IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 10, December 2014.
www.ijiset.com
ISSN 2348 – 7968

Towards an Extensive Survey on Legal Issues in Cloud Service Negotiation Techniques

Vijayasanthi M[1], Jaya Chandra S[2] and Chandrakanth M[3]

[1] CSE, AU/SVCE/Company Name,
Sriperumbudur, 602105, India

[2] EEE, JNTUA/YITS/Company Name,
Tirupati, 517507, India

[3] CSE, JNTUA/YITS /Company Name,
Tirupati, 517507, India

Abstract

The Abstract— Cloud computing is a subscription based service from which the networked storage space and the resources can be obtained. Collaborations in multiple institutions are increasing due to the world wide deployment of more cloud. Cloud uses more resource than the grid. Multiple computing resources from different clouds require in negotiation so resource co allocation is essential for Cloud vision. Resources demand and supply can be dynamic in cloud. Resource negotiation (exchange of trading of resource between clouds) enables cloud participants to face an unstable requirement environment. Consumer and provider need to agree negotiating the cloud-legal issues in cloud computing service-level agreements through negotiation for cloud resource reservation. The aim of this paper is to present a survey of challenges and current state of resource negotiation. In particular we show the different agent based methods for cloud negotiation. The most advanced agent cloud coordinator will able to deliver Quality of Service (QoS) for cloud provider. It allows an increase in performance, reliability and scalability of applications.

Keywords:—*Cloud Computing, Cloud Negotiation, Negotiation Agent, Resource Management.*

1. Introduction

Cloud computing provide illustration of resources. Resource management is done by load balancing and scalability. Key feature of cloud computing is virtualization. Negotiation based on Service Level Agreement (SLA) is an agreement between service providers and service consumers. All resources are rented using cloud computing and utility computing but in cloud computing the company have less knowledge about source of the services. In negotiation mechanism, agents negotiate over both contract price and commitment [3].

Negotiation activities are needed for establishing contracts and resolving difference between consumer and provider in resource allocation [6]. In negotiation mechanism, an agent make contract between provider and consumer for a fixed time interval. Negotiation evaluation is conducted on simulation test bed.

The rest of the paper is structured as follows: Session2 motivates the need for resource negotiation.Session3 present the challenges and current state. Session4 constitute of comparison about the different negotiation mechanism.

2. Cloud Resources

Cloud is environmental friendly and promotes telecommuting techniques. Cloud provides a platform where three elements such as Infrastructure as a service (IaaS), Platform as a Service (PaaS) and Software as a service (SaaS) to provide the requirements of the customer in most efficient manner. In cloud shared resources, software, and information are provided to computers as a metered service. IaaS providers give a virtual server to start, stop, and access and configure an online storage. This allow a company to pay only as much capacity as needed. PaaS providers host a set of software and product development tools as online infrastructure, to allow the developers the ability to create applications on platform. SaaS provides no investment in servers or software licensing. Desktop as a Service (DaaS) is an emerging service which deals with providing a whole desktop experience over the internet. It is also referred as desktop virtualization [13].

Elasticity means that platform can handle sudden, unanticipated and extraordinary loads. Scalability is a planned level of capacity with ability to scale in a quick

ISSN 2348 – 7968

and easy manner when need more or less resources. Data integrity is a property that ensures that the data is of high quality, correct, consistent and accessible. Reliability is the ability to perform and maintain its function in routine as well as unexpected circumstances.

Resource allocation is very important for virtualization platform. Resource allocation can be done based on the information from different domains. It depends on bandwidth and time. In the method of weighted allocation, all the domains are of same weight. It provides a better scheduling and performance. Resource allocation considers the factors such as resource cost, resource reliability, execution time and bandwidth. Different type allocation algorithms are used in cloud for allocating resources.

3. Cloud Negotiation

Cloud computing is powerful, since it does not rely on any one source. Cloud may look like virtualization because it appears that the application is running on a virtual server detached from any connection to a single physical host. Virtualization is part of a physical infrastructure and technique which allow running more than one server on same hardware component.

With cloud computing, the software programs are stored on servers placed elsewhere and it is accessed via the internet. Even if the computer crashes, then software is available for users. In virtualization technique, one physical computer is pretending to be many computing environments whereas in cloud computing, many different computers pretending to be the one computing environment.

The selection of negotiation protocol determines the scope of information flow which in turn influences the changes upon the agreement. The fundamental phases of business transaction are product offers and discovery, negotiation process, payment activities, and the delivery of the product to customers.

A negotiation coordinator is responsible for coordinating the actions taken by its various negotiation phases. An important feature of negotiation model is simultaneous negotiation of many buyer-seller pairs [7]. Accessing several resources by multiple resource providers is a challenging task for consumers. Grid calls for a shared environment on a computer system from multiple administrative domains. Both grid and cloud provide scalability. Cost of deploying is also high. Cloud computing is an abstraction of traditional server hosting applications. Instead of buying server, the server is taken for lease from a vendor to run and manage the system in data center.

Negotiation mechanism differs from auction. Negotiation focus on cooperating to create the value of objects while auction determining the object's unknown value [8].

Negotiation agents play very important role in the mechanism [4]. Agent acts as a bridge between different networks and creates an infrastructure. Business infrastructure coordinates the dealers. Resource management is central to the operations. Conflicting request from multiple cloud participants are hard to manage. In order to achieve high system utilization, the negotiation is conducted [5].

