A Gateway-based Access Control Scheme for Collaborative Clouds

Yongdong Wu, Vivy Suhendra, Huaqun Guo
Institute for Infocomm Research, 1 Fusionopolis Way, Connexis, Singapore
{wydong,vsuhendra,guohq}@i2r.a-star.edu.sg

***Abstract*—A collaborative cloud, formed by private enterprise clouds, is usually task-oriented and tightly correlated. It brings new ways to build and manage computing systems in terms of software development, resource sharing, and maintenance. However, there is little research on the security of collaborative clouds. This paper presents a virtual private cloud for collaborative clouds based on security-enhanced gateways. It enables users in each private cloud to access other private clouds in the collaboration transparently, dynamically and anonymously.**

***Keywords*-Virtual cloud computing; Identity management; Access control.**

I. Introduction

In the computing field, the requirements of cost, security and ease of use are conflicting. PC users have full control of their computers, but in return have to take full responsibility for software installation, patching-up, viruses, spyware, crashes, software and hardware upgrades. This makes the total maintenance cost very high. On the other hand, the low-cost NetPC (or Network PC), known as a thin client, is intended to be centrally managed and to function without diskette drive nor CD-ROM drive. All NetPC software and data are stored on a server and accessed over a private network from the NetPC box. Offering a trade-off between these two situations is the cloud computing paradigm[1], a system that provides services to customers at low cost [1].

In the cloud computing paradigm, a service provider builds the cloud infrastructure, and leases it to users with a "pay-as-you-go" business model. From the viewpoint of users, cloud computing has many merits such as "infinite" scalability, "always-on" availability, light-weight system maintenance[2], fast access to best-of-breed applications, and the potential to significantly reduce operating costs [2]. Thus, cloud computing is becoming one of the most important topics in the IT world, and the use of cloud computing services is an attractive opportunity for companies to improve their IT services. For instance, EMEA (Europe, Middle East and Africa) will spend $18.8 billion on cloud services provided by third-party suppliers in 2014 [3], while China will invest about $154 billion to develop cloud computing hubs. The South Korean government has also decided to invest $500m in cloud initiatives, and intended to raise $2 billion investment by 2014 [4].

Despite the value proposition that cloud computing has, its adoption has been slow due to issues of reliability, consistency, privacy, and federation, especially security issues [5]–[8]. For example, the security breach of Twitter and Vaserv.com (via a zero-day vulnerability) in 2010 and the data breach at Sony Corporation and Go-Grid in 2011 [9], compromising data of 100 million customers [10], have made it quite clear that stringent security measures need to be taken in order to ensure security and proper data control in the cloud. As IDC researchers indicated, "*Security was a long-term inhibitor to cloud adoption*" [11]. Although Cloud Security Alliance promoted the use of best practices for providing security assurance within cloud computing [12], it did not propose a concrete security solution for collaborative clouds, where security risk is amplified and accelerated by the potential spread of a security flaw from a compromised cloud to a collaborative peer.

A collaborative cloud is a cloud community which consists of private enterprise clouds. It comprises virtual computing resources dedicated to a particular collaborative activity (e.g., correlated intrusion analysis [13] or detection [14]), and is subject to information sharing policies that restrict the scope of information sharing within the cloud. Users in each private cloud is able to access the resources of other private clouds in the collaboration (henceforth termed *peer clouds*) in a controllable way. Additionally, as it is impossible to require that all cloud providers offer the same services, users in different clouds may exchange information via third-party platforms (e.g., Facebook). In all, a collaborative cloud is a task-oriented, high-access relationship.

This paper proposes a Virtual Private Cloud (VPC), similar to a virtual domain [15] in Grid computing, based on secure inter-connective cloud gateways. The VPC enables each user to perform authentication in its own cloud so as to obtain access to peer clouds anonymously. It also provides a secure channel for users in the virtual cloud to communicate with each other via a third-party platform.

The remainder of this paper is organized as follows. Section II elaborates the security structure in a VPC environment, particularly the authentication diagram. Section III discusses the security, property and implementation of the proposed VPC. Section IV presents the related work, and a conclusion is drawn in Section V.

[1] According to the definition from National Institute of Standards and Technology (NIST): Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, storage, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

[2] The end user may have to upgrade/patch some basic components such as the OS, browser, media decoders etc.

