isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337

Dasce-Data Security for Cloud Environment with Semi-Trusted Third Party Key Managers

Karthik Selvakumar[1], Alwin KoilRaj.A[2], Mrs. Beena Godbin.A[3]

Student, Dept. of Computer Science and Engineering, Agni College of Technology, India.[1, 2]
Asst. Professor, Dept. of Computer Science and Engineering, Agni College of Technology, India [3]

ABSTRACT:

Off-site data storage is an application of cloud that relieves the customers from focusing on data storage system. However, outsourcing data to a third-party administrative control entails serious security concerns. Data leakage may occur due to attacks by other users and machines in the cloud.

Wholesale of data by cloud service provider is yet another problem that is faced in the cloud environment. Consequently, high-level of security measures is required. In this paper, we propose Data Security for Cloud Environment with Semi-Trusted Third Party (DaSCE), a data security system that provides (a) key management (b) access control, and (c) file assured deletion. The DaSCE utilizes Shamir's (k, n) threshold scheme to manage the keys, where k out of n shares are required to generate the key. We use multiple key managers, each hosting one share of key. Multiple key managers avoid single point of failure for the cryptographic keys.

We (a) implement a working prototype of DaSCE and evaluate its performance based on the time consumed during various operations, (b) formally model and analyze the working of DaSCE using High Level Petri nets (HLPN), and (c) verify the working of DaSCE using Satisfiability Modulo Theories Library (SMT-Lib) and Z3 solver. The results reveal that DaSCE

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337

can be effectively used for security of outsourced data by employing key management, access control, and file assured deletion.

KEYWORDS: Key spliting analysis , Data Security In cloud, Off-site data storage.

1.INTRODUCTION

Cloud computing has emerged as a promising computing paradigm and has shown tremendous potential in managing the hardware and software resources located at third-party service providers. On-demand access to the computing resources in a pay-as-you-go manner relieves the customers from building and maintaining complex infrastructures. Cloud computing presents every computing component as a utility, such as software, platform, and infrastructure. The economy of infrastructure, maintenance, and flexibility makes cloud computing attractive for organizations and individual customers. Despite benefits, cloud computing faces certain challenges and issues that hinder widespread adoption of cloud. For instance, security, performance, and quality are a few to mention. Off-site data storage is a cloud application that liberates the customer from focusing on data storage systems.

Representing system characteristics and capabilities as utility, causes the user to focus on aspects directly related to data (security, transmission, processing). However, moving data to the cloud, administered and operated by certain vendors requires high level of trust and security. Data being the principal asset for organizations needs to be secured. Especially, when data must enter a public cloud. To avoid unauthorized access to cloud data, access control mechanism must be enforced. Moreover, data leakage and data privacy strategies must be employed so that only authorized users can access and utilize data. Refraining cloud service providers from utilizing the customer data requires high preventive measures. Encryption techniques provide a solution to ensure privacy and confidentiality of stored data.

2.SYSTEM ANALYSIS

2.1 EXISTING SYSTEM

The FADE is a light-weight and scalable technique that assures the deletion of files from cloud when requested by the user. However, during our analysis, FADE fell short on issues of security of keys and authentication of participating parties. In this existing process there is a man-in-the-middle (intruder) between client and KM.

The intruder can intercept user policy and send modified policy to KM. Now client didn't receive appropriate key from KM, this compromise may lead to the loss of data.

2.2 PROPOSED SYSTEM

In our proposed system we propose a data security scheme that uses key manager servers for the management of cryptographic keys. Shamir's (k, n) threshold scheme is used for the management of keys that uses k shares out of n to rebuild the key. Therefore, cryptographic keys must be stored in a robust manner and a single point of failure should not affect the availability of data.

To avoid man-in-the-middle attack user can access their key and data is ensured through a policy file that states policies under which access is granted to the keys. The DaSCE makes use of both symmetric and asymmetric keys. The confidentiality and integrity services for data are provided through symmetric keys that are secured by using asymmetric keys.

Asymmetric key pairs are generated by third party KM's. Out of the key pair, only public key is transmitted to the client. For secure transmission of keys, a secret key is established between client and KM through STS protocol.

3.Modules

- **Cataloging of Users & Policy Setting.**
- **File Upload & Policy File Creation.**
- **File Download.**
- **Policy Revocation and Renewal**

3.1.Cataloging of Users and Policy Setting:

In this module user has to register to become a member in cloud, once they registered user has to choose some attributes (e.g. name, email, address etc..,) and also give some user defined attributes to encrypt their policy file which is created while file uploading process. This Attribute Based Encryption performed using elgammal algorithm.

3.2.File Upload and Policy File Creation:

After completing the above process, authentication process will be performed between user and key manager using Diffie-Hellman key exchange Algorithm.

After that user will encrypt their file using secret key which is provided by cloud, based on user attributes and then it will uploaded into cloud and also policy file is generated simultaneously and it contains username, filename and access permission, by default user access permission will be allowed. Now user breaks up secret key into n shares (S1, S2…Sn) by using Shamir's key sharing technique and user encrypts their i-th key share with public key of i-th key manager.

