International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 2, Issue 7, July 2015, PP 27-40
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

A Survey on Intercloud and its Security

V. Ashok Kumar

Assistant Professor, Department of CSE,
Srikalahasteeswara Institute of Technology (SKIT), Srikalahasti,
Endowments Department, Government of Andhra Pradesh, India.
ashokcse.skit@gmail.com

Abstract: *A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumer. Inter cloud is the dynamic set of connected clouds based on service-level agreements established through negotiation between the service providing clouds and service consuming clouds. This paper gives a glance at Cloud, Cloud computing Environment, Intercloud, Intercloud History, Benefits of Intercloud, Intercloud Interoperability, System Architecture and Elements of Intercloud, Security management in Intercloud and Security in inter cloud communication and inter cloud's security, integrity and privacy.*

Keywords: *parallel, Distributed, Cloud, virtual computers, Inter-Cloud, Coordinator, Broker, Exchange, Cloud Communication, identity, Access, Interface, Interpreter Persistence, Data Centres and security.*

1. INTRODUCTION

The cloud is the service being delivered from remote sites. As public and private industry budgets continue to shrink, executives are plotting new strategies to become more efficient and cost effective. Cloud computing has gleaned a lot of attention over the past several years as a means to reduce IT expenditures, improve scalability and reduce administration over head. As savings amount and efficiencies increases, cloud computing will continue to grow. Most of the enterprises are already operating their applications or infrastructure in a cloud environment. Now a day's most of the personal and general purpose services are also provided to personal cloud user by the cloud service providers. Up to 2015 the top 10 cloud services[1] are Rack space, Amazon Web Services (AWS), Site Ground, Storm On Demand, Microsoft Azure, Digital Ocean, Liquid web, Net magic Solutions, Ctrls and Servint.

1.1. Definition of cloud Computing

The National Institute of Standards and Technology has defined Cloud computing[2] as "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". (Mell & Grance, 2011, p. 2).

There is little consensus on how to define the Cloud and I add yet another definition [3] [4]to the already saturated list of definitions for Cloud Computing:

A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the internet.

Cloud Computing is anything that provides hosted services over the internet [5]. These services are sharing to the end users. The main uses of cloud are data storage, process and management services on the internet rather than having local servers. The service provider has to look up all the issues related to the cloud. The end-user doesn't require any server to maintain, simply requesting the services from the cloud and pay for using it. Fig.1 depicts the cloud computing layout diagram.

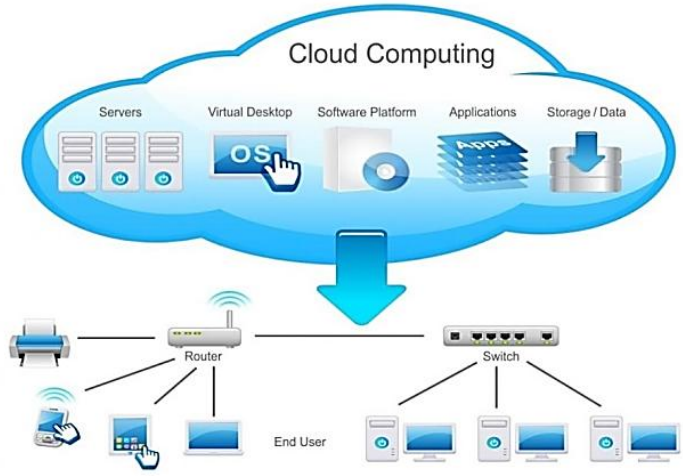

Figure 1. *Cloud Computing Layout Diagram*

2. CLOUD COMPUTING ENVIRONMENT

NIST also defines five key and essential characteristics, three service models and four deployment models are shown in below [2].

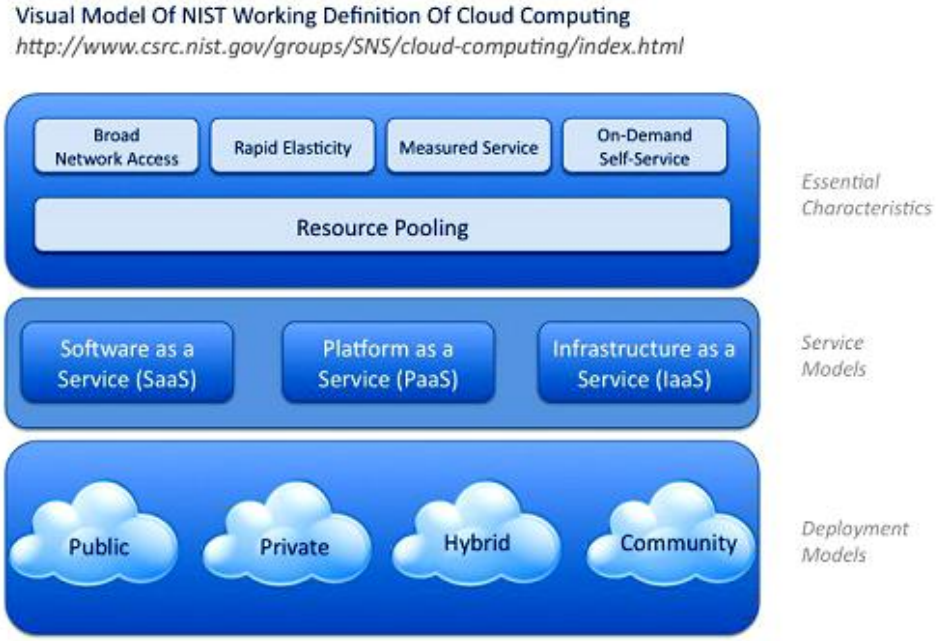

Figure 2. *NIST defined Essential characteristics, Service models and Deployment models.*

2.2. Characteristics of Cloud

According to National Institute of Standard Technology [2] (NIST, U. S. Department of Commerce), cloud has five essential characteristics as follows.

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

NIST categorizes Cloud computing into a Service Model and a Deployment Model.

2.3. Service Models of Cloud Computing

As per NIST mainly the Service Model consists of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) as shown below along with the services provided by the cloud with challenges Security, integrity and privacy at different levels [2].

