DESIGN AND IMPLEMENT A NEW CLOUD SECURITY METHOD BASED ON MULTI CLOUDS ON OPEN STACK PLATFORM

Mohamad Reza Khayyambashi and Sayed Mohammad Hossein Mirshahjafari and EhsanShahrokhi

Department of Computer, Faculty of Engineering,
University of Isfahan, Isfahan-Iran
M.R.Khayyambashi@eng.ui.ac.ir, m.mirshah@irisaco.com,
ehsantux@gmail.com

ABSTRACT

Deployment of using cloud services as a new approach to keep people's platforms, Infrastructure and applications has become an important issue in the world of communications technology. This is a very useful paradigm for humans to obtain their essential needs simpler, faster ,more flexible, and safer than before. But there are many concerns about this system challenge. Security is the most important challenge for cloud systems. In this paper we design and explain the procedure of implementation of a new method for cloud services based on multi clouds on our platform which supplies security and privacy more than other clouds. We introduce some confidentiality and security methods in each layer to have a secure access to requirements. The architecture of our method and the implementation of method on our selected platform for each layer are introduced in this paper.

KEYWORDS

Cloud Computing, Security, MultiClouds, Secure Cloud Architecture, Public Cloud, Personal Cloud

1. INTRODUCTION

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." This is NIST's (National Institute of Standards and Technology) definition of cloud computing. Definition of cloud computing is based on five attributes: multi tenancy (shared resources), massive scalability, elasticity, pay as you go, and self-provisioning of resources.Cloud data can take many forms. For example, for cloud-based application development, it includes the application programs, scripts, and configuration settings, along with the development tools. For deployed applications, it includes records and other content created or used by the applications, as well as account information about the users of the applications.

David C. Wyld et al. (Eds) : CCSEA, CLOUD, DKMP, SEA, SIPRO - 2016
pp. 83–91, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.60208

Data that is stored on cloud must be secured while at rest, in transit, and inuse, and access to the data needs to be controlled. Standards for communications protocols and public key certificates allow data transfers to be protected using cryptography.Currently, the responsibility for cryptographic key management falls mainly on the cloud service subscriber.

Threewidely referenced service models have evolved:

- Software-as-a-Service (SaaS) enables a software deployment model in which one or more applications and the computing resources that run them are provided for use on demand as a turnkey service. It can reduce the total cost of hardware and software development, maintenance, and operations.

- Platform-as-a-Service (PaaS) enables a software deployment model in which the computing platform is provided as an on-demand service which applications can be developed upon and deployed. It can reduce the cost and complexity of buying, housing, and the managing of hardware and software components of the platform.

- Infrastructure-as-a-Service (IaaS) enables a software deployment model in which the basic computing infrastructure of servers, software, and network equipment is provided as an on-demand service upon which a platform to develop and execute applications can be founded. It can be used to avoid buying, housing, and managing the basic hardware and software infrastructure components.

In September2009, IDC Enterprise Panel held its annual survey on cloud computing organizations about the most important challenges of cloud services. The result of this survey showed security among people who want to use cloud services is the most important challenge. Figure 1 shows the result in percentage of the survey's concerns.

So if we want cloud computing as a useful service we should provide confidentiality and security for it to reduce this concern. Otherwise clouds can't reach a good position among people for using.

Cloud users and providers have many concerns about using it as a new technology. When considering using a cloud service, the user must be aware of the fact that all data given to the cloud provider leaves his/her own control and protection sphere.

