Definition**	**Explanation**
1	Equal Importance	Both activities equally contribute to the main objective
3	Moderate Importance	One activity is slightly more important than the other activity
5	Strong Importance	One activity strongly favor the judgement over the other activity
7	Demonstrated Importance	One activity dominates the judgement of other activity
9	Extreme Importance	Highest possible priority than other
2,4,6,8	Intermediate value between two judgements	Compromised value between two extremes

Based on the Satty scale, the given rules are used to construct the Reciprocal Comparison Matrix *A*.

- For *n* attributes the size of matrix *A* is $n \times n$.
- For $i = j$, the value of element $A_{ij} = 1$.
- For $i > j$, the value of element A_{ij} is taken from user following the Satty scale.
- Otherwise $A_{ij} = 1/A_{ji}$.

	A_1	A_2	A_3
A_1	1	w_1	w_2
A_2	$1/w_1$	1	w_3
A_3	$1/w_2$	$1/w_3$	1

Fig 3.2: Reciprocal Comparison Matrix According to Satty scale

Some problems are associated with this Reciprocal Comparison matrix as the weights are assigned by the user there may be some inconsistencies present in the input. The comparison matrix is acceptable if the matrix is either perfectly consistent or approximately consistent. The condition satisfied for a perfectly consistent matrix is given in equation 3.4.

$$A_{ij} \times A_{ijk} = A_{ik} \qquad \forall\, i, j \text{ and } k$$
$$\text{Or} \qquad AA - nA = 0 \tag{3.4}$$

For approximately consistent, the condition is given in equation 3.5.

$$A_{ij} \times A_{jk} \approx A_{ik} \qquad \forall i, j \text{ and } k$$
$$\text{Or} \qquad AA - nA \approx 0 \tag{3.5}$$

To find the appropriate alternatives, we need to define a unique rank i.e. the priority vector of each alternative based on the priority assigned by the user. Principle eigen

vector [37] is one of the solution to find the priority vector [38]. We take the normalized value of principle eigen vector to easily show the priority. Before giving the final rank, any inconsistency in the comparison matrix is to be checked and removed. The condition for checking the consistency is given below in equation 3.6.

$$CR = \frac{CI}{RI} < 0.1$$

Where *CR* is Consistency Ratio, *CI* is Consistency Index, *RI* is Random Index (dependent on the size of the matrix). *CI* is calculated as given in equation 3.7 with the help of maximum eigen value, λ_{max} and the order of the matrix, *n*.

$$CI = \frac{\lambda_{max} - n}{n - 1} \tag{3.7}$$

For varying n, the value of random index changes as given in in table 3.2.

Table 3.2: Random Index Value

n	1	2	3	4	5	6	7	8	9	10
RI	0	0	.58	.90	1.12	1.24	1.32	1.41	1.45	1.49

If the matrix is found to be inconsistent, we need to make it consistent. The various steps in inconsistency identification and correction proposed by Egru et.al [39] are as follows.

I. The location of inconsistent element is identified as follows.
   i. Construct an induced matrix *C* as given in equation 3.8

$$C = AA - nA \tag{3.8}$$

   ii. Identify the largest possible value (s) C_{ij} in *C* deviating farthest from 0 and record the location as i^{th} row and j^{th} column.

II. Use bias identifying vector to identify the potential inconsistent element.
   iii. Take the i^{th} row and transpose of j^{th} column of comparison matrix *A* as R_i and $C_j{}^T$.
   iv. Perform the scalar multiplication of R_i and $C_j{}^T$ as given in equation 3.9.

(3.9)

$$B = R_i \times C_j^T$$

v. Find the farthest deviating element from A_{ij} by constructing a bias identifying vector *F* using following formula given in equation 3.10.

$$F = B - A_{ij} = (A_{i1}A_{1j} - A_{ij}, A_{i2}A_{2j} - A_{ij}, ...,A_{in}A_{nj} - A_{ij}) \quad (3.10)$$

III. Find the inconsistent element by applying identification method and matrix order reduction.

vi. Find the error element in *A* causing inconsistency by analyzing the values in bias identifying vector *F*.

vii. Verify the value of C_{ik} and C_{kj} in the induced matrix *C* and check the value of A_{ik} and A_{kj} causing inconsistency.

Repeat the above process until the matrix becomes consistent. After matrix *A* becomes consistent, find the normalized principle eigen vector which represents the priority value of each attribute.

3.2 The Proposed Model

The proposed model addresses the problem of resource provisioning with a special attention on various security issues in an efficient manner. The proposed solution is divided in to four steps as given below.

1) Characterization of cloud service provider (CSP) and users' job
2) Screening process using L_p metric
3) Assigning weights to the criteria & ranking of CSPs using Analytical Hierarchical Process (AHP)
4) Final Selection of CSP for user's job

3.2.1 Characterization of Cloud Service Provider (CSP) and User's Job

A cloud service provider (CSP) is characterized by three tuples as (Sec_i, ES_i, PUC_i), where

Sec_i = Security provided by i^{th} Cloud Service Provider,

ES_i = Execution Speed of VM provided by i^{th} Cloud Service Provider in terms of GFLOPS,

PUC_i = Per Unit Cost of the resources provided by i^{th} Cloud Service Provider in terms of $/hr.

The user's job is characterized by four tuples *J* ($Len, SecReq_j, Dead_j, Cost_j$), where

Len = Length of the job in terms of Number of Instructions (GI (Giga floating point Instructions)),

$SecReq_j$ = Security Requirements of j^{th} job in terms of 1-0 specifications,

$Dead_j$ = Maximum allowable deadline of j^{th} job in terms of minutes,

$Cost_j$ = Maximum incurred cost for execution of j^{th} job in terms of $.

Metrics for Cloud Attributes

- ✓ $\boldsymbol{Sec_i}$ **&** $\boldsymbol{SecReq_j}$*:* The security is a qualitative parameter which cannot be measured by any device. To incorporate security as a QoS parameter, the questionnaire provided by CAIQ (Consensus Assessment Initiative Questionnaire V1.0.1) of CSA (Cloud Security Alliance) [40] is considered. The Boolean yes-no answers given by CSPs are converted into numeric 1-0 format i.e. yes as 1 and no as 0. The various security attributes considered in this dissertation work is Compliance (CO), Facility Security (FS), Risk Management (RM) and Resiliency (RS). For Compliance the various sub-attributes are Audit Planning (AP), Independent Audit (IA) and Contact/Authority Maintenance (C/AM). The various sub-attributes of Facility Security includes User Access and Secure Area Authorization. Program and Policy Change Impacts are the considered sub-attributes of Risk Management. Impact Analysis is the only considered attribute for Resiliency.
- ✓ $\boldsymbol{ES_i}$: The speed with which the i^{th} virtual machine executes the instructions is known as Execution Speed of i^{th} virtual machine. It is generally measured in Giga FLOating Point instructions per Seconds (GFLOPS).