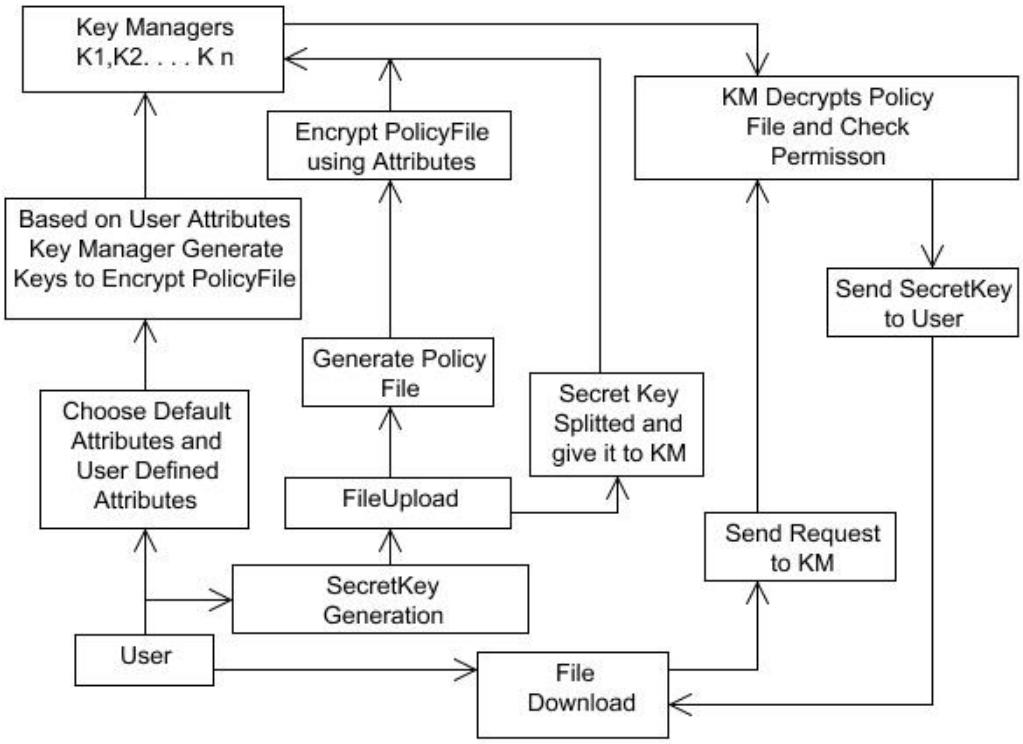
3.3.File Download:

If users need to download their file, then they will send request to Key-Manager with appropriate attributes. Key-Manager will check their attributes and decrypt the appropriate users policy file and check the user's file access permission for authenticate user, now Key-Manager will decrypts user secret key by using their own private key and they provide decrypted i-th share to the requested user. The secret key will be reformed by shamir secret scheme only if the attributes and credentials are proven. Now user will receive their secret key and download their file and decrypt using their secret key.

3.4.Policy Revocation and Renewal:

In this phase user will set revocation and renewalling of policies, for policy revocation user send revocation request to the key manager. Revocation is nothing but user will remove all the policies that he/she set before. User policy revocation request send to key manager, they delete all the policies of the user, in policy renewal key manager will allow to renew the user existing policy. Once he/she got approval from key manager user will renew their policy. Now

key manager will generate new set of keys and encrypt the user's policy file by using user's new policy.



System Architecture

4.Conclusion And Enhancement

- Hence we proposed and developed the DaSCE protocol, a cloud storage security system that provided key-management, access control, and file deletion. The key management was accomplished using (k, n) threshold secret sharing mechanism.
- Policy File Encryption-Policy files are generated when user upload their files in cloud. Inside the policy file contains username, filename which is upload by the user and access permission. This policy file will be encrypted by KeyManager by using user attributes.

REFERENCES:

1.M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Ktaz, A. Konwin-ski, G. Lee, D. Patterson, A. Rabkin, I. Stoics, and M. Zaharia, "A View of Cloud Computing," Communications of the ACM, Vol. 53, No. 4, 2010, pp. 50-58.

2. M. S. Blumenthal, "Is Security Lost in the Clouds?"Communica-tions and Strategies, No. 81, 2011, pp. 69-86.

3. C. Cremers, "The Scyther Tool: Verification, falsification, and analysis of security protocols." In Computer Aided Verification, Springer Berlin Heidelberg, 2008, pp. 414-418.

4. W. Diffie, P. C. V. Oorschot, and M. J. Wiener, "Authentication and authenticated key exchanges,"Designs, Codes and Cryptography,Vol. 2, No. 2, 1992, pp. 107-125.

5. N. En and N. Srensson, "An extensible SAT-solver," Lecture Notes in Computer Science, vol. 2919, Springer, 2003, pp. 502-518.

6. C P. Gomes, H. Kautz, A. Sabharwal, and B. Selman, "Satisfia-bility solvers," In Handbook of Knowledge Representation, Elsevier, 2007.

7. A. Juels and A. Opera, "New approaches to security and availabil-ity for cloud data," Communications of the ACM,Vol. 56, No. 2, 2013, pp. 64-73.

8. M. Kaufman,"Data security in the world of cloud compu-ting,"IEEE Security andPrivacy,Vol. 7, No. 4, 2009, pp. 61-64.