Negotiation among cloud resource providers and cloud applications are unavoidable due to the following reasons:

1. To maximize the selling of providers and minimize the price payment by consumers
2. To balance the market of cloud services [2]
3. To obtain a contract for provisioning of resources

4. Negotiation Agent

Provider agent and consumer agent are present in a negotiation environment. Both the agents register in cloud market registry. From the registry users get agent's information. Agents are used for the negotiation mechanism. Provider agents are responsible for giving advertisement of service and consumer agent discovers the services from the test bed.

Simulations are done periodically. Negotiator manages Service Level Agreement (SLA). Negotiators are the mediators between consumers and providers [9]. Agents concentrated on time, price, market factors such as competition and opportunity [15]. Negotiation protocol for the negotiation mechanism evaluates offers until both agreements will be reached. Customer satisfaction is necessary for cloud computing. Different Quality of Levels

is provided for services. Negotiation fails when agent's deadline expires before reach an agreement.

5. Issues Of Cloud Negotiation Mechanism

1) Decrement in the cost of resources
2) Dynamic demand for resources
3) Resource availability
4) Reservation of resources

ISSN 2348 – 7968

Key Legal Issues

5.1. Protection of Information Privacy

Information about the privacy obligations for Commonwealth contracts can be found on the

Office of the Australian Information Commissioner's (OAIC) website. Agencies are also strongly advised to consider the Better Practice Guide–Privacy and Cloud Computing for Australian Government Agencies9before entering into any cloud computing arrangement.

Cloud computing does not necessarily have to be privacy invasive, but moving data into the cloud means that the data will move outside of the direct control of the agency and may, in some instances, be processed and stored outside of Australia. Different levels of indirect control of this data are possible depending on the type of cloud service selected and the legal protections put in place by the agency.

Agencies need to be aware of their privacy and data security obligations when transferring personal information into any cloud environment. If privacy issues cannot be adequately addressed, the OAIC advises that it will not be appropriate to transfer 'personal information' into a public cloud.

Section 95B of the Privacy Act 1988 requires agencies entering into contracts for the provision of services to the Commonwealth, to:

- take contractual measures to ensure contracted services providers do not do an act or engage in a practice that would breach any Information Privacy Principles (IPPs)
- Ensure agreements do not authorize providers or their subcontractors to do or engage in an act or practice that would breach any IPPs, if done or engaged in by the agency itself.

In addition, agencies should ensure that the provider is contractually prohibited from using the data for any of the provider's own purposes – such as advertising or other commercial services – as this is likely to be inconsistent with the IPPs and the intentions of the agency in entering the agreement.

Agencies engaging cloud service providers need to take appropriate contractual measures to ensure personal information is protected, regardless of whether or not the provider (and any subcontractors) are based in Australia or overseas. When contracting offshore, agencies need to take particular care to ensure they are able to enforce the provisions of the agreement.

Agencies should also consider the practical implications of their Privacy Act obligations, including whether specific contractual measures enabling them to meet their obligations are required. For example, IPP 7 *Alteration of records containing personal information* requires agencies, where an individual's request to alter a record has been refused, to attach a statement to the record on request. Agencies would need to ensure that a cloud service provider is obliged to meet this requirement.

5.2. Future Privacy Compliance

From March 2014, 13 new Australian Privacy Principles (APP's) will apply to both the public and private sector. For Australian Government agencies these APP's will replace the current IPP's. The APP's are structured to reflect the information life cycle from notification and collection, through to use and disclosure, security, access and correction.

While the changes to the Privacy Act will not take effect until March 2014, agencies should start preparing now to ensure compliance with the new APP's. This may include considering the impact of the APPs in any cloud computing procurements agencies anticipate undertaking.

The OAIC will produce detailed guidance published on the OAIC website to assist agencies to understand the impact of the reforms and make the necessary changes to agency information handling practices.

5.3. Security

Clearly one significant issue for any cloud computing agreement where the provider holds, or is able to access, an agency's data is the security of that data. This issue is heightened from a risk perspective where the data is sensitive (including personal information).

Agencies should refer to the Defense Signals Directorate's Cloud Computing Security Considerations for detailed guidance on issues to consider from a security perspective. In following this guidance, agencies should develop a comprehensive risk assessment to make an informed decision on the suitability of adopting a cloud based solution and assess the appropriate security protections it requires. The following are contractual measures that may, depending on the circumstances including the type of cloud service used, be appropriate to include in an agreement for cloud computing services:

- where the service is to be provided from a location within Australia, a prohibition on the provider transmitting data outside of Australia without the prior approval of the agency
- he level of security and encryption to be applied to agency data held and transmitted by the provider

ISSN 2348 – 7968

- he level of access security protocols to be implemented by the provider to defeat unauthorized attempts to access the data by third parties, provider personnel and other customers of the provider
- here physical media is damaged and replaced, requirements for the sanitization or deletion of data in the damaged media
- the storage of separate packages of data – for example, it may be important to avoid the provider aggregating separate packages on the same hardware (as such aggregation may increase the sensitivity of data or risks to security of the information)
- a requirement for the provider to notify the agency immediately in the event of security incidents or intrusions, or requests from foreign government agencies for access to the data, to enable the agency to manage these events proactively
- a requirement for the provider to store data so as to prevent other customers of the provider from accessing the agency's data. For less sensitive data, logical separation supported by strong technical security measures (where data may be held on the same servers as other customer data) may be sufficient. If the data is more sensitive, storage on specified hardware that is unique to the agency may be appropriate so that there can be physical security precautions set up between the hardware storing the agency's information and other hardware held by the provider
- a requirement for the provider to destroy or sanities (or de-identify in the case of personal information) sensitive information held by the provider at the end of the agreement, where such data is not or cannot be returned to the agency. This may need to extend to destruction of physical hardware on which such data is held to avoid risk that the data may be recovered
- Specific security requirements depending on the nature of the service and the sensitivity of the data.