- ✓ $\boldsymbol{PUC_i}$ **&** $\boldsymbol{Cost_j}$: The cost includes the processing charge as well as communication cost for a job. Per Unit Cost (PUC_i) is measured in terms of dollar per hour and Cost is measured in dollar ($).
- ✓ $\boldsymbol{Dead_j}$: The deadline is the maximum time allocated for execution of a job j. It includes processing time as well as waiting time and is represented in terms of minutes.
- ✓ $\boldsymbol{Len}$: The length of the job is given by the user and is defined in terms of number of Giga Instructions (GI). This is used by CSP to find the total cost and total execution time of the job.
- ✓ $\boldsymbol{Exetime_i}$**:** It represents the total time to execute the specified job. It depends on the size of the job and is presented as given in equation 3.11.

$$Exetime_i = Len/ES_i \tag{3.11}$$

- ✓ $\boldsymbol{TCost_i}$**:** It represents the total cost required for complete execution of the job. It depends on the size of the job as well as per unit cost charged by the CSP and is given by equation 3.12.

$$TCost_i = Len \times PUC_i \tag{3.12}$$

- ✓ $\boldsymbol{WT_i}$: The waiting time is the time specified by CSP after which the job can be executed. This depends on many factors e.g. previous load on the CSP, number of other waiting jobs, priority of the job, etc.
- ✓ $\boldsymbol{TET_i}$**:** The total time taken in the completion of job is the sum of execution time and waiting time as shown in the equation 3.13 given below:

$$TET_i = Exetime_i + WT_i \tag{3.13}$$

Finally, a table is prepared consisting of all CSPs named *PROVIDER* with attributes (Sec_i, TT_i *and* $TCost_i$). Also a vector *USER* is formed with the minimum qualifying criteria as the attributes ($SecReq_j$, $Dead_j$ *and* $Cost_j$). Both the tables are used for the evaluation in the next step.

The various terms used in the rest of the dissertation is listed in the table 3.3.

Table 3.3: Table Showing Used Entity

TERM	MEANING	TERM	MEANING
USER	Vector containing list of user requirements	z	Total number of criterion used in the evaluation purpose
SELECT	Table containing CSP satisfying user's requirement	w_z	Comparable weight of attribute in matrix C
m	Number of CSP in SELECT	EV	Eigen vector of matrix C
$\max_k$	Maximum value of attribute k	v_i	i^{th} eigen vector
$\min_k$	Minimum value of attribute k	CM_z	Comparison Matrix of CSP for z^{th} attribute
R_k	Range for attribute k	x_{ji}	j^{th} element of i^{th} attribute
NormProv	Table of CSP containing normalized value of attributes	FM	Final criterion rank matrix for CSP
Rank	Table containing Rank of CSP	RV	Overall rank vector for CSP
FINAL	List of CSP for final evaluation	n	Number of CSP selected for evaluation

3.2.2 Screening of CSP using L_p Metric Method

In this step, a unique list of CSP is prepared for each job which best suites the requirement. The purpose of using L_p metric, in this step, is to reduce the number of CSP from very high to manageable without much effort. A small list of CSP is not only easy to handle but also efficient for the next step. The algorithm for this step is explained as follows.

Step 1: Compare the *PROVIDER* table with the vector *USER*. Select all the CSPs which satisfy the minimum requirement of the user and make a table *SELECT*.

Step 2: Normalize the table *SELECT* to make all the attributes in one scale between 0 and 1. To do this, we find the maximum value max_k and minimum value min_k for each criterion *k* and then find the range R_k as given in equation 3.14. The formula for normalization varies according to the condition as given in equation 3.15. Finally prepare a table *NormProv* which contains the normalized value of all the attributes.

$$R_k = max_k - min_k \tag{3.14}$$

$$NormProv_{jk} = \begin{cases} \frac{SELECT_{jk} - min_k}{R_k} & when\ maximization\ is\ done \\ \frac{max_k - SELECT_{jk}}{R_k} & when\ minimization\ is\ done \end{cases} \tag{3.15}$$

Step 3: With the help of L_2 metric, rank $Rank_i$ of each selected CSP is calculated as given below in equation 3.16.

$$Rank_i = \sqrt{\sum_{i=1}^{m}(1 - NormProv_{ik})^2} \tag{3.16}$$

Step 4: Sort the CSPs in the increasing order of the Rank value.

Step 5: Select top n CSP from and form a new table *FINAL* the list for further calculation in the next step.

The significance of L_p metric is that it selects only most significant CSPs from available list of CSPs. While applying AHP for ranking of CSP, it uses matrix multiplication. The complexity of matrix operation is very high and depends on the value of n. For large number of CSP the value of n is very high thus the complexity is very high. To reduce the complexity, we reduce the number of CSP i.e. only those CSPs are selected which suites the requirement well.

3.2.3 Assigning Weights to the Criteria & Ranking of CSPs using Analytical Hierarchical Process (AHP)

In this step, AHP is applied on the result of previous step. The procedure is as follows.

Step 1: *Defining Overall Structure* In this step, the overall hierarchy for selecting the appropriate CSP is performed. The entire criterion in the form of hierarchy level is defined. The related attributes are clubbed to form a single domain. At the top there is one goal to select the appropriate CSP. The hierarchy is shown in fig 3.3.

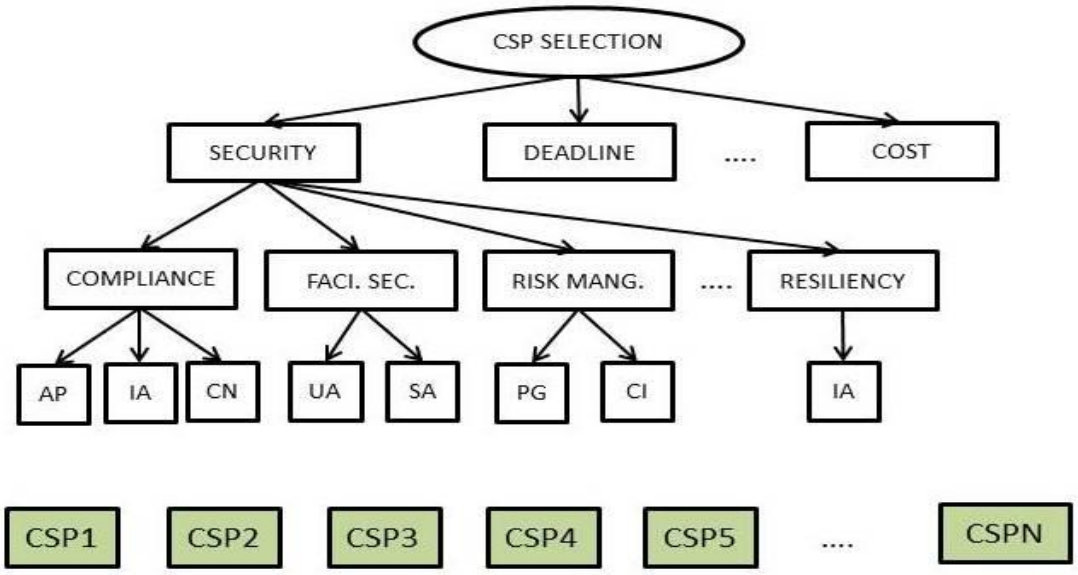


Fig 3.3: Hierarchy Definition for Ranking of CSP

Step 2: *Formation of Comparison Matrix C for Criteria* The weights are assigned to each criterion based on Satty scale and as specified by the user. Based on the assigned weight, a comparison matrix C is constructed as shown in fig 3.4. The size of matrix C is $z \times z$. The principle eigen vectors for comparison matrix C is calculated and normalized. The normalized principle eigen vector represents the contribution of each criterion for the final ranking. The inconsistency in the matrix results in the inaccuracy of contribution of a particular criterion.

$$C = \begin{bmatrix} 1 & w_2 & w_3 \cdots & w_z \\ 1/w_2 & & \ddots & \vdots \\ 1/w_3 & & & \\ \vdots & & \cdots & 1 \\ 1/w_z & & & \end{bmatrix}$$

Fig 3.4: Comparison matrix for criteria

Step 3: *Consistency Check for Comparison Matrix* The matrix *C* is checked for consistency by applying the methods for consistency check. If the matrix *C* is found to be inconsistent, make it consistent by updating the weights.

