Intercloud Exchanges and Roots Topology and Trust Blueprint

D. Bernstein[1], **D. Vij**[1]
[1]Huawei Technologies, Ltd, Santa Clara, California, USA

Abstract - *Cloud computing is a new design pattern for large, distributed datacenters. Initially, Service providers offering included cloud enabled productivity applications such as search, email, and social networks. Recently they have expanded their offerings to include compute-related capabilities such as virtual machines, storage, and complete operating system services. The cloud computing design yields breakthroughs in geographical distribution, resource utilization efficiency, and infrastructure automation. These "public clouds" have been replicated by IT vendors for corporations to build "private clouds" of their own. Public and private clouds offer their end consumers a "pay as you go" model - a powerful shift for computing, towards a utility model like the electricity system, the telephone system, or more recently the Internet. However, unlike those utilities, clouds cannot yet federate and interoperate. Such federation is called the "Intercloud". Working groups have proposed a layered set of protocols called "Intercloud Protocols" to solve this interoperability challenges. Instead of each cloud provider establishing connectivity with another in a Point-to-Point manner resulting into an n^2 complexity problem, Intercloud interoperability embodies 1-to-many and many-to-many models as opposed to mere cloud to cloud. This paper is in continuation and subsequently builds on to our earlier "Intercloud" related work. The paper proposes the overall design of decentralized, scalable, self-organizing federated "Intercloud" topology by specifically delving deep into how each "Intercloud" component fits in within the overall topology and how these components interact with each other.*

.

Keywords: "Cloud Computing", "Cloud Standards", "Intercloud", "Cloud Exchange", "RDF", "Ontology"

1. Introduction

Cloud Computing has emerged recently as a new design pattern for a particular type of datacenter, or most commonly, a group of datacenters. Service providers offering applications including search, email, and social networks have pioneered this specific to their application. Recently they have expanded offerings to include compute-related capabilities such as virtual machines, storage, and complete operating system services.

Cloud Computing services as defined above are best exemplified by the Amazon Web Services (AWS) [1][2] or Google AppEngine [3][4]. Both of these systems exhibit all eight characteristics as detailed below. Various companies are beginning to offer similar services, such as the Microsoft Azure Service [5], and software companies such as VMware [6] and open source projects such as UCSB Eucalyptus [7][8] are creating software for building a cloud service.

For the purposes of this paper, we define Cloud Computing as a single logical datacenter which:

- May be hosted by anyone; an enterprise, a service provider, or a government.
- Implement a pool of computing resources and services which are shared amongst subscribers.
- Charge for resources and services using an "as used" metered and/or capacity based model.
- Are usually geographically distributed, in a manner which is transparent to the subscriber (unless they explicitly ask for visibility of that).
- Are automated in that the provisioning, upgrade, and configuration (and de-configuration and roll-back and un-provisioning) of resources and services occur on the "self service", usually programmatic request of the subscriber, occur in an automated way with no human operator assistance, and are delivered in one or two orders of seconds.
- Resources and services are delivered virtually, that is, although they may appear to be physical (servers, disks, network segments, etc) they are actually virtual implementations of those on an underlying physical infrastructure which the subscriber never sees.
- The physical infrastructure changes rarely. The virtually delivered resources and services are changing constantly.
- Resources and services may be of a physical metaphor (servers, disks, network segments, etc.; often called "Infrastructure as a Service" or IaaS) or they may be of an abstract metaphor (blob storage functions, message queue functions, email functions, multicast functions, all of which are accessed by running of code or script to a set of API's for these abstract services; often called

"Platform as a Service" or PaaS). These may be intermixed.

The terms are well accepted now [9]. Use Cases and Scenarios for Cloud IaaS and PaaS interoperability [10][11] have been detailed in the literature along with the challenges around actually implementing standards-based federation and hybrid clouds. The high level architecture for interoperability including a protocol suite and security approach was proposed where the term "Intercloud" was first coined [12].

