Towards Secure Cloud Storage

(Demo for CloudCom2010)

SeongHan Shin and Kazukuni Kobara
Research Center for Information Security (RCIS)
National Institute of Advanced Industrial Science and Technology (AIST)
1-18-13 Sotokanda, Chiyoda-ku, Tokyo 101-0021 Japan
Email: seonghan.shin@aist.go.jp

***Abstract*—In this extended abstract, we explain a demo of the leakage-resilient authentication and data (key) management system which can be regarded as a prominent solution for secure cloud storage.**

I. Cloud Computing

Cloud computing (so-called, cloud) represents one of the magnificent shifts in information technology which can enhance collaboration, agility, scaling and availability, and provide the potential for cost reduction through optimized and efficient computing. Different from the existing technologies and computing approaches, cloud is defined [1] with five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service), SPI service models (Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)), and deployment models (Public, Private, Hybrid, Community). Due to its characteristics and models, Gartner Inc. expected worldwide cloud services revenue to reach $148.8 billion in 2014, and estimated that over the next five years entrepreneurs would spend $112 billion on SaaS, PaaS and IaaS [2].

However, security concern has become the biggest obstacle to adoption of cloud because all information and data (including real location of data, and security management level) are completely under the control of cloud service providers. For such a reason, CSA [3], ENISA [4] and NIST [5] published general security guidance and recommendations for the cloud usage in order to provide some level of protection ranging from physical security to network/system/application security. In March 2010, CSA [6] announced the top threats in cloud computing which, if not properly secured, may cause devastating impacts on the mission-critical cloud services. Among those threats,

- Data Loss or Leakage: Some examples to compromise data are 1) operational failures (e.g., improper data deletion or alteration); 2) inconsistent use of encryption and software keys (or loss of encryption keys); 3) unreliable data storage; and 4) insufficient AAA controls to allow unauthorized parties to access sensitive data. The threat of data compromise is mainly due to the architectural or operational characteristics of the cloud environment.
- Account or Service Hijacking: Account and service hijacking, usually with stolen credentials, remains a top threat. With the stolen credentials, an attacker can access critical areas of the deployed cloud services to compromise confidentiality, integrity, and availability of data and those services. If cloud service providers also provide SSO (Single Sign-On) or ID management services, the account and service hijacking would cause the collateral damage on those services as well.

Some general security guidance to deal with the above threats can be found in [3], [6]:

- Encryption and Key Management: Encryption provides data protection while key management enables access to protected data. It is strongly recommended to encrypt data in transit over networks, at rest, and on backup media. In particular, data encryption at rest (e.g., for long-term archival storage) can avoid the risk of malicious cloud service providers or malicious multi-tenants abuse. At the same time, secure key stores (including key backup and recoverability) and access to key stores must be securely implemented since improper (or access to) key storage could lead to the compromise of all encrypted data.
- Identity and Access Management: Secure management of identity and access control is a critical factor to prevent account and service hijacking. It is strongly recommended to prohibit sharing of account credentials, to leverage strong (multi-factor) authentication if possible, and to consider delegated authentication and managing trust across all types of cloud services.

In order to guarantee security against 'Data Loss or Leakage' and 'Account or Service Hijacking' threats, this security guidance would be summarized with three important keywords: Credential Management, Strong Authentication, and Key Management.

A. Problem Statement

In fact, 'Data Loss or Leakage' and 'Account or Service Hijacking' threats must be solved in Storage as a Service that is a specific sub-offering within the IaaS family. Currently, Amazon S3, Amazon EBS, CTERA Portal, Mosso Cloud Files, and Nirvanix are providing such cloud storage services.

For credential management, strong authentication and key management, one can employ the corresponding techniques such as standard network encryption (e.g., SSL/TLS, IKE, VPN), several authentication options (e.g., one-time passwords, biometrics, digital certificates) and Kerberos. However,