5.4. Confidentiality

An agency may have contractual, equitable or statutory obligations to keep particular information confidential. Therefore it is important that these obligations are also transmitted to the provider in circumstances where the provider is storing or accessing an agency's data.

In most cases, an agency will want a provider to meet a minimum level of confidentiality for the agency's information. In cases where the provider is obtaining access to particularly sensitive information, the level of protection will need to be significantly stronger.

Where an agreement requires an agency to maintain provider information as confidential, agencies should be aware of Commonwealth policies which require: w

- restricting the type of provider information that is subject to confidentiality
- the inclusion of standard Commonwealth exceptions to confidentiality including the right to provide information to the relevant minister as well as houses of Parliament

5.5. Records Management Requirements

Agencies should refer to Records management and the cloud - a checklist prepared by the National Archives of Australia for records management considerations in cloud computing. That advice requires agencies to include appropriate controls and protections (for example through agreement with the cloud service provider) that match the value of the records and address the risks of cloud computing for an agency's records.

5.6. Audit

All the protections described in this section may potentially be worthless unless the agency is able to confirm that required information protection requirements are in fact being met. Audit of cloud computing arrangements is one way of checking compliance. Audit of such arrangements is however potentially complicated by:

- the location of the data – which, unless specifically identified and locked down in the agreement, may be unknown to the agency, and could be located in one or more discrete sites in foreign countries
- the nature of cloud computing itself which may involve agency data being spread across a large number of different provider computing devices (in order to harness the economies of scale and on-demand provision of computing that cloud computing services offer).

As a result, agencies should consider including the following rights in any agreement:

- restricting the locations/countries in which agency data may be held (with movement to new locations permitted with advance approval in writing from the agency)
- rights to audit the provider's compliance with the agreement including rights of access to the

ISSN 2348 – 7968

provider's premises where relevant records and agency data is being held

- audit rights for the agency (or its nominee), the Auditor-General and the Information Commissioner
- right for the agency to appoint a commercial auditor as its nominee (as this allows the agency to appoint an auditor in the same location as the provider's data center to save costs and ensure compliance with relevant jurisdictional laws)
- where technically available, the right for the agency to remotely monitor access to its data and where this is not possible, a requirement that the provider maintain an audit log of access to the agency's data and provide that log to the agency on request.

5.7. Compensation for Data Loss/Misuse

It is possible that data could be permanently lost by a cloud computing services provider in a number of circumstances such as technical or operator error as well as fire or other disasters. Similarly, there is always the risk of misuse of data by rogue employees of the provider or compromise by external parties.

While the probability of such problems can be minimized by the provider ensuring offsite data back-up, proper technical and security training and hardware maintenance, it is important for an agency to consider how to address data loss or misuse in its agreement with the provider.
This is particularly the case where the data is provided by third parties (such as members of the public) and the agency risks legal liability in the event data is unrecoverable or used inappropriately.

An agency, in determining the risks posed by a cloud computing arrangement, should consider which party is best placed to manage those risks and therefore whether the agreement with the cloud service provider should:

- require the provider to be responsible for indirect and consequential losses (which will typically be the type of losses that flow from data loss and misuse)
- include an indemnity from the provider in respect to data loss or misuse as a result of the negligent, illegal or will fully wrong act or omission of the provider or its personnel
- have a separate liability cap for data loss or misuse that is sufficiently high to cover potential liability arising from such loss or misuse

For more detail on the above terms, refer to the Liability section of this guide.

5.8. Subcontractors

A critical component of ensuring that an agency has proper protection for its information is to ensure, in the agreement with the provider, that any subcontractors of the provider are also obliged to meet the same requirements as the provider. If this is not done, an agency may find that any protections it has negotiated into the agreement with the provider do not end up giving it the desired protection where the services are carried out by subcontractors. It will also be important to know who a provider's subcontractors are so that an agency understands what companies may have access to the agency's systems and data.

5.9. Liability

5.9.1. Limitations on Liability

In common with traditional information technology agreements, cloud service agreements typically seek to minimize the provider's liability for any loss that arises from the provision of the service. This may include:

- excluding indirect and consequential losses (such as data loss)
- setting low liability caps (typically equivalent to one year's fees under the agreement) or in some cases excluding liability entirely
- not excluding key types of liability from any liability cap

Agencies should seek to comply with the Commonwealth's policy on capping supplier liability in information technology contracts (see Finance Circular 2006/03) when negotiating limitations with providers. The starting point is that the Commonwealth will accept a cap on the provider's liability as a default position in information technology contracts provided that a list of exceptions to the cap is agreed by the provider. These exceptions are:

- personal injury (including sickness and death)
- loss or damage to tangible property
- breach of privacy, security or confidentiality obligations
- intellectual property infringement
- unlawful, or illegal, acts or omissions

In addition to the standard exceptions, agencies should consider whether the risks of their procurement justify additional protection such as including the following as exceptions to a provider's liability cap:

ISSN 2348 – 7968

- loss caused by service interruption
- data loss
- misuse of data

Decisions made by agencies about the amount of any liability cap should be informed by a risk assessment that examines all identifiable potential liabilities and determines the likelihood and effect of such risks being realized.