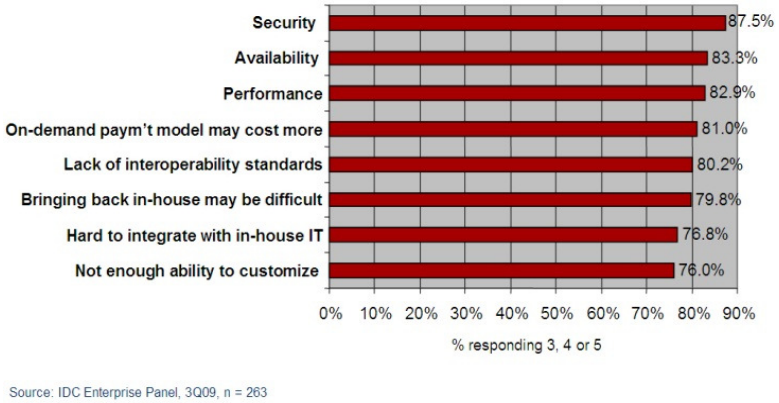

Figure 1. Result of percentage of survey's concerns by IDC, 2009

Even more so, if deploying data-processing applications to the cloud (via IaaS or PaaS),a cloud provider gains full control on these processes. If an attacker is able to intrude the cloud system, all of the data and processes of users operating on that cloud system, may become subject to malicious actions by that attacker. So the methods that cloud providers use to protect their clouds from threats and also the policy for accessing to the cloud by the users must be declared.

2. SECURITY THREATS FOR CLOUDS

As described security is the most important concern in cloud computing. This issue is organized into several general categories: trust, architecture, identity management, software isolation, data protection, and availability. So many threats to cloud computing can exist.

CSA(Cloud Security Alliance) is a research group on cloud security. They released their research results as “Top Threats to Cloud Computing” in 2010 in which they introduce the 7 top threats to clouds security challenges. The top threats they released consist of :

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking
- Unknown Risk Profile

The purpose of these are to provide desirable context to assist organizations in making educated risk management decisions regarding their cloud adoption strategies.

For the common case of a cloud provider hosting and processing all of its user’s data, an intrusion would immediately affect all security requirements: accessibility, integrity, and confidentiality of data and processes may become violated,and further malicious actions may be performed on behalf of the cloud user’s identity.

So providing a strong trusting relationship between the cloud providers and the cloud users is still indispensable.Providers should make and represent their security solutions for cloud threats to decrease consumer and organization's concerns.

Security must be provided in each layers of clouds. If we only have a safe physical layer, users will still have concerns about network layers, application layers and others. Although security approach should being applied on all cloud services contains infrastructure-as-a-service (IaaS) security, providers’ platform-as-a-service (PaaS) security and software-as-a-service (SaaS) security.

So our method should be complete and shouldn’t allow any attackers to access or change our cloud's content.

Security problems for clouds do not have any real comprehensive solutions 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.

Cloud providers and researchers all over the world worked on this issue and tried many solutions to reduce security risks of the cloud and they reached some solutions for each threat such as authentication, authorization and identification to provide confidentiality, isolation and encryption of cloud data in other layer. But cloud computing becomes bigger and bigger and its challenges grow too.

3. SECURE CLOUD BASED ON MULTICLOUDS METHODOLOGY

Cloud costumers and users worry about using this phenomenon today. We decided to suggest a useful method to decrease cloud's security threats of which we then designed its architecture. And last,we used a platform to implement our security model . We will now explain these steps.

Our method is based on multiple clouds. In other words we use this model to create a secure cloud. We think this model increases our cloud's transparency for consumers and decreases some user's concern about the complexity of clouds and their type of needs of our requests for variety of access level. We have some clouds in our model's architecture that user's data has been put on them. Our clouds are nested and each of them have an access level that according to the needs, this data put on each of them.

For choosing which cloud layer we want to put our data in, first after connecting to the server it asks us about which cloud we want to save our data. In other word we design a contract that forces clients to choose their level of storage and give their username and convert it to hash and save it. The server should sign an international security communication protocol mutuall to ensure user data security and save or recover their data in any circumstances. As we described one of the most common compliance issues facing an organization is data location. In our method we use external audits and security certifications to alleviate this concern. These certifications are different in various countries and it depends on where our method swere used for example DSS(Data Security Standards), The EC Data Protection Directive, GLBA (The Gramm-Leach Bliley Act), CPNI (The FCC Customer Proprietary Network Information rules) and so on.