Additional focus on security architecture was provided [13], and additional focus on how the overall architecture might be used to enable an exchange involving a marketplace was detailed and prototyped [14]. Finally, overall Intercloud technical topology and protocol blueprints have been architected [15], and implementation approaches including presence and dialog, security approach, and semantic ontology model and directory, [16][17][18] have been defined.

This paper initially briefly reviews this work and builds on that technology foundation. The paper goes on to propose detail blueprints of the Intercloud Topology describing how each component exists within the proposed topology and how these components interact with each other.

2. Review of Intercloud Technical Architecture

Cloud instances must be able to dialog with each other. One cloud must be able to find one or more other clouds, which for a particular interoperability scenario is ready, willing, and able to accept an interoperability transaction with and furthermore, exchanging whatever subscription or usage related information which might have been needed as a pre-cursor to the transaction. Thus, an Intercloud Protocol for presence and messaging needs to exist which can support the 1-to-1, 1-to-many, and many-to-many use cases. The discussion between clouds needs to encompass a variety of content, storage and computing resources.

The vision and topology for the Intercloud we will refer to is an analogy with the Internet itself: in a world of TCP/IP and the WWW, data is ubiquitous and interoperable in a network of networks known as the "Internet"; in a world of Cloud Computing, content, storage and computing is ubiquitous and interoperable in a network of Clouds known as the "Intercloud"; this is illustrated in Figure 1.

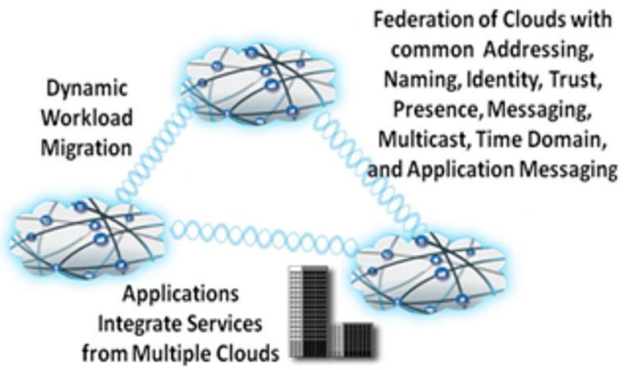

Figure 1. The Intercloud Vision

The reference topology for realizing this vision is modeled after the public Internet infrastructure. Again, using the generally accepted terminology, there are Public Clouds, which are analogous to ISP's. There are Private Clouds which is simply a Cloud which an organization builds to serve itself. There are Intercloud Exchanges (analogous to Internet Exchanges and Peering Points) where clouds can interoperate, and there is an Intercloud Root, containing services such as Naming Authority, Trust Authority, Directory Services, and other "root" capabilities. It is envisioned that the Intercloud root is of course physically not a single entity, a global replicating and hierarchical system similar to DNS [19] would be utilized.

All elements in the Intercloud topology contain some gateway capability analogous to an Internet Router, implementing Intercloud protocols in order to participate in Intercloud interoperability. We call these Intercloud Gateways. The entire topology is detailed in Figure 2.

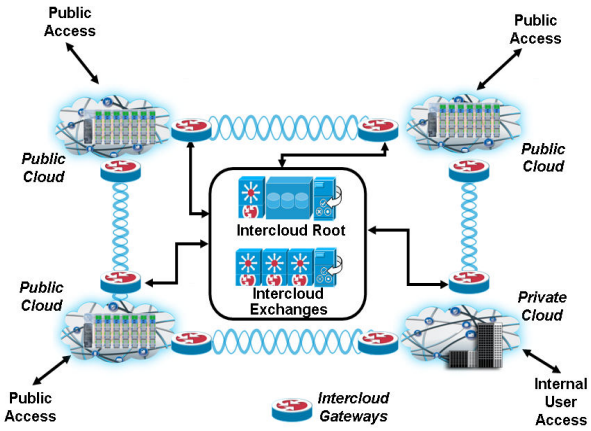

Figure 2. Reference Network Intercloud topology and elements

The Intercloud Gateways would provide mechanism for supporting the entire profile of Intercloud protocols

and standards. The Intercloud Root and Intercloud Exchanges would facilitate and mediate the initial Intercloud negotiating process among Clouds.

