Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 38 (2012) 125 – 129

Procedia Engineering

www.elsevier.com/locate/procedia

ICMOC - 2012

Agent Based Security for Cloud Computing using Obfuscation

[a]K.Govinda*, [b]E.Sathiyamoorthy

[a]SCSE, VIT University, Vellore, India
[b]SITE, VIT University, Vellore, India

Abstract

Cloud computing is a class of the next generation highly scalable and distributed computing platform in which computing resources are offered 'as a service' leveraging virtualization and Internet technologies. Cloud computing does not clearly define boundaries to protect the user data. The data, communications, services and other important resource are controlled by the cloud service provider. The alarming situation is the probable leakage of sensitive data by service provider. To protect the data from service provider, In this paper we propose an agent based model that would secure the users data over the cloud and implemented various algorithms to provide a secured system.

Keywords: Agent; Cloud; Obfuscation; Security; Multi-tenancy.

1. Introduction

Cloud computing dynamically allocates, deploys, redeploys and cancels the cloud services as per user requirements. It makes computing power more efficient [1]. Cloud computing combines the data-sharing model and service statistical model. From a technical point of view, a data base cloud has the following three basic characteristics [2]: (a) Hardware infrastructure architecture is based on the clusters, which is large-scale and low-cost. The infrastructure of cloud computing is composed of a large number of low-cost servers, and even the X86 server architecture. Through the strong performance, the traditional mainframe's prices are also very expensive. (b) Data centers running in a simultaneous cooperated and distributed manner. Individual user's data is stored in multiple physical locations for Collaborative development of the underlying services and the applications to achieve maximum resource utilization.(c) Cloud service layer provides applications which is closest to the user's service like data mining, and allows various data manipulations.

However, current cloud services pose an inherent challenge to data security, because they typically result in data being present in unencrypted form on machine owned and operated by a different organization from the data owner. There are threats of unauthorized uses of the data by service providers and of theft of data from machines in the cloud. Fears of leakage of sensitive data or loss of security are a

1877-7058 © 2012 Published by Elsevier Ltd.
doi:10.1016/j.proeng.2012.06.018

significant barrier to the adoption of cloud services. The leading U.S. market research firm Gartner released a report "Assessing the Security Risks of Cloud Computing" in June 2008， this report said that cloud computing has great risk on data integrity, data recovery and privacy, etc[3].

In this paper we propose agent-based security model. The reason for having an agent for ensuring security rather than leaving them to be implemented entirely on the server side is that this architecture provides a user-centric trust model that helps users to control their sensitive information and it also ensures that the client has fewer burdens at its side. These features can assist the user in clearly communicating his security-related preferences to the service provider, and can also assist the service provider in compliance with security laws and regulations. The key feature of the agent is *obfuscation*, which can be used by users to protect the security of their data even if there is no cooperation from the service provider - indeed, even if the service provider is malicious [4].

2. Architecture

Here, we present our "Agent Based Security Model Using Obfuscation" as a solution to the above mentioned problem. And then, discusses how our model addresses several problems raised in this scenario. Using this model we tried to meet some challenges proposed by IBM on security in the cloud [5], which pointed out that the ability to manage the security environment is one of the main challenges and also the new guidelines [6] published by Cloud Security Alliance (CSA). Agent maintains Obfuscator and Data Retriever that obfuscate the data sent by user to the cloud. It retrieves the data sent by cloud to user.

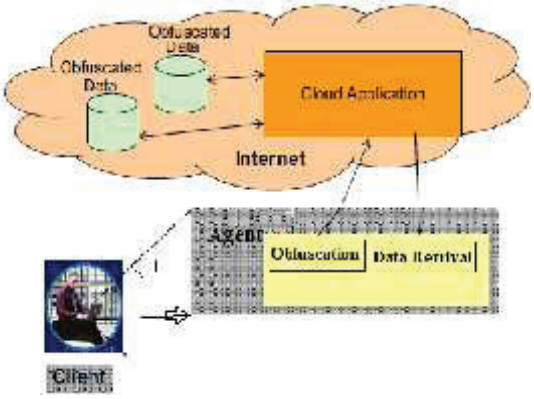

Fig.1. Architecture

3. Agent

The key feature of the Security Agent provides obfuscation and data retrieval. Agent can automatically obfuscate some or all of the fields in a data structure before it is sent off to the cloud for processing, and translate the output from the cloud back into de-obfuscated form. The obfuscation and data retrieval is done using a key which is chosen by the agent and not revealed to cloud service providers. This means that applications in the cloud cannot de-obfuscate the data. Moreover, an attacker who uses the same application will not be able to retrieve the user's data by observing the results when he obfuscates his own data, since his obfuscation key will not be the same as the agent's key. Since this obfuscation is controlled by the agent, it should be more attractive to security-sensitive users than

techniques for data minimization that they do not control. In general, the more information that is obfuscated within a data structure, the smaller the set of applications which can run using the obfuscated data structure as input, and the slower the obfuscation process. In some cases, it is not an option to obfuscate all the personal and sensitive data in the data structure. Data items that are not obfuscated may be used by cloud services for personalization of user content and targeting of advertising.

