

# Intercloud Security

William Strickland  
COP 6938 Fall 2012  
University of Central Florida  
10/08/2012

# Overview

- Problem and motivation
- Intercloud concept
- Security issues in Intercloud
- Intercloud trust model
- Intercloud identity & access management
- Encryption and key management
- Governance considerations

# Problem and Motivation


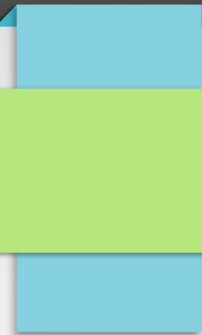
- A 'Cloud' is really just a special type of datacenter (or design pattern for datacenters).
  - Pool of resources shared by subscribers with pay-per-usage billing model.
  - Automated provisioning and configuration from self-service interactions of users.
  - Providing resources that are either of physical metaphor (CPU, disk, network, etc) or abstract metaphor (blob storage, queues, multicast, etc).
  - Services/Resources provided virtually (implementations of virtual resources which is transparent to the user).
  - Physical infrastructure static, virtual infrastructure constantly changing.

- 
- 
- While the Cloud approach provides many benefits it still has limitations.
    - Limited amount of resources.
    - Limited types of services provided.
    - Limited geographical presence.
    - Good but not perfect fault tolerance.
  - Solution – combine the clouds.
    - Federate individual clouds to allow resource sharing
    - Governed by pre-arranged peering / exchange relationship.
    - Requires standardization and communication between clouds.