Once the initial negotiating process is completed, each of these Cloud instance would collaborate directly with each other via a protocol and transport appropriate for the interoperability action at hand; for example, a reliable protocol might be needed for transaction integrity, or a high speed streaming protocol might be needed optimized for data movement over a particular link.

3. Intercloud Topology – Resources Directory Deployment

As described earlier that various providers will emerge in the enablement of the Intercloud. We first envision a community governed set of Intercloud Root providers who will act as brokers and host the Cloud Computing Resource Catalogs for the Intercloud computing resources. They would be governed in a similar way in which DNS, Top Level Domains [20] or Certificate Authorities [21]: by an organization such as ISOC [22] or ICANN [23]. They would also be responsible for mediating the trust based federated security among disparate clouds by acting as Security Trust Service providers using standards such as SASL [24] and SAML [25].

As part of the proposed topology, we propose that Intercloud Root providers would be federated in nature. Each of these federated nodded in the overall Intercloud topology will independently manage the "root" capabilities such as Cloud Resources Directory Services, Trust Authority, Presence Information etc. Additionally, each Intercloud Root instance will be associated with its affiliated Exchanges by defining the affiliation relationship as part of the Intercloud "root" instance.

In order for the Intercloud capable Cloud instances to federate or otherwise interoperate resources, a Cloud Computing Resources Catalog system is necessary infrastructure. This catalog is the holistic and abstracted view of the computing resources across disparate cloud environments. Individual clouds will, in turn, will utilize this catalog in order to identify matching cloud resources by applying certain Preferences and Constraints to the resources in the computing resources catalog.

The technologies to use for this are based on the Semantic Web [26] which provides for a way to add "meaning and relatedness" to objects on the Web. To accomplish this, one defines a system for normalizing meaning across terminology, or Properties. This normalization is called Ontology. Our earlier work [17] outlined approach for how Cloud Computing resources can be described, cataloged, and mediated using Semantic Web Ontologies, implemented using RDF techniques [27].

Due to the sheer size of global resources ontology information, a centralized approach for hosting the repository is not a viable solution due to the fact that one single entity can not be solely responsible and burdened with this humongous and globally dispersed task:

- Single-point-of-failure
- Scalability
- Security ramifications
- Lack of autonomy as well as arguments related to trust and the authority on data
- etc …

Instead, Intercloud Roots will host the globally dispersed computing resources catalog in a federated manner.

Intercloud Exchanges, in turn, will leverage the globally dispersed resources catalog information hosted by federated Intercloud Roots in order to match cloud resources by applying certain Preferences and Constraints to the resources. From overall topology perspectives, Intercloud Exchanges will provide processing nodes in a peer-to-peer manner on the lines of Distributed Hash Table (DHT) overlay based approach in order to facilitate optimized resources match-making queries. Ontology information would be replicated to the Intercloud Exchanges (DHT overlay nodes) from their affiliated Intercloud Roots using a "Hash" function.

There has already been lot of work done on Semantic Peer-to-Peer based systems – GridVine[28], RDFPeers[29], Piazza[30], PIER[31], and "Distributed Overlay for Federation of Enterprise Clouds" [32].

The basic idea of DHT overlay system is to map a key space to a set of peers such that each peer is responsible for a given region of this space and storing data whose hash keys pertain to the peer's region. The advantage of such systems is their deterministic behavior and the fair balancing of load among the peers (assuming an appropriate hash function).

Furthermore, DHT overlay system provides location transparency: queries can be issued at any peer without knowing the actual placement of the data. Essentially, the DHT peer-to-peer overlay is a self-organizing, distributed access structure, which associates logical peers representing the machines in the network with keys from a key space representing the underlying data structure.