ISBN: 978-1-61208-201-1

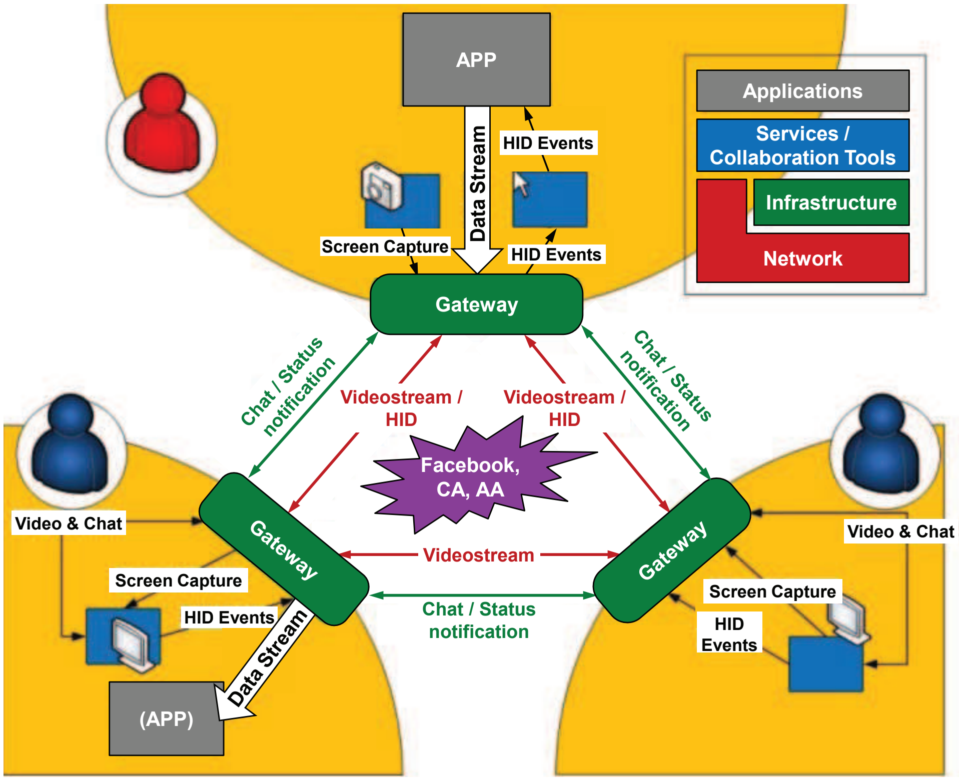

Fig. 1. Gateway-based architecture of VPC, adapted from [16].

II. Virtual Private Cloud

In this paper, we assume that each enterprise has its own private cloud. In order to complete a task, several enterprises will form a collaborative cloud so that they can share resources. As a collaborative cloud is task-oriented, users involved in the task form a virtual team. The team members are dynamic and anonymous to the peer clouds. Further, team members may need to use a third-party platform to communicate with each other because the peer clouds may not have the same communication platform.

As an illustrative example, assume two team members Alice and Bob localized in two different cloud environments, Alice prepared a project presentation for their collaborative project. Bob likes to download the proposal from the database of Alice's home cloud. After reading the proposal, Bob has some questions and wants to solve them with Alice. Because their clouds does not share the same interactive platform, they agree to use Facebook to communicate with each other, but they do not like to disclose their discussion to Facebook.

A. Virtual Private Cloud Diagram

In a VPC, a user in one cloud is able to access the resources in a peer cloud. As each peer cloud has its own authentication mechanism, an identity management mechanism is required to enable users of one private cloud to securely access resources of a peer cloud seamlessly, without requiring redundant user administration. Additionally, in a dynamic collaborative environment, some resources (e.g., enterprises, users, applications or services) may join or leave the environment at any point of time. Hence, we design a gateway-based structure (adapted from [16]) as shown in Figure 1.

In the present diagram, the gateway plays a critical role. It enables secure connection between two private clouds transparently. In addition, as it is highly possible that the clouds do not have the same communication platform, the team members may have to use the third-party platform (e.g., social network) to exchange message or interactive communication such as instant-messenging. The present diagram enables secure communication between two team members when a third-party platform is used.

B. Secure Gateway Structure

We adapt the Grid security architecture [17] [18] for the VPC gateways by adding the data security unit. The architecture includes:

- Traffic Collection Unit: collects traffic from network devices such as routers and servers, or peer secure gateways.
- Traffic Processing Unit: classifies the traffic data from the Traffic Collection Unit, then records information such as IP source and destination addresses along with timestamps in a database.
- Network Security Unit: comprises firewall, IDS and virus scanner, etc., which handles the network security function as local legacy gateway. When a threat is identified, it notifies the Response Unit.
- *Data Security Unit*: the security core of the present VPC