5.10. Indemnity

An indemnity is a legally binding promise by which one party undertakes to accept the risk of loss or damage another party may suffer. In some cloud computing service agreements the provider will require an indemnity from the agency. These typically might include indemnities for:

- infringement of a third party's rights (including privacy and intellectual property rights) by the provider as a result of the provider's processing of third party data supplied by the agency
- any loss or damage arising from the agency's use of the service
- breach of the agreement by the agency

Agreeing to give an indemnity may expose an agency to the risk of liability or costs that it would not otherwise be liable for. Indemnities given by an agency must comply with:

- the Commonwealth's indemnity guidelines – these guidelines make clear that agencies should only give indemnities where the expected benefits outweigh the level and cost of risk being accepted and that generally the party best placed to manage a risk should bear that risk
- the FMA Act and Regulations – an indemnity will form a contingent liability that may require an FMA agency to obtain agreement under FMA Regulation 10

- For further details on the handling of liability caps and indemnities, agencies can refer to AGS Legal Briefing 93 - Indemnities in Commonwealth Contracting.

5.11. Performance Management

5.11.1. Service Levels

Service levels are an important way of ensuring that a provider meets the level of service expected by the agency. This is particularly important where the cloud computing service is Critical either to the functioning of an agency or to the agency's clients. There are three elements common to an effective service level regime:

- The service levels have to be meaningful – that is, they need to measure performance that is important to the agency.
- The provider's performance against service levels should be able to be easily measured and auditable.
- The incentive (whether stick or carrot or combination of both) for the provider to meet the service levels has to be sufficient to encourage performance at the required level. Any service level credits paid to an agency for the provider's failure to meet the service levels should not exceed a genuine pre-estimate of the loss to avoid being a penalty and therefore unenforceable.

It should come as no surprise that providers will generally only offer to meet service levels that they know are well within their performance capability and so considerable negotiation may be required for an agency to achieve levels that are suitable for its needs, where these exceed the standard commercial offerings.

5.11.2. Response Times

Where an interruption to all or part of the service does occur, it will be important to contractually tie the provider to investigate and, where it is in the domain of the provider, resolve the interruption as soon as possible. An agency may wish to categorize response times based on the severity of the fault.

5.11.3. Flexibility of Service

One of the key advantages of a cloud computing services model is that it should offer flexibility of service with the ability to easily scale up or down the required level of service depending on agency needs. It is therefore important for an agency to consider its requirements in this regard. Key issues to consider are:

- making sure that the pricing model is suitable – if the agency's demand for computing rises or falls, will the agency be required to pay higher prices (on a per unit basis) for the change in scale of the service?
- Does the agreement allow for changes in the agency's demand to be easily implemented or will it require a potentially time consuming negotiation process?
- How will the agency ensure compliance with FMA Act requirements (for example, FMA Regulations

ISSN 2348 – 7968

9 and 10) as a result of scalable service costs?

5.12. Business Continuity and Disaster Recovery

Business continuity and disaster recovery will often be a critical consideration in cloud computing service agreements given the reliance that an agency may have on obtaining uninterrupted access to that service. Threats to business continuity in this context can include:

- interruption to communications networks
- hardware or software failure
- power failure
- Disaster (fire, storm, riot etc) that disables access to the service.

Agencies should therefore consider including protections in their agreement with the provider where necessary to ensure access to the service is not disrupted. As an example, these could include:

- ensuring the provider has a geographically separate disaster recovery site with seamless transition
- ensuring the provider is able to operate in the event that mains power is disrupted (for example, use of Uninterruptible Power Supply and back-up generators)
- ensuring that business continuity is a strict requirement and not subject to qualifiers such as 'reasonable efforts'
- requiring a business continuity and disaster recovery plan be submitted for comment and approval by the agency
- limiting the right for the provider to suspend their service for force majeure reasons to circumstances where the business continuity and disaster recovery plan has been properly followed and implemented
- ensuring that scheduled maintenance outages of provider systems do not occur during hours that the agency requires access and use of the system (a common problem if the service is provided from a substantially different time zone)

Agencies may also need to take other precautions outside of the agreement (for example, in relation to their communications providers) to minimize disruptions (for example, issues with an agency's internet gateway) that are not the fault of the cloud computing provider. The provision of substantial services by way of the cloud could amplify the impact of any failures that occur in supporting contracts.

5.13. Ending the Arrangement

Termination for convenience and early termination fees

As with all government contracts it is important to consider inclusion of an early termination clause (without the default of the provider) in the agreement that allows an agency to terminate or reduce the agreement at any time for any reason (these are often known as 'termination for convenience' clauses).

Where there is provision for early termination, agencies should consider what payments apply to the early termination. If compensation is appropriate, it should not exceed reasonable costs associated with the termination and would not, for example, extend to additional costs such as to cover loss of profit on the part of the provider. Significant early termination fees may act as a barrier to competition in the cloud services market and agencies may wish to consider this issue when determining whether to accept early termination fees or not.

5.14. Termination for Default

An agency should ensure that it has the right to terminate for default where the provider does not meet the agency's reasonable requirements as set out in the agreement. The agency should also consider whether specific rights to terminate for default are required (for example, see the discussion of change of control in this guide).

5.14.1. Provider's Right to Terminate

Providers will ordinarily seek a right to terminate the agreement in certain circumstances, for example for agency default. In respect to any such right, the agency should consider including a sufficiently long notice period before the termination becomes effective to enable the agency to find a suitable alternative provider.