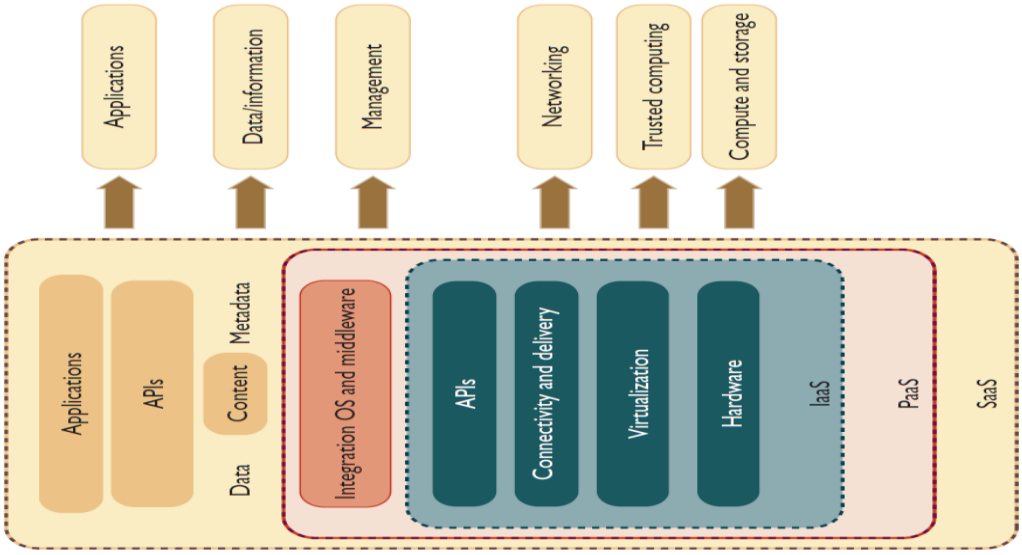

Fig 3. *Cloud service model along with the services.*

This "stack" of functionality begins with Infrastructure as a Service where consumers utilize hardware only. Moving up the stack is Platform as a Service. This layer offers the consumer an application environment where programming libraries and software can be used for development. At the top of the stack is Software as a Service. The consumer utilizes the Cloud providers' application and has no access to the infrastructure or Operating System platform.

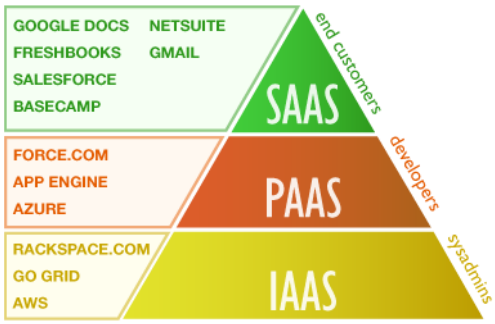

Fig 4. *Basic Cloud service Types SaaS, PaaS and IaaS*

Apart from the above three main service models there several services oriented cloud models categorized based on the services provided by the clouds and some of them are listed below:

1. Storage-as-a-Service (SaaS)
2. Database-as-a-Service(DaaS)
3. Information-as-a-Service (InfaaS)
4. Process-as-a-Service (PraaS)
5. Software-as-a-Service (SaaS)
6. Platform-as-a-Service (PaaS)
7. Integration-as-a-Service (IntaaS)
8. Security-as-a-Service (SeaaS)
9. Management/Governance-as-a-Service (MaaS)
10. Testing-as-a-Service (TaaS)
11. Infrastructure-as-a-Service (IaaS), etc.

2.4. Cloud Deployment models

Cloud has four deployment models. These are public cloud, private cloud, community cloud, hybrid cloud and inter cloud shown below figure 5 and figure 6.

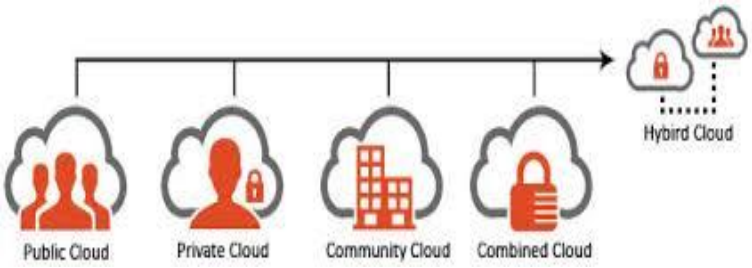

Figure 5. *Cloud Deployment types.*

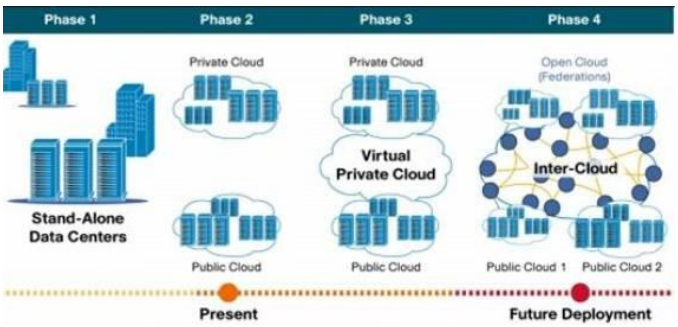

Figure 6. *Cloud Deployment Models.*

These deployment models are briefed as follows:

2.4.1. *Public cloud*: The public cloud can utilize for general public, anyone can use it.

2.4.2. *Private cloud*: Private cloud is meant solely for an organization.

2.4.3. *Community cloud*: Community is for special community composed of several organizations with shared concerns.

2.4.4. *Hybrid cloud*: Hybrid cloud is a combination of the clouds. (I.e. public, private or community clouds)

3. INTRODUCTION TO INTER-CLOUD

3.1. What is Intercloud

The Intercloud [6] is an interconnected global "cloud of clouds" and an extension of the Internet "network of networks" on which it is based.[7] The term was first used in the context of cloud computing in 2007 when Kevin Kelly opined that "eventually we'll have the intercloud, the cloud of clouds". It became popular in late 2008 and has also been used to describe the datacenter of the future.[8]

The Intercloud scenario is based on the key concept that each single cloud does not have infinite physical resources or ubiquitous geographic footprint. If a cloud saturates the computational and storage resources of its infrastructure, or is requested to use resources in a geography where it has no footprint, it would still be able satisfy such requests for service allocations sent from its clients. The Intercloud scenario would address such situations where each cloud would use the computational, storage, or any kind of resource (through semantic resource descriptions, and open federation) of the infrastructures of other clouds. This is analogous to the way the Internet works, in that a service provider, to which an endpoint is attached, will access or deliver traffic from/to source/destination addresses outside of its service area by using Internet routing protocols with other service providers with whom it has a pre-arranged exchange or peering relationship. It is also analogous to the way mobile operators implement roaming and inter-carrier interoperability. Such forms of cloud exchange, peering, or roaming may introduce new business opportunities among cloud providers if they manage to go beyond the theoretical framework [9].

