Personal Cloud Computing Security Framework

Sang-Ho Na, Jun-Young Park, Eui-Nam Huh
Dept. of Computing Engineering
KyungHee University
1 Seocheon-dong, Giheung-gu, Yongin-si, Gyeonggi-do, 446-701, Korea
{shna|jypark}@icns.khu.ac.kr, johnhuh@khu.ac.kr

Abstract— **Cloud computing is an evolving term these days. It describes the advance of many existing IT technologies and separates application and information resources from the underlying infrastructure. Personal Cloud is the hybrid deployment model that is combined private cloud and public cloud. By and large, cloud orchestration does not exist today. Current cloud service is provided by web browser or host installed application directly. According to the ITU-T draft, we might consider cloud orchestration environment in collaboration with other cloud providers. Previous work proposed security framework that has limitation of scalability for cloud orchestration. In this paper, we analyze security threats and requirements for previous researches and propose service model and security framework which include related technology for implementation and are possible to provide resource mobility.**

Keywords-component;Personal Cloud Computing; PCC; Threat; Security Framework;

I. INTRODUCTION

The Personal Cloud Computing is a popular concept these days. Like everything, "cloud" it has a rather fuzzy meaning, or at least one that is very changing, depending on the context. The Personal Cloud describes a user-centric model of Cloud computing where an individual's personal content and services are available anytime and anywhere, from whatever device they choose to access it. Today, most people have to juggle multiple devices to access all their services. What the personal Cloud could provide is a single and portable access-point to multiple Clouds. And in emerging economies, where people often share mobile devices, each individual would be able to log into their own Cloud from the shared device. Frank Gillet, an analyst with Forrester Research, recently authored a report on the Personal Cloud and how it will shift individual computing "from being device-centric to information-centric". He concludes that digital devices and services will combine to create the Personal Cloud, "an internal resource for organizing, preserving, sharing and orchestrating personal information and media."

The basic characteristics of a personal cloud server include the following:

1) Ease of use (which includes simplified deployment and maintenance) and portability

2) Instant availability (you can access the server via a direct cable connection, over the local network, and the Internet)

3) Subset of functionality (e.g., a simple blog engine to maintain a personal blog instead of a full-blow blog application like WordPress)

4) Absolute privacy (you, and only you, have full control over who has access to your content)

5) Complete control of the software and data

In this article we consider security threats and requirements of personal cloud computing through major cloud service such as Amazon EC3 and Azure. Also we propose a generalized security framework for personal cloud computing using personal cloud model. The remainder of this paper is organized as follows: Section 2 provides an overview of researches and trends of cloud computing and features of security of cloud computing. Section 3 proposes our personal cloud service model and workflow which illustrated the process of how the personal cloud works. In addition, we provide personal cloud security framework with related technologies. Finally, conclusion summarizes this paper and discusses ongoing and future work.

II. RELATED WORK

A. Personal Cloud Computing and Services

There are 4 deployment models of cloud computing [6]: public cloud, private cloud, community cloud and hybrid cloud. Personal Cloud is hybrid cloud which public cloud and private cloud comes to combine.

Personal cloud is three categories of personal cloud computing [5]: online storage, online desktop and Web-based applications. Each of these categories free up resources, either in processing power, as in the case of Web-based applications, or in the case of an Internet-based desktop (known as webtop) any computer with an Internet connection can become "our personal computer" via a Web browser.

Online storage gives users a reliable and secure place to store user data such as documents, MP3, movies. User is able to access to personal storage wherever there is an Internet

978-0-7695-4305-5/10 $25.00 © 2010 IEEE
DOI 10.1109/APSCC.2010.117

connection and whatever device user has. The Naver, for example, which is one of the major web-service portals in Korea provides 'N Drive' storage service combined with their web service.

Web-Based Applications like 'google docs' is another very recent advance in personal cloud computing. Hosted software applications do not have to download and install on user computer or mobile devices.

Webtop service is slightly different to the two mentioned above, as its goal is to provide the highly personalized setting of our own desktop with an virtualization we can access anywhere we can connect to the Internet. For example, when the user is away from his desk, the webtop allows access to information formally found only on the desktop of his own computer, such as contacts, e-mail, and files through personalized and familiar desktop with synchronization tools.

B. Cloud Security Threats and Domains Analysis

According to reports of CSA (Cloud Security Alliance), the 13 security domains [4] and the 7 top threats [3] on cloud computing were defined as follows Table 1 and Table 2.