5.14.2. Legal Advice on Termination

Termination of any agreement is a serious matter and should only be undertaken, no matter how clear the wording of the agreement, following specific legal advice.

5.15. Disengagement/Transition of Services

Disengagement can be a key issue where the cloud

ISSN 2348 – 7968

computing services are critical services for the agency. In addition, easy and smooth disengagement and transition may ultimately lead in the longer term to greater competition and lower prices for cloud computing services to government as the barriers to transferring from one provider to another are reduced.

If an agency is transitioning to a new cloud computing services provider or alternatively bringing the services back in-house, then it will be important for the agency to consider including requirements in the agreement that the provider will:

- ive all reasonable assistance in helping with the disengagement and transition including retrieval of all data in formats approved by the agency
- upply a detailed disengagement and transition plan to give the agency confidence in the nature and scope of the provider's disengagement services
- not delete any data at the end of the agreement without the express approval of the agency

5.16. Dispute Resolution

It is important to be clear about how disputes in relation to the cloud computing agreement will be resolved. Agencies should ensure that, at a minimum, the agreement states what country's (and jurisdiction's) laws apply to the agreement, which courts can hear disputes about the agreement (known as the choice of law provisions) and whether alternative dispute resolution mechanisms such as arbitration are proposed.

Even if carefully drafted choice of law provisions are included in an agreement, it will not necessarily preclude a court from applying different laws where the nominated laws, or forum, are not appropriate in the context of the relevant agreement or dispute.

'Choice of law' provisions may also have no effect on non-contractual legal issues that arise in the context of a cloud computing arrangement. For example, any contractual provision which purports to exclude the operation of a non-excludable warranty arising under the Competition and Consumer Act 2010(Cth) would be void under Australian law. The appropriate forum for hearing disputes about defamation or another civil wrong may also be determined without reference to any agreed contractual clause. Agencies should therefore consider seeking legal advice regarding all risks associated with cloud arrangements rather than just risks arising directly from the agreement.

Agencies should carefully consider the implications of choice of law provisions and proposed dispute resolution processes, particularly where such processes are compulsory. It may be necessary for agencies to obtain legal advice from lawyers in all relevant jurisdictions including the jurisdiction where the service is actually to be provided and the jurisdiction whose laws apply to the agreement. That advice may need to address potential costs, hidden risks and practical implications of the proposed arrangements.

5.17. Other Legal Issues

g

There are a range of other legal issues which may appear in a cloud computing services agreement.

s

5.17.1. Introduction of Harmful Code

A potential threat to an agency's systems and data will always be posed by harmful code (such as viruses and other malicious code). In the cloud computing environment, agencies will need to rely on the provider applying sufficient protection against the introduction of harmful code in hosted data and systems as well as via any communication with an agency's local systems.

Agencies should therefore consider in each case the potential risks posed by harmful code and the relevant obligations that should be imposed on the provider to ensure that agency systems and data are protected.

5.17.2. Change of Control and Assignment/Novation

It is critically important that an agency knows what entity it is entering into a cloud computing services agreement with and that it can control whether it allows another entity to obtain control of the initial provider. This is especially important where the provider stores sensitive data or provides services for sensitive computing tasks. There are, for example, some entities that the Australian Government is not permitted to contract with (for example, entities that Australia has agreed under international law not to deal with) and others that are deemed to pose a threat to the national security of Australia. Some ways of dealing with this issue include:

- requiring the provider to inform the agency in advance (subject to any listing rules of a relevant stock exchange) of any proposed change in control of the provider – such as changes in key management positions or changes in significant shareholders
- providing the agency with a right to terminate in

ISSN 2348 – 7968

the event that a change of control compromises the agency or the Australian Government

- requiring that any transfer of the provider's rights and obligations under the agreement to another entity (commonly referred to as 'assignment' in the case of rights and 'novation' in relation to rights and obligations) be subject to approval in advance by the agency
- requiring that any subcontractors be made known to the agency for consideration before the agreement is entered into and providing the agency with a right to approve the involvement of any new subcontractors

5.17.3. Change of Terms at Discretion of the Provider

Some cloud computing agreements, typically standardized services in the public cloud that are available to many customers, include clauses allowing the provider to change the terms of the agreement at any time at their sole discretion (that is, without input from the agency). From a commercial point of view, it is easy to understand why a provider may include such a clause – especially where it has many thousands of customers using the service. However, such a clause will create a very substantial risk for an agency, particularly if the agency has negotiated with the provider to include the types of clauses that are set out in this guide. As a result, agencies should consider either:

- deleting the right or making the right subject to the agency's agreement to any change, or
- ensuring that the provider is obliged to notify the agency well in advance of any changes and give the agency the right to terminate the agreement if it does not agree to the changes

5.17.4. Application of Foreign Laws and Trans Border Data Transfer

When contracting cloud computing services, agencies should be aware that information may be processed or stored in jurisdictions with privacy and information protection laws significantly different from those in Australia.

It may also be possible for foreign governments to access an agency's data held in the foreign jurisdiction or to access information held in Australia by any company with a presence in the foreign jurisdiction.

Agencies should therefore determine the jurisdictions their data may transit or be stored in and seek legal counsel, as appropriate, to assist in determining the application of foreign laws to their data. Any such foreign jurisdictional risks arising for an agency should be considered in the context of the nature and classification of the agency's data that is to be stored in the cloud.