3.2. Intercloud definition

Inter-cloud or 'cloud of clouds' is a term refer to a theoretical model for cloud computing services based on the idea of combining many different individual clouds into one seamless mass in terms of on-demand operations. The inter-cloud would simply make sure that a cloud could use resources

beyond its reach, by taking advantage of pre-existing contracts with other cloud providers. Cisco inter-cloud strategy is shown below.

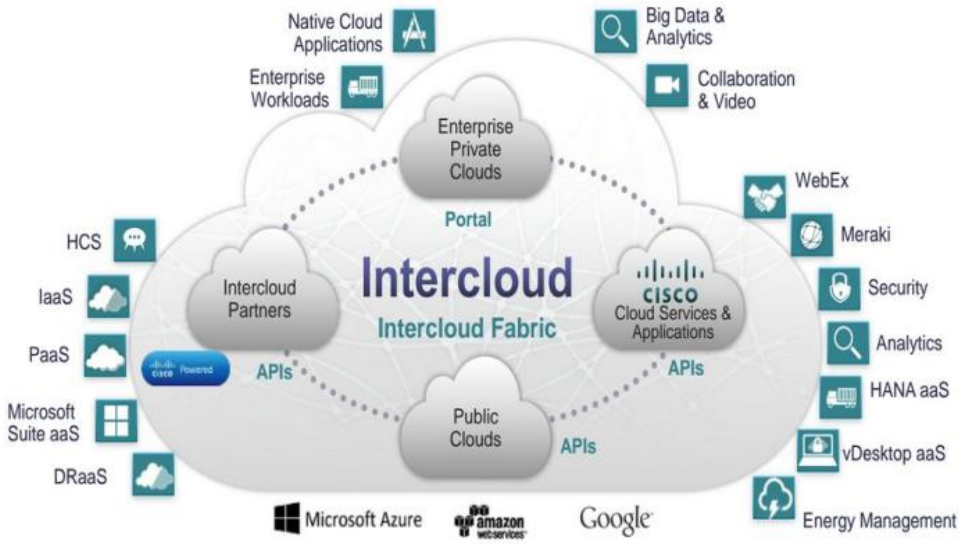

Figure 7. *Cisco Inter-cloud Strategy*

Essentially, an Inter-Cloud allows for the dynamic coordination and distribution of load among a set of cloud data centres [13] - see figure 8.

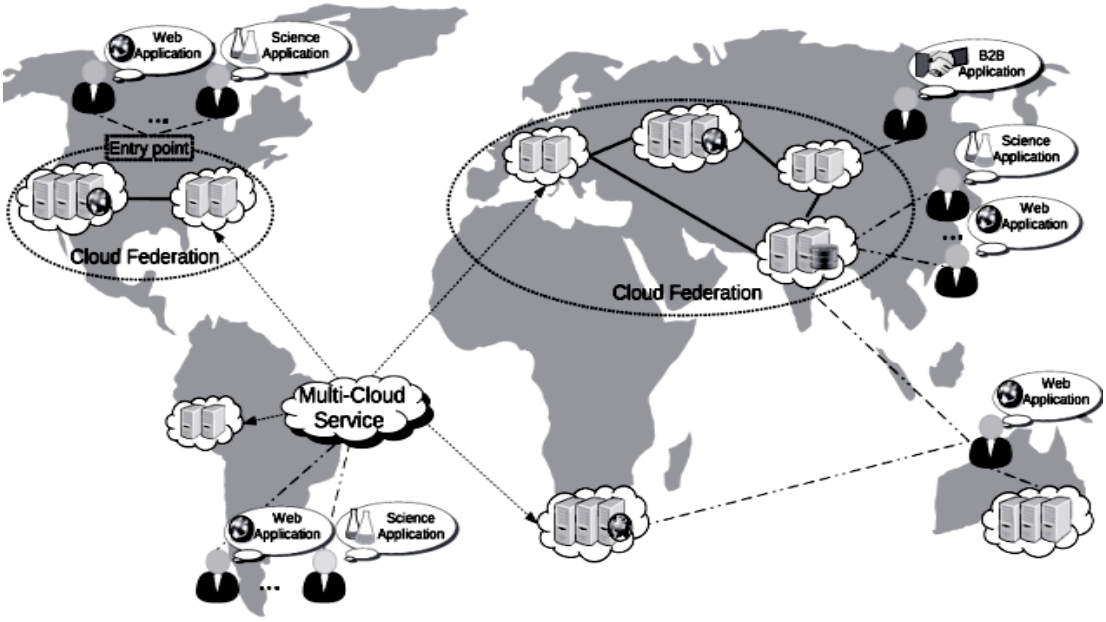

Figure 8. *Overviews of Inter-Cloud approaches and use cases.*

3.3. Intercloud History

- In July 2009 in Japan, an effort called the Global Inter-Cloud Technology Forum (GICTF)[10] was launched with the stated goal of "We aim to promote standardization of network protocols and the interfaces through which cloud systems interwork with each other, and to enable the provision of more reliable cloud services than those available today".
- In February 2011 the IEEE launched a broad cloud computing initiative IEEE Cloud Computing including a technical standards effort called P2302 - Standard for Intercloud Interoperability and Federation (SIIF)[11]. The stated goal of the working group is to produce a standard as such: "This standard defines topology, functions, and governance for cloud-to-

cloud interoperability and federation. Topological elements include clouds, roots, exchanges (which mediate governance between clouds), and gateways (which mediate data exchange between clouds). Functional elements include name spaces, presence, messaging, resource ontologies (including standardized units of measurement), and trust infrastructure. Governance elements include registration, geo-independence, trust anchor, and potentially compliance and audit. The standard does not address intra-cloud (within cloud) operation, as this is cloud implementation-specific, nor does it address proprietary hybrid-cloud implementations."

