ISSN No. 0976-5697

Volume 8, No. 4, May 2017 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Intercloud Trust Model: An Architecture for secure Federated Inter-Cloud identity management

Sangeet kumar
Research Scholar
Ph.D. (CSA), SBBS University
Jalandhar, Punjab, India.
sangeetkumararora@yahoo.com

Niraj Passi
Assistant Professor
PG Dept. Of Computer Science
DAV College
Jalandhar, Punjab, India.
niraj.passi@yahoo.in

***Abstract*— similar as the internet is the network of networks, the evolution from clouds towards the Inter-cloud, a global cloud of clouds, represents a huge development of new innovative value-added services. One of the challenges in the field of Inter-Cloud is identity Management. Up to now, no concepts have been developed that consider the characteristics of Inter-clouds as well as the needs and rights of the users. Therefore, Trust model DHT (Distributed Hash Table) aims to develop technical and organizational solutions from secure federated inter-Cloud Identity management. This paper shows the work in progress on this specific aspect introducing a realistic scenario (inter-cloud services used in a disastrous event), giving an overview on the subject, identifying key issues of Federated Identity Management and presenting an outlook on further research.**

Keywords-cloud computing,intercloud,federated.

I .INTRODUCTION

In July 2009 in Japan, an effort called the Global Inter-Cloud Technology Forum (GICTF) 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"[15]. As of mid-2012 they have over 85 member companies and have published proposed use cases as well as technical documents. 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 [13]. A 'Cloud' is really just a special type of datacenter (or design pattern for datacenters). It is a pool of resources shared by subscribers with pay-per-usage billing model. It is an 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. The Cloud forces enterprises to reshape their connectivity .Existing networks have not been designed to support the new paradigm created by cloud computing. The internet is not enterprise-grade: it lacks security, visibility and reliability. Neither rigid legacy WANs can properly address the cloud connectivity challenges. It is all about integrating the complexity of corporate networks with the diversity of geographically distributed cloud providers. These new requirements force IT organizations to reshape their external connectivity.

II. INTERCLOUD

Intercloud is a term used in IT to refer to a theoretical model for cloud computing services. The idea of the intercloud relies on models that have already been shown to be effective in cases like the global Internet and the 3G and 4G wireless networks of various national telecom providers. Experts sometimes refer to the intercloud as a cloud of clouds. The idea behind an intercloud is that a single common functionality would combine many different individual clouds into one seamless mass in terms of on-demand operations. To understand how this works, it's helpful to think about how existing cloud computing setups are designed. Cloud hosting is largely intended to deliver on-demand services. Through careful use of scalable and highly engineered technologies, cloud providers are able to offer customers the ability to change their levels of service in many ways without waiting for physical changes to occur. Terms like rapid elasticity, resource pooling and on-demand self-service are already part of cloud hosting service designs that are set up to make sure the customer or client never has to deal with limitations or disruptions. Building on all of these ideas, the intercloud would simply make sure that a cloud could use resources beyond its reach by taking advantage of pre-existing contracts with other cloud providers.

WHAT'S DIFFERENT ABOUT INTERCLOUD?

What makes the intercloud differ from today's global application delivery architectures is the ability to base the data-center decision on businessy-type (non IT) data. This data is necessary to construct the appropriate rules against which request decision making processes can be evaluated. While global application delivery systems today are capable of understanding a great many variables, there are a few more nascent data points it doesn't have such as cost to serve up an application (service) or labor costs or a combination of time of day and any other variable

.

III. INTERCLOUD ARCHITECTURE FRAMEWORK

The Intercloud Architecture Framework as depicted in fig 1, introduced in [7], address the interoperability and integration issues in the current and emerging heterogeneous multidomain and multi provider clouds that could host modern and future critical enterprise and e-Science infrastructures and applications [16] including integration and interoperability with legacy campus/enterprise infrastructure. The ICAF consist of the flowing components shown in figure.