Availability is one of our main targets for our secure cloud method. Availability means that an organization has its full set of computing resources accessible and usable at all times. It can be affected temporarily or permanently, and a loss can bepartial or complete. Denial of service attacks,equipment outages, and natural disasters are all threatsto availability.The level of reliability of our cloud service and also its capabilities forbackup and recovery is taken into account inthe organization’s contingency planning to address the restoration and recovery of disrupted cloud layers and operations, using alternate services, equipment,and locations.

In our method we describe a cloud that is in the outer surface. We named this cloud "Cloud by public access" and called it CBPA as abbreviation. This is a public cloud. All of our clouds are in this. Data and application that put in CBPA don’t have any protection. So in this layer of our cloud, typically, we have some costumer's data, open source programs and applications and platforms which they don’t want to do any security method or authentication on it. (So developers don't put any preventive method from intruders attack on it. Here is a diagram of our cloud in which CBPA is determined.

Notice that everyone can have access to all things that are put in this layer so all of the data that’s put in this layer is not secure and costumers shouldn't put their important data on it. This is

appropriate for only open source applications or infrastructures or data that they want to show to all costumers. This access level can increase transparency of our cloud and access to this layer is faster than other layers but it has less security than other layers of our method.

Besides authentication, the capability to adapt user privileges and maintain control over access to resources is also required, as part of identity management. Standards like the Extensible Access Control Markup Language (XACML) can be employed to control access to cloud resources, instead of using a service provider's proprietary interface. XACML focuses on the mechanism for arriving at authorization decisions, which complements SAML's focus on the means for transferring authentication and authorization decisions between cooperating entities. Messages transmitted between XACML entities are susceptible to attack by malicious third parties, making it important to have safeguards in place to protect decision requests and authorization decisions from possible attacks, including unauthorized disclosure, replay, deletion and modification.

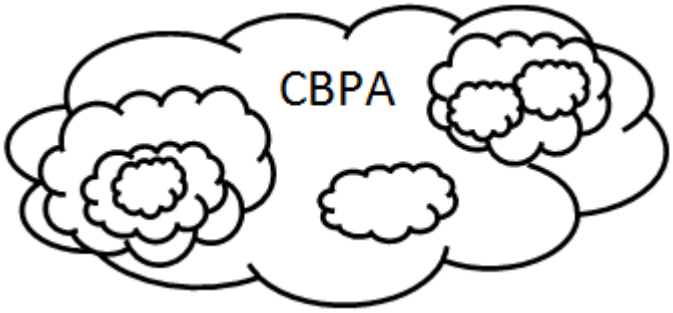

Figure 2. Secure Cloud Architecture base on Multi Clouds

This cloud type includes two types of private clouds: "cloud by group access (CBGA)" and "cloud by personal access (CBPeA)"that_are in the CBPA.

Another cloud in our model that we want to define is "cloud by group access (CBGA)" that located in CBPA. In other wordsthis layer is a branch of our multi cloud model that is in cloud by public access and provides different access level for data.In this layer we considered some security solutions for accessing the contents.

Group access means having some users in a group by identical access level. This model is useful for companies, organizations or any groups that want to have a cloud to put their data in platforms on it for their clients to read, write and edit their information. In our design for this cloud we put some security proceeding to have a more secure level. As we explained before for access to secure clouds we should provide confidentiality. So in this level we supplyconfidentiality by three security methods: Identification, authentication and authorization and supply cloud security by isolation of data. As a service provider we have to ensure dynamic flexible delivery of service and isolation of user resources. For doing this security level we used OpenStack platform and it used two layers for isolating data.