- In mid-2011 the NIST Cloud Computing Reference Architecture was published fully describing hybrid clouds, cloud brokers, and so on. In late 2011 NIST published a whole set of Cloud Computing Technology Roadmaps including referencing the IEEE P2302 approach as an example of a future national/global federated cloud architecture.
- In March 2012 "Intercloud" made the Wired Magazine Jargon Watch list and in October 2013 the IEEE announced a Global Testbed initiative.
- In late 2013 Cisco made their first announcement relating to the Intercloud. Their product Cisco Intercloud Fabric (ICF) allows VM migrations between public and private clouds. In 2014 Cisco made another announcement [12] Cisco revealed that it "will invest $1Bn in the next two years to build its expanded cloud business" and that "Our cloud will be the world's first truly open, hybrid cloud. The Cisco Intercloud will be built upon Open Stack for its open standards-based global infrastructure. We plan to support any workload, on any hypervisor and interoperate with any cloud" (again assuming all clouds are using Cisco's proprietary technology).
- As of June 2015, The Intercloud has yet to show real world demonstration of federation and interoperability, and challenges remain regarding security and trust, governance and legal issues, QoS, monitoring, arbitrage, and billing.

3.4. Benefits of Intercloud

The benefits of an Inter-Cloud environment for cloud clients are numerous and can be broadly summarized as follows:

3.3.1. Diverse geographical locations. Leading cloud service providers have established data centers worldwide. Only by utilizing multiple clouds can one gain access to so widely distributed resources and provide well-performing and legislation-compliant services to clients.

3.3.2. Better application resilience. In the present days most of the major cloud vendors advised their clients to design their applications to use multiple data centers for fault tolerance [14]. Furthermore, in Berkeley's report on Cloud computing, Armbrust *et al.* emphasize that potential unavailability of service is the number one inhibitor to adopting Cloud computing [15]. Thus, they advise the use of multiple providers. Besides fault tolerance, using resources from different providers acts as an insurance against a provider being stopped because of regulatory or legal reasons as well.

3.3.4. *Avoidance of vendor lock-in*. By using multiple clouds and being able to freely transit workload among them, a cloud client can easily avoid vendor lock-in. In case a provider changes a policy or pricing that impact negatively its clients, they could easily migrate elsewhere.

A cloud provider should ensure enough resources at all times. But how much is enough? Workload spikes can come unexpectedly, and thus, cloud providers need to overprovision resources to meet them.

Cloud providers' benefits can be summarized as follows:

- *Expand on demand.* A cloud should maintain in a ready to use state enough resources to meet its expected load and a buffer for typical load deviations. If the workload increases beyond these limits, resources from other clouds can be leased.
- *Better service level agreement (SLA) to customers.* Knowing that even in a worst-case scenario of data centre outage or resource shortage the incoming workload can be moved to another cloud, a cloud provider can provide better SLAs to customers.

3.4. Intercloud Interoperability

Currently, in Intercloud Computing, shared cloud services has been increasingly utilized by diverse users, the research on Intercloud computing is still at an early stage.

Intercloud addresses the interoperability between various cloud computing instantiations where each cloud would use computing resources of other clouds. Cloud Computing environments need to be interoperable in order to reduce scaling/producing cost within the development of the components. Cloud costumers should be able to migrate in and out of the cloud and switch between providers based on their needs, without a lock-in which restricts customers from selecting an alternative provider. The present Intercloud network merely connects different cloud systems and each cloud provider has its own way on how cloud applications/customers interact with the cloud. Feldhaus [16] summarized the current challenges in Cloud Interoperability as follow:

- Several different Cloud Standards from different parties are available.
- Existing Open Grid Forum (OGF) standards not or only partly ready for the cloud.
- A consistent OGF Cloud Portfolio is needed.
- Strategies for combining different Cloud Standards / APIs are needed.
- Existing implementations of Cloud APIs need to get interoperable.
- Combined Interoperability Verification Suites need to be developed.
- It is essential to discuss on issues related to specifications and implementation.

Currently different organizations, such as IEEE, are working on developing essential standards and appropriate APIs for Intercloud Interoperability. The future Intercloud network will expand the required functions to prepare collaboration among cloud services. Grozev & Buyya summarized their studies and classified 20 major Intercloud developments including both academic and industry projects [17]. According to their studies, Intercloud is classified as *Volunteer federation* and *Independent* shown in the figure 9.

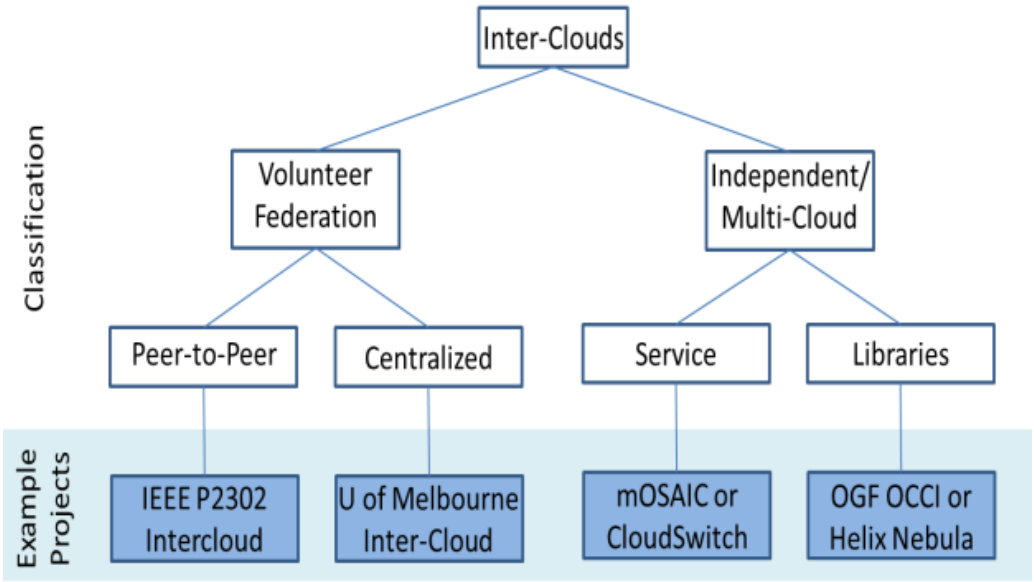

Figure 9. *Architectural classification of intercloud*[17].

1. *Volunteer federation*: when there is voluntarily collaboration between cloud providers that is often feasible for governmental clouds or private cloud portfolios and is classified as two architectural categories *Centralised & Peer-to-Peer* as in figure 10.
2. *Independent:* when an application or its broker independently from the cloud providers (both governmentally and private clouds) exploit multiple clouds and is classified in two architectural categories *Services* & *Libraries* as in figure 10.