5.18. Further Issues

Agencies should closely check cloud service agreements to identify any other provisions that may be problematic. Examples of other potential legal issues that may need to be addressed include:

- Freedom of Information Act 1982: issues–the agency should ensure that the cloud services arrangement does not prevent it from complying with its obligations under the FOI Act. This would include ensuring that it can access the agency's data in the event that an FOI request is received and amend personal information in response to a request for amendment under the Privacy Act or FOI Act.
- Intellectual property ownership – the agency should ensure that the agreement does not transfer intellectual property ownership to the provider in any data stored by the provider on behalf of an agency.
- Publicity by the provider in respect of agreement – normally this would only be by agreement of an agency.
- Use of Commonwealth branding and logos by the provider – this is only permitted in accordance with the It's an Honor website managed by the Department of the Prime Minister and Cabinet.
- Responsibility for end-users – agencies should be very careful about taking on responsibility for what public end users may do with data and applications made available to them through government websites and applications as the agency will generally have little or no control over the activities of end-users.
- Export controls – where data is provided across country borders (and back again) the agency will need to consider the impact of export control laws in the relevant jurisdictions which may impact on the type of data that may be provided to a cloud services provider and the country in which the cloud services provider operates. This is an evolving area that agencies should keep a watchful eye on.

ISSN 2348 – 7968

3. Comparisons

A. Sla in Cloud Systems

An SLA is a document that contains an agreement between both the consumer and provider. Service Level Agreement contain the elements such as cloud storage, load balancing, location of data and security. Requirements needed to support negotiation activities are QoS parameters. SLA negotiation is done with multiple cloud providers by a broker in market. SLA monitoring means without violate the agreements increase the utilization of resources by providers.

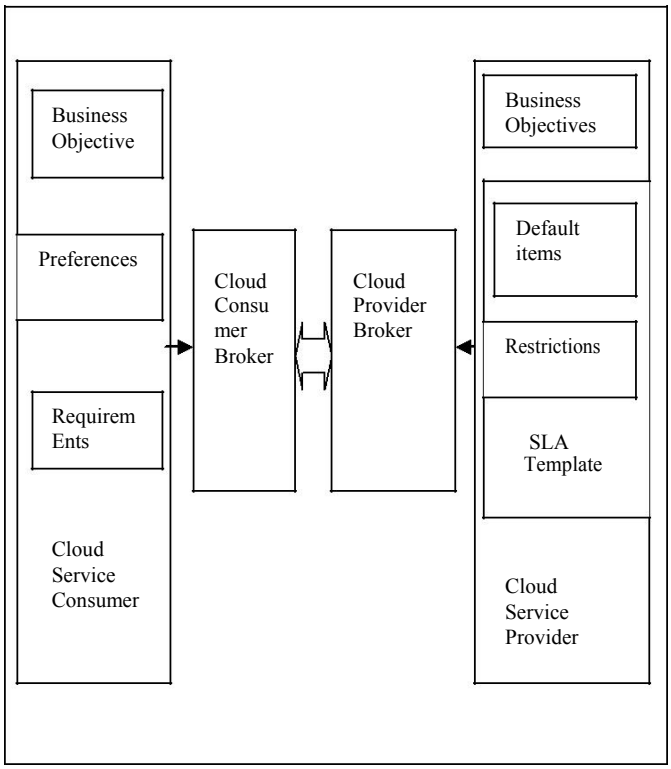

Figure.1 SLA Negotiation Process

Advantages:

- Automated contract creation
- Identify expectations, clarify responsibilities and make communication between a service provider and consumer.
- Ensure QoS for services

Disadvantages:

Creation of mapping to public SLA template such as price, performance and availability need higher cost.

B. Automated Negotiation

This paper presents the negotiation mechanism for the problem of dynamic resource allocation. Multiple buyers and sellers are negotiating concurrently with each other. By paying penalty an agent can be commit from the agreement.

Here provider and consumer negotiate resource leasing contacts automatically. Each seller has different type of resources. Here only a single set of resources is allowed for each task. By analyzing negotiation history buyer estimate seller's cost and market competition [1].

Advantages:

- Performs combinatorial auction mechanisms
- Applied in dynamic resource allocation problems

Disadvantages:

- Agent will make decision immediately after receive a message.
- Impossible to make agent's equilibrium strategies in dynamic resource allocation

C. Global Cloud Exchange For Market Oriented Architecture

Global cloud exchange gives a vision for trading services. Cloud gives chance to providers for select the providers according to their requirements. This is by executing SLAs in advance. The negotiation process ends at the time of SLA formation or withdrawal of participants.

The resource management system provides advance reservations. Broker can choose the users depending on their applications [12].

Advantages:

- Negotiation between users and providers for establish SLAs
- Allocation of Virtual Machine resource to meet SLAs
- Manage risk associated with the SLA violation

ISSN 2348 – 7968

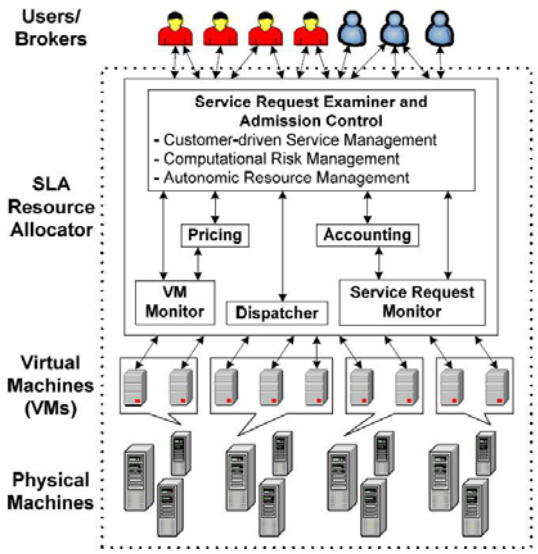

Figure2.High-Level market oriented cloud architecture

D Generic Model for Pricing

This paper gives the definition of dynamic pricing strategies of cloud providers. Due to the simple implementation genetic algorithm is used. For buying the cloud resources client send the request to market. The request which contain the information about resource, QoS and time slot for execute the task. The provider sends reply with price according to the user's needs. Resources with lowest price will be purchased by client. The frequency of client request for resources is dynamic [10].