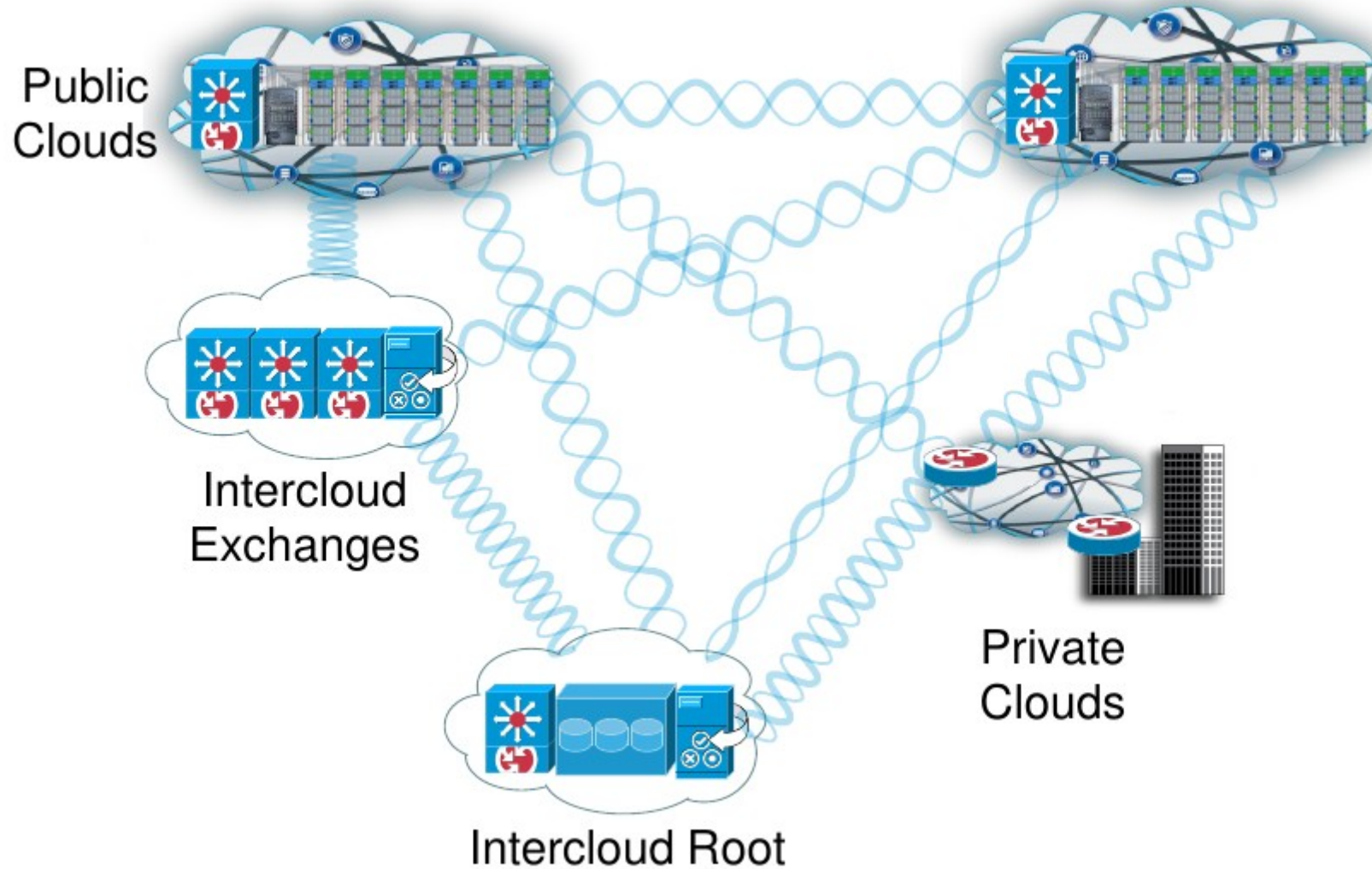
# Intercloud Concept

- Intercloud – “the cloud of clouds”. Name derived from the Internet (network of networks).
- Does not dictate the internal organization or structure used inside of a cloud (intracloud), but rather only the connection between clouds.
- Coordinating the delivery of ubiquitous and interoperable services for content, storage, computation, etc.
- Modeled after the Internet (network of networks) infrastructure.
- Intercloud relies on the generation, maintenance and usage of gathered information about the federated clouds.
- Create among federated clouds common: naming, addressing, Identity, trust, presence, messaging, multicast, time domain and application messaging.

- If every cloud connected to every other cloud directly then there would be  $O(n^2)$  point-to-point connections.
- Uses hierarchy to manage complexity of agreements and communication between clouds. However, not a traditional hierarchy.
  - Governed by a set of Intercloud roots which act as brokers and host listings of resources of other clouds (similar to DNS). Intercloud exchanges facilitate negotiation and communication between clouds.
  - Intercloud roots replicate 'sideways' and 'upwards' methods like p2p technology. Sideways using master node method. Upward by multiply interconnected peers.
  - Clouds communicate with one another as clients.

- 
- 
- Intercloud roots maintain a catalog of all the resources in disparate clouds. The catalog will contain abstract information that will allow users to find matching resources based on their preferences and constraints.
  - This information cannot be centralized because of its scale.
  - Intercloud exchanges provide optimized query services using a Distributed Hash Table overlay. The complete set of all useful information to any given query will not likely be resident (or owned) by a single root.
  - Exchanges get their ontological (normalized semantic information about services provided) data from connected Intercloud roots.
  - Because the internal cloud is not Intercloud aware, an interface between clouds must be made. These connections are made by Intercloud gateways that manage the Intercloud protocol traffic and negotiations of the cloud they are resident in.
  - Extensions to several existing protocols, standards and formats have been proposed to accomplish the goals of Intercloud.

