Next Generation Cloud Computing Issues and Solutions

Jeon SeungHwan[1], Yvette E. Gelogo[1] and Byungjoo Park[1]*

[1]*Department of Multimedia Engineering, Hannam University 133 Ojeong-dong,
Daeduk-gu, Daejeon, Korea
jeoninoldenburg@daum.net, vette_mis@yahoo.com, bjpark@hnu.kr
Correspondent Author: Byungjoo Park (bjpark@hnu.kr)*

Abstract

Cloud computing is a new computing paradigm that attracted many computer users. Among these are big companies, small and big enterprise, agencies and individual users. Cloud computing brought a lot of advantages especially in ubiquitous services where everybody can access computer services through internet. With cloud computing, there is no need of physical hardware or servers that will support the company's computer system, internet services and networks. It will basically cut down the expenses of the company allotted for the maintenance of the computer system. Along with the good benefits of Cloud Computing has to offer, there are security problems which make users anxious about the safety, reliability and efficiency of migrating to cloud computing. In this paper, the authors tried to study the threats and attacks that possibly launch in cloud computing and the possible solutions to mitigate these attacks. Aside of having network and application securities being adopted, there must be a security that authenticate the user when accessing the cloud services that is bound to the rules between the cloud computing provider and the client side.

Keywords: *Cloud Computing, virtual machines, authentication, access control, digital ID*

1. Introduction

Cloud computing is a new computing paradigm where in computer processing is being performed through internet by a standard browser [1]. Cloud computing builds on established trends for driving the cost out of the delivery of services while increasing the speed and agility with which services are deployed. It shortens the time from sketching out application architecture to actual deployment. Cloud computing incorporates virtualization, on-demand deployment, Internet delivery of services, and open source software [2]. The Cloud Computing Architecture of a cloud solution is the structure of the system, which comprises on-premise and cloud resources, services, middleware, and software components, geo-location, the externally visible properties of those, and the relationships between them. The term also refers to documentation of a system's cloud computing architecture. Documenting facilitates communication between stakeholders, documents early decisions about high-level design, and allows reuse of design components and patterns between projects [3]. The benefits of cloud computing are many. One is reduced cost, since you pay as you go. Other benefits are the portability of the application is that users can work from home, work, or at client locations. This increased mobility means employees can access information anywhere they are. There is also the ability of cloud computing to free-up IT workers who may have been occupied performing updates, installing patches, or providing application support. Along with the good services of Cloud Computing has to offer, there are security problems which make users anxious about the safety, reliability and efficiency of migrating to cloud computing. Big companies have second thought whether to move into the cloud because they might compromise the operation and the important information of the company. After analyzing and calculating the possible risk. Migrating into the "Cloud" will make computer processing much more convenient to the users. One of the considerations when moving to cloud is the security problems. In this paper, we assume that the readers already have backgrounds about Cloud Computing and that the terms that we used are known by them.

2. Layers of Cloud Computing Model

There are five layers in cloud computing model, the Client Layer, Application Layer, Platform layer, Infrastructure layer and server layer. In order to address the security problems, every level should have security implementation.

Client Layer-In the cloud computing model, the cloud client consist of the computer hardware and the computer software that is totally based on the applications of the cloud services and basically designed in such way that it provides application delivery to the multiple servers at the same time, as some computers making use of the various devices which includes computers, phones, operating systems, browsers and other devices.

Application layer-The Cloud application services deliver software as a service over the internet for eliminating the need to install and run the application on the customer own computers using the simplified maintenance and support for the people which will use the cloud interchangeably for the network based access and management of the network software by controlling the activities which is managed in the central locations by enabling customers to access the applications remotely with respect to Web and application software are also delivered to many model instances that includes the various standards that is price, partnership and management characteristics which provides the updates for the centralize features.

Platform layer-In the cloud computing, the cloud platform services provides the common computing platform and the stack solution which is often referred as the cloud infrastructure and maintaining the cloud applications that deploys the applications without any cost and complexity of the buying and managing the hardware and software layers.

Infrastructure layer-The Cloud Infrastructure services delivers the platform virtualization which shows only the desired features and hides the other ones using the environment in which servers, software or network equipment are fully outsourced as the utility computing which will based on the proper utilization of the resources by using the principle of reusability that includes the virtual private server offerings for the tier 3 data center and many tie 4 attributes which is finally assembled up to form the hundreds of the virtual machines.

Server layer- The server layer also consist of the computation hardware and software support for the cloud service which is based on the multi-core processors and cloud specific operating systems and coined offerings.

3. Cloud Computing Attacks

As more companies move to cloud computing, look for hackers to follow. Some of the potential attack vectors criminals may attempt include:

Denial of Service (DoS) attacks - Some security professionals have argued that the cloud is more vulnerable to DoS attacks, because it is shared by many users, which makes DoS attacks much more damaging.