Advantages:

- Genetic algorithm is very simple.
- It provides best pricing.
- Quicker coverage to best solutions.

Disadvantages:

- It cannot define the more complex parameters relation
- Not yet used in real computing environment.

Service discovery provide in test bed through the message passing. Periodic simulation controlled by the simulation controller. Cloud status recorder shows the information about the cloud market and negotiation from all negotiation round.

Two algorithm named tradeoff and concession-making algorithm are implemented for PTN. Cloud reservation is doing in memory array. Here single issue and multi issue negotiation is considered [14]. Consider other negotiation issues for quality of services (QoS). Introduce a coordinator which distribute the applications across different data centers which enabling SLA's for improving application's performance, reliability and scalability.

Provisioning of virtual machine provide security.

PTN mechanism follows the negotiation protocol is agent make negotiation in alternate rounds. It will accept when both the consumer agent and provider agent reached in an agreement for price and time. The negotiation fails when one of agent's deadlines expires before reach the agreement.

In future work we advocate creation of federated Cloud computing environment (Inter Cloud) that facilitates just-in-time, reliable and scalable provisioning of application services, and consistently achieving QoS targets under variable workload. It is used to counter the problem such as the inability to predict geographic distribution of users consuming their services. Propose architecture for Cloud Coordinator and an extensible design that allows its adoption in different public and private Clouds.

Advantages:

- Time and price slot negotiation mechanism used for agent's different level of satisfaction
- Enhance negotiation speed by using the tradeoff algorithm
- Establish SLA

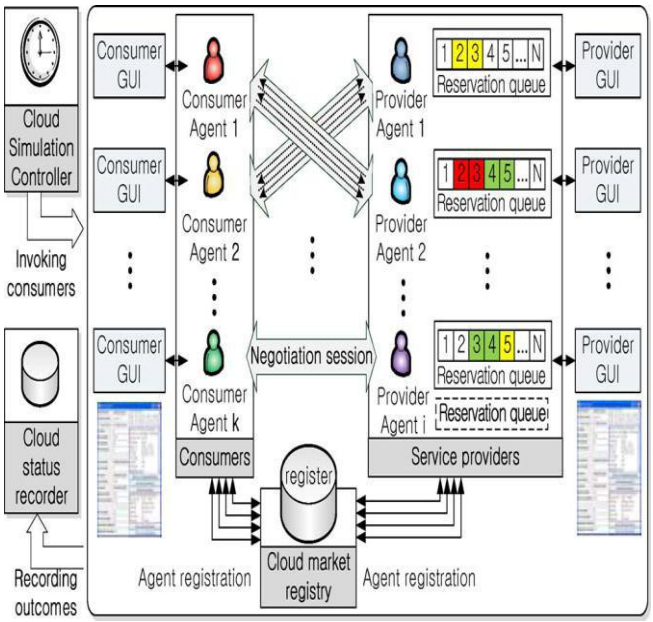

Figure 3.Agent-Based Cloud Test bed

ISSN 2348 – 7968

4. Conclusions

The intention of this paper is to compare the works applies in cloud service reservation to solve cloud resource allocation. This article has provide an overview of cloud computing in which its definition, cloud resources, negotiations and issues are discussed. More than four papers were surveyed regarding the cloud resources negotiation. Various techniques of negotiation are discussed and the legal issues are identified. In order to provide quality of service and to enhance negotiation, Cloud Coordinator is implemented. Finally, the future research directions have been outlined for providing more quality of services.

Acknowledgments

The authors would like to thank the Editor-in-Chief, the Associate Editor and the anonymous Referees for their comments.

References

[1]Bo An, Victor Lesser, David Irwin,Michael Zink "AutomatedNegotiation with Decommitment for Dynamic Resource Allocation inCloud Computing" , Proc. of 9th Int. Conf. on Autonomous Agents and Multiagent System, May, 10–14, 2010

[2]Chris Peiris, Dharmendra Sharma "C2TP: A Service Model for Cloud" CLOUD COMPUTING 2010 : The First International Conference on Cloud Computing, GRIDs, and Virtualization

[3]Divya Jyothi "Ecommerce Dealer Agent Mechanism in Cloud Computing Environment" International Journal of Advanced Research in Computer Science and Electronics Engineering Volume 1, Issue 4, June 2012

[4]DivyJyothi, Madhe ,D.R.Ingle "Dealer Agent based Cloud EcommerceFramework" ICACACT 2012

[5] Edwin Yaqub, Philipp Wieder, " A Generic Platform for Conducting SLA Negotiations"

[6] Gaurav Raj, Ankit Nischal "Efficient Resource Allocation in Resource provisioning policies over Resource Cloud Communication Paradigm" ICCSA,Vol.2, No.3, June 2012

[7] Kwang Mong Sim "Grid Resource Negotiation:Survey and NewDirections" IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS, VOL. 40, NO. 3, MAY 2010 245

