APPLIED SCIENCE LETTER
Vol. 4, No.4, OCT (2014), pp.01–04

CLOUD COMPUTING SECURE APPROACH FOR INTRA DOMAIN AND INTER DOMAIN

RANJITHA[1], KIRAN[2], SOWJANYA[3]

Abstract- *Controlling data flow between Primary Domain Controller (PDC) systems is referred to as inter-domain. Different computer protocols and services are used by this kind of computer to function. The most typical application is for multicasting across internet domains. Information inside the same domain is redistributed intra-domain. It has been suggested to use identity-based proxy re-encryption strategies to transfer the responsibility for managing many files from the owner to a proxy server. However, there are a number of issues with the current options. The plan is unworkable since, for example, the central authority decides on the access permission. They lack protection from collusion-based assaults. Finally, only intra-domain inquiries are taken into consideration. We point out that the cloud computing environment is one of the key applications for identity-based proxy re-encryption techniques. Nevertheless,*

***Key Words*: Access-control, Auditing, Inter- domain, Intra-Domain, Cloud computing, Identity, Security, Storage, Query, Encryption.**

1. INTRODUCTION

1.1 Instead of using a local server or a personal computer, cloud computing is the process of storing, managing, and processing data on a network of remote computers housed on the Internet. The term "cloud computing," which is relatively new, refers to the usefulness and use of computing resources. In order to provide centralized data storage and online access to computer services and resources, cloud computing entails the deployment of groups of remote servers and software networks. Private, public, and hybrid clouds are the different types of clouds. User-based access control (UBAC), role-based access control (RBAC), and attribute-based access control (ABAC) are the three types of access control. The list of users who are authorized to access data is known as the access control list.

1.2 Encryption

In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those

who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor.

1.3 Re-Encryption

Proxy re-encryption serves as a promising solutionto secure the data sharing in the cloud computing. It enables a data owner to encrypt shared data in cloud under its own public key, which is further transformed by a semi trusted cloud server into an encryption, intended for the legitimate recipientfor access control.

2. AUDITING

Cipher text-attribute based encryption (CP-ABE) isthe attribute based cryptosystems offers a way to encrypt a file for multiple users according to their privileges and also solve the queries of users. Data owner is the user

ISSN 2454 - 7239

who wants to outsource their data into the cloud and also responsible for encrypting files and generating access structure policies. User can check the data integrity based on two-party storage auditing protocols. In cloud storage system, itis improper to let either side of cloud service providers or user conduct such auditing, because no one could be guaranteed to provide unbiased auditing result. For this situation, third party auditing is a choice for the storage auditing in cloud computing. A third party auditor (auditor) that has expertise and capabilities can do a more efficient work and convince both cloud service providers and user. For the third party auditing in cloud storage systems, it has several important requirements which have been proposed in some previous works. The auditing protocol should have the following properties:

1. Confidentiality: The auditing protocol should keep user's data confidential against the auditor.

2. Dynamic Auditing: The auditing protocol should support the dynamic updates of the data which is stored in the cloud.

3. Batch Auditing: The auditing protocol should also be able to support the batch auditing for multipleuser and multiple clouds.ACCESS CONTROL

Access Control is one of the basic and fundamental security components in cloud computing and for the most part it is an approach or security technique thatpermits denies or limits access to a system/system resource. It permits one application to believe the identity of another application.

4. SECURITY

One of the benefits of cloud services is that you can operate at scale and still remain secure. It is similar to how you currently manage security, but now you have new ways of delivering security solutions that address new areas of concern. Cloud security does not change the approach on how to manage security from preventing to detective and corrective actions. but it does however give you the ability to perform these activities in a more agile manner. Your data is secured within data centers and where some countries require data to be stored in their country, choosing a provider that has multiple data centers across the world can help to achieve this.

Data Storage

Data storage often includes certain compliance requirements especially when storing credit card numbers or health information. Many cloud providers offer independent third party audit reports to attest that their internal process exist and are effective in managing the security within their facilities where you store your data.