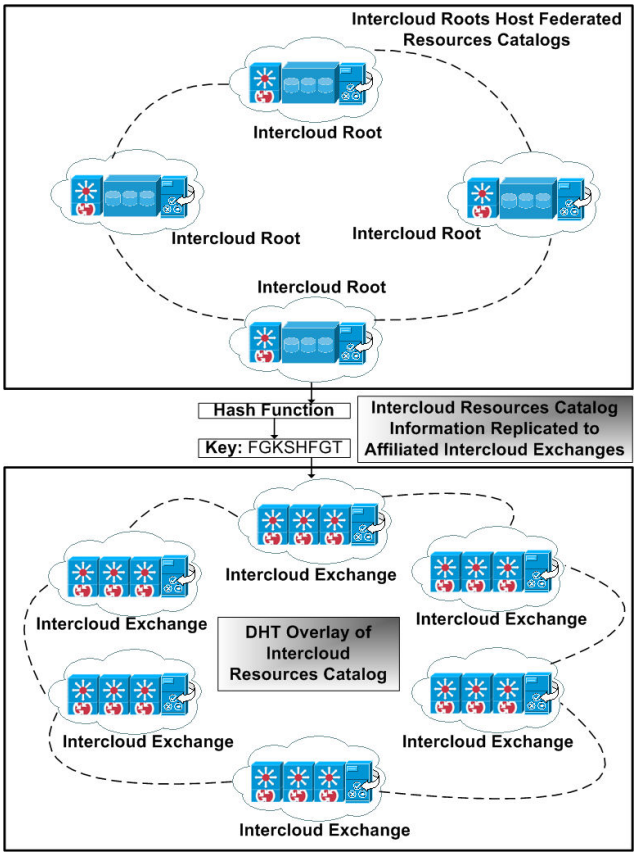

Figure 3. Intercloud Topology – Resources Directory Deployment

Nodes within the DHT overlay system are uniformly distributed across key space and maintain list of neighbors in the routing table. Each peer in the DHT overlay system is responsible for some part of the overall key space and maintains additional routing information to forward queries to neighboring peers. As the number of machines taking part in the network and the amount of shared information evolve, peers opportunistically organize their routing tables according to a dynamic and distributed binary search tree.

4. Intercloud Topology – Collaboration Details

Part of interoperability is that cloud instances must be able to conduct dialog with each other, one cloud must be able to find another cloud, which for a particular interoperability scenarios, is ready, willing, and able to accept an interoperability transaction with and furthermore, exchanging whatever subscription or usage related information which might have been needed as a precursor to the transaction. Thus, an Intercloud Protocol for presence and messaging needs to exist.

Extensible Messaging and Presence Protocol (XMPP) is exactly such a protocol. XMPP is a set of open XML technologies for presence and real-time communication developed by the Jabber open-source community in 1999, formalized by the IETF in 2002-2004, continuously extended through the standards process of the XMPP Standards Foundation. XMPP supports presence and structured conversation of XML data. Our earlier work [18] explains in great detail as far as feasibility of XMPP as control plane operations protocol for Intercloud.

Instead of each cloud provider establishing connectivity with another cloud provider in a Point-to-Point manner resulting into n2 complexity problem, as part of the Intercloud topology we propose that Intercloud Exchanges will help facilitate as mediators for enabling connectivity and collaboration among disparate cloud providers. As stated earlier that Intercloud Exchanges will leverage XMPP as control plane operations protocol for such collaboration and host the XMPP servers in a **Trusted Federated** manner to facilitate the end-to-end collaboration.

In order to establish collaboration with another cloud, an Intercloud enabled cloud will simply send a XMPP message to its affiliated Intercloud Exchange which hosts the XMPP server. If the recipient cloud is affiliated to the same Intercloud Exchange, the XMPP server will send the message directly to the recipient cloud.