Side Channel attacks – An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack.

Authentication attacks – Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users; for example, based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers.

Man-in-the-middle cryptographic attacks – This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.

Inside-job – This kind of attack is when the person, employee or staffs who is knowledgeable of how the system runs, from client to server then he can implant malicious codes to destroy everything in the cloud system.

4. Security Issues

Security measures assumed in the cloud must be made available to the customers to gain their trust. There is always a possibility that the cloud infrastructure is secured with respect to some requirements and the customers are looking for a different set of security. The important aspect is to see that the cloud provider meets the security requirements of the application and this can be achieved only through 100% transparency. Open Cloud Manifesto exerts stress on transparency in clouds, due the consumer's apprehensions to host their applications on a shared infrastructure, on which they do not have any control

In order to have a secured Cloud computing deployment, we must consider the following areas, the cloud computing architecture, Governance, portability and interoperability, traditional security, business continuity and disaster recovery, data center operations, incident response, notification and remediation, Application Security, Encryption and Key management, identity and access management [1]. One if the reason why users are very anxious of the safety of their data being saved in the cloud is that they don't know who is managing it while in the server of the cloud computing service provider. Typical users who use the cloud computing service like storing their files on the server to access it anywhere they want through internet, don't bother much about the security of their files, those documents are common files that don't need to be secured. But in the case of big companies which have very important information to take care of, they need to have secured cloud computing system.

4.1 Security Analysis

4.1.1 Level of Security

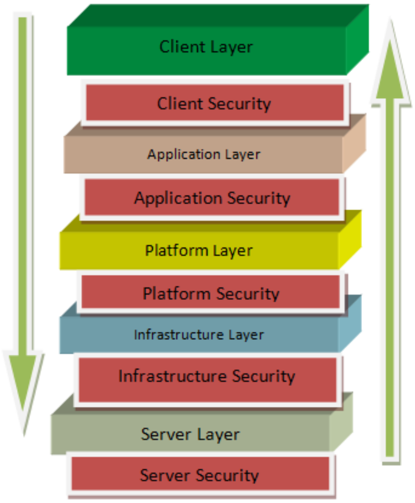

Figure 1. Security Deployment in each Layer

As illustrated in the above figure, there must be a security deployed in each layer of the cloud computing to ensure that the information coming from the side of the client and the server or vice versa is secured and legitimate. Let us discuss first the Server Security requirements, the cloud computing service provider must ensure that there is necessary security for the data centers for both hardware and software they are using. There must be a disaster and recovery plan in case there is unexpected natural disasters, for lacking of preparation may cause a lot of damages that would affect the clients day to day operations. The provider must have back-ups and necessary precautions to handle this kind of problems.

Aside from having a physical security, data centers must have strong security Identification mechanism to avoid unauthorized access. Data centers must be secured enough because the core of cloud computing is being maintained inside it. Servers must have its security in form of software like antivirus program, Intrusion Detection and Prevention Systems and other software for maintain the security, also the username, password and Digital ID for Access Control.

Second is the Infrastructure Layer Security, as we know infrastructure layer provides platform virtualization to the clients/users. The type of the security that is necessary for this layer is internal to the cloud computing provider and the developer of the virtual machines. Let us image the scenario where after the authenticating the user, the virtual machine interface will be loaded and all the virtual services like applications, software, virtual storage is visible to the user. If it happens that it is unauthorized access, then the perpetrator can copy, modify, and sabotage the virtual machine not within the physical location or the premises of the company or the client. That is why it is a must that there must be a strong Authentication and ID Management.

Third is the Platform layer, platform layer must be well developed and that is reliable enough to run in any run-time platform. Secure enough that it cannot be used as a tool to launch an attack.

Fourth is the Application layer, the cloud application services deliver software as a service over the internet for eliminating the need to install and run the application on the customer own computers. The cloud computing provider must ensure that these applications are free from bugs and cannot be used as a tool to launch attacks.

Lastly, is the client layer, the cloud client consist of the computer hardware and the computer software that is totally based on the applications of the cloud services. Security needed for this layer is the safety of the hardware and the user access control, the company or enterprise has to ensure the user is legitimate and that is he/she is authorized to access that certain computer.

As a whole, we can say that if we meet all the security requirements of each layer then we can have secured Cloud Computing System.