Step 4: *Ranking of Criterion* The normalized eigen vector *EV* of matrix *C* is calculated as given in equation 3.17 which represents the final rank of each criterion.

$$EV = {}^{1}/_{(v_1 + v_2 + \cdots + v_z)} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_z \end{bmatrix} \tag{3.17}$$

Step 5: *Formation of Comparison Matrix for CSPs* According to the requirements of user's job as specified in *USER* and the selected CSPs as given in *FINAL*, prepare *z* number of matrices CM_i for i =1 to *z*, where *z* is the number of criteria. Each matrix is of size $n \times n$ where *n* is the number of CSP as shown in fig 3.5.

$$CM_i = \begin{bmatrix} 1 & x_{2i} & x_{3i} \cdots & x_{ni} \\ 1/x_{2i} & & \ddots & \vdots \\ 1/x_{3i} & & & \\ \vdots & & \cdots & 1 \\ 1/x_{ni} & & & \end{bmatrix}$$

Fig 3.5: Comparison matrix of CSP for one criterion

Step 6: *Consistency Check for* CM_i The matrix C is checked for consistency by applying the methods for consistency check. If the matrix *C* is found to be inconsistent, make it consistent by updating the weights.

Step 7: *Construction of final order matrix FM* The normalized eigen vector of all the CM_i are placed to form a matrix *FM*. The matrix *FM* is of size $n \times z$ as given in fig 3.6.

$$FM = \begin{bmatrix} r_{11} & r_{21} & r_{31} \cdots & r_{n1} \\ r_{12} & & \ddots & \vdots \\ \vdots & & & \\ r_{1z} & & \cdots & r_{nz} \end{bmatrix}$$

Fig 3.6: Final Order Matrix

Step 8: *Determination of Final Rank of CSPs* A matrix multiplication is performed between *FM* and *EV* resulting in to a vector *R* which represents the final rank of CSPs as given in equation 3.18.

$$R = FM \times EV = \begin{bmatrix} r_{11} & r_{21} & r_{31} \cdots & r_{n1} \\ r_{12} & & \ddots & \vdots \\ \vdots & & & \\ r_{1z} & & \cdots & r_{nz} \end{bmatrix} \times \begin{bmatrix} v_1/(v_1 + v_2 + \cdots v_z) \\ v_2/(v_1 + v_2 + \cdots v_z) \\ \vdots \\ v_z/(v_1 + v_2 + \cdots v_z) \end{bmatrix} = \begin{bmatrix} R_1 \\ R_2 \\ \vdots \\ R_z \end{bmatrix} \quad (3.18)$$

3.2.4 Final Selection of CSP for User's Job

From the final rank matrix *R*, the CSP with maximum rank value is selected. The CSP with maximum ranking represents the provider which best suites the requirements i.e. all the requirements are best satisfied in minimum investment.

3.3 Conclusion

The proposed model gives an efficient solution for the resource provisioning problem which addresses the security issues along with other quality attributes like deadline and cost. For each user's job, the model recognizes a suitable CSP which satisfies the entire requirement with minimum overhead.

Chapter 4

EXPERIMENTAL EVALUATION

This chapter presents a case study on the model proposed in the previous chapter and verifies that the results are as per expectation. The proposed model has been evaluated on a data set of 30 cloud service providers and a user's job.

4.1 Case Study

In this case study evaluation, we consider security, execution speed and per unit cost characteristic of cloud service provider. The data of cloud security parameter (S_i) is gathered from CSA's (Cloud Security Alliances) CAIQ (Consensus Assessment Initiative Questionnaire) V1.1 STAR repository [40]. In security Compliance (CO) (Audit Planning, Independent Audits & Contact/Authority Maintenance), Facility Security (FS) (User Access & Secure Area Authorization), Risk Management (RI) (Programs & Policy Change Impacts) and Resiliency (RS) (Impact Analysis) is considered. The data on execution speed (ES_i) is generated randomly based on the benchmarks as given in [41]. The cost (C_i) varies according to security provided and execution speed and thus calculated from both security values and execution speed value using a function as given below.

$$C_i = f_1(f_2(S_{ij})) + f_3(ES_i)$$

The function f_1 represents division by 10, f_2 represents $\sum_{j=1}^{x}(2^j . S_j)$ (x be the number of security parameters to be considered) and f_3 represents multiplication by 10.The overall process is divided into four steps as explained below.

4.1.1 Characterization of Cloud Service Provider (CSP) and Users' Job

The detailed information of CSP is tabulated as shown in table 4.1.

Table 4.1: Information of CSPs

SL. NO.	SECURITY										EXE SPEED (GFLOPS)	PER UNIT COST ($/hr)
	COMPLIANCE				FAC. SEC.		RISK MAN.		RESILENCY			
	AP	IND. AUD.		CON.	UA	SAA	PG	PC	IMP. ANA.			
	C11	C21	C23	C41	F21	F41	R12	R41	R21	R23		
1	1	1	1	1	1	0	1	1	1	1	7.2453	171.5538
2	1	1	1	0	1	0	1	1	1	0	7.5462	122.5622
3	0	0	0	0	0	1	1	0	1	1	8.4617	171.0172
4	1	1	1	1	1	1	1	1	0	0	7.1496	96.99674
5	1	1	1	1	1	0	0	1	1	1	8.6790	179.4905
6	0	1	1	0	1	1	0	1	1	1	8.3415	178.4156
7	1	1	1	1	1	1	1	1	1	1	7.9306	181.6064
8	1	1	0	1	1	1	1	1	1	0	8.0834	131.5349
9	1	1	1	1	1	1	1	1	1	1	7.5033	177.3338
10	1	1	1	1	1	1	0	1	1	1	7.8800	174.7004
11	0	0	1	1	1	0	0	1	0	0	8.7372	102.9725
12	1	1	1	0	1	1	1	1	0	0	8.0295	104.9957
13	1	1	0	1	1	1	1	1	1	1	7.9859	181.7593
14	1	1	1	1	1	1	1	1	1	1	7.4937	177.2371
15	0	1	1	1	1	1	1	1	1	1	7.9311	181.5113
16	0	0	1	0	1	1	0	1	0	0	8.1609	99.60902
17	1	1	1	1	1	1	1	1	1	1	8.2545	184.8453
18	1	1	1	1	1	0	1	1	1	1	7.7723	176.8238
19	1	1	1	0	1	1	1	1	1	1	7.7246	178.7464
20	1	0	1	1	1	1	1	1	1	1	8.7795	189.8957
21	0	1	1	1	1	1	0	1	1	0	7.1641	116.2416
22	1	1	1	1	1	1	1	1	1	1	8.6047	188.3479
23	1	1	1	1	1	1	0	1	1	1	8.6525	182.4259
24	1	1	1	0	1	1	1	1	1	1	8.4535	186.0351
25	0	0	1	1	1	1	0	0	1	1	7.2678	155.4781
26	1	1	1	1	1	1	1	0	1	1	7.5451	164.9518
27	1	1	1	1	1	1	1	1	0	0	7.6701	102.2011
28	1	1	1	1	1	1	1	1	0	0	8.2555	108.0554
29	1	0	1	1	1	0	0	1	0	0	7.3321	89.0214
30	1	1	1	1	1	0	0	1	1	0	8.3260	124.7609

In this case study, the specification of job is given in terms of length expressed as Number of Instructions (GI), deadline (minutes), cost ($) and security requirements as expressed for cloud service providers. The user's job with all its requirements is specified as given in table 4.2.

