International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 11 (2015) pp. 28439-28446

http://www.ripublication.com

Secure Resource Authentication Module In Public Cloud Access Management

S Ramamoorthy[*] N Kumaran[#] JS Shyam mohan[*] MThirunavukkarasu[*]
*Assistant Professor, Department of CSE,SCSVMV University**
Assistant Professor, Department of IT,SCSVMV University#
Kanchipuram, Tamilnadu, India.
ramamoorthys@kanchiuniv.ac.in[1] natarajankumn@rediffmail.com[2]
jsshyammohan@kanchiuniv.ac.in[3]
mthiru@kanchiuniv.ac.in[4]

Abstract

Data Security and Privacy in cloud data storage plays important role to retain the existing customers and attracting new business firms towards cloud. Outsourcing cloud data will reduce the overall Capital expenditure and maintenance overheads for the cloud users. File data deduplication is one of the most important data compression techniques for eliminating duplicate copies of repeating data, and has been widely used in cloud storage to reduce the amount of storage space and save bandwidth. To protect the confidentiality of sensitive data, in cloud storage the given data will be encrypted while its uploading into the cloud. In the same it was decrypted when its downloaded from the cloud storage for the future use. The Proposed work focusing on the data encryption and decryption process on the confidential data which is outsourced to the third party cloud Different from traditional deduplication systems, the different access privileges of users are considered for authenticated data access in the cloud. The proposed algorithm with Random token generation allow the authorized user to perform the updating and deletion process in the cloud data. This unique feature will eliminate the data security and privacy attack from unauthorized user. The Proposed methods effectively handle the duplicate file system and user access privileges on the cloud data. The results shows that proposed method incurs the maximum secrecy compare to the other schemes.

Keywords: cloud, security, De-duplication, Authentication

Introduction

Cloud computing internet based Technology allows the user to outsource their confidential data to the cloud storage space. The storage space can be offered as a

Service by Storage as a Service(SaaS) in cloud computing. Example like Amazon EC2,Rackspace,Microsoft Azure etc., This facility reduce the maintenance overheads and investment cost to deploy storage infrastructure at the user level. Through public networks user can able to store and access the data from cloud from any geographical region in the world. Cloud provide the centralized storage repository to store, access and manipulate the user data in the cloud environment.

The cloud data which is outsourced for the data storage and maintenance to the cloud server may face the deduplication and security issues related to the confidential user data. The data updation and access process need to authenticated effectively in order to avoid malicious activity over the data which is stored on the cloud. The data access privileges needs to be strength to restrict unauthorised effort over the data. The network traffic also get increased because of the duplication of data which is present in the outsourced data from the client.

Existing Related Work

File Data deduplication systems on the public cloud is involved as a proxy to allow data owner/users to securely perform duplicate check with differential privileges.

Insufficient user auditing security schemes to perform data security and file duplication check on the public cloud storage.

The security key exchange between the user and cloud administrator become a challenging task under the real public network communication. The Certificate signature generation and Certificate Verification on the signed data become more complex task for the cloud service providers.

The data owners only outsource their data storage by utilizing public cloud while the data operation is managed in public cloud.

Drawbacks In The Existing Model:

Traditional encryption, while providing data confidentiality techniques are insufficient to protect the data which is stored on the third party cloud. The data which is used in the live applications are need to be avoid de duplication to maintain the consistency of the results.

Identical data copies of different users will lead to different cipher texts, and more storage space on the cloud also making data traffic high.

Proposed Model:

In this, we enhance our system in security. Specifically, we present an advanced scheme to support stronger security by encrypting the file with differential privilege keys. In this way, the users without corresponding privileges cannot perform the duplicate check. Furthermore, such unauthorized users cannot decrypt the cipher text even collude with the cloud CSP. Security analysis demonstrates that our system is secure in terms of the definitions specified in the proposed security model.

Advantages of Proposed Model:
The user is only allowed to perform the duplicate check for files marked with the corresponding privileges. We present an advanced scheme to support stronger security by encrypting the file with differential privilege keys.

Table 3.1.2: Notations and symbols Used

S.No	Notation Used	Description
1	CSP	Cloud Service provider
2	Pow	Proof of Concept
3	Pk,Prk	User Public and Private Keys
4	?	Random token
5	PU	Privileged Users
6	PF	Specified privilege set of file F

Reduce the storage size of the tags for integrity check. To enhance the security of deduplication and protect the data confidentiality.