[8]Kwang Mong Sim, Senior Member, IEEE, and Benyun Shi"Concurrent Negotiation and Coordination for Grid Resource Coallocation" IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: CYBERNETICS, VOL. 40, NO. 3, JUNE 2010

[9]Mario Macıas, J. Oriol Fito and Jordi Guitart "Rule-based SLA Management for Revenue Maximisation in Cloud Computing Markets", CNSM 2010

[10] Mario Macías, Jordi Guitart "A Genetic Model for Pricing in Cloud Computing Markets"

[11]Rabi Prasad Padhy, Dr. Manas Ranjan Patra,Dr. Suresh Chandra Satapathy"SLAs in Cloud Systems: The Business Perspective", InternatIonalJournal ofComputerSCIenCe and technology Vol 3, ISSue1, Jan. - MarCh2012

[12]Rajkumar Buyya, Chee Shin Yeo and Srikumar Venugopal " Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities"

[13]Rajkumar Buyya,Rajiv Ranjan, Rodrigo N.C "InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services"

[14]Seokho Son and Kwang Mong Sim "A Price- and-Time-Slot-Negotiation Mechanism for Cloud Service Reservations", IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART B: CYBERNETICS, VOL. 42, NO. 3,JUNE 2012

[15]Vivek Shrivastava, D.S. Bhilare "Algorithms to Improve Resource Utilization and Request Acceptance Rate in IaaS Cloud Scheduling" Int. J. Advanced Networking and Applications 1367 Volume: 03, Issue: 05, Pages: 1367-1374 (2012)

[16]Wang Xiaojing, Tong Wei ,Ren Jia,Ding Linjie, Liu Jingning "Weighted Fairness Resource Allocation of Disks in XEN" IJCCSA,Vol.2, No.3,June12M. Miller, Cloud Computing: Web-Based Applications that Change theWay You Work and Collaborate Online. Que, 2009.

[17] I. Foster et al., "Cloud Computing and Grid Computing 360-Degree Compared," Proc. Grid Computing Environments Workshop (GCE '08), pp. 1-10, Nov. 2008.

[18]R. Buyya et al., "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility," Future Generation Computer Systems, vol. 25, no. 6, pp. 599- 616, June 2009.

[19]K.M. Sim, "Agent-Based Cloud Commerce," Proc. IEEE Int'l Conf.Industrial Eng. and Eng. Management, pp. 717-721, 2009.

[20]M. Wooldridge, An Introduction to Multiagent Systems, second ed.John Wiley & Sons, 2009.

[21]K.M. Sim, "Towards Complex Negotiation for Cloud Economy,"Proc. Int'l Conf. Advances in Grid and Pervasive Computing (GPC '10),R.S. Chang et al., eds., pp. 395-406, 2010.

[22]K.M. Sim, "Towards Agent-Based Cloud Markets (Position Paper)," Proc. Int'l Conf. E-CASE, and E-Technology, pp. 2571-2573, Jan. 2010.

[23]K.M. Sim, "Complex and Concurrent Negotiations for Multiple Interrelated E-Markets," IEEE Trans. Systems, Man and Cybernetics,Part B, preprint, 2012, doi:10.1109/TSMCB.2012.2204742.

[24]K.P. Joshi, T. Finin, and Y. Yesha, "Integrated Lifecycle of IT Services in a Cloud Environment," Proc. Third Int'l Conf. Virtual Computing Initiative (ICVCI '09), pp. 475-478, 2009.

[25]K.M. Sim and B. Shi, "Concurrent Negotiation and Coordination for Controlling Grid Resource Co-Allocation," IEEE Trans. Systems,Man and Cybernetics, Part B, vol. 40, no. 2, pp. 753-766, June 2010.

ISSN 2348 – 7968

[26]K.M. Sim, "Grid Resource Negotiation: Survey and New Directions," IEEE Trans. Systems, Man and Cybernetics, Part C, vol. 40, no. 3, pp. 245-257, May 2010.

[27]K.M. Sim, "Evolving Fuzzy Rules for Relaxed-Criteria Negotiation,"IEEE Trans. Systems, Man and Cybernetics, Part B, vol. 38, no. 6, pp. 1486-1500, Dec. 2008.

[28]K.M. Sim and B. Shi, "Adaptive Commitment ManagementStrategy Profiles for Concurrent Negotiations," Proc. First Int'l Workshop Agent-Based Complex Automated Negotiations (ACAN) held in Conjunction with Seventh Int'l Conf. Autonomous Agents and Multi-Agent Systems (AAMAS), pp. 16-23, 2008.

First Author Biographies should be limited to one paragraph consisting of the following: sequentially ordered list of degrees, including years achieved; sequentially ordered places of employ concluding with current employment; association with any official journals or conferences; major professional and/or academic achievements, i.e., best paper awards, research grants, etc.; any publication information (number of papers and titles of books published); current research interests; association with any professional associations. Do not specify email address here.

Second Author biography appears here. Degrees achieved followed by current employment are listed, plus any major academic achievements. Do not specify email address here.

Third Author is a member of the IEEE and the IEEE Computer Society. Do not specify email address here.

M.Vijayasanthi received the M. Tech. degree, B. Tech. degree in Comupter science and Engineering from Jawaharlal Nehru Technological University, Anantapur, India in 2005 and 11.At present working in SVCE, Tamilnadu. Previously worked in VCE,Hyderabad andSNIST,Hyderabd. Her area of interest includes Cloud Computing and Data Mining. She is associated with ISTE.