Table 4.2: User Specification

User	SECURITY										DEAD.	COST	LENGTH
U1	1	0	1	0	1	0	1	0	0	0	160	545	62400

Waiting time of each CSP is assumed between 0 - 25 minute and is calculated randomly as it depends on the prior load, number of jobs waiting, priority, etc. For this period of time user need to wait. The execution time is based on length of the job and the execution speed. Total cost is calculated based on the execution time and the per unit time cost of given CSP. Here we consider the Costing in terms of per hour billing i.e. the range of payment is per hour. For the given job the CSP's table is modified and is shown in table 4.3.

Table 4.3: CSP's Properties According to User's Requirement

CSP	SECURITY										Total Time (min)	Total Cost (in $)
1	1	1	1	1	1	0	1	1	1	1	150.8394	514.6613
2	1	1	1	0	1	0	1	1	1	0	148.6086	367.6866
3	0	0	0	0	0	1	1	0	1	1	123.2936	513.0517
4	1	1	1	1	1	1	1	1	0	0	170.0628	290.9902
5	1	1	1	1	1	0	0	1	1	1	124.008	358.981
6	0	1	1	0	1	1	0	1	1	1	127.3323	535.2469
7	1	1	1	1	1	1	1	1	1	1	140.4473	544.8191
8	1	1	0	1	1	1	1	1	1	0	133.6102	394.6048
9	1	1	1	1	1	1	1	1	1	1	150.8464	532.0015
10	1	1	1	1	1	1	0	1	1	1	140.4663	524.1013
11	0	0	1	1	1	0	0	1	0	0	142.8213	205.945
12	1	1	1	0	1	1	1	1	0	0	152.5296	314.9871
13	1	1	0	1	1	1	1	1	1	1	131.546	545.2779
14	1	1	1	1	1	1	1	1	1	1	157.2295	531.7113
15	0	1	1	1	1	1	1	1	1	1	137.8569	544.5338

16	0	0	1	0	1	1	0	1	0	0	138.0078	298.8271
17	1	1	1	1	1	1	1	1	1	1	139.6882	554.5359
18	1	1	1	1	1	0	1	1	1	1	157.3756	530.4713
19	1	1	1	0	1	1	1	1	1	1	145.0777	536.2393
20	1	0	1	1	1	1	1	1	1	1	143.0331	379.7914
21	0	1	1	1	1	1	0	1	1	0	152.7035	348.7247
22	1	1	1	1	1	1	1	1	1	1	138.3904	565.0436
23	1	1	1	1	1	1	0	1	1	1	136.8537	547.2776
24	1	1	1	0	1	1	1	1	1	1	136.5039	558.1054
25	0	0	1	1	1	1	0	0	1	1	160.5494	466.4343
26	1	1	1	1	1	1	1	0	1	1	154.4995	494.8554
27	1	1	1	1	1	1	1	1	0	0	140.0446	306.6032
28	1	1	1	1	1	1	1	1	0	0	129.1764	324.1661
29	1	0	1	1	1	0	0	1	0	0	166.8183	267.0642
30	1	1	1	1	1	0	0	1	1	0	129.1866	374.2826

4.1.2: Screening of CSP using L_p Metric Method

If the security provided by CSP is at least equal to the user's requirement, total time (Execution time and Waiting time) is less than the deadline and the total cost is less than the cost incurred, the CSP satisfies screening criterion and is used for the next step evaluation according to L_2 metric method. The result of above step as presented in the form of selected CSP's is given in the table 4.4.

Table 4.4: Selected CSPs According to Screening Process

CSP	SECURITY										Total Time (min)	Total Cost (in $)
1	1	1	1	1	1	0	1	1	1	1	150.8394	514.6613
2	1	1	1	0	1	0	1	1	1	0	148.6086	367.6866
7	1	1	1	1	1	1	1	1	1	1	140.4473	544.8191
9	1	1	1	1	1	1	1	1	1	1	150.8464	532.0015
12	1	1	1	0	1	1	1	1	0	0	152.5296	314.9871
14	1	1	1	1	1	1	1	1	1	1	157.2295	531.7113
18	1	1	1	1	1	0	1	1	1	1	157.3756	530.4713
19	1	1	1	0	1	1	1	1	1	1	145.0777	536.2393
20	1	0	1	1	1	1	1	1	1	1	143.0331	379.7914
26	1	1	1	1	1	1	1	0	1	1	154.4995	494.8554

27	1	1	1	1	1	1	1	1	0	0	140.0446	306.6032
28	1	1	1	1	1	1	1	1	0	0	129.1764	324.1661

The ranges of various attributes are different which cannot be compared with the other. To make them in the same range, we need to normalize the values of each attribute in a fixed range (here the normalized range is 0 to 1).The list of cloud provider is normalized based on the best possible value and given value of each attribute. The table 4.5 presents the normalized list of CSP. It can easily be visualized from the graph shown in fig 4.1.

Table 4.5: Normalized list of CSPs

CSP	Security	Total Time	Total Cost
1	0.833333	0.297194	0.127261
2	0.5	0.369567	0.743774
7	1	0.634343	0.000759
9	1	0.296969	0.054525
12	0.5	0.242361	0.964832
14	1	0.089882	0.055742
18	0.833333	0.085141	0.060943
19	0.833333	0.48412	0.036749
20	0.833333	0.55045	0.692998
26	0.833333	0.17845	0.210341
27	0.666667	0.647405	1
28	0.666667	1	0.926329

For the selected CSP's, the rank of each CSP is obtained by applying L_2 metric method on the normalized criteria. The table 4.6 shows the rank of each selected CSP's. The rank of CSPs can be easily visualized from the graph shown in fig 4.2.

Table 4.6: Rank of Selected CSPs

CSP	1	2	7	9	12	14	18	19	20	26	27	28
Rank	1.132	0.844	1.064	1.178	0.908	1.311	1.321	1.105	0.569	1.151	0.485	0.341