On the other hand, if the recipient cloud is affiliated to another Intercloud Exchange, the XMPP server will send the message to the recipient's XMPP server hosted by the affiliated Intercloud Exchange. This is essentially termed as XMPP federation — the ability of two deployed XMPP servers to communicate over a dynamically-established link between the servers. In the Intercloud topology, a server accepts a connection from a peer only if the peer supports TLS and presents a digital certificate issued by a root certification authority (CA) that is trusted by the server — **Trusted Federation**.

In a typical federated identity model, in order for a cloud provider to establish secure communication with another cloud provider, it asks the trust provider service for a trust token. The trust provider service sends two copies of secret keys, the encrypted proof token of the trust service along with the encrypted requested token.

For scenarios where collaboration between initiating cloud provider and recipient cloud provider is across Intercloud Root or Intercloud Exchange, Intercloud Root systems will serve as a Trust Authority and act as the identity providers to mediate trust relationship as part of

the **Trusted Federation**. The detail flow for this scenario is illustrated in Figure 4.

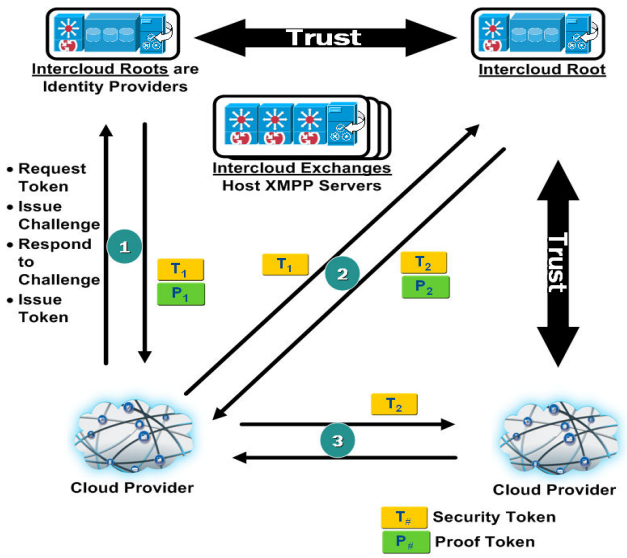

Figure 4. Inter "Intercloud Root" and Inter "Intercloud Exchange" Collaboration Scenario

For scenarios where collaboration between initiating cloud provider and recipient cloud provider is within the same Intercloud Exchange, Intercloud Exchanges will themselves will serve as a Trust Authority and act as the identity providers to mediate the trust relationship as part of the **Trusted Federation**. The detail flow for this scenario is illustrated in Figure 5.

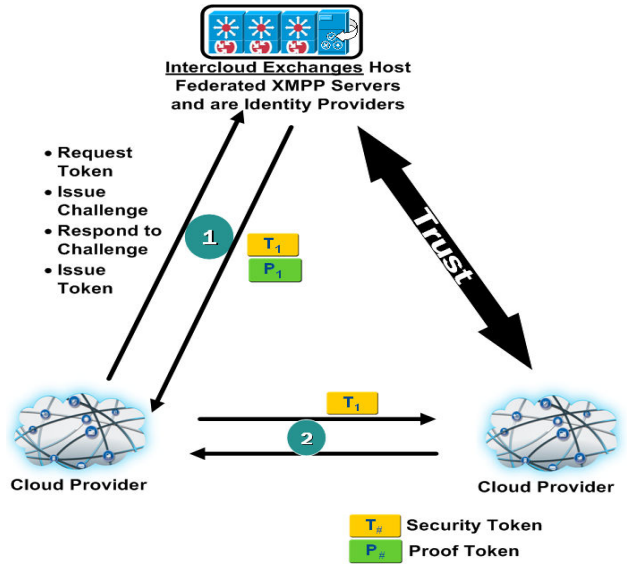

Figure 5. Intra "Intercloud Exchange" Collaboration Scenario

5. Intercloud Topology – PKI Certificates Deployment

In an Intercloud cross-clouds federated environment, security concerns are even more important and complex. Intercloud paradigm or cloud computing paradigm, in general, will only be adopted by the users, if they are confident that their data and privacy are secured. Trust is one of the most fundamental means for improving security across heterogeneous independent cloud environments.