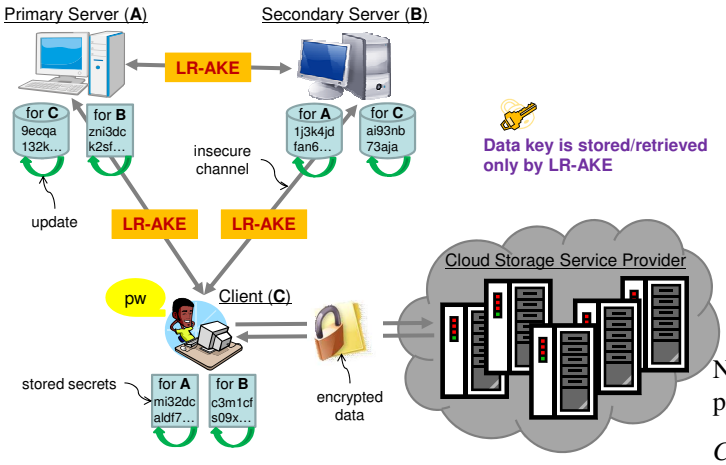

Fig. 1. The overall structure for secure cloud storage

employing independent techniques for cloud storage services does not necessarily mean that it can guarantee a high level of security against various attacks (e.g., with lost/stolen credentials)[1], and its implementation is cost-effective.

II. Contribution

A. Our Solution

For realizing secure cloud storage, we fully utilize the leakage-resilient authentication and data management system [7] which is constructed by tightly coupling the LR-AKE (Leakage-Resilient Authenticated Key Exchange) protocols [8] with data (key) management. This system not only guarantees a high level of security against active attacks as well as leakage of stored secrets (i.e., credentials and keys) but also makes a user possible to securely store/retrieve data keys in a distributed manner. For more detailed information, please refer to [7], [8] and the references therein. Actually, this system can be regarded as a prominent solution for cloud storage services since it provides credential management, strong authentication and key management *securely* and *cost-effectively* at the same time.

B. Overall Structure of Demo

The overall procedure for secure cloud storage is simple (see Fig. 1): A cloud user can store/retrieve data keys (to be used for encrypting/decrypting bulk data) by utilizing the leakage-resilient authentication and data management system [7]. More specifically,

1) A cloud user inputs his/her personal password pw that is usually chosen from a low-entropy dictionary. This password is combined with the stored (high-entropy) secrets so that the resultant values are used to perform the LR-AKE protocol between client C and authentication servers (i.e., primary server A and secondary server B), respectively[2].
2) If the authentication finishes successfully, client C securely recovers the data keys that have been distributed between a pair of the two parties (e.g., client C and primary server A). Moreover, the stored secrets of client C and authentication servers are updated to new ones (i.e., proactive secret sharing property). The recovered data keys can be used to encrypt/decrypt bulk data where the encrypted data are placed in the cloud storage.

Note that key management is segregated from the cloud service provider as recommended in [3].

C. Demo

In the demo, we show how the leakage-resilient authentication and data management system works for secure cloud storage. Also, we introduce the LR-AKE client interface (called, LR-Passwords). What a cloud user have to do with LR-Passwords is just to input his/her personal password. That's all! If the password is correct, the recovered data keys are automatically cached into the memory during the determined time period (of course, the user can change this parameter at his/her will).

Below is information to CloudCom2010 organizers.

- Category of this demo: hot topics
- Required facilities: Internet access (mandatory), power cable, and monitor (if available)

References

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Version 15", Information Technology Laboratory, NIST (National Institute of Standards and Technology), October 2009. Available at http://csrc.nist.gov/groups/SNS/cloud-computing/.

[2] Gartner Inc., "Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010", June 2010. Available at http://www.gartner.com/it/page.jsp?id=1389313.

[3] CSA (Cloud Security Alliance), "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", December 2009. Available at http://www.cloudsecurityalliance.org/guidance/.

[4] ENISA (European Network and Information Security Agency), "Cloud Computing: Benefits, Risks and Recommendations for Information Security", November 2009. Available at http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

[5] P. Mell and T. Grance, "Effectively and Securely Using the Cloud Computing Paradigm", Information Technology Laboratory, NIST, May 2009. Available at http://csrc.nist.gov/groups/SNS/cloud-computing/.

[6] CSA, "Top Threats to Cloud Computing V1.0", March 2010. Available at http://www.cloudsecurityalliance.org/topthreats.html.

[7] H. Imai, S. H. Shin, and K. Kobara, "New Security Layer for OverLay Networks (Invited Paper)", *Journal of Communications and Networks*, Vol. 11, No. 3, pp. 211-228, June 2009.

[8] LR-AKE webpage, https://www.rcis.aist.go.jp/project/LR-AKE/index.html.

[1] In the cloud environment, sensitive data should be hidden even to cloud service providers so that cloud users need to manage key stores (along with credentials) securely by themselves. But, it is not an easy task since credentials/key leakages are very common in the real world due to social engineering attacks (e.g., Phishing attacks), lost/stolen mobile devices (including USB memory), system bugs, and side-channel attacks.

[2] It is called cluster mode in [7].