CAIPT 2014
The 2nd International Conference on Computer Applications and Information Processing Technology

Ulaanbaatar, Mongolia
27~28, June, 2014

Organized by
Korea Information Processing Society (KIPS)

Hosted by
National University of Mongolia

Sponsored by
KCC Information & Communication
Mocomsys, Visual Infosys, Seaseung
Sigong Education, Alphonsus Tech, Innodep
Tomato System, Yire Information System
Yonsei University CPRC
(Communication Policy Research Center)
Presentation Sessions Schedule

Friday, 27, June, 2014

Registration:
08:00 ~ 09:00 Registration of Participants

09:00~10:20

Presentation Session 1
I Presentation Session (4 papers) I

Chair : Chagnaa Altangerel, National University of Mongolia

1-1. Long integer multiplication algorithm using CUDA architecture
   Gantulga G., Bolormaa D (National University of Mongolia, Mongolia) ................................................................. 3

1-2. Memory Dump of Executable Code for Malicious App Analysis on Android
   Dongwoo Kim, Wootak Jung, Jinseok Oh, Jaecheol Ryou (Chungnam National University, Korea) .................. 7

1-3. A Key Management Framework for Inter-cloud Environment
   Jun-Young Park, Sang-Ho Na, Eui-Nam Huh (Kyung Hee University, Korea) .................................................. 11

1-4. A Context Inference Framework for Enabling Smart Services
   Moon Kwon Kim, Soo Dong Kim (Soongsil University, Korea) ................................................................. 15
Abstract

A collaborated cloud service has been receiving much attention to a cloud user. However it has a critical problem in sharing data and service due to privacy and security issues. While a cloud user is provided with collaboration service from cloud providers, the cloud providers shared service/data of user among cloud providers. However most cloud providers do not support data encryption mechanism in sharing with other cloud providers. Therefore, we propose Inter-cloud key management requirements and the proposed key management framework in collaborated cloud service environment (Inter-cloud).

1. Introduction

According to the security report [1], “The Notorious Nine Cloud Computing Top Threats in 2013” of CSA(Cloud Security Alliance), Data Breaches, Data Loss and Account & Service Traffic Hijacking are the most known threats in cloud computing. For these reasons, cloud service providers might consider data protection solution and data loss measure.

Cloud service providers take cognizance security problems and provide encryption service to protect data and personal information. For example, in the Dropbox providing cloud storage service, user can use encryption service on uploading data.

According to increasing security requirements of cloud users, cloud service providers have been trying to provide secure protection mechanism for user data using variety security methods.

By providing data encryption service to users, cloud services collaboration is more difficult as the data encryption service of cloud providers is isolated from other services. Hence, it leads to incompatible cloud environments.

In collaboration service, other cloud providers cannot access encrypted data located in other cloud service providers due to their incompatible encryption system. So each data encryption system will disable service collaboration among cloud providers.

Attackers can snoop the data using MITM (Man in the Middle) attack which leads to data loses, snoop and breaches. These problems may be solved using security communication protocols as SSL (Secure Socket Layer) but the SSL also have a weakness from MITM attack. So users might use encryption services with secure communication protocols. Attackers cannot read the data even if they hijack the data using MITM or snooping.

However the encryption services also need to exchange a key or a key pair. If CSP transmits the encrypted data to other CSP, the receiver (other CSPs) needs the key for decrypting the encrypted data. Moreover the decryption key also can be stolen from attackers using MITM or data hijacking.

Therefore, this paper proposes a secure key management method among CSPs for service collaboration in Inter-cloud environment.

The remainder of this paper is organized as follows: Section 2 describes definition, architecture and deployment models of Inter-cloud, existing Cloud Key Management Infrastructure and key chain method. Section 3 specifies Inter-cloud key management requirements and proposes Inter-cloud key management framework, address key exchange workflow and key management evaluation. Finally we conclude in Section 4 by deriving some future work.

2. Related Work

2.1. Inter-cloud

According to the technical report of Global Inter-cloud Technology Forum[2], The Inter-cloud is “A cloud model that, for the purpose of guaranteeing service quality, such as the performance and availability of each service, allows on-demand reassignment of resources and transfers of workload through a interworking of cloud systems of different cloud providers based on coordination of each consumers requirements for service quality with each provider’s SLA and uses of standard interfaces.”.

2.1.1. Inter-cloud Architecture [3]

Inter-cloud architecture is consisted of two types; Federations and Multi-clouds.
Federation Inter-cloud consists of two models; (A) Centralized Inter-cloud Federation: Clouds use a central entity to facilitate resource sharing. (B) Peer-to-Peer Inter-cloud Federation: Clouds collaborate directly with each other.

Multi-clouds consist of two models; (C) Multi-cloud Service: Clients access multiple clouds through a service. (D) Multi-cloud Library: Clients develop their own brokers by using a unified cloud API in the form of a library.

Our proposed key management framework is considered four possible architectures illustrated in Figure 1.

2.1.2. Inter-cloud Deployment Model [4]
In this subsection, based on Inter-cloud architecture, 4 possible deployments are illustrated as following figure.

(A) Replication of application
✓ Allows receiving multiple results from one operation performed in distinct clouds and to compare them within the own premise.

(B) Partition of application system into tiers
✓ Allows separating the logic from the data. This gives additional protection against data leakage due to flaws in the application logic.

(C) Partition of application logic into fragments
✓ Allows distributing the application logic to distinct clouds. This has a benefit that lead to data and application confidentiality.