Currently, Public Key Infrastructure (PKI) based trust model is the most prevalent one. PKI trust model depends on a few leader nodes to secure the whole system. The leaders' validity certifications are signed by well established Certificate Authorities ("CA"s).

At a basic level, proposed Intercloud topology subscribes to the PKI based trust model. In accordance to the PKI trust model, the Intercloud Root systems will serve as the Root Certificate Authority (CA) [33] and issue certificates to their affiliated Intercloud Exchange systems.

PKI Certificates not only need to identify the clouds, but the resources the clouds offer, and the workloads that the cloud wishes federation with other clouds, to work upon. Where web sites are somewhat static, and a certificate can be generated to trust the identity of that web site, cloud objects such as resources and workloads are dynamic, and the certificates will have to be generated by a CA. As per the proposed Intercloud topology, the Intercloud Exchange will serve as the intermediate "CA"s, issue temporary PKI certificates to their affiliated cloud providers acting in a just-in-time fashion to provide limited lifetime trust to the transaction at hand.

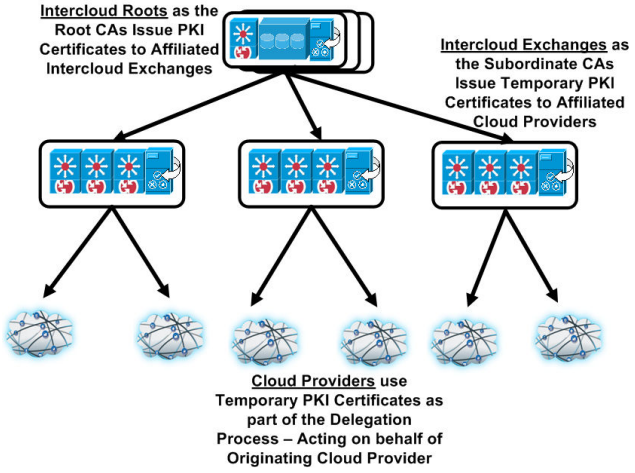

Figure 6. Intercloud PKI Certificates Topology

Cloud Providers, in turn, will use the temporary PKI certificates as part of the delegation process – acting on behalf of the originating cloud provider.

6. Intercloud Topology – Trust Management

From Intercloud topology perspectives, Intercloud Roots will provide PKI CA root like functionality. According to the current PKI based trust model, once the CA authorizes the certificate for an entity, the entity is either trusted or non-trusted. However, in the cloud computing environment, especially in the Intercloud environment, this model needs to be extended to have "Trust Zone" to go along with the existing PKI based trust model. Intercloud exchanges will be responsible for the "Trust Zone" based trust model layered on top of the PKI certificate based trust model.

The overall trust model is more of a "Domain based Trust" model. It divides the cloud provider computing environment into several trust domains. Nodes in the same domain usually are much more familiar with each other; they have a higher degree of trust for each other.

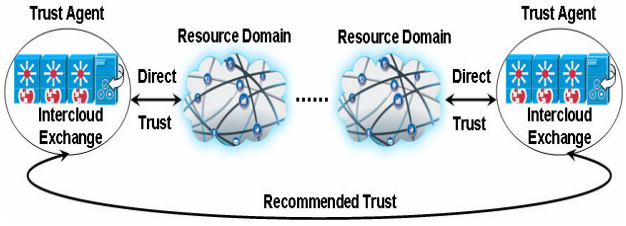

Figure 7. Intercloud Trust Management Model

Exchanges are the custodians/brokers of "Domain based Trust" systems environment for their affiliated cloud providers. Cloud providers rely on the Intercloud exchanges to manage trust. As part of the identification process for matching desired cloud resources, individual consumer cloud provider will signify the required "Trust Zone" value such as "Local Intercloud Exchange" domain or "Foreign Intercloud Exchange". Depending on the desired "Trust Zone" value, for example, one Intercloud provider might trust another provider to use its storage resources but not to execute programs using these resources. Intercloud Exchanges, in turn, will utilize the desired "Trust Zone" value as part of the matching Preferences and Constraints in order to identify matching cloud resources.