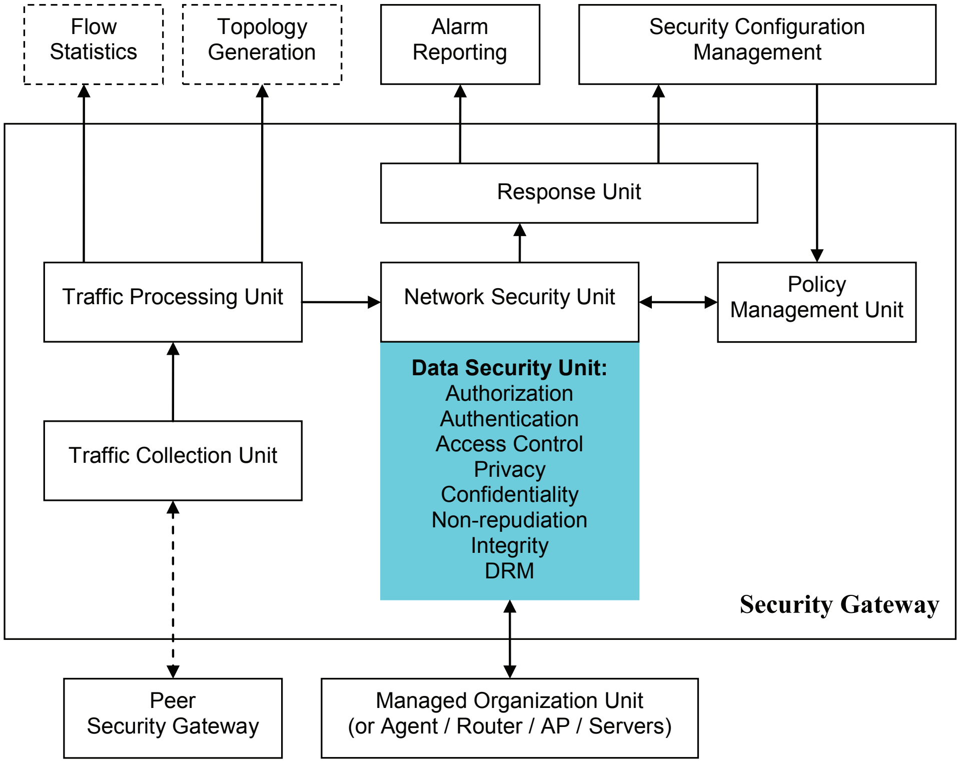

Fig. 2. A VPC gateway structure showing the functional modules.

gateway. It uses the database in Traffic Processing Unit together with the rules from Policy Management Unit to analyze network traffic. When a threat is identified, it notifies the Response Unit.

- Policy Management Unit: provides predefined rules for the Behavior Analysis Unit to identify network anomalies. Depending on management requirement, policies may be updated by Security Configuration Management.
- Response Unit: in the event of detected threats, notifies the Alarm Reporting and Security Configuration Management, who will then react correspondingly.

With reference to Figure 2, a Managed Organization Unit (MOU) may be installed in each computer of the enterprise in order to reduce the burden of the security gateway and to reduce the risk of information leakage. The MOU acts as a coordination point for security functionalities. As different users in an enterprise may have different access priorities and different applications may have different connectivity priorities, the MOU locally enables the users to enjoy cooperation and share resources and services. This capability opens up exciting opportunities for different applications in various fields, such as entertainment, business, healthcare, emergency and education.

C. Secure Connection between VPC Gateways

Figure 3 shows the diagram of the VPC gateway, which comprises two layers. The first layer is used to define and enforce inter-enterprise security, while the second layer is used to define and enforce intra-enterprise security. At the inter-enterprise layer, the gateway includes Network Security Unit (NSU), which is beyond the scope of this paper, and Data Security Unit (DSU). As shown in Figure 2, DSU should implement security functions such as authorization, authentication, access control, confidentiality, and privacy for any transaction between the two private (or enterprise) clouds. In addition, a VPC shall be compliant with the existing private clouds (or peer clouds) and require little change to the intra-enterprise layer. To this end, when a user from a collaborative cloud would like to make use of the resource of a peer cloud, he/she should be treated as a user of the target cloud. Thus, the gateways shall ensure that the security functions can take effect in the process.

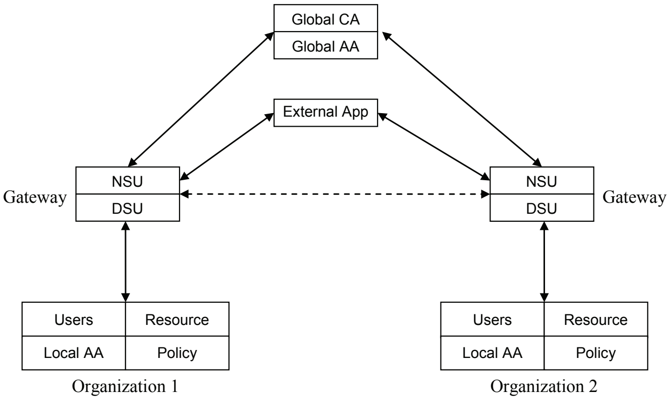

Fig. 3. VPC Gateway connections

ISBN: 978-1-61208-201-1

For simplicity, we assume the channel between two gateways is mutually authenticated with Public Key Infrastructure (PKI). This assumption can be satisfied easily if each gateway has a digital certificate issued by a trusted Certificate Authority (CA). This secure channel ensures the security of communication traffic such as identification management among private clouds.