4. Algorithms

In order to obfuscate the data we have developed some algorithms that would obfuscate the data depending on the attributes.

4.1. Algorithm1: Attributes participating in mathematical operations as shown in Table1.

Table1. For Attributes

Obfuscation	Data retrieval
1. Input=x, obfuscated data =F(x). 2. F(x) = (x*y)+z Where y<=5 and 1000<z<5000.	1. Obfuscated data = F(x), Original data=G(x) 2. G(x)=(f(x)-z)/y If G(x) relates to average. 3. G(x) = (f(x)-z)/y If G(x) relates to sum.

4.2. Algorithm2 : Identification specific attributes shown in Table2.

Table2. Identification of Specific attributes

Obfuscation	Data retrieval
1. Original data=y 2. Create table of size > 1000. 3. Store random and meaningful values in the table. 4. For every entry in DB, serial number=s 5. Calculate x=s%1000 6. Append value corresponding to x, say k in the table to y 7. Then obfuscated data is ky.	1. Read the word from first and remove string before first space.

4.3. Algorithm3 : Mail id's and Web address as shown in Table3.

Table3. For e-mail id's

Obfuscation	Data retrieval

1. Add ASCII equivalent of last two digits to the user name. As shown in Table4	1. The last two ASCII equivalents are removed. according to the table the original data is obtained.

Table4. E-mail transformation

Original Data	*Obfuscated data*
Gmail	Yahoo
.com	.ac.in
.edu	.gov.in
Yahoo	Rediff

4.4. Algorithm4 (a): Account numbers as shown in Table5.

Table5. For Account numbers.

Obfuscation	Data retrieval
1. For account numbers, the number is broken down into parts. 2. These parts are swapped according to certain pattern.	1. The obfuscated data is swapped to obtain original data.

4.5. Algorithm4 (b):Phone numbers as shown in Table6.

Table6. For Phone numbers.

Obfuscation	Data retrieval
1. For phone numbers modify the first digit. 2. A table is made using the common patterns of first 5 digits 90472, 90033, 97901 and so on... 3. All numbers are replaced with these common patterns.	1. Replace the first 5 digits by cross checking them with the table to obtain the original data.

To check if the data is modified by the cloud provider we develop an algorithm. It can only check if the data is modified and the user needs to take proper steps to handle this misbehaviour.

4.6. Algorithm5 : Amount as shown in Table7.

Table7. For amount values.

Obfuscation	Data retrieval
1. In the amount field Least significant digit=x, Most significant digit=y. 2. Identifier field= k 3. Then obfuscated data=kxy.	1. Remove the numbers in the identifier. 2. Let it be xy then LSD=x, MSD=y, 3. Compare x and y with amount column if both of them match then data is retrieved not modified. 4. If they don't match data is modified.

Now let us check out one transaction made by the user. If user wants to store the information of Vijay who purchased for 20,000 and it he wants to retrieve it back. User inputs
Name: Vijay, Amount: 20,000. Agent Obfuscates data and sends to cloud as Name: Sai Vijay Kumar, Amount: 40,100
The user queries for Vijay's transaction, Cloud sends Name: Sai Vijay Kumar, Amount: 40,100. Agent retrieves the data and sends it to client as follows Name: Vijay Amount: 20,000.

5. Conclusion

In this paper we developed Agent based security for cloud computing using Obfuscation technique. We ensured sensitive data given by the user cannot be misused by malicious cloud provider through an Agent. We reduced work load at user end by having an agent who maintains the security. We developed different algorithms that obfuscates and retrieves the data. For a sample transaction we have shown how obfuscation and data retrieval takes place. As a next step, we work at improving the algorithms complexity and extending this security model to other cloud services.

References

[1] A Client-Based Privacy Manager for Cloud Computing Miranda Mowbray, Siani Pearson HP Labs ..
[2] Amazon Web Services LLC. 2009. Case Studies: TC3 Health. Web page http:// aws.amazon.com/ solutions/ casestudies/.
[3] Cloud securityAlliance.Securitybestpracticesforcloudcomputing,2010,http://www.cloudsecurityalliance.org.
[4] Fischer-H_bner, S."IT-Security and Privacy:Designand Use of Privacy-Enhancing Security Mechanisms".Springer LNCS Series 1958,2001.Springer Berlin / Heidelberg.DOI= http://dx.doi.org/10.1007/3-540-45150-1.
[5] Greenberg, A. 2008. Cloud Computing's Stormy Side.Forbes Magazine (19 Feb 2008).
[6] Heiser.J , Nicolett M. " Assessing the Security risks of cloud computing ". http : //www .gartner .com/ Display Document ?id=6 85308, 2008.
[5] IBM. Security challenges in the cloud, 2009.
[6] Salesforce.com, Inc. 2000-2009. Sales Force
[7] Wikipedia, http://en.wikipedia.org/wiki /Cloud_Computning.
[8] Xue Jing 1,Zhang Jian."A Brief Survey on the Security Model of Cloud Computing",9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science.,2nd Jun 2010.