This method here is performed in two levels: first we do these work to authenticate the user that was in this CBGA which this level eliminate one of the most important concerns of cloud consumers but after this security level because we want attackers or Intruders can't access to group's information or to prevent information access by illegal clients, when one of our privileged

clients loses his/her public keys we introduce a second level for this type of cloud that is used to authenticate person who is in the group. This authentication method is used for group members to secure their access on groups and make group safe.

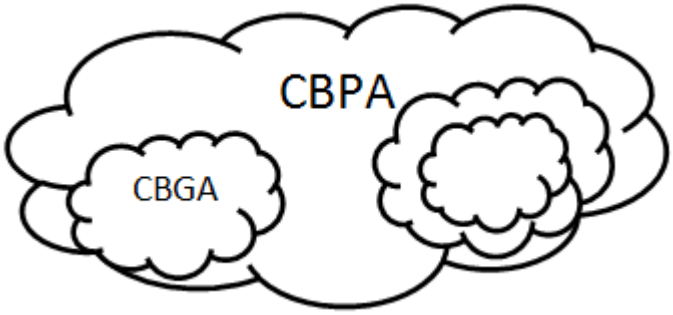

Figure 3. Architecture of CBPeA and ABGA

Another cloud _ we designed is "cloud by personal access (CBPeA)" that is suitable for saving personal data.

In this cloud we have some solutions to keep data secure too. Usage of this type of cloud is more than other types because all of the consumers can save their information on this cloud layer which only they can access and it provides confidentiality and isolation of data like CBPA. But we have some difference in this cloud designing. CBPeAconsists another cloud in itself named "cloud by secure personal access (CBSPeA) that is more secure than normal personal access. In this type we designed encryptionfor data that consumers want to save in addition to the authentication, authorization, identification and isolation.

So we have a secure cloud in this layer that no one can access _ unless main users whose data it is. This cloud is appropriate for user information that is personal and they want to be more secure than other information for example they can put their confidential documents, personal tools or anything that they don't want anyone to access _. Here is the view of this cloud type in our model.

4. IMPELEMENTATION OF METHOD ON OPENSTACK PLATFORM

So we designed our method and explained our architecture.For implementing our cloud model we use OpenStack platform. OpenStack offers open source software to build public and private clouds.This platform has three main components: Compute, Object Storage, and Image Service. OpenStack Compute is a cloud fabric controller, used to start up virtual instances for either a user or a group. It's also used to configure networking for each instance or project that contains multiple instances for a particular project. OpenStack Object Storage is a system to store objects in a massively scalable large capacity system with built-in redundancy and failover. OpenStack Image Service is a lookup and retrieval system for virtual machine images. Our public and private clouds have these components. The OpenStack Compute component of our public cloud can control & manage the inner private clouds. It connects to the compute component of the private clouds. The following diagram shows the basic relationships between the projects, how they relate to each other:

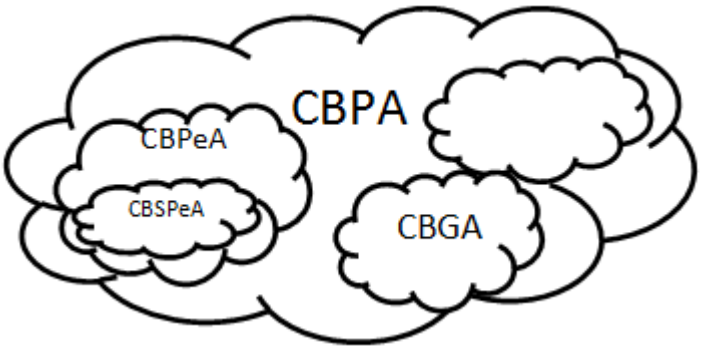

Figure 4. Cloud Secure Architecture with cloud layers names

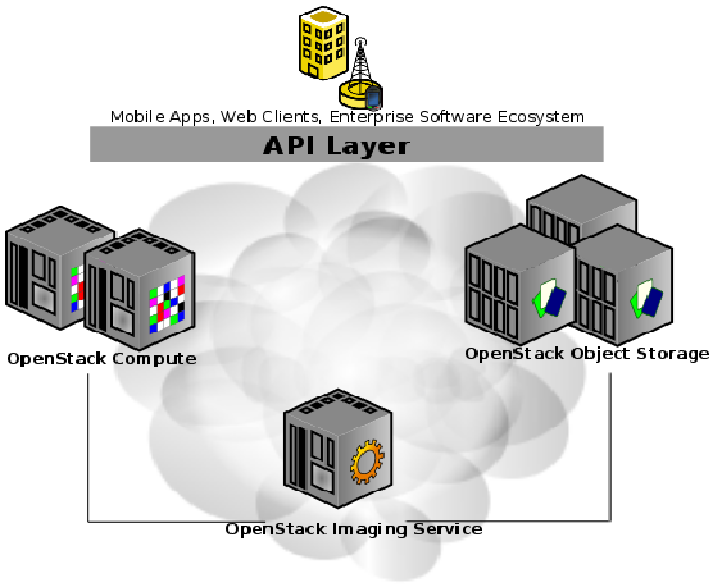

Figure 5. API Layer on openStack platform

In OpenStack compute component we have three subcomponents: Cloud controller, Cluster controller, and Node Controller. The main task of Cloud Controller(CC) are management & controlling the current cloud & the other clouds which are connected to main cloud. This component have a relation to other components. They are Cluster Controller(CLC),Object Storage, and Image Service. These relations are done by REST/SOAP messaging over http protocol. Cluster Controller(CLC) is the manager of the clusters. A cluster is a collection of computers(Nodes) which have been connected to a main server(Frontend). In a cloud we could have one or some clusters. Object Storage has a server that manage the space of the storage of our cloud, we name this server Storage Controller(SC). Image Service has a server for managing the instances of virtual machines and saving of images, we name this server Instance Controller(IC).Each of these server applications run as a daemon (A computer program runs as a background process) in a Linux base OS. Since the each cloud computing service needs a graphical user interface web application for accessing to it, we need a web server for saving & running the web application scripts(We use PHP). This web server is usually in CC server, but it could be in the other assigned server or an external server(Host).This web based interface has a relation to the CC server and uses the primary authentications for accessing to it. In our model,

the main cloud which is public(CBPA) has a CC server that has a connection to its CLCs,SCs & ICs. We assigned for each server a static class C IP(eg. 192.168.100.1 for CC,192.168.100.2 for CLC,192.168.100.3 for SC & 192.168.100.4 for IC). The inner clouds which are private(CBGA,CBPeA,CBSpeA) have these components too. The CC of the main cloud has connection to the CCs of these clouds. In fact one of the tasks of our main CC is management of the inner clouds CC. The procedure is that the user enters his/her username & password in web application UI and after a authentication He/She can se the cloud. In this mode the user can use the public services in cloud such as a application programs(SaaS) ,Platforms(Paas) and a resources(IaaS).If the user(Often a organization) want to has a private cloud, they can use the inner private clouds. For accessing to these they are authenticated again. Each of the authentication actions are done via the components of Object Compute(CC). The users of each group or organization have access to their clouds by group access(CBGA) data jointly. For accessing to each data we define a policy for each of them. It means that which user or group can access to that data or instance. This is what we name it Authorization in security. These authorization are done via the components of Object Storage(SC) and Image Service(IC). The isolation of the data is done by these components too.

5. CONCLUSION

Cloud computing will soon be a big approach in the entire world that conquers all ancient technology. But it depends on removing all concern about this challenge. The migration to a cloud computing environment isin many ways an exercise in risk management. Bothqualitative and quantitative factors apply in ananalysis. An appropriate balancebetween the strength of controls and the relative riskassociated with particular programs and operationsmust be ensured.