(D) Partition of application data into fragments
✓ Allows distributing fine-grained fragments of the data to distinct clouds.

Thus, our key management framework to be a reasonable solution must consider four deployment models as shown illustrated in Figure 2 and discussed in the next subsection.

2.2. Cloud Key Management Infrastructure
A cloud key management infrastructure (CKMI) is a collection of technology, policies and procedures for managing all kinds of cryptographic keys in the Cloud environments, which serves for all kinds of cloud application encryption, and results in less costs for development and management [5].

But the CKMI has limitation to the Inter-cloud environment as it only supporting key management between service layers within a single cloud. So we need Inter-cloud Key Management Service (IKMS) to support a key management in multi-cloud environment.

2.3. TESLA One-way Key Chain
This section explains about TESLA[6], one of key chain method. TESLA is based on source
authentication and uses MAC (Message Authentication Code). Also it uses symmetric cryptosystem and need to loose synchronization for meeting asymmetric attributes between senders and receivers. TESLA has low overhead for verification and creation of authentication information. Furthermore the receiver needs protection mechanism from DoS Attack.

Figure 4 illustrates one-way key chain architecture of TESLA. User might know the data size in advance because generation key of TESLA perform in reverse order.

3. Inter-cloud Key Management (IKM)

3.1. Inter-cloud Key Management Requirements

Cloud providers have a security system which is independent from each other. So when cloud providers provide cloud collaboration service to users, the cloud provider might meet a security policy of other cloud providers.

We need integrated key management in Inter-cloud environment because security policies of cloud provider are different.

For the solution to Inter-cloud case, we specify Inter-cloud key management requirements and then propose Inter-cloud Key Management Framework (IKMF) based on the requirements. The requirements are described below:

(A) **Support encryption service for user data.**
- CSPs provide encryption service for protecting data of user individually when user requires the data encryption service. Also encryption key might be managed by corresponding CSP.

(B) **Use secure communication protocol.**
- For preventing data loss and information leakage, CSPs might use secure communication protocol that support to encrypt data.

(C) **One-time key usage.**
- The encryption key might be a one-time key because if the key is exposed, it will become dangerous.

(D) **Support variety encryption communication methods.**
- The key management might support variety of encryption methods; symmetric key, asymmetric key, digital signature, etc.

3.2. Inter-cloud Key Management Framework

The IKMF are consist of IKM can be the 3rd Party and Cloud Service Providers (CSPs).

If CSPs want to use IKM service, CSPs register at IKM service preferentially. Also CSPs have the same key generation algorithms.
Figure 6. Inter-cloud Key Management Workflow

Step 1. CSP1 require EKreq to the IKM server.
Step 2. At first, IKM server authenticates CSP1 and then generates and sends EKinfo. The EKinfo has a key generation algorithm and the key generation value.
Step 3. CSP1 generates an EK and ED using the encryption key (key chain) by any block unit.
Step 4. If CSP2 receives the ED, CSP2 requires DKinfo to IKM server.
Threat 1. If a MITM attacker steals the ED, he need DK to decrypt ED.
Step 5. IKM server authenticates CSP2 and then generates and sends DKinfo to CSP2.
Threat 2. If a MITM attacker steals the DKinfo, he need same key generation algorithm to generate DK.
Step 6. CSP2 generates decryption key and decrypts the encrypted data.

3.4. Evaluation

The IKM service generates higher overhead than existing plain text communication systems. But security of the IKM service is considered more important than performance in secure data communication of Inter-cloud environment.

In this paper, we compare IKM and CKMI about top threats of CSA and Inter-cloud requirements.

<table>
<thead>
<tr>
<th>Evaluation Domains</th>
<th>CKMI</th>
<th>IKM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data breaches</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Data loss</td>
<td>X</td>
<td>O</td>
</tr>
<tr>
<td>Account or service traffic hijacking</td>
<td>X</td>
<td>O</td>
</tr>
<tr>
<td>Insecure interfaces and APIs</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Denial of service</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Malicious insiders</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Abuse of cloud services</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Insufficient due diligence</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Shared Technology Vulnerabilities</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Support encryption service for user data.</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Use secure communication protocol.</td>
<td>X</td>
<td>O</td>
</tr>
<tr>
<td>One-time key usage.</td>
<td>X</td>
<td>O</td>
</tr>
<tr>
<td>Support variety encryption communication methods.</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>

Actually the CKMI is a key management in single cloud environment. So it has insufficient functions for Inter-cloud environment. However the IKM is proper in Inter-cloud environments because it designed based on features and requirements of Inter-cloud.

4. Conclusion

In this paper, we describe overview of Inter-cloud, and define Inter-cloud Key Management requirements and proposed the Inter-cloud key management framework for Inter-cloud environment.

The contribution of this paper is two-fold. First, we proposed IKM framework for Inter-cloud environment. The framework designed based on requirements of key management in Inter-cloud. Second, we described how to protect the user data for collaborated cloud services.

In the future, we will design extended IKM framework that is include relation of user to CSPs and define IKM protocol for CSPs. In addition, we will make improvements to adapt our IKM framework to practical Inter-cloud environment.

5. ACKNOWLEDGMENT

This research was supported by the MSIP (Ministry of Science, ICT & Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2014(H0301-14-1020)) supervised by the NIPA (National IT Industry Promotion Agency).

The corresponding author is professor Eui-Nam Huh.

6. References