Proposed Architecture

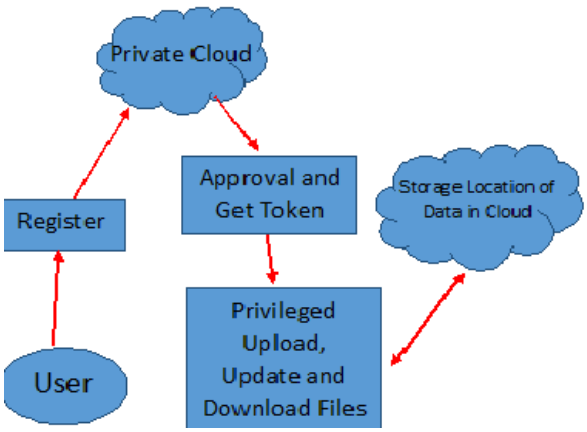

Figure 4.1: Proposed system Architecture

Proposed System Description
We propose another advanced DE duplication system supporting authorized duplicate check. In this new DE duplication system, a public cloud architecture is introduced to solve the problem. The public keys for privileges will not be issued to users directly, which will be kept and managed by the public cloud server instead. In this way, the users cannot share these public keys of privileges in this proposed construction, which means that it can prevent the privilege key sharing among users in the above straightforward construction. To get a file token, the user needs to send a request to the public cloud server. The intuition of this construction can be described as follows. To perform the duplicate check for some file, the user needs to get the file token from

the public cloud server. The public cloud server will also check the user's identity before issuing the corresponding file token to the user. The authorized duplicate check for this file can be performed by the user with the public cloud before uploading this file. Based on the results of duplicate check, the user either uploads this file or runs Proof of ownership.

Implementation and Result Analysis

The proposed work implemented based on the following modules.

Modules:

- Cloud Service Provider
- Data Users Module
- Public Cloud Module
- Secure Cloud Storage System

Modules Descripton:

Cloud Service Provider

In this module, focused on the development of Cloud Service Provider module. This is an entity that provides a data storage as a service to its customer through public cloud.

The S-CSP provides the data outsourcing service and stores data on behalf of the users.

To reduce the storage cost, the S-CSP eliminates the storage of redundant data via File data deduplication and keeps only unique data file system in the cloud.

In this work its is assumed that S-CSP is always online and has abundant storage capacity and computation power to synchronize with the business application.

Data Users Module

A user is an entity that wants to outsource data storage to the S-CSP and access the data later.

In a storage system support File deduplication, the user only uploads unique data but does not upload any duplicate data to eliminate the wastage of excessive bandwidth consumption, which reduce the overall flow rate of data transfer between cloud and its users.

In the authorized data access from the cloud storage system, each user is issued a set of privileges in the setup phase of the system. Each file is protected with the convergent encryption key and privilege keys to realize the authorized data and file deduplication with differential privileges. This feature may eliminate the data duplication and file complexity on the cloud storage.

Public Cloud Module

Compared with the traditional Data storage system architecture in cloud computing, this is a new entity introduced for facilitating user's for secure usage of cloud service.

Specifically, since the computing resources at data user/owner side are restricted and the public cloud is not fully trusted in practice, public cloud is able to provide data user/owner with an execution environment and infrastructure working as an interface between user and the public cloud.

The private keys for the privileged user access are managed by the public cloud, who answers the file token requests from the users. The interface offered by the public cloud allows user to submit files and queries to be securely stored and computed respectively.

Secure Cloud Storage System

In the proposed work considered several types of privacy issues need to focus by the cloud users, namely i) Remembrance of duplicate-check token: There are two types of adversaries, that is, external adversary and internal adversary.

As shown below, the external adversary can be viewed as an internal adversary without any privilege. If a user has privilege X, it requires that the adversary cannot forge and output a valid duplicate token with any other privilege X' on any file F, where X does not match X'.

Random token Generator Scheme

For the given set of N users in the organization access the cloud storage with the private key and the file name known in advance.The set of users privileges in the system defined as

U= { Pn1,Pn2,Pn3,…..PnN}.

For each privilege X in P, a private key Prk will be selected. For a user U with a set of privilegesPU, he will be assigned the set of keys Fpki.gpi∈PU . for File Uploading case Suppose that a data owner U with privilege set PU wants to upload and share a file F with users who have the privilege set PF = fpjg. The user computes and sends S-CSP the file token ϕ′.Fpk= TokGen (F, kp) for all X.If a duplicate is found by the S-CSP, the user proceeds proof of ownership of this file with the CSP. If the proof is passed, the user will be assigned a Pointer, which allows him to access the file.Otherwise, if no duplicate is found, the user computes

The encrypted file CF = EncCE (kF, F) with the convergent key kF = KeyGenCE (F) and uploads (CF , fϕ′F,pg) to the cloud server. The convergent key kF is stored by the user locally.