# Federation Illustration




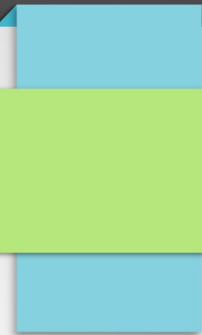


# Security Issues in Intercloud

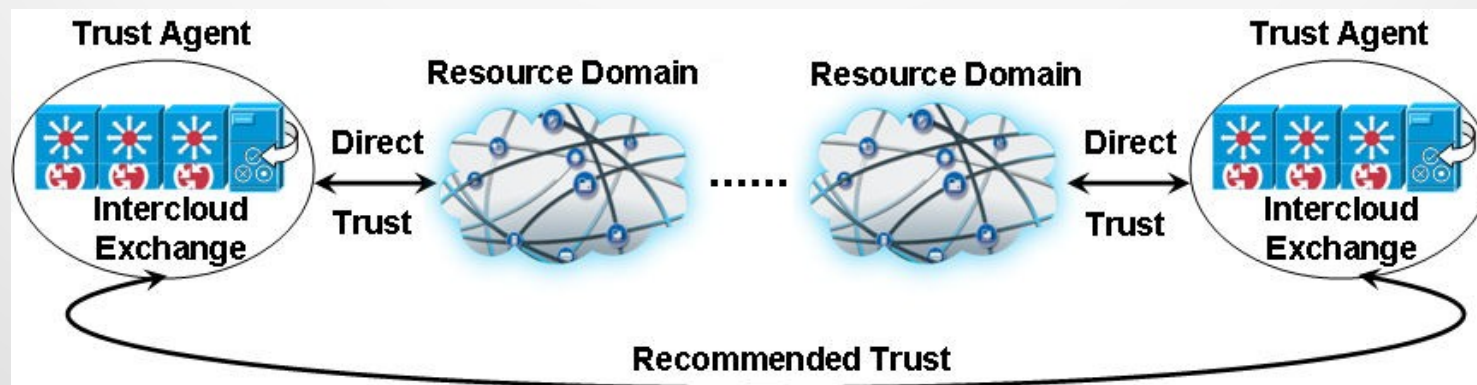
- The goal of Intercloud is the ability to dynamically manage workload between cloud providers with maximum flexibility and choice given to users.
- The primary security concern is the ability of tasks to cross from one administrative domain to another and be serviced (at some cost) for the user.
- A trust model is required to allow tasks to seamlessly migrate from one cloud to another without user intervention.
- Additionally, sensitive information about the tasks (and user) should not be disclosed during the migration.

# Intercloud Trust Model

- Fundamentally based on the PKI trust model, but accepting that the PKI all-or-nothing concept of trust is ill-suited to the Intercloud.
- A trust index is instead utilized between providers.
- This allows a provider to limit the access that another cloud may have on a user's behalf; e.g. Allow disk storage, but not the creation of virtual servers.
- The trust index of one provider to another is dynamic and will fluctuate over time. Unlike static PKI certificates.
- Intercloud roots provide the PKI Certificate Authority function in this model. However, the Intercloud exchanges facilitate the determination of the trust index between clouds.

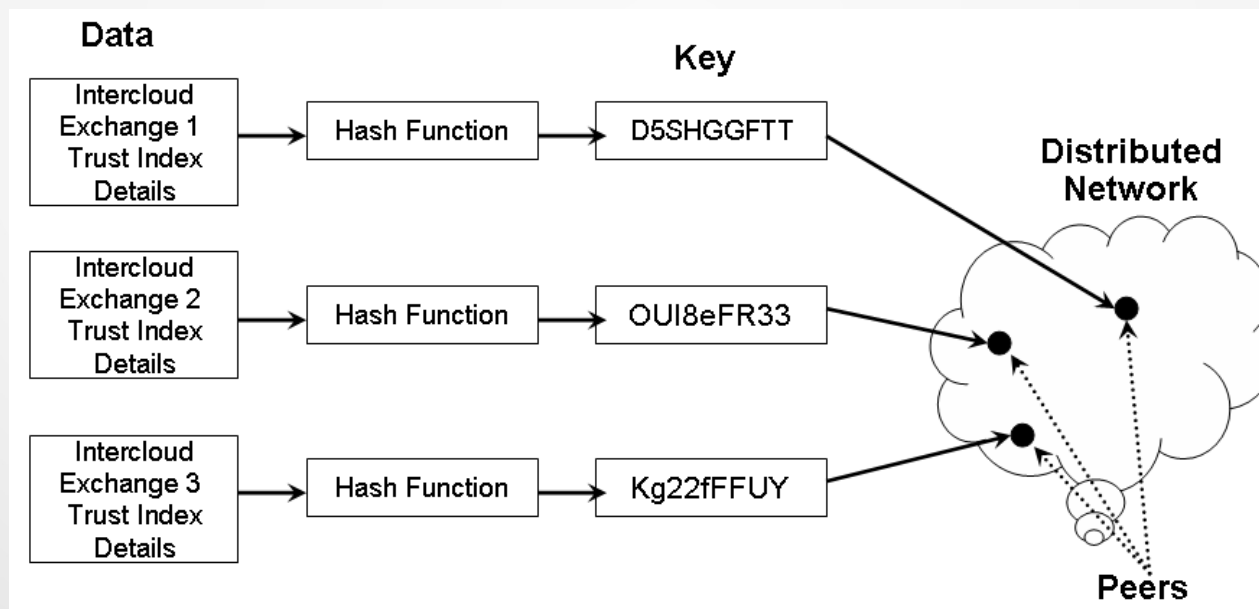
- 
- 
- While very successful for the Web, PKI is argued to not be suitable for the Intercloud.
    - PKI trust is established periodically (usually annual) when certificates are renewed.
    - Trust not only be granted to the cloud itself, but to each and every resource/workload that is to be federated.
    - Issuing a all-or-nothing trusted certificate works well for trusting relatively static web sites, but not for dynamically (potentially short lived) resources and workload.
    - Intercloud exchanges become analogous to intermediate certificate authorities in PKI as they must provide trust (by trust granted by the root) and provide trust to the operating levels (the cloud providers resources/workloads).
    - Unlike PKI, Intercloud exchanges must provide just-in-time short term trust.