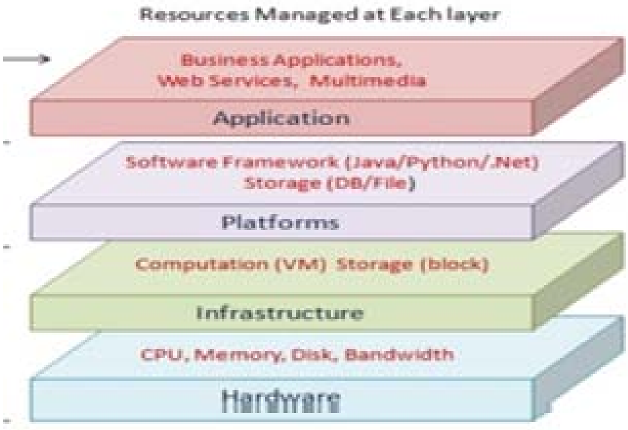
Resources Managed at Each layer
Business Applications, Web Services, Multimedia
Application
Software Framework (Java/Python/.Net) Storage (DB/File)
Platforms
Computation (VM) Storage (block)
Infrastructure
CPU, Memory, Disk, Bandwidth
Hardware

Fig 1: Intercloud Layered Architecture

1) Multilayer Cloud Services Model (CSM) for vertical cloud services interaction, integration and compatibility that defines both relations between cloud service models (such as IaaS, PaaS, SaaS) and other required functional layers and components of the general cloud based services infrastructure [19].

2) Intercloud Control and Management Plane (ICCMP) for Intercloud applications/infrastructure control and management, including inter-applications signaling, synchronization and session management, configuration, monitoring, run time infrastructure optimization including VM migration, resources scaling, and jobs/objects routing[14].

3) Intercloud Federation Framework (ICFF) to allow independent clouds and related infrastructure components federation of independently managed cloud based infrastructure components belonging to different cloud providers and/or administrative domains; this should support federation at the level of services, business applications, semantics, and namespaces, assuming necessary gateway or federation services.

4) Intercloud Operation Framework (ICOF) which includes functionalities to support multi-provider infrastructure operation, including business workflow, SLA management and accounting [14]. ICOF defines the basic roles, actors and their relations in sense of resources operation, management and ownership. ICOF requires support from and interacts with both ICCMP and ICFF. The ICFF is the main framework which creates the Intercloud itself.

IV. 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 [1]. 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.

V. INTERCLOUD TRUST MODEL

Fundamentally based on the PKI (Public Key Infrastructure) 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 establish 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 trusted (by trust granted by the root) and provide trust to the operating levels (the cloud provider's 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 antivirus, but also quality of service metrics such as success rate and turnaround time on previous requests. Intercloud exchanges are proposed to use DHT (Distributed Hash Table) 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.

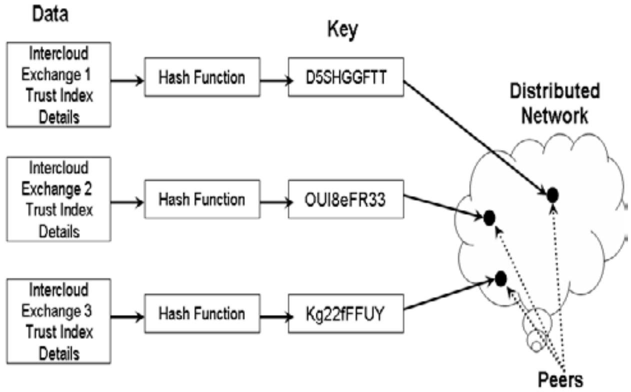
Data
Key
Intercloud Exchange 1 Trust Index Details
Hash Function
D5SHGGFTT
Intercloud Exchange 2 Trust Index Details
Hash Function
OUI8eFR33
Intercloud Exchange 3 Trust Index Details
Hash Function
Kg22fFFUY
Distributed Network
Peers

Fig II. Intercloud Security Model using Encryption.

VI. INTERCLOUD IAM

Another key problem in federating clouds is the management of identify and access permissions across clouds [3].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 XACML language (standardized by OASIS) is used to standardize the communication of access controls and policies between clouds.

VII. ENCRYPTION AND KEY MANAGEMENT

Because of 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 [12]. 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) [2] is the proposed method for key management for Intercloud.

VIII. GOVERNANCE CONSIDERATIONS

Data privacy and security is a critical question with Intercloud [22]. 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 an opt-in process rather than Opt-out.