At present, as mentioned in the previous paragraph, we are considering a static "Trust Zone" as an extended trust model layered on top of the PKI certificate based trust model. However, in the future, we will also evaluate a dynamic "Trust Index" value assigned to each and every cloud resource type. "Trust Index" is essentially a level of trust demonstrated by cloud providers. Depending on the level of trust (40%, 50%, 60%, or 100%), for example, one Intercloud provider might trust another provider to use its storage resources but not to execute programs using these resources. The *trust level* is specified within a given time because the *trust level* today between two entities is not necessarily the same *trust level* a year ago. Unlike static PKI certificates and "Trust Zone" model, Trust Level is something dynamic in nature.

"Trust Level" is something that is computed in a real time basis by utilizing a Trust algorithm. The algorithm will evaluate the underlying security attributes of a cloud provider such as "Firewall Capabilities", "Intrusion Detection and Anti-Virus Capabilities" and so on. Additionally, cloud provider reputation parameters such as "Prior Success Rate", "Turnaround Time" and so on would be considered as part of the overall determination of "Trust Index". Accordingly, the fuzzy logic based aggregation algorithm will establish the "Trust Index" of a cloud provider. Once calculated, the "Trust Level" of every Intercloud provider could be cached at the affiliated Intercloud Exchange for performance reasons.

7. Conclusions and Future Work

This paper proposes the overall design of decentralized, scalable, self-organizing federated "Intercloud" topology by specifically delving deep into how each "Intercloud" component fits in within the overall topology and how these components interact with each other. In this context, the paper describes various aspects of Intercloud topology components such as Intercloud Resources Directory, Intercloud Collaboration and last but not the least, Intercloud Security.

In order to make this a reality, an operational Intercloud topology must be experimented with in a live public trial. To that regard, we are working towards establishing the Intercloud "Testbed" by collaborating with various well known academic institutions and industry leaders.

8. References

[1] Amazon Web Services at http://aws.amazon.com/
[2] James Murty, *Programming Amazon Web Services; S3, EC2, SQS, FPS, and SimpleDB,* O'Reilly Press, 2008.
[3] Google AppEngine at http://code.google.com/appengine/
[4] Eugene Ciurana, *Developing with Google App Engine,* Firstpress, 2009.