- The Intercloud trust model divides individual cloud provider computing environment into domains.
- Nodes in a domain typically have higher trust to other nodes in that domain due to familiarity.
- Intercloud exchanges must then manage trust between domains.
- Trust is stored by domain and resource type (e.g. compute, storage, etc.).
- It is proposed that trust is ranked by not only audited facts such as firewall or anti-virus, but also quality of service metrics such as success rate and turn around time on previous requests.



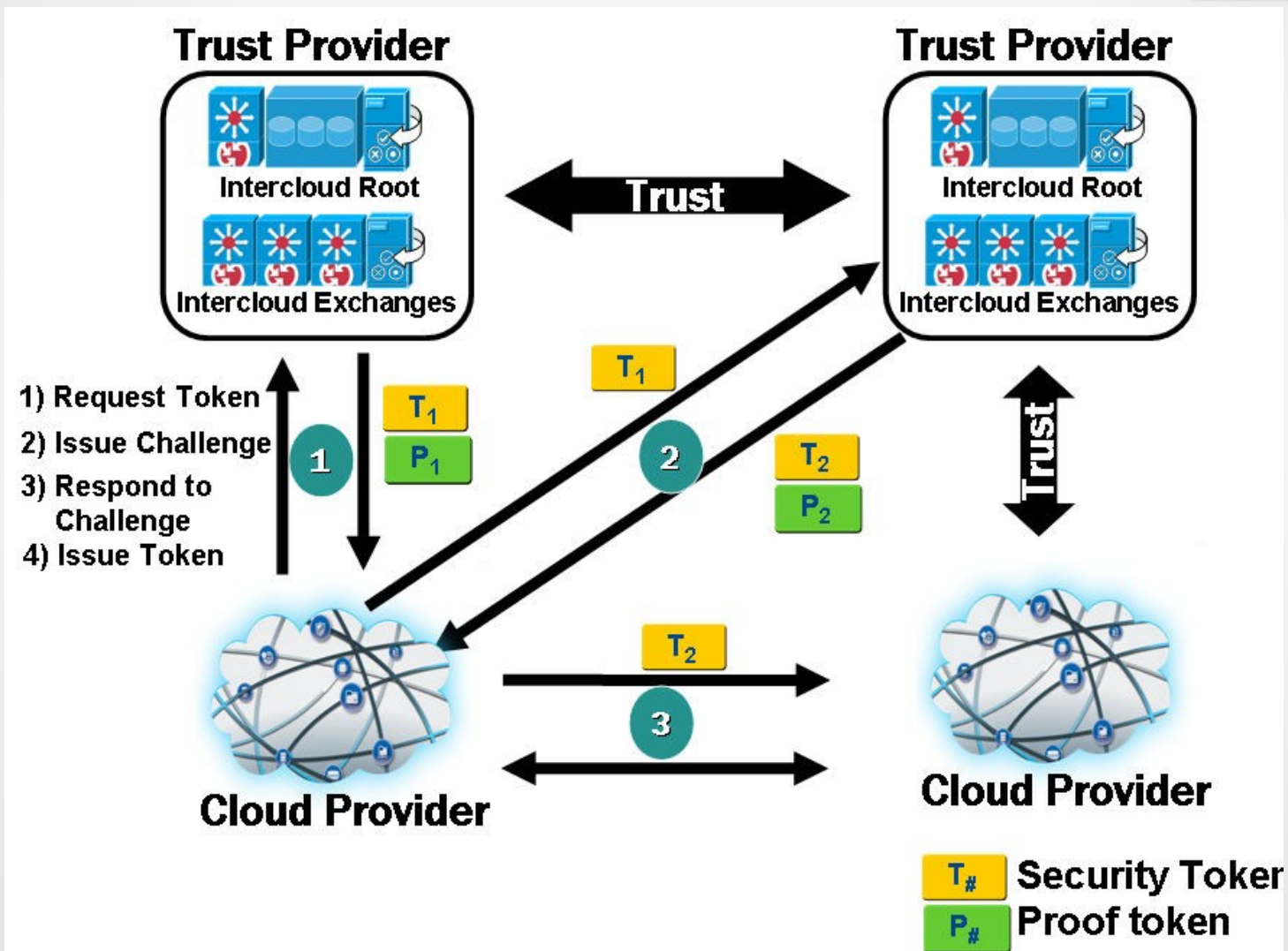
### Distributed Hash Table

- Intercloud exchanges are proposed to use DHT for trust information (similar to how query data is stored)
- Trust queries use DHT to deterministically retrieve the partitioned data, without the requesting exchange actually knowing the location of the exchange with the data.



# Intercloud IAM (Identity and Access Management)

- Another key problem in federating clouds is the management of identify and access permissions across clouds.
  - Key functionality provided by IAM includes: user provisioning, user management, authorization and identify data integration/virtualization.
- Intercloud exchanges facilitating this functionality by being the trusted third parties between cloud providers to establish cryptographic session keys for communication.
- Currently, most cloud providers only have proprietary means of controlling granular (resource level) access.
- It is proposed that the eXtensible Access Control Markup Language XACML language (standardized by OASIS) is used to standardize the communication of access controls and policies between clouds.





# Encryption and Key Management

- Because of the the inherent lack of a well defined perimeter with Intercloud, data must be protected at rest and in transit.
- Encryption can (potentially) protect the data in both cases.
- Unfortunately, encryption is only as strong as its key management policy.
- There is no silver bullet for key management as it is more than a technical problem and involves people and processes as well.
- Key management is also complicated by the fact that the data must be encrypted/decrypted everywhere it is used or generated. For Intercloud this could be potentially anywhere.