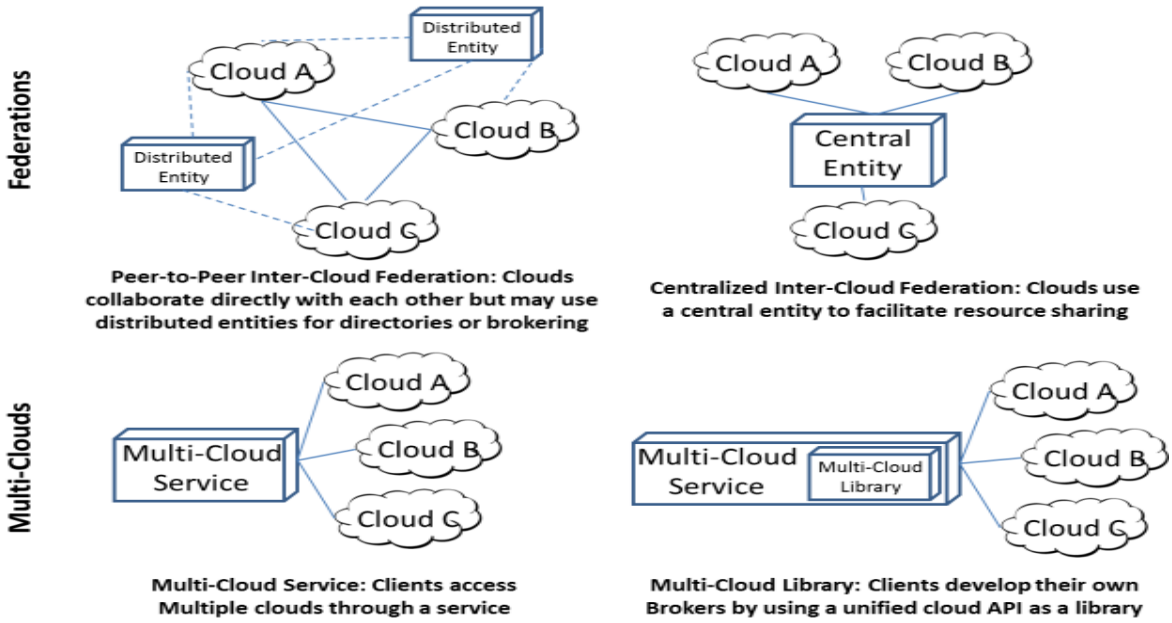

Figure 10. *Intercloud developments' architecture.*

4. System Architecture and Elements of Intercloud

Figure 11 shows the high level components of the service-oriented architectural framework consisting of client's brokering and coordinator services that support utility-driven federation of clouds: application scheduling, resource allocation and migration of workloads. The architecture cohesively couples the administratively and topologically distributed storage and computes capabilities of Clouds as parts of single resource leasing abstraction. The system will ease the cross-domain capabilities integration for on demand, flexible, energy-efficient, and reliable access to the infrastructure based on emerging virtualization technologies[18][19]. The Cloud Exchange (CEx) acts as a market maker for bringing together service producers and consumers. It aggregates the infrastructure demands from the application brokers and evaluates them against the available supply currently published by the Cloud Coordinators. CEx allows the participants (Cloud Coordinators and Cloud Brokers) to locate providers and consumers with fitting offers. Every client in the federated platform needs to instantiate a Cloud Brokering service that can dynamically establish service contracts with Cloud Coordinators via the trading functions exposed by the Cloud Exchange.

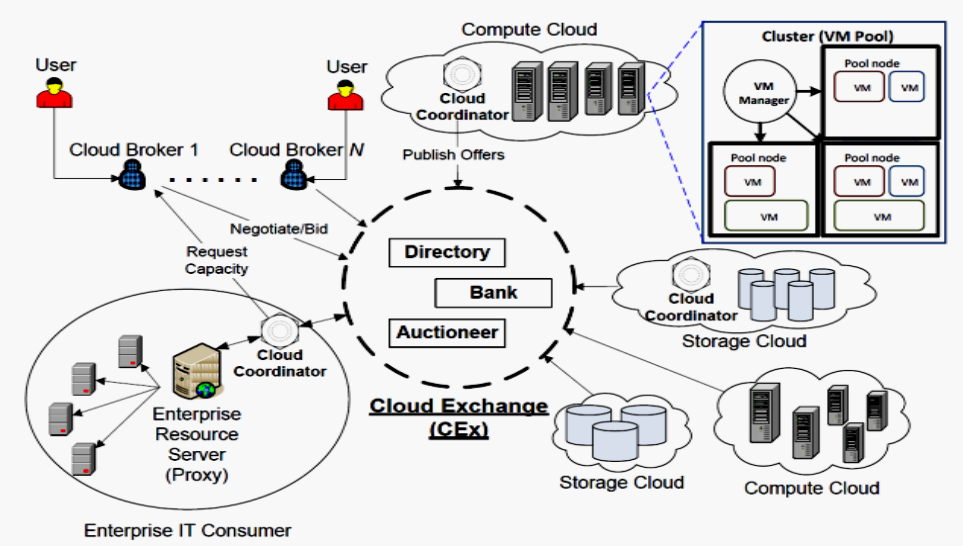

Figure 11. *Federated n/w of cloud mediated by Cloud Exchange.*

4.1. Cloud Coordinator (CC)

The Cloud Coordinator service is responsible for the management of domain specific enterprise Clouds and their membership to the overall federation driven by market-based trading and negotiation

protocols. It provides a programming, management, and deployment environment for applications in a federation of Clouds. Figure 12 shows a detailed depiction of resource management components in the Cloud Coordinator service. The Cloud Coordinator exports the services of a cloud to the federation by implementing basic functionalities for resource management such as scheduling, allocation, (workload and performance) models, market enabling, virtualization, dynamic sensing/monitoring, discovery, and application composition as discussed below:

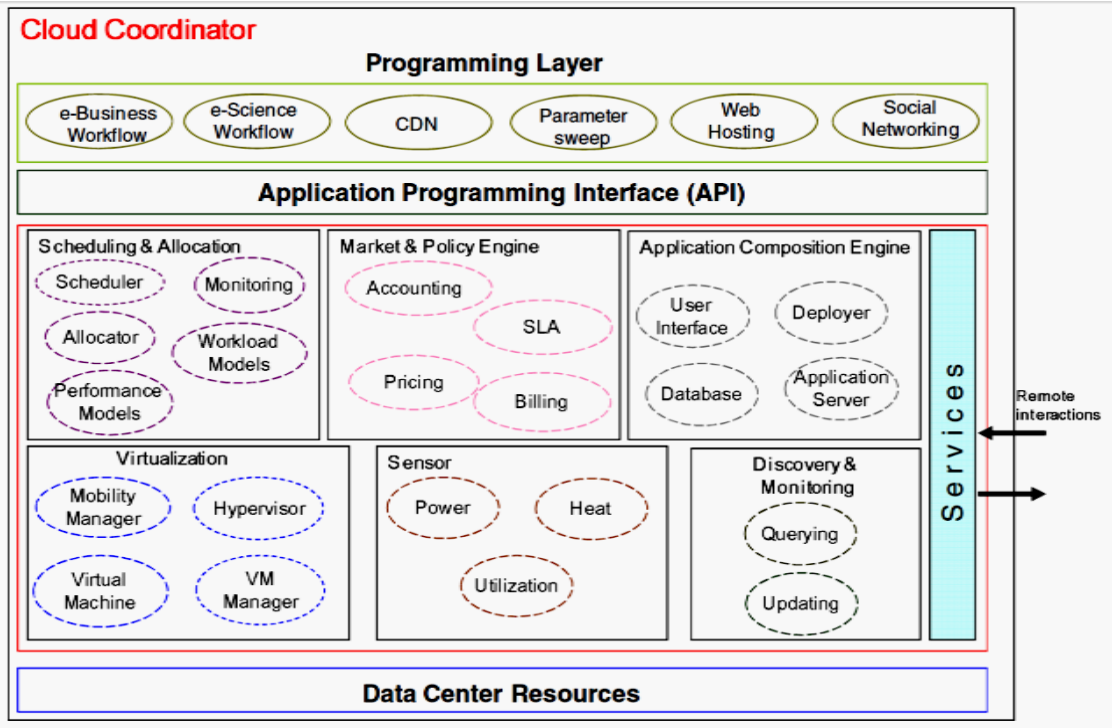

Figure 12. *Cloud Coordinator Software Architecture.*

4.1.1. Scheduling and Allocation: This component allocates virtual machines to the Cloud nodes based on user's QoS targets and the Clouds energy management goals. A request is termed as accountable if the concerning user has available credits in the Cloud bank and based on the specified QoS constraints the establishment of SLA is feasible. In case all three components reply favourably, the application is hosted locally and is periodically monitored until it finishes execution. This contains *Scheduler, Monitoring, Allocator, Workload module and performance model.*

4.1.2. Market and Policy Engine: The *SLA* module stores the service terms and conditions that are being supported by the Cloud to each respective Cloud Broker on a per user basis. Based on these terms and conditions, the *Pricing* module can determine how service requests are charged based on the available supply and required demand of computing resources within the Cloud. The *Accounting* module stores the actual usage information of resources by requests so that the total usage cost of each user can be calculated. The *Billing* module then charges the usage costs to users accordingly.

4.1.3. Application Composition Engine: This component of the Cloud Coordinator encompasses a set of features intended to help application developers *create and deploy* [20] applications, including the ability for on demand interaction with a *database* backend such as SQL Data services provided by Microsoft Azure, an *application server* such as web applications, and a SOAP driven Web services *API* for programmatic access along with combination and integration with other applications and data.

4.1.4. Virtualization: VMs support flexible and utility driven configurations that control the share of processing power they can consume based on the time criticality of the underlying application. The *Mobility Manager* is responsible for dynamic migration of VMs based on the real-time feedback given by the Sensor service. Currently, *hypervisors* such as VMware [18] and Xen[19] have a limitation that VMs can only be migrated between hypervisors that are within the same subnet and share common storage.

4.1.5. Sensor: Sensor infrastructure will monitor the *power* consumption, *heat* dissipation, and *utilization* of computing nodes in a virtualized Cloud environment.

4.1.6. Discovery and Monitoring: In order to dynamically perform scheduling, resource allocation, and VM migration to meet SLAs in a federated network, it is mandatory that *up-to-date* information related to Cloud's availability, pricing and SLA rules are made available to the outside domains via the Cloud Exchange. *Querying* is the process to know the status of each and every thing in the cloud.

4.2 Cloud Broker (CB)

The Cloud Broker acting on behalf of users identifies suitable Cloud service providers through the Cloud Exchange and negotiates with Cloud Coordinators for an allocation of resources that meets QoS needs of users. The architecture of Cloud Broker is shown in Figure 13 and its components are discussed below:

*4.2.1. User Interface***:** This provides the access linkage between a user application interface and the broker.

- *Application Interpreter* translates the execution requirements of a user application which include what is to be executed, the description of task inputs including remote data files (if required), the information about task outputs (if present), and the desired QoS.
- *Service Interpreter* understands the service requirements needed for the execution which comprise service location, service type, and specific details such as remote batch job submission systems for computational services.
- *Credential Interpreter* reads the credentials for accessing necessary services.

4.2.2. Core Services: They enable the main functionality of the broker.

- *Service Negotiator* bargains for Cloud services from the Cloud Exchange.
- *Scheduler* determines the most appropriate Cloud services for the user application based on its application and service requirements.
- *Service Monitor* maintains the status of Cloud services by periodically checking the availability of known Cloud services and discovering new services that are available.