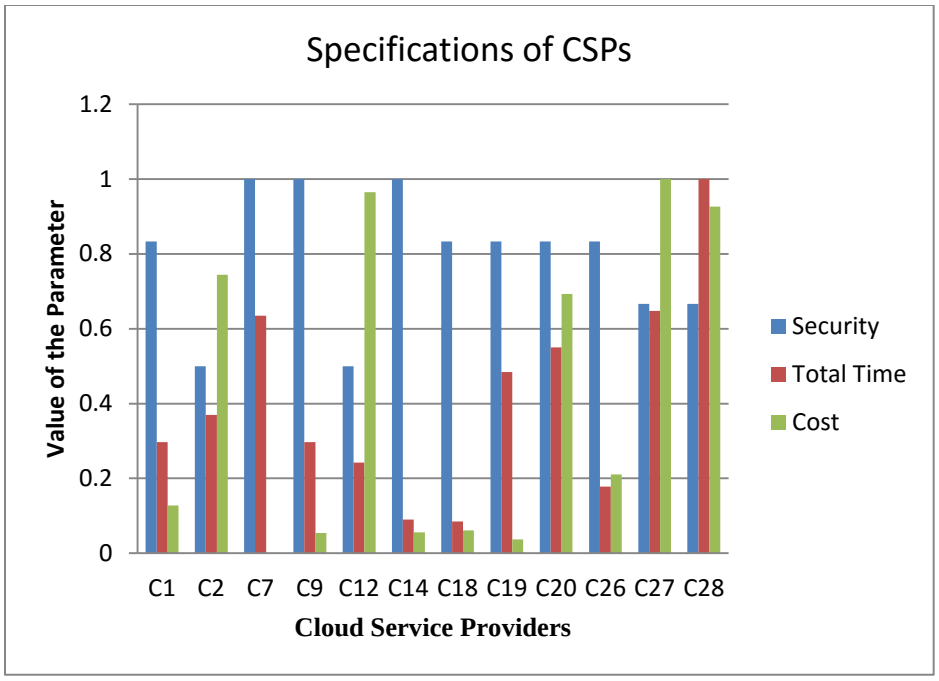


Fig 4.1: Histogram Showing Normalized Cloud Service Provider

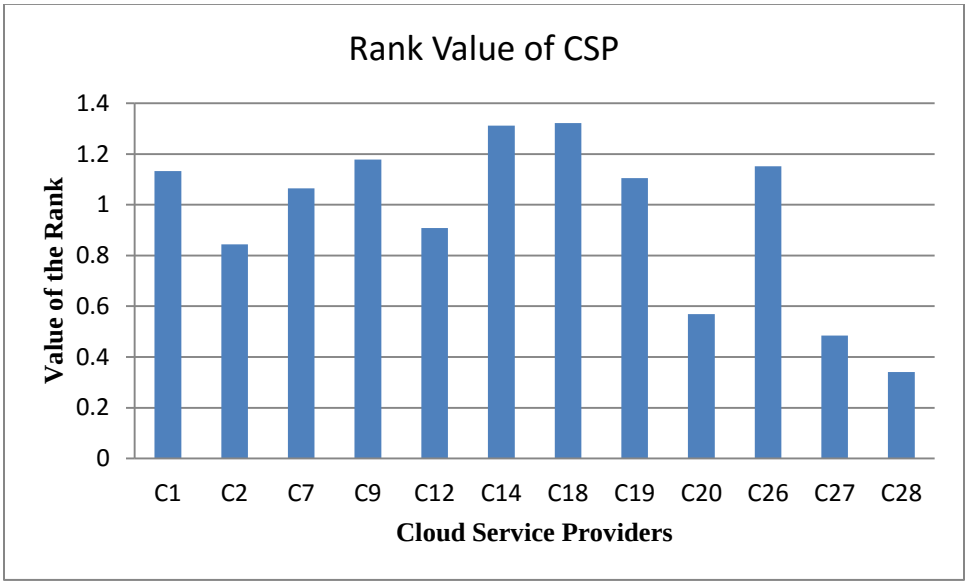


Fig 4.2: Histogram Showing the Rank of Selected CSPs

The rank table is then sorted in ascending order (table 4.7) as the smallest rank is the lowest deviation from the best option and a small number of CSP is chosen for the next step evaluation.

Table 4.7: Rank of CSPs Arranged in Ascending Order

CSP	28	27	20	2	12	7	19	1	26	9	14	18
Rank	0.341	0.485	0.569	0.844	0.908	1.064	1.105	1.132	1.151	1.178	1.311	1.321

From the table 4.7, we select top five CSPs for next step evaluation i.e. on which we apply AHP for the final selection of appropriate CSP. The list of top five CSP is shown in table 4.8.

Table 4.8: Final Selected List of CSPs

CSP	SECURITY										TT	Cost
28	1	1	1	1	1	1	1	1	0	0	129.1764	324.1661
27	1	1	1	1	1	1	1	1	0	0	140.0446	306.6032
20	1	0	1	1	1	1	1	1	1	1	143.0331	379.7914
2	1	1	1	0	1	0	1	1	1	0	148.6086	367.6866
12	1	1	1	0	1	1	1	1	0	0	152.5296	314.9871

4.1.3 Assigning Weights to the Criteria & Ranking of CSPs using Analytical Hierarchical Process (AHP)

Various attributes at each level are assigned priorities according to user specification and matrices are constructed accordingly. The matrix at first level is constructed as shown below.

$$A = \begin{array}{c} \\ Sec \\ TT \\ Cost \end{array} \begin{array}{c} \begin{array}{cccc} Sec & TT & Cost & Prio. \end{array} \\ \begin{bmatrix} 1 & 4 & 7 \\ 1/4 & 1 & 2 \\ 1/7 & 1/2 & 1 \end{bmatrix} \begin{array}{c} 0.7153 \\ 0.1870 \\ 0.0977 \end{array} \end{array}$$

The normalized principal eigen vector gives the priority of each attribute. The comparison matrix is checked for consistency by verifying the value of consistency ratio (CR_A) of comparison matrix.

$$CR_A = 0.0017 \ (< 0.1)$$

The value of CR is less than 0.1 which indicates that the comparison matrix is consistent. There exists only one comparison matrix for security at second level as security has

different parameters (Compliance (CO), Facility Security (FS), Risk Management (RI) and Resiliency (RS)). The matrix constructed by taking value from user is shown below.

$$B = \begin{array}{c} \\ CO \\ FS \\ RI \\ RS \end{array} \begin{array}{c} \begin{array}{cccc} CO & FS & RI & RS \end{array} \\ \begin{bmatrix} 1 & 2 & 3 & 6 \\ 1/2 & 1 & 2 & 3 \\ 1/2 & 1/2 & 1 & 2 \\ 1/6 & 1/3 & 1/2 & 1 \end{bmatrix} \end{array} \begin{array}{c} Prio. \\ 0.4959 \\ 0.2672 \\ 0.1542 \\ 0.0826 \end{array}$$

The comparison matrix B is also found to be consistent as the Consistency Ratio (CR_B)

$$CR_A = 0.0038$$

The comparison matrix B is for first attribute Sec of matrix A. After step 2 the priority vector is as follows.

$$Priority_2 = \begin{bmatrix} 0.3547 \\ 0.1911 \\ 0.1103 \\ 0.0591 \\ 0.1869 \\ 0.0977 \end{bmatrix}$$

There are four comparison matrices at level 3, one for each security attributes for Compliance of size 3 × 3 (Audit Planning (AP), Independent Audits (IA) and Contact/Authority Management (AM)), for Facility Security of size 2 × 2 (User Access (UA) and Secure Area Access (SAA)), for Risk Management of size 2 × 2 (Program (PG) and Policy Change Impacts (CI)) and for Resiliency of size 1 × 1 (Impact Analysis (IA)). At lowest level there are eight comparison matrices of each upper level attributes. All the security parameters are equally important for the user but varies according to the job so the comparison matrices contain all ones. The final priority matrix is of size 12 × 1 and is shown below.

$$Priority\ Vector_{final} = \begin{bmatrix} 0.1182 \\ 0.0591 \\ 0.0591 \\ 0.1182 \\ 0.0956 \\ 0.0956 \\ 0.0552 \\ 0.0552 \\ 0.0296 \\ 0.0296 \\ 0.1870 \\ 0.0977 \end{bmatrix}$$

This vector is used to find the final ranking of Cloud Service Provider (CSP). Based on the data of previous step showing the specifications of the selected CSP, matrices are constructed which yields the priority of one CSP over other. There are 12 requirements, for each one we find a vector showing the efficiency to satisfy the requirement. For each security parameter we construct a matrix showing if the requirement is satisfied or not. The normalized principal eigen vector of the matrix gives the efficiency of that CSP. For Total Time (TT) and Cost, the weighted normalized value represents the efficiency of Cloud Service Provider to satisfy the requirements. There are 5 CSPs considered for this step so the matrices are of size 5 × 5 as shown below:

P_1 =

	C_{28}	C_{27}	C_{20}	C_2	C_{12}	Prio
C_{28}	1	1	1	1	1	0.2
C_{27}	1	1	1	1	1	0.2
C_{20}	1	1	1	1	1	0.2
C_2	1	1	1	1	1	0.2
C_{12}	1	1	1	1	1	0.2