D. Access Control in the VPC

In the collaborative cloud, the resource are accessible to the cloud users in two modes which are transparent to the users.

1) Access to Intra-cloud Resources: In an enterprise, any user can be verified using the legacy authentication mechanism (e.g., LDAP). If we regard a gateway as a special user of the enterprise, the user and the gateway can be authenticated via the enterprise's internal mechanism so that they can achieve mutual authentication. As the security structure in Figure 3 does not require any change to the internal access control mechanism of an enterprise, access to the internal resources is transparent to the enterprise members.

2) Access to Inter-cloud Resources: In the VPC diagram shown in Figure 4, the gateway can represent any user within its enterprise to send and receive data across clouds. When a user requests a service or resource from the collaborative enterprise, the gateway is authorized to complete the request on the user's behalf once the user-gateway authentication and the user's privilege checking are successful.

As it is impractical to demand that all the collaborative enterprises adopt the same access control strategy, a VPC gateway should translate the access request from its local user to a standard format (e.g. SAML (Security Assertion Markup Language)) so that the gateway in the target enterprise can enforce the access control. For instance, if the user requests access to the resources of a peer cloud, the gateway in the user's enterprise will translate the request into another format that is compliant with the target enterprise, so that the request can be handled as a local request by the target enterprise. In the collaborative inter-cloud access, the requestor pays the target cloud in name of his/her home cloud so as to maintain the anonymity.

Figure 4 illustrates the authentication process for inter-cloud access. When a user wants to access the resource (or service) of one collaborative enterprise, he sends a request to the local authenticator A1 along with his authentication information (e.g., credential, identity/role/attribute). He also notifies the local gateway (e.g., by network traffic sniffing) to send its credential to the local authenticator A1. After the local authenticator A1 verifies their authenticity, it sends the request to the gateway G1.

The gateway G1 translates the request into a "standard" Collaborative Clouds request format (e.g., SAML format), replaces the requestor with an authorized identity, and signs on the translated request. Then it sends the request to the target gateway G2.

The target gateway G2 verifies the request based on the signature of the sending gateway G1 and translates the "standard" request format into its own request format. Then it sends the request to its own authenticator A2. Once A2 authenticates the request, the user can access the resource or service.

3) Access to External Resources: When two users want to communicate with each other via a third-party platform (e.g., Facebook), the virtual cloud should build its own protection, as the third-party platform may provide no protection at all. To guarantee the security level defined by the enterprises, the VPC gateways should ensure end-to-end security. Loosely speaking, both gateways should create a secure channel for any information exchange between them. Specifically, after each user authenticates himself/herself to the third-party platform as usual, the gateway will encrypt all outgoing messages and decrypt all incoming messages.

III. Discussions

A. Security

In the gateway-based access control scheme, we should consider three security issues. The first issue is the intra-cloud security. As the present scheme does not modify the intra-cloud access or identification method, the security level of the private cloud remains the same. The second issue is the inter-cloud security. As the channel between two gateways is authenticated and confidential, the scheme maintains the security of the inter-cloud. Further, as requestors are authenticated in their own private cloud, the inter-cloud has the same level of security as the intra-cloud. The third security issue is third-party attacks. As the present scheme adopts end-to-end security, it has the same security level as the widely-deployed security systems such as HTTPS-based e-business.

B. Property

Transparency: In the present scheme, a user can access intra-cloud resources and inter-cloud resources in the same way (differing only in the target URI), hence the access mechanism is fully transparent to the users.

Anonymity: When a user sends a request to a peer cloud, a pseudo user name will be used to inform the peer cloud, thus enforcing anonymity.

Dynamics: Due to the anonymity property, when a user joins or leaves the virtual cloud (or task group), the home cloud can handle the dynamics without informing the peer clouds. This property simplifies the collaboration management greatly.

C. Implementation

As proof of concept, we built a simple VPC consisting of three private clouds. Each cloud is constructed with computers supporting BIOS virtualization technology so as to simulate a group of computers. And the network is configured with *OpenStack Flat Network* mode.