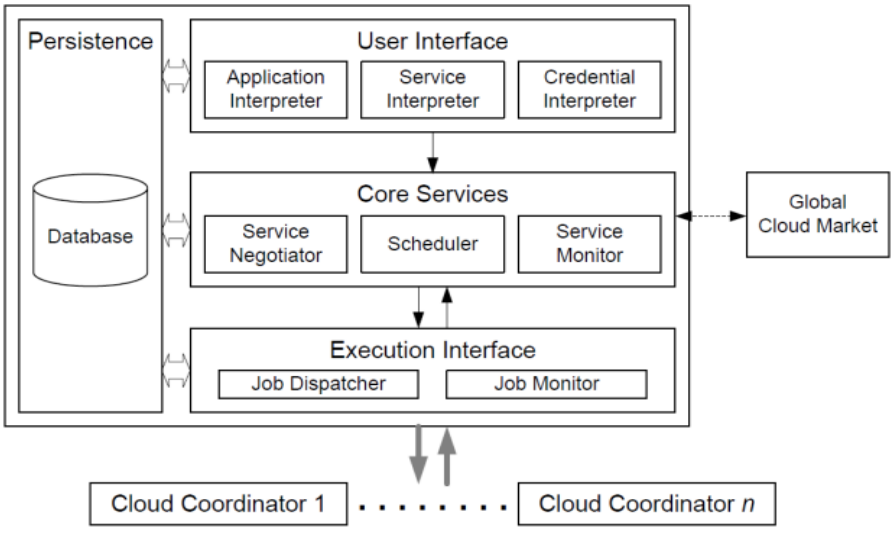

Figure 13. *High level Architecture of Cloud Broker Service*

4.2.3. Execution Interface: This provides execution support for the user application.

- *Job Dispatcher* creates the necessary broker agent and requests data files (if any) to be dispatched with the user application to the remote Cloud resources for execution.
- *Job Monitor* observes the execution status of the job so that the results of the job are returned to the user upon job completion.

4.2.4. Persistence: This maintains the state of the User Interface, Core Services, and Execution Interface in a database. This facilitates recovery when the broker fails and assists in user-level accounting.

4.3 Cloud Exchange (CEx)

As a market maker, the CEx acts as an information registry, that stores the Cloud's current usage costs and demand patterns. Cloud Coordinators periodically update their availability, pricing, and SLA policies with the CEx. Cloud Brokers query the registry to learn information about existing SLA offers and resource availability of member Clouds in the federation. Furthermore, it provides match-making services that map user requests to suitable service providers. Mapping functions will be implemented by leveraging various economic models such as Continuous Double Auction (CDA) as proposed in earlier works [21].

5. SECURITY MANAGEMENT IN INTERCLOUD

The Inter-Cloud faces many challenges other than solutions of concerning federation, security, interoperability, consumers, trust issues, legal issues, monitoring and Quality of Service (QoS). In the Inter-Cloud environment, overall security issues and requirements can be evaluated from the points of Cloud providers and consumers. Moreover, a provider that participates in both roles in a progressively complex and distributed Inter-Cloud environment has the need for a constant overview about security management components that guide future implementation and amendment within their Cloud system.

Inter-Cloud model has several techniques in the cloud computing, such as Inter-Cloud Exchange model, Inter-Cloud Trust model, Inter-Cloud Identity and Access Management with Security Assertion Markup Language (SMAL) and eXtensible Access Control Markup Language (XACML) Model.

5.1. Inter-Cloud Exchange Model: Vij et al [22] explained the Inter-Cloud Exchange Model as much as a preferred alternative to each cloud consumers to establish connectivity and collaboration among themselves as P2P, which would not scale physically or in a business sense. Since Inter-Cloud Exchange provider will facilitate the negotiation, discussion and collaboration among disparate heterogeneous cloud environments, Inter-Cloud Root instances will work with Inter-Cloud Exchanges to solve the issues by acting as mediators for allowing connectivity.

Subsequently the Inter-Cloud Root offers services such as Trust Authority, Naming Authority, Directory Services, and other root capabilities. Also it's working similarly to DNS in the network.

5.2. Inter-Cloud Trust Model: Inter-Cloud Trust Model is a basic level model [24]. With regards to the Public Key Infrastructure (PKI) trust model, the Inter-Cloud Root systems will serve as a Trust Authority in the current trust architecture by issuing certificates in a fashion similar to the Certificate Authority (CA).

5.3. Inter-Cloud Identity and Access Management: [36] Gunjan et al present Inter-Cloud Identity and Access Management (IdAM) with Security Assertion Markup Language (SMAL) and eXtensible Access Control Markup Language (XACML) model. Celesti et al [23] suggested that one of the key requirements to be successful is to effectively managing identities.

6. INTERCLOUD COMMUNICATION SECURITY

The major security problem in Intercloud is Intercloud communication [25].

6.1. Problems in inter cloud communication:

6.1.1. Security in communication: The relative security of cloud computing services is a contentious issue which may be delaying its adoption. Issues barring the adoption of cloud computing is due in large part to the private and public sectors unease surrounding the external management of security based services. It is the very nature of cloud computing based services, private or public, that promote external management of provided services.

6.1.2. *Open standards:* Most cloud providers expose APIs which are typically well-documented but also unique to their implementation and thus not interoperable. Some vendors have adopted others' APIs and there are a number of open standards under development, including the OGF's Open Cloud Computing Interface [26]. The Open Cloud Consortium is working to develop consensus on early cloud computing standards and practices.

6.2. Solutions to the problems in the intercloud communication:

As shown in figure 14 we can see the various security perimeters which describe where the security needs to be implemented.

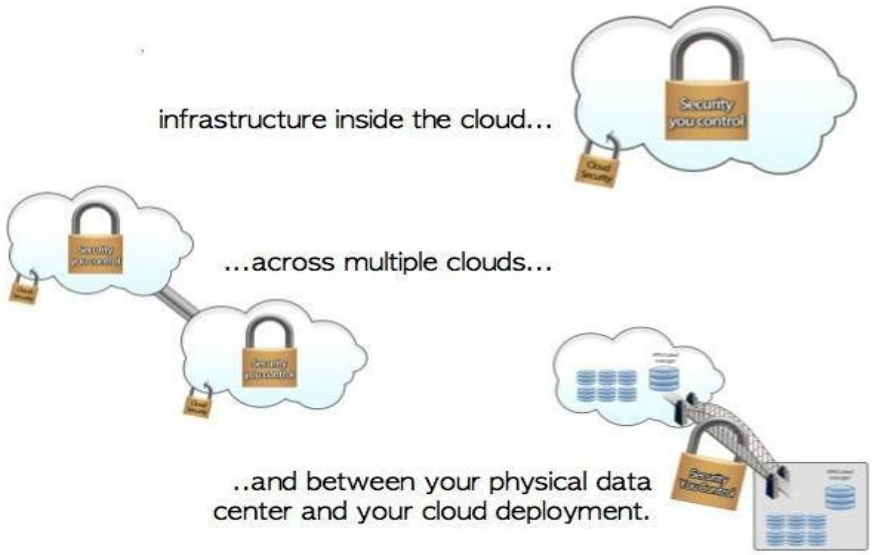

Figure 14. *Security parameter for cloud computing.*

6.2.1. Security in Infra structure inside the cloud: The Main issue with cloud computing is that when we move our information into the cloud, we lose control over it. The cloud gives us access to the data, but we have no way of ensuring no one else has access to the data.SSL protocol is the basis of all that protocol that implements security. For handling security Cloud will contain one more component known as "Cloud Certifier" is installed. Cloud Certifier is responsible for assigning maintaining reviewing node controller key within the cloud infrastructure so that there is no external intrusion that takes place in cloud.