Nowadays Many companies, researchers and cloud developers are working on clouds and most of them work spatially on cloud security as the biggest challenge of like Amazon, Google, IBM and so on.They design their methods and publish them. Also they alwaystest their new method on cloud systems or even big social networks but still they don't find a complete way to create a secure cloud. Some organizations like ENISA, CSA and ISAKA survey the future of cloud security.

We think our designed model has more secure levels than other models that can make clouds more secure. But we don't claim our model is complete because several critical pieces of technology, such as a solutionfor federated trust, are not yet fully realized, impingingon successful deployments. In security issues completeness is an ultimate goal but no one can access it.

REFERENCES

[1] Wayne A. Jansen, ―Cloud Hooks: Security and Privacy Issues in Cloud Computing‖, 44th Hawaii International Conference on System Sciesnces 2013.

[2] D. Hubbard and M. Sutton, “Top Threats to Cloud Computing V1.0,” Cloud Security Alliance, 2013. Available:http://www.cloudsecurityalliance.org/topthreats

[3] P. Mell, T. Grance, The NIST Definition of Cloud Computing, Version 15, National Institute of Standards and Technology, October 7, 2011,http://csrc.nist.gov/groups/SNS/cloud-computing

[4] http://www.openstack.org/projects/openstack-security/

[5] L. Youseff, M. Butrico, D. D. Silva, Toward a Unified Ontology of Cloud Computing, Grid Computing Environments Workshop, held with SC08, November 2014 http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntolo gy.pdf

[6] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "On technical security issues in cloud compxuting," in Proceedings of the IEEE International Conference on Cloud Computing (CLOUD-II), 2012.

[7] D. Cappelli, A. Moore, R. Trzeciak, T. J. Shimeall, Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition, Version 3.1, CERT, January 2015, http://www.cert.org/archive/pdf/CSG-V3.pdf

[8] M. Burkhart, M. Strasser, D. Many, and X. Dimitropoulos,"SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics," in USENIX Security Symposium, 2013.

[9] Y. Keleta, J. H. P. Eloff, H. S. Venter, Proposing a Secure XACML Architecture Ensuring Privacy and Trust, Research in Progress Paper, University of Pretoria, 2005, http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/093_A rticle.pdf

[10] http://docs.openstack.org/trunk/openstack/compute/admin/content/components-of-openstack.html

[11] S. Ramgovind, M.M. Eloff, and E. Smith, "The Management of Security in Cloud Computing," IEEE, 2010,

[12] X. Jing, and Z. Jian-jun, "A brief Survey on the Security model of Cloud Computing," IEEE, 2013

[13] M. P. Eisenhauer, Privacy and Security Law Issues in Off-shore Outsourcing Transactions, Hunton& Williams LLP, The Outsourcing Institute, February 15, 2012, http://www.outsourcing.com/legal_corner/pdf/Outsourcing_Privacy.pdf

[14] B. R. Kandukuri, R. Paturi V, A. Rakshit, Cloud Security Issues, IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2015

[15] S. Overby, How to Negotiate a Better Cloud Computing Contract, CIO, April 21, 2010, http://www.cio.com/article/591629/How_to_Negotiate_aBetter_Cloud_Computing_Contract

[16] T. Ristenpart, E. Tromer, H. Shacham, S. Savage, Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, ACM Conference on Computer and Communications Security, November 2014

[17] C. Wang, "Forrester: A Close Look At Cloud Computing Security Issues," CSO. 2009

[18] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "Breaking the clouds – security analysis of cloud management interfaces," (in submission),2014.

[19] S. Pearson, Taking Account of Privacy when Designing Cloud Computing Services, ICSE Workshop on Software Engineering Challenges of Cloud Computing, May 23, 2013, Vancouver, Canada

[20] A. Greenberg, IBM's Blindfolded Calculator, Forbes Magazine, July 13, 2014