Within each private cloud, local authentication and identity management is performed with *Kerberos* 10.04, using the GSS-API mechanism. All local users are registered in the Kerberos system. Upon login, the user is issued with a Kerberos ticket that can be forwarded to other Kerberos users, including the VPC gateway, as proof of his identity. Any two Kerberos

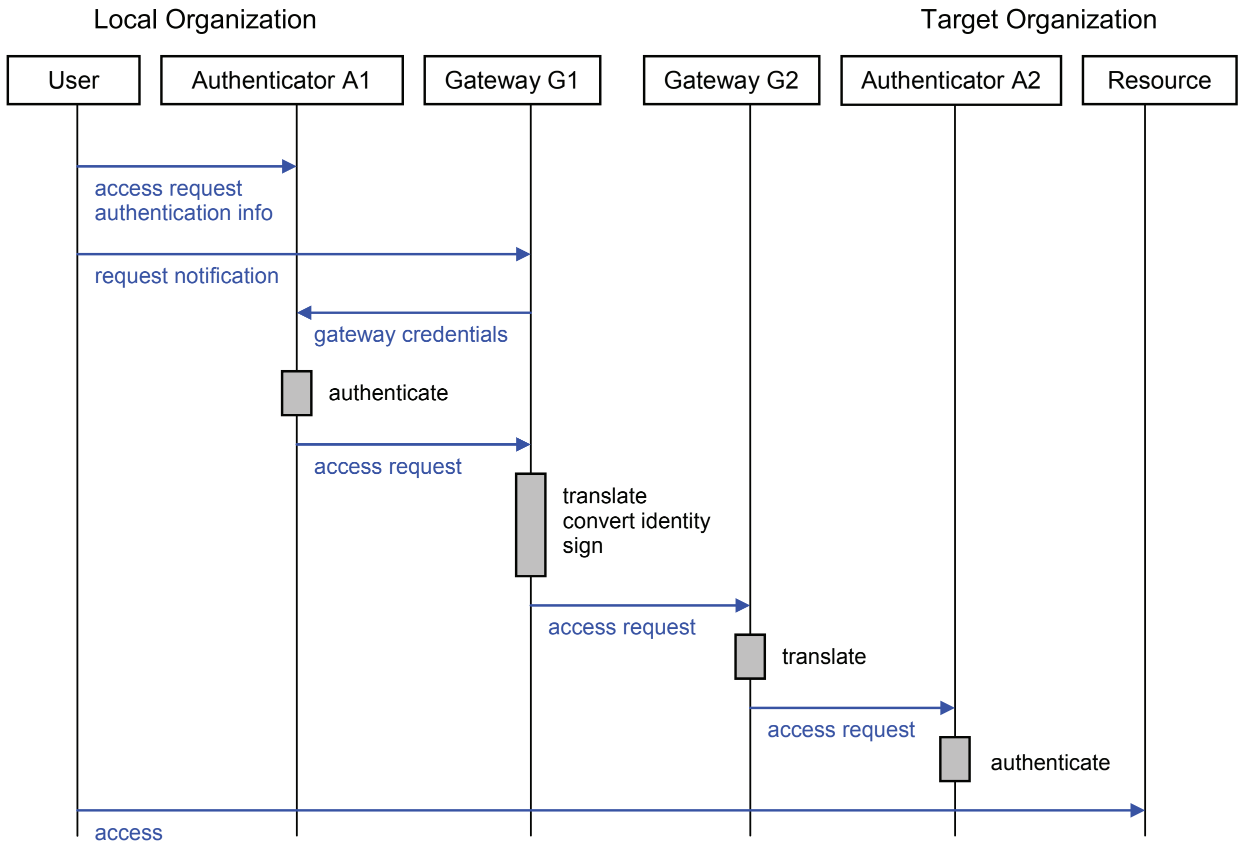

Fig. 4. One-way inter-cloud access

users communicate through a secure channel built by Kerberos GSS-API upon successful mutual authentication. Note that here Kerberos is our choice of mechanism to simulate an existing authentication mechanism in the real practice; the VPC scheme shall apply to any legacy authentication system and identity management. As described earlier in the paper, user identity is verified within his own enterprise and shall be anonymous to peer clouds; hence, there is no need for a dedicated collaborative identity management.

Authentication among VPC gateways across the collaborative cloud uses the Station-to-Station (STS) mutual authentication and key exchange protocol based on PKI. We create a CA within the collaborative cloud that issues signed digital certificates to VPC gateways as they are added to the cloud community. When a VPC gateway contacts another for an inter-cloud request, it first initiates the STS protocol, which includes exchanging certificates for verification and agreeing on a session key, to build a secure communication channel for further processing of the request. Each gateway also keeps a list of known peer gateways along with the services offered within the peer clouds, so that the gateway knows where to route each request.

We tested two scenarios on the VPC. In the first scenario, a user issues a request for a local data resource (i.e., download a file) in the private cloud. In this case, the user is authenticated by his local identity server normally (via Kerberos mechanism in our setting). Upon authorization of access based on the local policy, he then accesses the data directly from the private cloud. In this scenario, the user goes through the same process as he would without the VPC.