Table 1. Security domains in cloud computing

No	Domain definition
1	Cloud Computing Architectural Framework
2	Governance and Enterprise Risk Management
3	Legal and Electronic Discovery
4	Compliance and Audit
5	Information Lifecycle Management
6	Portability and Interoperability
7	Traditional Security, Business Continuity, and Disaster Recovery
8	Data Center Operations
9	Incident Response, Notification, and Remediation
10	Application Security
11	Encryption and Key Management
12	Identity and Access Management
13	Virtualization

Table 2. Threats in cloud computing security

No	Threat definition
1	Abuse and Nefarious Use of Cloud Computing
2	Insecure Interfaces and APIs
3	Malicious Insiders
4	Shared Technology Issues
5	Data Loss or Leakage
6	Account or Service Hijacking
7	Unknown Risk Profile

This paper analyzed reports of CSA. And it show that associated 7 security threats and domains by service models in figure 1.

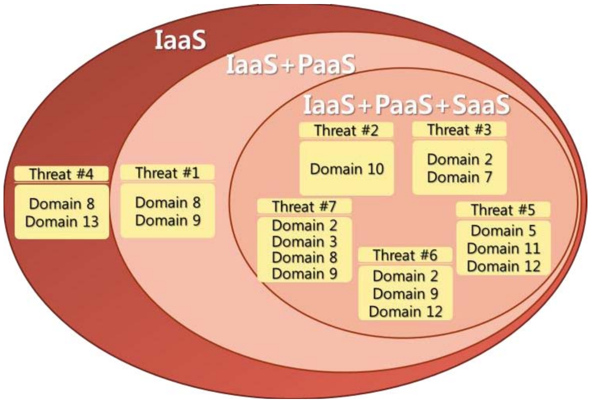

Figure 1. Security Threats and Domains

C. Major Cloud Service Evaluation

In this subsection, security processes of major cloud services such as EC2, App Engine Service [12] and Azure [13] has already analyzed in [1]. We will discuss Amazon's Web Service for requirements for security framework.

Amazon's Web Service (AWS): EC2 is an IaaS cloud, an virtual computing environment by secure and seamless bridge as Figure 2, that allows clients to use web service interfaces to launch instances with a variety of operating systems, load them with your custom application environment, manage your network's access permissions, and run your image using as many or few systems as you desire [2]. According to the 'Amazon Web Services: Overview of Security Processes', the AWS provides an overview of security as it pertains to control environment, certifications and accreditations, shared responsibility environment, risk management, secure design principles, monitoring, and etc [8].

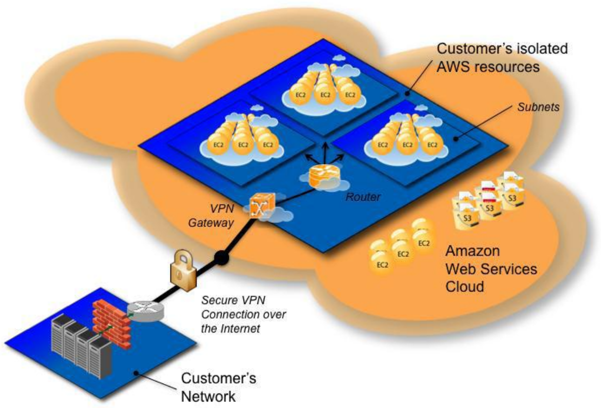
Customer's isolated AWS resources
Subnets
EC2
Router
VPN Gateway
S3
Amazon Web Services Cloud
Secure VPN Connection over the Internet
Customer's Network

Figure 2. Amazon Virtual Private Cloud (VPC)

Even though various security processes, as mentioned in [1], security problem of EC2 is that Amazon does not take responsibility for the services that are run inside the virtual machines. And the Amazon protects user's data and information by access control, monitoring, backup, and etc; they cannot ensure whether user's data are not infected and secure against to virtual machine from malicious code. User usually use and access by numerous compromised personal machines to cloud service, then can store already infected files to cloud storage without knowing that.

D. Cloud Security Framework

An analysis of the cloud security problems and the current state of security of the best known clouds shows that these problems do not have any real comprehensive solution and existing cloud security is in its infancy. There is a need for an approach to cloud security that is holistic, adaptable, and reflects client requirements. Brock et al.[1] summarized the requirements of the Cloud Security Framework (CSF) into six categories as follows and proposed security models and workflow as in Figure 3

1) *The CSF has to be service based.*

2) *The CSF has to use the non-discretionary model so that resource and service semantics are considered.*

3) *The CSF has to be capable of assigning clearance to clients, i.e., users and services.*

4) *A single sign-on environment should be provided for each cloud.*

5) *The security method has to be transferable.*

6) *Communication among clients should be encrypted – only initial request could be sent in clear.*