- Key Management Interoperability Protocol (KMIP, also standardized by OASIS) is the proposed method for key management for Intercloud.



# Governance Considerations

- As with all cloud issues. Data privacy and security is a critical question with Intercloud. In fact, the inherent leverage of multiple cloud providers (even transparently) makes issues concerning governance even more complicated.
- It is likely that the criteria and preferences of an applications data must include not only performance and reliability attributes, but also those of legal importance.
- For this to gain acceptance, a user must have the ability to limit where sensitive data can be migrated.
- Not all clouds will be suitable to host all data and applications due to security measures of the provider, government regulations on the cloud itself and also trust given the provider by the user.
- It is advised that migration between clouds be a opt-in process rather than Opt-out.

# Resources

- [1] Bernstein, D.; Vij, D.; , "Intercloud Security Considerations," Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on , vol., no., pp.537-544, Nov. 30 2010-Dec. 3 2010 doi: 10.1109/CloudCom.2010.8
- [2] Bernstein, D.; Ludvigson, E.; Sankar, K.; Diamond, S.; Morrow, M.; , "Blueprint for the Intercloud - Protocols and Formats for Cloud Computing Interoperability," Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference on , vol., no., pp.328-336, 24-28 May 2009 doi: 10.1109/ICIW.2009.55
- [3] Bernstein, D.; Vij, D.; Diamond, S.; , "An Intercloud Cloud Computing Economy - Technology, Governance, and Market Blueprints," SRII Global Conference (SRII), 2011 Annual , vol., no., pp.293-299, March 29 2011-April 2 2011 doi: 10.1109/SRII.2011.40
- [4] Bernstein, D.; Vij, D.; , "Intercloud Directory and Exchange Protocol Detail Using XMPP and RDF," Services (SERVICES-1), 2010 6th World Congress on , vol., no., pp.431-438, 5-10 July 2010 doi: 10.1109/SERVICES.2010.131
- [5] Muhammad Bilal Amin, Wajahat Ali Khan, Ammar Ahmad Awan, and Sungyoung Lee. 2012. Intercloud message exchange middleware. In Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication (ICUIMC '12). ACM, New York, NY, USA, , Article 79 , 7 pages. doi: 10.1145/2184751.2184845