P_2 =

	C_{28}	C_{27}	C_{20}	C_2	C_{12}	Prio
C_{28}	1	1	1	1	1	0.2
C_{27}	1	1	1	1	1	0.2
C_{20}	0	0	0	0	0	0
C_2	1	1	1	1	1	0.2
C_{12}	1	1	1	1	1	0.2

P_3 =

	C_{28}	C_{27}	C_{20}	C_2	C_{12}	Prio
C_{28}	1	1	1	1	1	0.2
C_{27}	1	1	1	1	1	0.2
C_{20}	1	1	1	1	1	0.2
C_2	1	1	1	1	1	0.2
C_{12}	1	1	1	1	1	0.2

P_4 =

	C_{28}	C_{27}	C_{20}	C_2	C_{12}	Prio
C_{28}	1	1	1	1	1	0.3
C_{27}	1	1	1	1	1	0.3
C_2	1	1	1	1	1	0.3
C4	0	0	0	0	0	0
C_{12}	0	0	0	0	0	0

P_5 =

	C_{28}	C_{27}	C_{20}	C_2	C_{12}	Prio
C_{28}	1	1	1	1	1	0.2
C_{27}	1	1	1	1	1	0.2
C_{20}	1	1	1	1	1	0.2
C_2	1	1	1	1	1	0.2
C_{12}	1	1	1	1	1	0.2

P_6 =

	C_{28}	C_{27}	C_{20}	C_2	C_{12}	Prio
C_{28}	1	1	1	1	1	0.25
C_{27}	1	1	1	1	1	0.25
C_{20}	1	1	1	1	1	0.25
C_2	0	0	0	0	0	0
C_{12}	1	1	1	1	1	0.25

P_7 =

	C_{28}	C_{27}	C_{20}	C_2	C_1	Prio
C_{28}	1	1	1	1	1	0.2
C_{27}	1	1	1	1	1	0.2
C_{20}	1	1	1	1	1	0.2
C_2	1	1	1	1	1	0.2
C_{12}	1	1	1	1	1	0.2

P_8 =

	C_{28}	C_{27}	C_{20}	C_2	C_{12}	Prio
C_{28}	1	1	1	1	1	0.2
C_{27}	1	1	1	1	1	0.2
C_{20}	1	1	1	1	1	0.2
C_2	1	1	1	1	1	0.2
C_{12}	1	1	1	1	1	0.2

P_9 =

	C_{28}	C_{27}	C_{20}	C_2	C_{12}	Prio
C_{28}	0	0	0	0	0	0
C_{27}	0	0	0	0	0	0
C_{20}	1	1	1	1	1	0.5
C_2	1	1	1	1	1	0.5
C_{12}	0	0	0	0	0	0

P_{10} =

	C_{28}	C_{27}	C_{20}	C_2	C_{12}	Prio
C_{28}	0	0	0	0	0	0
C_{27}	0	0	0	0	0	0
C_{20}	1	1	1	1	1	1
C_2	0	0	0	0	0	0
C_{12}	0	0	0	0	0	0

The priority of each vector is used to construct an Individual Priority matrix ($Prio_{ind}$). As there are 12 attributes (10 security attributes, TT and Cost) and 5 CSPs, so the size of $Prio_{ind}$ is 5 × 12. The priority of each criterion can be easily visualized by the graph as shown in fig 4.3. The resulting matrix is given below.

$Prio_{ind}$ =

	CO 01-1	CO 02-1	CO 02-3	CO 04-1	FS 02-1	FS 04-1	RM 01-2	RM 04-1	RS 02-1	RS 02-3	TT	COST
C_{28}	0.2	0.25	0.2	0.33	0.2	0.25	0.2	0.2	0	0	0.1811	0.1914
C_{27}	0.2	0.25	0.2	0.33	0.2	0.25	0.2	0.2	0	0	0.1963	0.1811
C_{20}	0.2	0	0.2	0.33	0.2	0.25	0.2	0.2	0.5	1	0.2005	0.2243
C_2	0.2	0.25	0.2	0	0.2	0	0.2	0.2	0.5	0	0.2083	0.2171
C_{12}	0.2	0.25	0.2	0	0.2	0.25	0.2	0.2	0	0	0.2138	0.1860

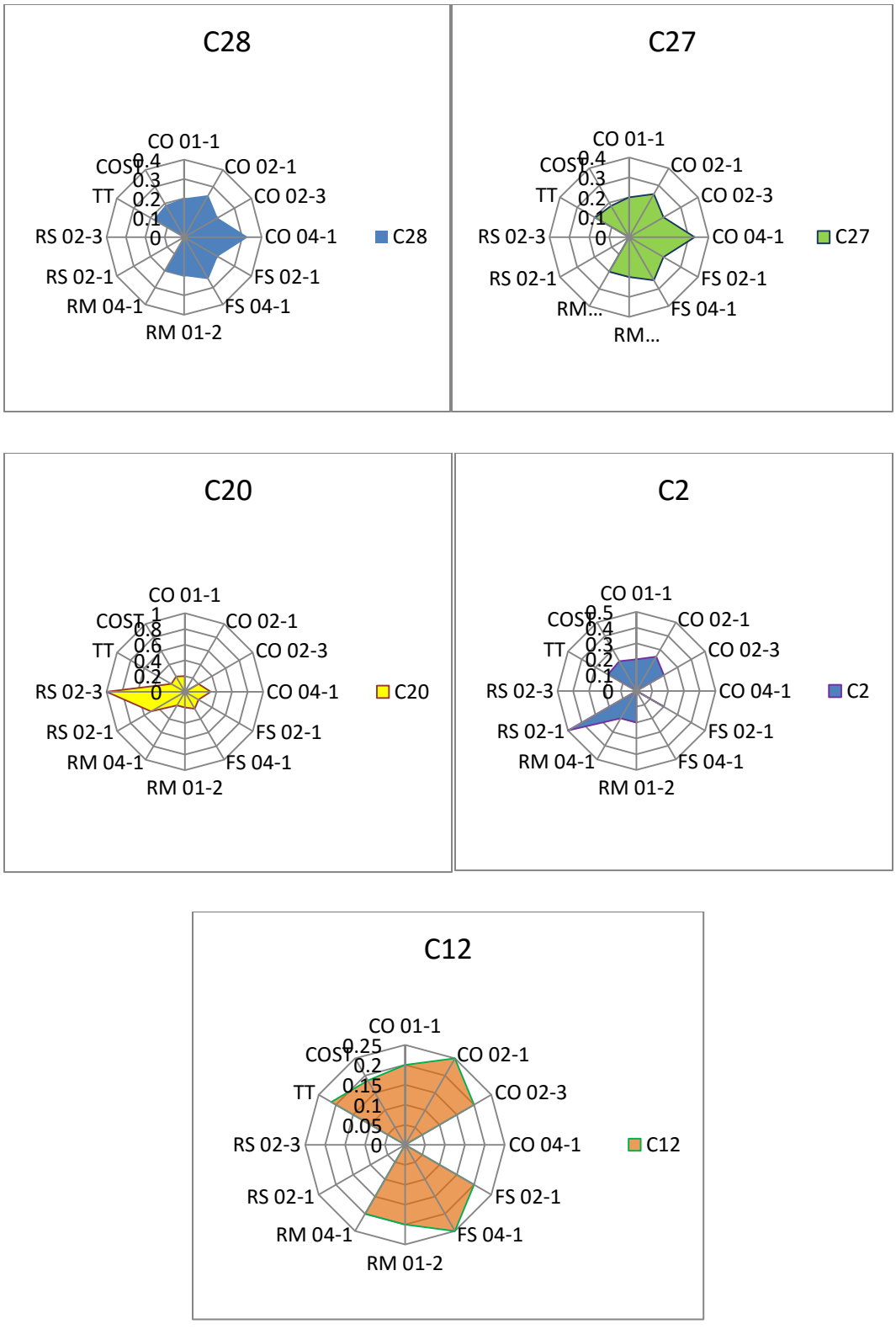


Fig 4.3: Radar Graph Showing the Characteristics Satisfied by CSP

The final rank of CSPs is calculated by multiplying Priority vector by $Prio_{ind}$ and is calculated as shown below.