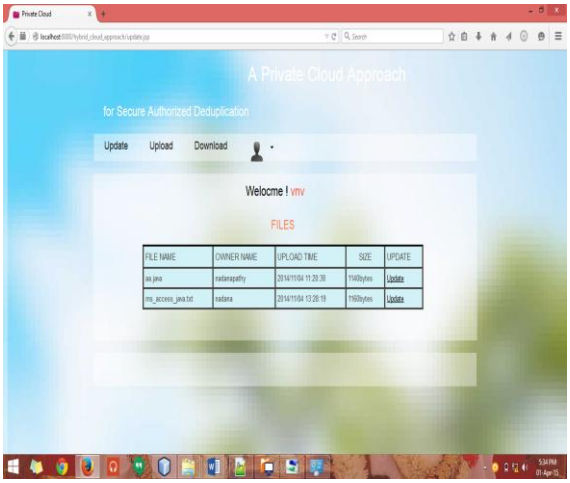

Figure 5.1.1: Secure Authentication Model

Privileged User Access and Modification

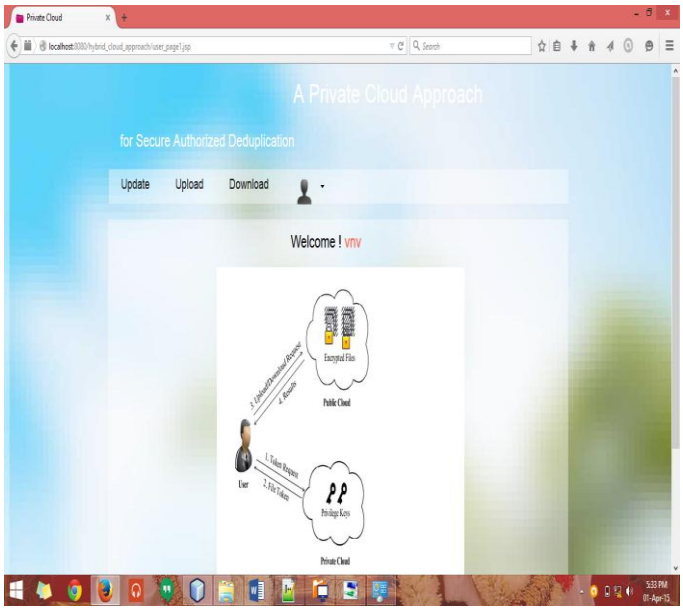

Figure 5.1.2: Update Operation

Figure 5.1.3: User Access Privileged updation

Result Analysis

The performance of the Proposed data Security model in cloud implement in the C++ simulator and the obtained results are shows that for the given number of user Access privileges the will increase the major file updation process in the cloud storage.

This will give the linear model relationship between the user access privileges and the give number of authorized updating operations on the cloud data in the cloud storage end.

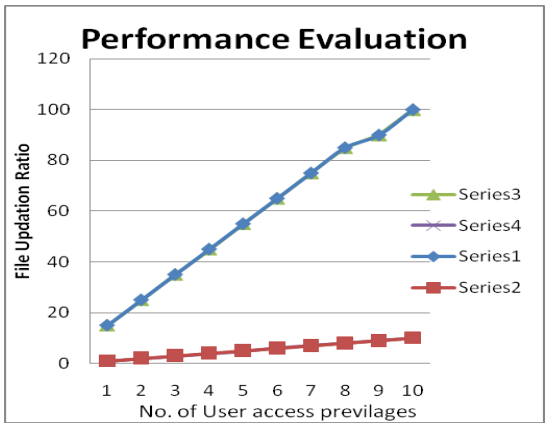

Figure 5.1.4: Performance analysis

Conclusion

The proposed work focused on the Privileged user access data access and updating process in the cloud storage services .It also enhancing the security aspects related to the data privacy in the cloud storage services. The data de duplication can eliminate the duplicate copies of the data which results the data inconsistency and network traffic issues. The proposed security prototype model also outperforms the existing model by providing sufficient security to the data storage in the Cloud environment.

Acknowledgement
The above work will be dedicated to my friends and my students who supported me to complete this paper in a effective way.

References

[1] Security of Applications Involving Multiple Organizations and Order Preserving Encryption in Hybrid Cloud Environments By Ahmadian, M. Paya, A.; Marinescu, D.C. in Parallel & Distributed Processing Symposium Workshops (IPDPSW), IEEE- 2014.

[2] Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment By Dubey, A.K. Namdev, M. Shrivastava, S.S. in Software Engineering (CONSEG), 2012

[3] A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud By Zhu, Z. Jiang, R. in IEEE Transactions on Parallel and Distributed Systems -2015

[4] Security of Applications Involving Multiple Organizations and Order Preserving Encryption in Hybrid Cloud Environments By Ahmadian, M. Paya, A.; Marinescu, D.C. in Parallel & Distributed Processing Symposium Workshops (IPDPSW), IEEE- 2014.

[5] An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds By Seung-Hyun Seo,Nabeel, M.; Xiaoyu Ding ; Bertino, E. in IEEE Transactions on Knowledge and Data Engineering -2014

[6] A privacy-preserving storage security for spatial data in dynamics cloud environment By Sakthivel, S. Dhiyanesh, B. in Computing, Communications and Networking Technologies (ICCCNT),2013

[7] A unidirectional data-flow model for cloud data security with user involvement during data transit By Bhatkalkar, B. J., Ramegowda in International Conference on Communications and Signal Processing (ICCSP), 2014.

[8] A Novel Zero-Knowledge Scheme for Proof of Data Possession in Cloud Storage Applications by Kaaniche, N., El Moustaine, E., Laurent, M. in 14th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (C C Grid), 2014.

[9] Secure data access in cloud computing by Sanka, S., Hota, C.; Rajarajan, M. in Internet Multimedia Services Architecture and Application (IMSAA), 2010 IEEE.

[10] Security Enhanced Anonymous Remote User Authentication and Key Agreement for Cloud Computing in Zheming Dong ,Lei Zhang ; Jiangtao Li in Computational Science and Engineering (CSE), IEEE- 2014.