[5] Microsoft Azure, at http://www.microsoft.com/azure/default.mspx
[6] VMware VCloud Initiative at http://www.vmware.com/technology/cloud-computing.html
[7] Nurmi D., Wolski R., Grzegorczyk C., Obertelli G., Soman S., Youseff L., Zagorodnov D., *The Eucalyptus Open-source Cloud-computing System,* Proceedings of Cloud Computing and Its Applications, Chicago, Illinois (October 2008)
[8] Nurmi D., Wolski R., Grzegorczyk C., Obertelli G., Soman S., Youseff L., Zagorodnov D., *Eucalyptus: A Technical Report on an Elastic Utility Computing Architecture Linking Your Programs to Useful Systems,* UCSB Computer Science Technical Report Number 2008-10 (August 2008)
[9] **Youseff, L., Butrico, M. and Da Silva, D.**: *Toward a unified ontology of cloud computing*, Proceedings of the GCE'08 Grid Computing Environments Workshop (2008).
[10] **Mei, L., W.K. Chan, and Tse, T.H.**: *A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues.*, APSCC pp.464-469, 2008 IEEE Asia-Pacific Services Computing Conference (2008).
[11] Cloud Computing Use Cases Google Group, http://groups.google.com/group/cloud-computing-use-cases , http://www.scribd.com/doc/18172802/Cloud-Computing-Use-Cases-Whitepaper
[12] **Bernstein, D., Ludvigson, E., Sankar, K., Diamond, S., and Morrow, M.**, *Blueprint for the Intercloud - Protocols and Formats for Cloud Computing Interoperability*. In Proceedings of ICIW '09, the Fourth International Conference on Internet and Web Applications and Services, pp. 328-336 (2009).
[13] **Yildiz, M., Abawajy, J., Ercan, T., and Bernoth, A.**: *A Layered Security Approach for Cloud Computing Infrastructure*, ISPAN, pp.763-767. In Proceedings of the 10th International Symposium on Pervasive Systems, Algorithms, and Networks (2009).
[14] **Buyya, R., Pandey, S., and Vecchiola, C.**: *Cloudbus toolkit for market-oriented cloud computing*. In Proceedings of the 1st International Conference on Cloud Computing (CloudCom) (2009).
[15] **Bernstein, D.: The Intercloud:** *Cloud Interoperability at Internet Scale*. In Proceedings of the 2009 NPC, pp. xiii (Keynote 2), Sixth IFIP International Conference on Network and Parallel Computing (2009).
[16] **Bernstein, D., Vij, D.**: *Using XMPP as a transport in Intercloud Protocols,* In Proceedings of CloudComp 2010, the 2nd International Conference on Cloud Computing (2010).
[17] **Bernstein, D., Vij, D.**: *Using Semantic Web Ontology for Intercloud Directories and Exchanges*. In Proceedings of ICOMP'10, the 11th International Conference on Internet Computing (2010).
[18] **Bernstein, D., Vij, D.**, *Intercloud Directory and Exchange Protocol Detail using XMPP and RDF*, Proceedings of IEEE 2010 International Workshop on Net-Centric Service Enterprises: Theory and Application (NCSE2010) (2010).
[19] Domain Names – Concepts and Facilities, and related other RFCs, http://www.ietf.org/rfc/rfc1034.txt
[20] *Domain Name System Structure and Delegation*, at http://www.ietf.org/rfc/rfc1591.txt
[21] *Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework,* at http://tools.ietf.org/html/rfc3647
[22] *The Internet Society,* at http://www.isoc.org/
[23] *The Internet Corporation for Assigned Names and Numbers*, at http://www.icann.org/
[24] *Simple Authentication and Security Layer (SASL*), at http://tools.ietf.org/html/rfc4422
[25] *Security Assertion Markup Language (SAML*), at http://saml.xml.org/saml-specifications
[26] *W3C Semantic Web Activity*, at http://www.w3.org/2001/sw/
[27] *Resource Description Framework (RDF*), at http://www.w3.org/RDF/
[28] **Aberer, K., Cudr´e-Mauroux, P., Hauswirth, M., and Van Pelt, T.**: *GridVine: Building Internet-Scale Semantic Overlay Networks*, International Semantic Web Conference, volume 3298 of Lecture Notes in Computer Science, pages 107–121. Springer (2004).
[29] **Cai, M. and F. Martin.**: *RDFPeers: a scalable distributed RDF repository based on a structured peer-to-peer network.*, WWW '04: Proceedings of the 13th international conference on World Wide Web, pages 650–657, New York, NY, USA. ACM Press (2004).
[30] **Tatarinov, I., Ives, Z., Madhavan, J., Halevy, A., Suciu, D., Dalvi, N., Dong, X., Kadiyska, Y., Miklau, G., and Mork, P.**, *The Piazza Peer Data Management Project*. SIGMOD Record, 32 (2003).
[31] **Huebsch, R., Hellerstein, J., Lanham, N., Loo, B. T., Shenker , S., and Stoica, I.**, *Querying the Internet with PIER.*, VLDB 2003, Proceedings of 29th International Conference on Very Large Data Bases, September 9-12, 2003, Berlin, Germany, pages 321– 332. Morgan Kaufmann (2003).
[32] **Ranjan, R., and Buyya, R.**, *Distributed Overlay for Federation of Enterprise Clouds (2008)*.
[33] Certificate Authority, http://en.wikipedia.org/wiki/Certificate_authority