$$Rank_{final} = Prio_{ind} \times Priority\ Vector_{final}$$

$$Rank_{final} = \begin{matrix} C_{28} \\ C_{27} \\ C_{20} \\ C_{2} \\ C_{12} \end{matrix} \begin{bmatrix} 0.2073 \\ 0.2091 \\ 0.2437 \\ 0.1664 \\ 0.1735 \end{bmatrix}$$

4.1.4 Final Selection of CSP for User's Job

From the vector$Rank_{final}$, it is clear that the final rank of C_{20} is highest among all. So the Cloud Service Provider 20 is chosen for the user's job. The graph 4.4 shows the priority significance of the cloud service providers. It can be clearly visualized that the CSP C_{20} has the highest rank value so is considered as the best choice.

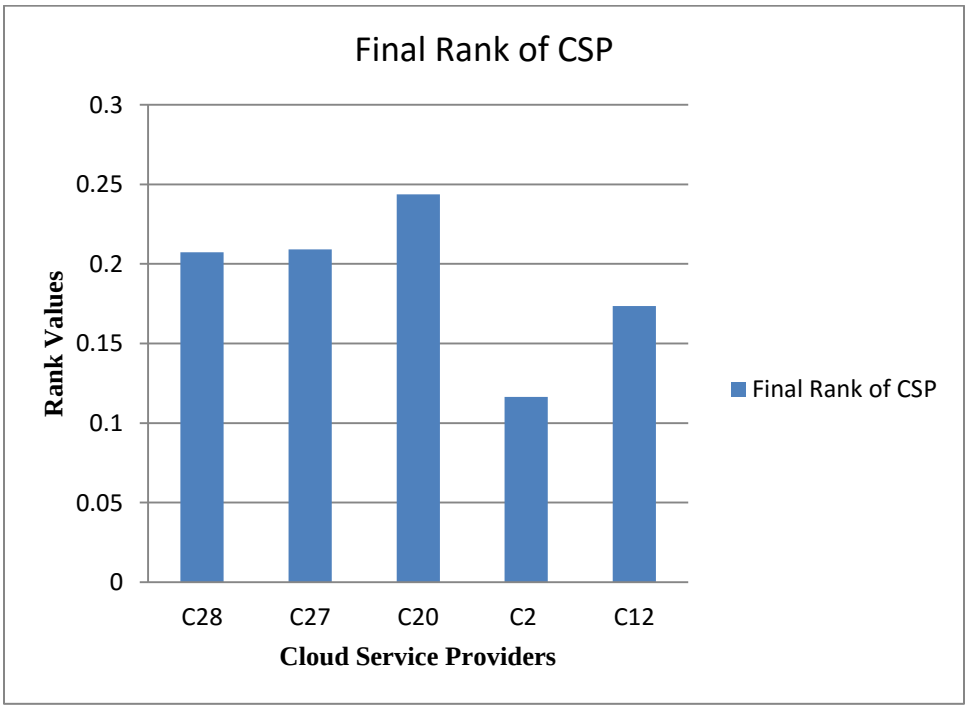


Fig 4.4: Graph Showing the Final Rank of CSPs

4.2 Conclusion

The case study analyses the effectiveness of the proposed framework. The experiment shows that the task is searched for the most appropriate CSP for the execution. The final rank gives the priority of top selected CSP. The CSP with the highest rank value is chosen for the execution of the task.

Chapter 5

CONCLUDING REMARKS

Cloud computing is the most emerging paradigm in contemporary computing. It is equipped with various advantages but some crucial issues such as security, resource provisioning, interoperability, etc. are also associated with this. There are numerous cloud providers present in the market and the number is continuously increasing. Different cloud provider offers services with varying performance attributes and cost. For a user, there are number of jobs and it is very difficult to select appropriate cloud provider for all the jobs. Even for one job, it is very difficult to select a cloud provider as the specifications of each cloud provider is unique and it is just difficult to compare them.

This chapter draws a concluding remarks towards the work done in this dissertation.

5.1 Conclusion

This dissertation work considers the issue of security and resource provisioning and proposes a framework which addresses these issues. It addresses various security parameters along with other QoS parameters for the selection of a cloud service provider. An AHP L_p metric based model is proposed which can evaluate the services of the cloud providers based on different criteria and their contribution in selecting the CSP. It is based on the priority value as defined by the user and is not affected by the variability in the range of the values of each attribute. AHP can perform well on small data set so a method is used to reduce the data space. L_p metric method is found to be a good choice to reduce the size of the data space so that AHP can perform well.

The case study shows the working of the proposed model in real environment. Various security parameters are considered with total time and cost for the selection of a particular CSP. In the first step of the model screening process is employed and the cloud service provider which satisfies the minimum user requirement is selected. In the second step, L_p metric method is applied and the data space is reduced to a smaller space which

is easily manageable. In third step, AHP examines all the attributes and find a rank for all the CSPs based on the user specification and the CSP information. In the last step, the CSP with maximum rank is selected for the user's job.

A case study on the real data set for the Cloud has been done in this work. It clearly shows the selection of appropriate cloud service provider for a user job. Among a number of available CSPs, the CSP that best suites the requirement in least cost is selected.

5.2 Future Work

This dissertation work addresses the resource provisioning model which provides best CSP according to the varying user's job demand. The future work considers the bidirectional utilization i.e. the job gets best CSP in least cost as well as the CSP get best job for maximum benefit. The future work also proposes to incorporate more attributes for the evaluation. Some more multi criteria decision making methods are intended to be employed for the evaluation process.

References

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," *Nist Spec. Publ.*, vol. 145, pp. 1-7, 2009.

[2] E. G. Report, "The Future Of Cloud Computing," *Commission of the European Communities, Information Security & Media Directorate-General*. 2010.

[3] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R Katz, A Konwinski, G Lee, D. PatterSon, A Rabkin and I. Stoica, "Above the Clouds: A Berkeley View of Cloud Computing," *Univ. California, Berkeley, Tech. Rep. UCB* , pp. 07–013, 2009.

[4] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-Oriented Cloud computing: Vision, Hype, and Reality for Delivering IT services as Computing Utilities," in *Proceedings - 10th IEEE International Conference on High Performance Computing and Communications, HPCC 2008*, pp. 5–13, 2008.

[5] I. M. Abbadi, *Cloud Management And Security*, 1st ed. John Wiley and Sons Ltd, 2014.

[6] "Centre4Cloud," [Online]. Available: http://www.centre4cloud.nl/ nl/kennis-ont wikkeling/definition-cloud-computing/deployment-models/, Feb-2015.

[7] N. Khan and M. S. Husain, "A Survey on Elasticity in Cloud Computing," in *2015 IEEE International Conference on Engineering and Technology (ICETECH)*, pp. 248–250, 2015.