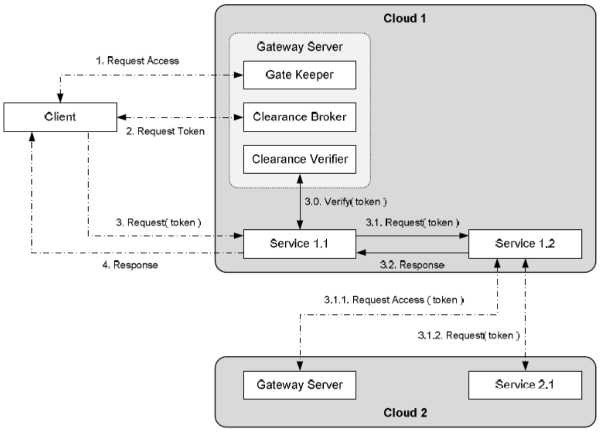

Figure 3. Security Model and Workflow

A security models and workflow shown in [1] describes services from the single provider. But, with multiple stakeholders involved, the cloud service model must be elastic to fit the needs of infrastructure providers, service providers and service resellers [7]. For that reason a security model and framework for access control on various cloud orchestrations has flexibility and scalability based upon design principle of 3rd party certificate authority and needs auditing which includes stored data as mentioned in subsection *C* and monitoring.

III. SECURITY FRAMEWORK FOR PERSONAL CLOUD COMPUTING

The scope of this section is to provide security frameworks with technology can be applied for personal cloud computing, which includes flexible personal service model, architecture and functional entities on various cloud collaboration environment.

A. Personal Cloud Security Framework Requirements

We will discuss requirements of personal cloud security framework referred to standardization trends of ITU-T. The additional requirements mentioned here can be divided into below three functional domains which are worked by ITU-T draft [7].

- **End User Request and Access**

The topmost functional domain comprises of end-users which include requesting, customizing services with cloud access APIs, clients for accessing cloud services and manageability interfaces for monitoring.

- **Provider Cloud Orchestration**

This domain is concerned with a cloud service orchestration framework. Service providers can orchestrate compute, network and storage resources into an end-user consumable service.

- **Virtualized Resources Management**

Virtualized resources management domain describes resources mobility that can be dynamically created, customized and destroyed.

According to the draft, cloud orchestration does not exist today. Current cloud service, such as EC2, N drive and etc, deployments directly connect the end-user access APIs to resource and customization mechanisms on the virtualized resource [7]. These kinds of service model have limitation and lack in resource mobility and security procedures. We focused on the provider cloud orchestration and virtualized resources management from a security point of view. The details of our point will be illustrated in next subsection by proposed service model and security framework.

B. Personal Cloud Service Model

In this subsection we describe service model for personal cloud computing against threats mentioned above in previous section, which focus on scalability, cloud orchestration and security. These functional service models are shown in Figure 4 below along with the separate concerns that each functional domain as discussed above must primarily address for cloud services to work effectively.

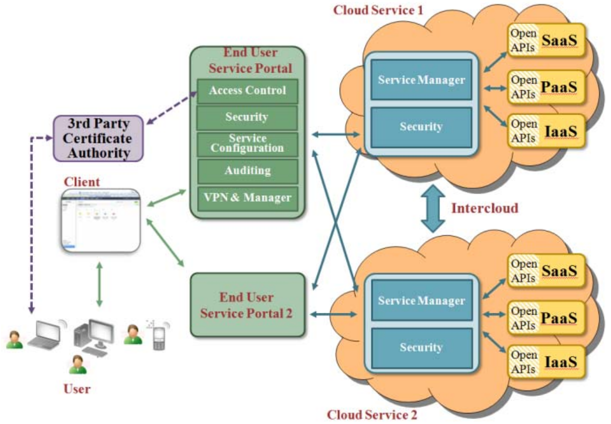

Figure 4. Personal Cloud Service Model and Workflows

User can be certificated by the 3rd party certificate authority, then can be issued token for service by End User Service Portal. After joining service portal, user can purchase and use cloud services which are provided by single service provider and collaborated service providers. End User Service Portal which is composed service configuration, access control, auditing, security and VPN & Manager provides secure access control using VPN and cloud service managing and configuration. An asset manager in service configuration can manage and initialize virtualized resources with communication protocol and open APIs. Details of asset manager are described in next subsection.

C. *Personal Cloud Security Framework*

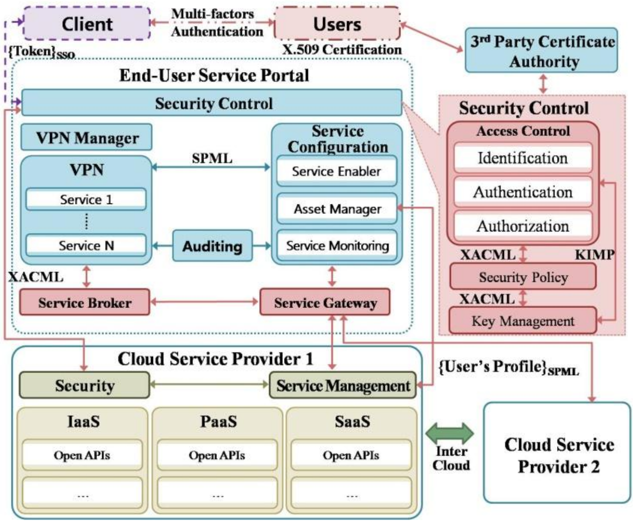

Figure. 5. Personal Cloud Security Framework

The security framework as shown in Figure 5 is based on the service model that will describe the details of each component and apply the needed security technologies for implementation between components in the Personal Cloud Computing.