4.1.2 Cloud Computing environment and Security Level

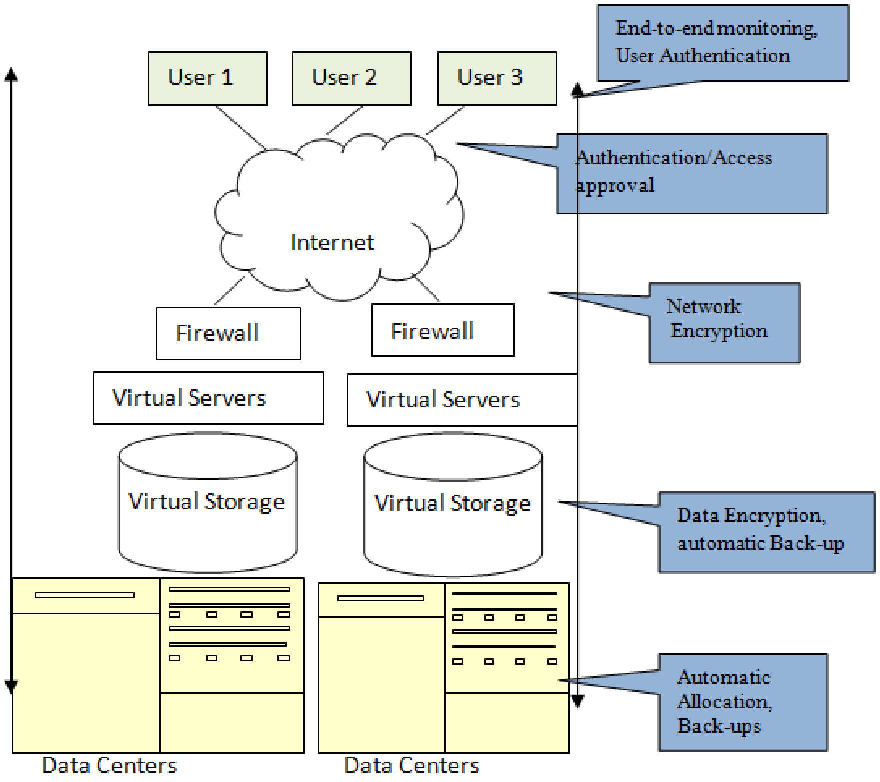

Figure 2. Cloud Computing Security Overview

5. Access Control

Access control is a key concern, because insider attacks are a huge risk. A potential hacker is someone who has been entrusted with approved access to the cloud. Anyone considering using the cloud needs to look at who is managing their data and what types of controls are applied to these individuals. The traditional model of application-centric access control, where each application keeps track of its collection of users and manages them, is not feasible in cloud based architectures. This is more so, because the user space maybe shared across applications that can lead to data replication, making mapping of users and their privileges a herculean task. Also, it requires the user to remember multiple accounts/passwords and maintain them. Cloud requires a user centric access control where every user request to any service provider is bundled with the user identity and entitlement information. User identity will have identifiers or attributes that identity and define the user. The identity is tied to a domain, but is portable. User centric approach leaves the user with the ultimate control of their digital identities. User centric approach also implies that the system maintains a context of information for every user, in order to find how best to react to in a given situation to a given user request.

6. Authentications and ID Management

There must be a strong authentications and ID Management for both the cloud provider and the client. One of the ideas of access monitoring is to implement of Key Management for both client and the cloud service provider. This Key must be known for both entities and will be remotely monitored. Server logs must be kept and Intrusion Detection and Prevention System must be deployed. To give trust to the cloud computing provider, that they kept the information well that is to avoid information leakage, there must be a shared key for both client and the provider, In order for the clients to access the cloud computing services, it must be first authenticated, not only using a mere username and password but a digital ID’s.

What is a Digital ID?

A Digital ID, sometimes called a digital certificate, is a file on your computer that identifies who you are. Some software applications use this file to prove your identity to another person or computer. Here are two common examples:

When you bank online, your bank must be sure that you are the correct person to get account information. Like a driver's license or passport, a Digital ID confirms your identity to the online bank.

When you send important e-mail to someone, your e-mail application can use your Digital ID to "digitally" sign the e-mail message. A digital signature does two things: it lets the recipient know the e-mail is from you, and it tells them the e-mail was not tampered with from the time you sent it to the time they received it.

Applying it to cloud computing, it is very useful as far as the authenticity of the data is concern.

What can I do with a Digital ID?

Software applications, networks, and computers can use your Digital ID in several ways:

Client authentication is the term used to describe how you (the client) prove your identity to someone else or to a computer. For example, online banks need to make sure you are the correct customer for a given bank account. When online, your software application presents your Digital ID. Some Web sites might request that you present your ID before letting you view Web pages that are hidden from others, such as pages for people who subscribe to a particular service on the Web site.

A Digital signature, like a hand-written signature, shows that a person created or otherwise agreed to the document containing the signature. A digital signature actually provides a greater degree of security than a handwritten signature because the digital signature verifies both that the message originated from a specific person and that the message has not been altered either intentionally or accidentally.