[8] J. Baliga, R. W. A. Ayre, K. Hinton, and R. S. Tucker, "Green Cloud Computing: Balancing Energy in Processing, Storage and Transport," in *Proceedings of the IEEE* 2010, vol. 99, no. 1, pp. 149–167, 2010.

[9] M. Armbrust, I. Stoica, M. Zaharia, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, and A. Rabkin, "A View of Cloud Computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[10] W. Kim, "Cloud Computing : Today and Tomorrow," *J. Object Technol.*, vol. 8, no. 1, pp. 65–72, 2009.

[11] T. Dillon, W. C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," in *2010 24th IEEE International Conference on Advanced Information Networking and Applications (AINA)*, pp. 27–33, 2010.

[12] N. Gonzalez, C. Miers, F. Redigolo, T. Carvalho, M. Simplicio, M. Naslund, and M. Pourzandi, "A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing," *J. Cloud Comput. a Springer Open J.*, vol. 1, no. 11, pp. 231–238, 2011.

[13] V. J. R. Samani, B. Honan and J. Reavis, *CSA Guide to Cloud Computing*, 1st ed. Elsevier Inc., 2015.

[14] Cloud Security Alliance, "The Notorious Nine Cloud Computing Top Threats in 2013," *Top Threats Working Group*, pp. 1–21, 2013.

[15] M. Sugumaran, B. B. Murugan, and D. Kamalraj, "An Architecture for Data Security in Cloud Computing," in *Proceedings - 2014 World Congress on Computing and Communication Technologies, WCCCT 2014*, pp. 252–255, 2014.

[16] K. L. Ossian, Miller, Canfield, Paddock and Stone PLC "Cloud Computing : Managing Legal Risks and Ethical Issues," *Institute of Continuing Legal Education*, vol. 399, pp. 1–8, 2013.

[17] J. Timmermans, V. Ikonen, B. C. Stahl and E. Bozdag "The Ethics of Cloud Computing A Conceptual review," in *Proceedings - 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom)*, pp. 614-620, 2010.

[18] M. Behrendt, B. Glasner, P. Kopp, R. Dieckmann, G. Breiter, S. Pappe, H. Kreger, and A. Arsanjani, "Cloud Computing Reference Architecture v2.0," *CCRA team IBM*, vol. 1, pp. 1–96, 2011.

[19] J. Orea et al., "Quick Guide to Reference Architecture: Trusted Cloud Initiative (TCI)." Cloud Security Alliance, pp. 1–22, 2011.

[20] Y. Hu, J. Wong, G. Iszlai, and M. Litoiu, "Resource Provisioning for Cloud Computing," in *Proceedings of the 2009 Conference of the Center for Advanced Studies on Collaborative Research*, pp. 101–111, 2009.

[21] S. K. Garg, S. K. Gopalaiyengar, and R. Buyya, "SLA-based Resource Provisioning for Heterogeneous Workloads in a Virtualized Cloud Datacenter," *Algorithms Archit. Parallel Process. Springer Berlin Heidelb.*, vol. 1, pp. 371–384, 2011.

[22] Q. Zhu and G. Agrawal, "Resource Provisioning with Budget Constraints for Adaptive Applications in Cloud Environments," in *Proceedings of the 19th ACM International Symposium on High Performance Distributed Computing*, pp. 1–12, 2010.

[23] R. Buyya, S. K. Garg, and R. N. Calheiros, “SLA-Oriented Resource Provisioning for Cloud Computing: Challenges, Architecture, and Solutions,” in *Proceedings - 2011 International Conference on Cloud and Service Computing, CSC 2011*, no. 1, pp. 1–10, 2011.

[24] S. Ding, C. Xia, Q. Cai, K. Zhou, and S. Yang, “QoS-Aware Resource Matching and Recommendation for Cloud Computing Systems,” *Appl. Math. Comput.*, vol. 247, pp. 941–950, 2014.

[25] C. Liu, X. Zhang, C. Yang, and J. Chen, “CCBKE - Session Key Negotiation for Fast and Secure Scheduling of Scientific Applications in Cloud Computing,” *Futur. Gener. Comput. Syst.*, vol. 29, no. 5, pp. 1300–1308, 2013.

[26] S. K. Garg, S. Versteeg, and R. Buyya, “A Framework for Ranking of Cloud Computing Services,” *Futur. Gener. Comput. Syst.*, vol. 29, no. 4, pp. 1012–1023, 2012.

[27] A. Taha, R. Trapero, J. Luna, and N. Suri, “AHP-Based Quantitative Approach for Assessing and Comparing Cloud Security,” in *The IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom2014) & The IEEE International Conference on Big Data Science and Engineering (BDSE 2014), 24th -26th Sept, Beijing*, pp. 1–8, 2014.

[28] E. D. Michel and M. Deza, “Metrics on Normed Structures,” in *Encyclopedia of Distances*, 2nd ed., pp. 89–99, 2013.

[29] T. L. Saaty, “Axiomatic Foundation of the Analytic Hierarchy Process,” *Manage. Sci.*, vol. 32, no. 7, pp. 841–855, 1986.

[30] T. L. Saaty, “The Analytic Network Process – Dependence and Feedback in Decision-Making: Theory and Validation Examples,” *in Business Applications and Computational Intelligence*, pp. 360–388, 2006.

[31] A. K. Rifai, “A Note on the Structure of the Goal Programming Model: Assessment and Evaluation,” *Int. J. Oper. Prod. Manag.*, vol. 16, no. 1, pp. 40–49, 1996.

[32] G. W. Wei, “GRA Method for Multiple Attribute Decision Making with Incomplete Weight Information in Intuitionistic Fuzzy Setting,” *Knowledge-Based Syst.*, vol. 23, no. 3, pp. 243–247, 2010.

[33] E. Triantaphyllou, “Multi-criteria Decision Making Methods: A Comparative Study,” *Springer US*, vol. 44, no. 1, pp. 5–21, 2005.

[34] J. Rezaei, “Best-Worst Multi-Criteria Decision-Making Method,” *Omega, Elsivier*, vol. 53, no. 1, pp. 49–57, 2015.

[35] X. Xu, “The SIR method : A Superiority and Inferiority Ranking Method for Multiple Criteria Decision Making q,” *Eur. J. Oper. Res.*, vol. 131, no. 1, pp. 587–602, 2001.

[36] T. L. Saaty, “How to Make a Decision: The Analytic Hierarchy Process,” *Eur. J. Oper. Res.*, vol. 48, no. 1, pp. 9–26, 1990.

[37] T. L. Saaty, “Decision-making with the AHP: Why is the Principal Eigenvector Necessary,” *Eur. J. Oper. Res.*, vol. 145, no. 1, pp. 85–91, 2003.

[38] N. Bronson and R. Teaneck, 32.Matrix Methods: An Introduction, 2nd ed. United States of America: Academic Press, INC. An impression of Elsevier, 1991.

[39] D. Ergu, G. Kou, Y. Peng, and Y. Shi, “A Simple Method to Improve the Consistency Ratio of the Pair-wise Comparison Matrix in ANP,” *Eur. J. Oper. Res.*, vol, 213, no. 1, 246-259, 2011.

[40] 'Cloud Security Alliance (CSA), Consensus Assessments Initiative (CAI) Questionnaire," 2012. [Online]. Available: https://cloudsecurityalliance.org/ research/initiatives/consensus-assessments-initiative/, Feb 2015.

[41] A. Iosup, S. Ostermann, N. Yigitbasi, R. Prodan, T. Fahringer, and D. Epema, “Performance Analysis of Cloud Computing Services for Many-Tasks Scientific Computing,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 6, pp. 931–945, 2011.