Access control process for providing flexible service on each component is as follows:

- **Client**: users could access the client side (i.e.: web browser or host installed application) via diverse devices like PDA, laptop, or mobile phone with Multi-factors authentication provided by End-User Service Portal. The client side is the portal where users get their personal cloud. Multi-factors authentication based on certification issued by 3rd party CA.

- **End-User Service Portal:** When clearance is granted, a Single Sign-on Access Token (SSAT) could be issued using certification of user. Then the access control component share the user information related with security policy and verification with other components in end-user service portal and cloud service providers by using XACML [9] and KIMP [10]. User could use services without limitation of service providers.

- **Service Configuration:** the service enabler makes provision for personalized cloud service using user's profile. This user's profile is provided to the service management in cloud service provider for the integration and interoperation of service provisioning requests from user. The SPML [11] can be used to share user's profile. The asset manager requests user's personalized resources with {user's profile}$_{SPML}$ to cloud service provider and configure service via VPN connection.

- **Service Gateway, Service Broker:** a service gateway manages network resources and VPN on the information lifecycle of service broker.

- **Security Control:** the security control component provides significant protection for access control, security policy and key management against security threats.

- **Service Monitoring:** an automated service monitoring systems to guarantee a high level of service performance and availability.

Security framework proposed here provides secure connection and convenient exposed Open APIs to the user for accessing to the cloud service. We consider cloud orchestration environments and Single Sign-On Token to provide seamless experience to user. Furthermore, we provide possible technologies for cloud collaboration.

IV. CONCLUSION

Cloud Computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. Personal Cloud Computing is one of the interesting and popular cloud services. Previous work provided security framework which considered single cloud service provider. Actually, there are no cloud service orchestrations nowadays. Cloud orchestration as mentioned in ITU-T draft is way the wind blows in the future.

In this paper, we analyze security threats and figure out the requirements for security personal cloud computing service from previous works. We propose personal cloud computing service model and frameworks. We will apply our service model and security framework to privacy-aware system for personal cloud computing in future works.

Acknowledgement

This research was supported by Korea Evaluation Institute of Industrial Technology (KEIT) granted by the Korea government (No. KI002153) and supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency)" (NIPA-2010-(C1090-1021-0003))

REFERENCES

[1] Michael Brock and Andrzej Goscinski, Toward a Framework for Cloud Security, Algorithms and Architectures for Parallel Processing, Volume 6082/2010, pp. 254-263.

[2] Amazon, Amazon Elastic Compute Cloud (2007), http://aws.amazon.com/ec2/

[3] Cloud Security Alliance, Top Threats To Cloud Computing V1.0, http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[4] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, http://www.cloudsecurityalliance.org/csaguide.pdf.

[5] Jose Rivera, Cloud Computing for Personal Use, the epoch times, 2010.

[6] P.Mell and T. Grance, The NIST Definition of Cloud Computing, (2009, 10)

[7] ITU-T Focus Group on Cloud Computing. "Draft deliverable on Functional Requirements and Reference Architecture" (2010, 9)

[8] Amazon Web Services, "Overview of Security Processes"(2010, 8)

[9] OASIS, "eXtensible Access Control Markup Language(XACML)"

[10] OASIS, "Key Management Interoperability Protocol (KMIP)"

[11] OASIS, "Service Provisioning Markup Language(SPML)"

[12] Google, App Engine (2009), http://code.google.com/appengine/

[13] Microsoft, Azure (2009), http://www.microsoft.com/azure/default.mspx

[14] Chappell, D.: Introducting the Azure Services Platform, White Paper. David Chappell & Associates (May 2009)

[15] Goscinski, A.: Resource Protection. In: Distributed Operating Systems: The Logical Design,pp. 585–649. Addison-Wesley, Reading (1991)

[16] Yuan, E., Tong, J.: Attributed based access control (ABAC) for Web services. In: IEEE International Conference on Web Services, ICWS 2005, Proceedings, p. 569 (2005)

[17] Goscinski, A., Pieprzyk, J.: Security in Distributed Operating Systems. Datenschutz and Datensicherung (5) (1991)

[18] Neuman, C.B., Ts'o, T.: Kerberos: an authentication service for computer networks.IEEE Communications Magazine 32(I.9), 33–38 (1994)