In the second scenario, a user issues a request for a data resource in a peer cloud. The access control mechanism in this scenario is as shown in Figure 4. The user request is intercepted by his home gateway, who re-directs the request to the local identity server. The user goes through local (Kerberos) authentication normally, after which, his request is forwarded to the VPC gateway. The VPC gateway proceeds to contact the peer VPC gateway in the target cloud and build a secure communication channel. The user's home VPC gateway processes the request before sending it through the channel, replacing the requestor identity with a pseudo user name to achieve anonymity. Upon receiving the request, the VPC gateway in the destination cloud checks its own local access policy and determines that the user is authorized to access the data requested. The gateway then forwards the request to the resource provider, who then sends the requested data to the user via the two gateways. This scenario shows how VPC can achieve inter-cloud access without altering user experience, that is, the user still goes through the same authentication process in his local server, and the remote authorization mechanism is fully transparent to him.

IV. Related Work

Cloud infrastructure commonly relies on virtualization machines so as to provide the properties of flexibility and application independence. When a user requests for resource properties (such as processor speed, time and memory size), the service provider will create a virtual machine satisfying the request.

Although virtual machines have become increasingly commonplace as a method of separating hostile or hazardous code from commodity systems, the potential security exposure from implementation flaws has increased dramatically. However, cloud security issues cannot be solved with just virtualization technologies [19]. Ormandy [20] investigated the state of popular virtual machine implementations for x86 systems, and assessed the security exposure to the hosts of hostile virtualized environments.

A. Intra-cloud security

Chow et al. [21] suggested to use trusted computing and computation-supporting encryption to enhance the security of cloud computing. Popovic and Hocenski [22] suggested considering privacy and security at every stage of a system design, while other researchers took care of trust [23], [24] and authorization [25].

Takabi et al. [26] proposed a comprehensive security framework for cloud computing environments. They also discussed challenges, existing solutions, approaches, and future work needed to provide a trustworthy cloud computing environment.

Demchenko et al. proposed an architectural framework for on-demand infrastructure service provisioning in [27], and discussed security mechanisms required for consistent DACI (Dynamically provisioned Access Control Infrastructure) operation using authorisation tokens in [28]. Shin and Akkan [29] proposed a domain-based framework for provisioning and managing users and virtualized resources in IaaS to support scalable management of users and resources, organization-level security policy, and flexible pricing model.

As a standard for identity management, SAML defines identity provider (IdP) and service provider (SP). The IdP focuses on identity management, access policy management, and security token generation, while SPs receive the remote security token, retrieve credential data, and reinforce user access policies locally. In practice, the schemes in compliance with IdP/SP model may focus on different properties, e.g., protocol flow [30], scalability [31], privacy [32], friendliness with device identity or user behavior [33], and SSO (Single Sign On) [34]. In all, SAML allows authentication so that a cloud can provide services to users both inside and outside the cloud.

B. Inter-cloud security

Riteau [35] built distributed large-scale computing platforms from multiple cloud providers, allowing to run software requiring large amounts of computation power so as to provide inter-cloud live migration and offer new ways to exploit the inherent dynamic nature of distributed clouds. Similarly, Nguyen et al. [36] presented a cloud architecture that allows users with different security authorizations to securely collaborate and exchange information using commodity computers and familiar commercial client software.

For a cloud community formed by different vendors or enterprises, Kretzschmar and Hanigk [37] intensified cloud security management domains, integrated various cloud security services of an organization and providing interoperability for the clouds. Moreover, Kretzschmar and Golling [38] identified functional components for a Security Manager architecture. These components, together with identified security data artifacts, are able to support the cloud provider community to some extent.

Bernstein et al. presented an InterCloud protocol to solve the cloud computing interoperability problem in [39], and also considered the InterCloud security such as identity management and access control in [40]. Generally, InterCloud is the focus of efforts especially in the public sector (e.g., USA Federal Government's Cloud Computing Initiative). It can be regarded as the second layer in the cloud computing stack [41]. In the inter-cloud layer, client-centric distributed protocols complement more provider-centric, large-scale ones in the intra-cloud layer. These client-centric protocols orchestrate multiple clouds to boost dependability by leveraging inherent cloud heterogeneity and failure independence. Celesti et al. [42] addressed the Identity Management (IdM) problem in the InterCloud context and showed how it can be successfully applied to manage the authentication needed among clouds for the federation establishment.

The above inter-cloud architectures or protocols enable to secure collaboration among clouds. However, they are self-contained, and may require modification of legacy authentication systems.