Encryption (or data scrambling) is a way of protecting information before sending it from one computer to another. Typically e-mail applications use the Digital ID that belongs to the person receiving the encrypted e-mail message. For you to send someone encrypted messages, you need their public key.

Why do I need a Digital ID?

Virtual malls, electronic banking, and other electronic services are becoming more commonplace. However, your concerns about privacy and security might be preventing you from taking advantage of this new medium for your personal business. A Digital ID can help.

Or, your employer might have a new network that requires you to have a Digital ID for applications that you use on the job. Because you will use this technology on the job, you need to learn to use Digital IDs quickly [5].

The same with the cloud computing services, the client or consumer are likely hesitant to use the cloud computing because they think that their top-secrets information might not be safe. Think about the scenario where one can distantly intercept or copy the information of the certain company outside their premises. It is a high risk if someone will try to sabotage the cloud computing servers or the data centers without the knowledge of the client or the consumer because typically these data centers, servers, and hardware who is hosting the cloud computing services is far from the company's physical location. It is an urge for the use of the security scheme which can assure the client that their data that is being stored in the cloud is secured and also the virtual machines that they are facing or working with is legitimate. This paper proposes a use of Digital signatures to accessing and authenticating the users. Like for example in a company, all employees must have a legitimate Digital Signatures issued by the company so that they have an authorized access of their company's system in the cloud.

Digital IDs are used by Web sites and network applications to scramble data passed between two computers. Encryption is a powerful tool, but encryption alone is not enough protection for your information. Encryption cannot prove your identity or the identity of someone sending you encrypted information. For example, an online stock broker might have a site that encrypts data sent to you through its Web pages. The site might even require you to enter a username and password. However, these types of usernames and passwords are easily intercepted and cannot be trusted to prove your identity. Without additional safeguards, someone could impersonate you online and get access to your accounts or other valuable and private information. Digital IDs address this problem, providing an electronic means of verifying your identity. Digital IDs provide a more complete security solution, assuring the identity of all parties involved in a transaction [5].

Because of the way Digital IDs work, they provide a function called nonrepudiation, which essentially prevents people from denying that they sent a message. For example, when you use a credit card, you have to sign a receipt authorizing payment. Because a signature is required on the receipt, you can prove someone stole or used your card by comparing your signature to theirs. With nonrepudiation, your "authorization" happens automatically when you send your Digital ID. If someone manages to steal your Digital ID, they cannot use it unless they have the password and your private key. This is why it is critical that you do not tell anyone your password.

Once a cloud virtual machine is load it will review the Digital ID, it will checks the validity of the ID. For example, it will be check to make sure the ID has not expired. The checker might also consider who issued the Digital ID. If the cloud computing access checker does not trust the CA who issued you the ID, then you might be denied access to the virtual machine and the interface will not be loaded. This is why it is important to use a reputable CA. The access checker can use any information in the Digital ID when determining what permissions the user has. The Digital ID might contain some or all of the following information about user, the public key, user name, expiration date of the public key, Name of the company (the CA) who issued your Digital ID, Serial number of the Digital ID, Digital signature of the CA and various information required by the CA.

Once the Cloud computing access checker confirms the user identity, it loads the virtual machine interface and the user can now access whatever the services of the company. Some cloud service provider or network applications use the information in your Digital ID to customize the information you see. This customization is sometimes called access control, but do not confuse access control for client authentication. Client authentication is simply proving your identity.

7. Conclusion

Cloud Computing brought many benefits in computing world. Along with these benefits, there some security issues that needs to be address to give assurance that indeed it is safe and reliable internet service. Migrating into the “Cloud” is not that easy but if carefully planned and deployed it will bring advantages in many areas like decreasing cost and resources. In this paper we discussed the security requirements of cloud computing and the solutions for the security problems. Using Digital ID’s for the employee in accessing the cloud computing services is the best way to minimize the unauthorized access, this also on way to address the nonrepudiation issues.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0024401, 2011-0026286).

References

[1] M. Okuhara, et. al., “Security Architecture for Cloud Computing”, FUJITSU Sci. Tech. J., vol. 46, no. 4, **(2010)** October , pp. 397-402.

[2] Sun Microsystems, Inc., “Introduction to Cloud Computing Architecture”, White Paper, 1st Edition, **(2009)** June.

[3] G. Kaefer, “Cloud Computing Architecture”, Corporate Research and Technologies, Munich, Germany, Siemens AG 2010, Corporate Technology, **(2010)**.

[4] A. Gopalakrishnan, “Cloud Computing Identity Management”, SETLabs Briefings, vol. 7, no. 7, **(2009)**.

[5] VeriSign, “Digital ID, A Brief Overview”, A VeriSign White Paper, 2004 VeriSign, http://www.verisign.com/static/005326.pdf.