IX. CONCLUSION

With the Intercloud Trust Model, Intercloud IAM and Encryption & key management we are able to propose a secure architecture for federated intercloud identity management. Trust Model proposed the use of DHT for secure exchange of trust information between clouds. IAM provides the key functionality: user provisioning, user management, authorization and identify data integration/virtualization. Key management and encryption technique deals with the secure mutual authentication between the source and the target clouds to counter measures potential attacks that may use the migration process to destroy the data being migrated. The protocol also ensures that the migration process is initiated by the authenticated owner of the data and not by a malicious one trying to modify the data. This also requires more investigation and experiments. Therefore, as future work we plan to investigate more on security and privacy for migration of trust information between different clouds.

REFERENCES

[1] Bernstein D., Vij D. "Intercloud Security Considerations," Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference., pp.537-544, doi: 10.1109/CloudCom.2010.8, Nov. 30 2010-Dec. 3 2010.

[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, doi: 10.1109/ICIW.2009.55, 24-28 May 2009

[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, doi: 10.1109/SRII.2011.40, March 29 2011-April 2 2011

[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, doi: 10.1109/SERVICES.2010.131, 5-10 July 2010

[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

[6] “NIST SP 800-145,”A NIST definition of cloud computing”, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, accessed February 2013.

[7] NIST SP 500-292, Cloud Computing Reference Architecture, v1.0.” http://www.nist.gov/customcf/get pdf.cfm?pub id=909505, accessed February 2013.

[8] “Amazon web services”,http://aws.amazon.com/products/, accessed February 2013.

[9] “Microsoft Window Azure.” http://www.windowsazure.com/, accessed February 2013.

10] “Google Cloud Platform.” https://cloud.google.com/, accessed February 2013.

[11] “Rackspace Cloud.” http://www.rackspace.com/cloud/, accessed February 2013.

[12] R. Buyya, R. Ranjan, and R. Calheiros, “Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services,” Algorithms and architectures for parallel processing, pp. 13– 31, 2010.

[13] Y. Demchenko, C. Ngo, M. Makkes, R. Strijkers, and C. de Laat, “Defining inter-cloud architecture for interoperability and integration,” in CLOUD COMPUTING 2012, The Third International Conference on Cloud Computing, GRIDs, and Virtualization, pp. 174–180, 2012.

[14] Y. Demchenko, C. Ngo, C. de Laat, J. Garcia-Espin, S. Figuerola, J. Rodriguez, L. Contreras, G. Landi, and N. Ciulli, “Intercloud architecture framework for heterogeneous cloud based infrastructure services provisioning on-demand.,” 2013.

[15] B. Khasnabish, “Cloud reference framework.” draft-khasnabish-cloud-reference-framework-04.txt, 2012.

[16] “European Grid Infrastructure (EGI).” http://www.egi.eu/about/EGI.eu/, accessed February 2013.

[17] “Geant project.” http://www.geant.net/pages/home.aspx, accessed February 2013.

[18] “Generalised Architecture for Dynamic Infrastructure Services (GEYSERS Project).” http://www.geysers.eu/, accessed February 2013.

[19] J. Garcia-Espin, J. Riera, S. Figuerola, and E. Lopez, “A multi-tenancy model based on resource capabilities and ownership for infrastructure management,” 2012.

[20] “OASIS IDCloud TC: OASIS Identity in the Cloud TC.” http://wiki. oasis-open.org/id-cloud/, accessed February 2013.

[21] Y. Demchenko, M. Cristea, and C. de Laat, “XACML policy profile for multidomain network resource provisioning and supporting authorisation infrastructure,” in Policies for Distributed Systems and Networks, 2009. POLICY 2009. IEEE International Symposium on, pp. 98–101, IEEE, 2009.

[22] G. Garzoglio, I. Alderman, M. Altunay, R. Ananthakrishnan, J. Bester, K. Chadwick, V. Ciaschini, Y. Demchenko, A. Ferraro, A. Forti, et al., “Definition and implementation of a saml-xacml profile for authorization interoperability across grid middleware in osg and egee,” Journal of Grid Computing, vol. 7, no. 3, pp. 297–307, 2009.

[23] Y. Demchenko, A. Wan, M. Cristea, and C. De Laat, “Authorisation infrastructure for on-demand network resource provisioning,” in Grid Computing, 2008 9th IEEE/ACM International Conference on, pp. 95– 103, IEEE, 2008.

[24] L. Gommans, L. Xu, Y. Demchenko, A. Wan, M. Cristea, R. Meijer, and C. De Laat, “Multi-domain lightpath authorization, using tokens,” Future Generation Computer Systems, vol. 25, no. 2, pp. 153–160, 2009.