V. Conclusions and Future Work

Collaborative cloud is used to develop a dedicated task such as flight design such that the users can share resources in a confidential, authentic and transparent way. The paper presents a VPC gateway mechanism so as to build a secure channel for the users in the collaborative environment. With few modifications on the private clouds, it supports the resource sharing among private clouds and 3rd-party communication platforms.

In our prototype, we implemented the one-way inter-cloud access protocol for demonstrating the soundness of the proposed diagram only. The future work will be to develop the whole system, in particular to integrating with the standard IdP/SP protocol, and securing the 3rd platforms.

Acknowledgement

The authors would like to appreciate the anonymous reviewers for their constructive comments and suggestions. Dr. Hui Fang and Zhigang Zhao helped to build the cloud computing platform and VPC gateways respectively.

References

[1] National Institute of Standards and Technology, DRAFT Cloud Computing Synopsis and Recommendations. http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf.. Last Access on 30.03.2012.

[2] David Bernstein, Erik Ludvigson, Krishna Sankar, Steve Diamond, and Monique Morrow, "Blueprint for the Intercloud -Protocols and Formats for Cloud Computing Interoperability," IEEE International Conference on Internet and Web Applications and Services, 2009, pp. 328-336.

[3] Giorgio Nebuloni, "Accelerate Hybrid Cloud Success: Adjusting the IT Mindset," IDC, 04.10.2011.

[4] Anuradha Shukla, "China to invest £98 billion in cloud computing," ComputerWorld UK, 14.09.2011.

[5] E. Messmer, "Are security issues delaying adoption of cloud computing?" Network World, 27.04.2009. http://www.networkworld.com/news/2009/042709-burning-security-cloud-computing.html. Last Access on 30.03.2012.

[6] V. Tchifilionova, "Security and Privacy Implications of Cloud Computing Lost in the Cloud," Open Research Problems in Network Security, Lecture Notes in Computer Science, Vol. 6555, 2011, pp. 149-158.

[7] D. Velev, and P. Zlateva, "Cloud Infrastructure Security," iNetSec 2010, Lecture Notes in Computer Sciences 6555, 2011, pp. 140-148.

[8] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, "A Survey on Security Issues in Cloud Computing," ACM Computing Research Repository, vol. abs/1109.5388, http://arxiv.org/abs/1109.5388, 2011. Last Access on 30.03.2012.

[9] Craig Balding, "Go-Grid Security Breach," 30.03.2011. http://cloudsecurity.org/blog/2011/03/30/gogrid-security-breach.html. Last Access on 30.03.2012.

[10] Czaroma Roman, "Sony Data Breach Highlights Importance of Cloud Security," Cloud Times, 09.05.2011. http://cloudtimes.org/sony-data-breach-highlights-importance-of-cloud-security/. Last Access on 30.03.2012.

[11] IDC press, "Cloud Adoption Will Have Major Impact on European Software Market in 2011," 07.03.2011. http://www.idc.com/about/viewpressrelease.jsp?containerId=prDK22728011&sectionId=null&elementId=null&pageType=SYNOPSIS. Last Access on 30.03.2012.

[12] Robert Mullins, "IDC Survey: Risk In The Cloud," Network Computing, 16.06.2010.

[13] Jia Xu, Jia Yan, Liang He, Purui Su, and Dengguo Feng, "CloudSEC: A Cloud Architecture for Composing Collaborative Security Services," IEEE International Conference on Cloud Computing Technology and Science, 2010, pp. 703-711.

[14] S. T. Zargar, H. Takabi, and J. B.D. Joshi, "DCDIDP: A distributed, collaborative, and data-driven intrusion detection and prevention framework for cloud computing environments," International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2011, pp. 332-341.

[15] T. Sasaki, M. Nakae, and R. Ogawa, "Content Oriented Virtual Domains for Secure Information Sharing Across Organizations," ACM Cloud Computing Security Workshop, 2010, pp. 7-12.

[16] A. Kipp, L. Schubert, and M. Assel, "Supporting Dynamism and Security in Ad-Hoc Collaborative Working Environments", Identity in the Information Society, 2(2):171-187, 2009.

[17] Chih-Mou Shih, and Shang-Juh Kao, "Security Gateway for Accessing IPv6 WLAN," IEEE/ACIS Int'l Conf. on Computer and Information Science and Int'l Workshop on Component-Based Software Engineering, Software Architecture and Reuse, 2006, pp. 83-88.

[18] Ying-Dar Lin, Huan-Yun Wei, and Shao-Tang Yu, "Building an Integrated Security Gateway: Mechanisms, Performance Evaluations, Implementations, and Research Issues," IEEE Communications Surveys & Tutorials 4(1):2-15, 2002.

[19] M. Christodorescu, R. Sailer, D. L. Schales, D. Sgandurra, and D. Zamboni, "Cloud Security Is Not (Just) Virtualization Security," ACM Cloud Computing Security Workshop, 2009, pp. 97-102.