Identity Based Storage

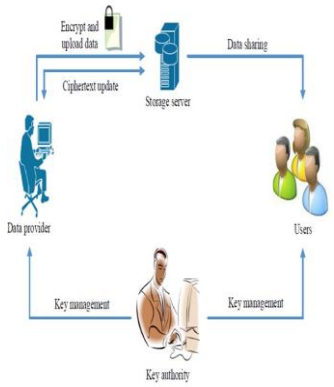
The cloud storage is one of the prominent services offered in cloud computing. Data stored over cloud in the plain text format represents a security threat. Thus, in this paper, we propose a method relying on the Identity Based Cryptography (IBE) for cloud storage that allows user to store and access the data securely and also the users can also clarify their doubts. Identity-based data storage scheme supporting intra-domain and

ISSN 2454 - 7239

inter-domain queries and prove its security and also against to collusion attacks.

Collusion Attacks

Collusion attack can be defined as the execution of operations that have the ability to combine multiple copies of the media or other files together so as to produce a new copy.



Cipher Text

Cipher text is encrypted text. Plaintext is what you have before encryption, and cipher text is the encrypted result. The term cipher is sometimes used as a synonym for cipher text, but it more properly means the method of encryption rather than the result.

5. PROPOSED SOLUTION

Cloud computing is a huge distributed system where multiple domains co-exist together. It is desirable that users in different domains can share sensitive data with others. Therefore, a sound identity-based data storage scheme in cloud computing should support not only the intra-domain query but also the inter- domain query. In this paper, we propose an data storage approach scheme which support both intra- domain and inter-domain queries. In our scheme, the
re-encryption key is computed by the data ownerindependently without the help of the primary key generator. For one query, the requester can only access one file of the owner, while the requester and the proxy server can cooperatively access all the files of the owner in previous schemes as the access permission (re-encryption key) is not bound to the cipher text in these schemes. This scheme is secure against the collusion attacks and selective-identity secure in the standard model.

6. CONCLUSION

Cloud computing is a distributed system where users in different domains can share data among each other. Identity-based proxy re-encryption schemes have been proposed to outsource sensitive data from the owner to an external party. For example, they can only support the intra-domain query and the access key is computed with the help of the private key generator . Additionally, the proxy server must be trusted. In this paper, we proposed an identity-based data storage scheme which is suitable to the cloud computing scenario as it supports both intra-domain and inter-domain queries and also avoids collusion attacks along with security. In our scheme, the accesskey is bound to not only the requester's identity but also the requested cipher text, and

can be computed by the owner independently without the help of the primary key generator. For one query, the requester can only access one file of the owner, instead of all files.

7. REFERENCES

[1] National Institute of Standards and Technology, Re- comeeded Elliptic Curves for Federal Government Use. http://csrc.nist.gov/groups/ST/toolkit/documents/dss/N ISTRe-Cur.pdf July

[2] Certicom Research, Standards for Efficient Cryptography SEC 2: Recommended El- liptic Curve Domain Parameters.http://www.secg.org/collateral/sec2final.pdf September.
.

[3] Weng J, Deng RH, Ding X, Chu CK, Lai J. Conditional proxy re- en-cryption secure against chosen-ciphertextattack. In: Li W, Susilo W, Tupakula UK, Safavi-Naini R, Varadharajan V, eds. Proceedings: ACM Symposium on Information, Computer and Communications Security -ASIACCS 2009. Sydney, Australia: ACM; 2009: 322-332.

[4] Fang L, Susilo W, Ge C, Wang J. Hierarchical conditional proxy re-encryption. Computer Standards & Interfaces 2012; 34(4): 380-389.

[5] Ateniese G, Fu K, Green M, Hohenberger S. Improved proxy re- en-cryption schemes with applications to secure distributed storage. In:Proceedings: Network and Distributed System Security Symposium -NDSS 2005. San Diego, California, USA: The Internet Society; 2005:1-15.

[6] Shamir A. Identity-based cryptosystems and signature scheme. In:Blak- ley GR, Chaum D, eds. Proceedings: Advances in Cryptology- CRYPTO 1984; vol. 196 of LectureNotes in Computer Science. SantaBarbara, California, USA: Springer-Verlag; 1984: 47-53.,Telangana.