6.2.2. Security across multiple clouds: In this Security aspect also cloud certifier plays an important role. Cloud Certifier not only manages node controllers but also maintains a unique key for the whole cloud architecture which helps in inter-cloud communication. Unique key will only come in picture when a Particular cloud approaches another cloud for resources or data sharing. This unique key will be exchanges between the clouds using "*Diffie-Hellman Algorithm*"[27]. After that whatever request and response any cloud wants to send to other cloud is secure.

6.2.3. Security in Data centers and clouds deployment: This security aspect is the makes use of above two algorithms for data interaction. When the data is sent from data centers to cloud it is encrypted with cloud's unique key. No role is played by public and private key of Node controller in this aspect of security.

7. CONCLUSION

As of June 2015, The Intercloud has yet to show real world demonstration of federation and interoperability, and challenges remain regarding security and trust, governance and legal issues, QoS, monitoring, arbitrage, and billing. The Intercloud is the only solution to the clouds to provide the unlimited services with no barriers by giving flexibility to the users. Hear I give a glans on Intercloud issues and are still under research and development led by the major companies like CISCO pumped with billions of funds

REFERENCES

[1]. "Twenty Experts Define Cloud Computing", SYS-CON Media Inc, http://cloudcomputing.sys-con.com/read/ 612375_p.htm, 2008.

[2]. NIST Cloud Computing Special publication, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, July 2011.

[3]. "Twenty Experts Define Cloud Computing", SYS-CON Media Inc, http://cloudcomputing.sys-con.com/read/612375_p.htm, (January 25, 2011

[4]. Foster, I., Zhao, Y., Raicu, I., Lu, S.: Cloud Computing And Grid Computing 360-Degree Compared. IEEE Grid Computing Environments, Gce (2008)

[5]. "What is Cloud Computing?", Whatis.com. http://searchsoa.techtarget.com/sDefinition/0,,sid26_gci1287881,00.html, 2008.

[6]. Bernstein, David; Ludvigson, Erik; Sankar, Krishna; Diamond, Steve; Morrow, Monique (2009-05-24). "Blueprint for the Intercloud - Protocols and Formats for Cloud Computing Interoperability". IEEE Computer Society.

[7]. Vint Cerf: Despite Its Age, The Internet is Still Filled with Problems

[8]. Head in the clouds? Welcome to the future

[9]. Celesti, F. Tusa, M. Villari, A. Puliafito - How to Enhance Cloud Architectures to Enable Cross-Federation - Cloud Computing (CLOUD). 2010 IEEE 3rd International Conference on Cloud Computing

[10]. http://www.gictf.jp/

[11]. http://standards.ieee.org/develop/project/2302.html

[12]. http://blogs.cisco.com/news/introducing-ciscos-global-intercloud

[13]. Inter-Cloud architectures and application brokering: taxonomy and survey by Nikolay Grozev*,† and Rajkumar Buyya Published online 12 December 2012 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/spe.2168

[14]. Buyya R, Ranjan R, Calheiros RN. InterCloud: utility-oriented federation of cloud computing environments for scaling of application services. In *Proceedings of the 10th International Conference on Algorithms and Architectures for Parallel Processing*. Springer-Verlag: Busan, Korea, 2010; 13–31.

[15]. Amazon. Summary of the Amazon EC2 and Amazon RDS Service Disruption. Available from: http://aws.amazon. com/message/65648/ [last accessed 1 June 2012].

[16]. F. Feldhaus, "Cloud Interoperability."

[17]. N. Grozev and R. Buyya, *"InterCloud architectures and application brokering: taxonomy and survey"*, Software: Practice and Experience, 2012.

[18]. Weiss, A.: Computing in the Clouds. NetWorker 11(4), 16–25 (2007)

[19]. VMware: Migrate Virtual Machines with Zero Downtime, http://www.vmware.com/

[20]. Spring.NET, http://www.springframework.net (March 17, 2010)

[21]. Buyya, R., Abramson, D., Giddy, J., Stockinger, H.: Economic Models for Resource Management and Scheduling in Grid Computing. Concurrency and Computation: Practice and Experience 14(13-15), 1507–1542 (2002)

[22]. D. Vij, D. Bernstein, "IEEE P2302™/D0.2 Draft Standard for Inter-Cloud Interoperability and Federation (SIIF)", Institute of Electrical and Electronics Engineers, Technical Report IEEE P2302/D0.2, January 2012.

[23]. A. Celesti, F. Tusa, M. Villari, and A. Puliafit, "Security and Cloud Computing: InterCloud Identity Management Infrastructure", in Proc. The 2010 IEEE 19th International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE'10), Larissa, pp. 263-265, June 28-30, 2010.

[24]. J. ABAWAJY, "ESTABLISHING TRUST IN HYBRID CLOUD COMPUTING ENVIRONMENTS", IN PROC. THE 2011 IEEE 10TH INTERNATIONAL CONFERENCE ON TRUST, SECURITY AND PRIVACY IN COMPUTING AND COMMUNICATIONS (TRUSTCOM'11),CHANGSHA, PP. 118-125, NOV 16-18, 2011.

[25]. "Are security issues delaying adoption of cloud computing?" Nestworkworld.com.

[26]. "Cloud Security Alliance Official web page". Cloudsecurityalliance.org

[27]. Diffie–Hellman Key Exchange – A Non-Mathematician's Explanation by Keith Palmgren

AUTHOR'S BIOGRAPHY

V. Ashok Kumar, was born in Srikalahasti, Andhra Pradesh, India on May 22, 1982, Since 2006, he has been working as an Assistant Professor, Dept. of CSE, Srikalahasteeswara Institute of Technology, Srikalahasti, India. He received B.Tech (CSE) in 2005 from SKIT, Srikalahsti, M.Tech in 2010 from School of IT, JNTUH, Hyderabad. His research interests Virtualization Techniques and Cloud Computing.