[20] Tavis Ormandy, "An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments," 15.04.2008. citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.105. Last Access on 30.03.2012.

[21] R. Chow, P. Golle, M. Jakobsson, R. Masuoka, J. Molina, E. Shi, and J. Staddon, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control," ACM Cloud Computing Security Workshop, 2009, pp. 85-90.

[22] K. Popovic, and Z. Hocenski, "Cloud computing security issues and challenges," Int'l Convention on Information and Communication Technology, Electronics and Microelectronics, 2010, pp. 344-349.

[23] Khaled M. Khan, and Qutaibah Malluhi, "Establishing Trust in Cloud Computing," IT Professional, 2010, 12(5):20-27.

[24] Jiyi Wu, Qianli Shen, Jianlin Zhang, and Qi Xie, "Cloud Computing: Cloud Security to Trusted Cloud," Advanced Materials Research, New Trends and Applications of Computer-aided Material and Engineering, vol. 186, 2011, pp. 596-600.

[25] P. Bryden, D. C. Kirkpatrick, and F. Moghadami, "Security Authorization: An Approach for Community Cloud Computing Environments," White Paper, Nov. 2009. http://www.techrepublic.com/whitepapers/. Last Access on 30.03.2012.

[26] Hassan Takabi, James B.D. Joshi, and Gail-Joon Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," IEEE 34th Annual Computer Software and Applications Conference Workshops, 2010, pp. 393-398.

[27] Yuri Demchenko, Jeroen Van der Ham, Volodymyr Yakovenko, Cees de Laat, Mattijs Ghijsen, and Mihai Cristea, "On-demand provisioning of Cloud and Grid based infrastructure services for collaborative projects and groups," International Conference on Collaboration Technologies and Systems, 2011, pp. 134-142.

[28] Y. Demchenko, C. Ngo, and C. de Laat, "Access control infrastructure for on-demand provisioned virtualised infrastructure services," International Conference on Collaboration Technologies and Systems, 2011, pp. 466-475.

[29] Dongwan Shin, and Hakan Akkan, "Domain-based virtualized resource management in cloud computing," International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2010, pp. 1-6.

[30] S. Eludiora, O. Abiona, A. Oluwatope, A. Oluwaranti, C. Onime, and L. Kehinde, "A User Identity Management Protocol for Cloud Computing Paradigm," Int. J. Communications, Network and System Sciences, vol. 4, No. 3, 2011.

[31] Anu Gopalakrishnan, "Cloud Computing Identity Management," SETLabs Briefings, 7(7):45-55, 2009.

[32] Elisa Bertino, Federica Paci, and Rudolfo Ferrini, "Privacy-Preserving Digital Identity Management for Cloud Computing," IEEE Computer Society Data Engineering Bulletin, 2009, pp. 1-4.

[33] R. Chow, M. Jakobsson, and R. Masuoka, "Authentication in the Clouds: A Framework and its Application to Mobile Users," CCSW, 2010, pp. 1-6.

[34] Juniper Networks, "Identity Federation in a Hybrid Cloud Computing Environment Solution Guide," Oct. 2009. www.ictnetworks.com.au/pdf/8010035-en.pdf. Last Access on 30.03.2012.

[35] Pierre Riteau, "Building Dynamic Computing Infrastructures over Distributed Clouds," International Symposium on Network Cloud Computing and Applications, 2011, pp. 127-130.

[36] T. D. Nguyen, M. A. Gondree, D. J. Shifflett, J. Khosalim, T. E. Levin, and C. E. Irvine, "A cloud-oriented cross-domain security architecture," Military Communications Conference, 2010, pp. 441-447.

[37] M. Kretzschmar, and S. Hanigk, "Security management interoperability challenges for Collaborative Clouds," International DMTF Academic Alliance Workshop on Systems and Virtualization Management, 2010, pp. 43-49.

[38] M. Kretzschmar, and M. Golling, "Functional components for a Security Manager within future Inter-Cloud environments," International Conference on Network and Service Management, 2011, pp. 1-5.

[39] D. Bernstein, and D. Vij, "Intercloud Directory and Exchange Protocol Detail Using XMPP and RDF," World Congress on Services, 2010, pp. 431-438.

[40] D. Bernstein, and D. Vij, "Intercloud Security Considerations," IEEE International Conference on Cloud Computing Technology and Science, 2010, pp. 537-544.

[41] C.n Cachin, R. Haas, and M. Vukolic, "Dependable Storage in the Intercloud," IBM Research Report, RZ 3783, 21.10.2010.

[42] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "Security and Cloud Computing: InterCloud Identity Management Infrastructure," IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises, 2010, pp. 263-265.