IJETIE
International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue I, December 2014
ISSN: 2394 - 6598

ACCESS CONTROL WITH AUTHENTICATION FOR SECURING DATA IN CLOUDS

M.Ruban Raja Rathinam
M.E Software Engineering
Mount Zion College of Engineering and Technology
Pudukkottai,Tamilnadu.
mrubancs@gmail.com

K.Shanmugapriya
Dept. of Computer Science and Engineering
Mount Zion College of Engineering and Technology
Pudukkottai,Tamilnadu.
Shanmugapriya1903@gmail.com

***Abstract*-- Cloud based data storage systems have many complexities regarding critical/confidential/sensitive data of client. The trust required on Cloud storage is so far had been limited by users. The role of the paper is to grow confidence and mutual trust between data owner and CSP. The paper handles key questions of the User about how data is uploaded on Cloud, data is available to only authorized User as per Client/User requirement, authorized users should receive the latest version of the data information, and perform dynamic operation. In this paper we look at the various current researches being done to solve these issues, the current trends in securing, availability of these data on cloud storage services.**

***Keywords*— Access control, Cloud Storage, Data Availability, Newness.**

I. PREAMBLE

In this paper we presented the technique to improve the performance through theoretical analysis and experimental evaluation of storage, communication, computation and Security for trusted outsourced storages in cloud. In existing system the CSP needs a protection from any false accusation that may be claimed by the owner to get illegal compensations.

Overall processes in communication between the Owner, User, CSP are maintained by TTP .Cloud storage is offered by Storage as a Service , SaaS is a business model in which a large company rents space in their storage infrastructure to a smaller company or individual. Cloud providers manage the infrastructure and platforms that run the applications. saas is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis.

On-Demand Self-Service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Identity-based systems allow any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys.

This paper is prepared by the following: The related works are discussed in the 2nd section. The proposed work about the different discussed in the 3rd section. The Results and discussion is discussed in the 4th section. The conclusion and the further research are discussed in the 5th section.

II. RELATED WORK REVIEW

In previous research papers, they are tried to improve the Storage method in untrusted outsourced storage in cloud. They are focusing to improve the reliability of communication .we doesn't focus any illegal interaction compensation. this trusted cloudme give the possible ways to improve the communication,and secured data.

Cloud computing is a promising computing model that enables convenient and on-demand network access to a shared pool of computing resources. Cloud storage is an important service of cloud computing, which allows data owners to move data from their local computing systems to the Cloud. More and more data owners start choosing to host their data in the Cloud.The local management of such huge amount of data is problematic and costly due to the requirements of high storage capacity and qualified personnel. Therefore, Storage-as-a-Service offered by cloud service providers (CSPs) emerged as a solution to mitigate the burden of large local data storage and reduce the maintenance cost by means of outsourcing data storage.

Cloud Storage Providers like Microsoft with Sky Drive, Google Documents, and Drop Box, CloudMe have successfully dropped rates of storage available on internet. They promise availability of the data from different systems/locations/networks. Basic security like User based authentication access of data and maintaining offline data to the client's machine is also supported. Given all the above features still User confidence on the Cloud storage still hampers the usage of the Cloud based Storage. The companies are investing heavily on the servers with massive storage devices divided geographically and interconnected with high bandwidth and speed networks. The utilization, if analyzed is still low in terms of Confidential/secure data hosted by clients.

The paper presents access control with authentication method which can be provided to client for authorized users can access and modify the data. cloud-based storage scheme that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. Grant or revoke access rights to the outsourced data, Misbehavior from Dishonest party is detected and the responsible party is identified.

Cloud storage : Simple Block Status Table (BST) to record and access file blocks . The structure of our block status table is similar to that of file block allocation table in file systems. Generally The BST consists of three columns: serial number (SN), block number (BN), and key version (KV). Different from the common index table, we must assure that all records in this kind of table differ from one another to prevent the forgery of data blocks a. In addition to record data changes, each record in table is used to secret key sk.

Access control : Authorized users are allowed to access the outsourced data. Revoked users can read unmodified data, however, they must not be able to read updated/new blocks. Access control to outsourced data with flexible and efficient management. The data owner needs to maintain only a few secrets for key derivation.

Proposed system formally defines protocols for provable data possession (PDP) that provide probabilistic proof that a third party stores a file. Introduce the first provably secure and practical PDP schemes that guarantee data possession. Implement one of our PDP schemes and show experimentally that probabilistic possession guarantees make it practical to verify possession of large data sets.

Audit service is constructed based on the techniques, fragment structure, random sampling, and index-hash table, supporting provable updates to outsourced data and timely anomaly detection. Also propose a method based on probabilistic query and periodic verification for improving the performance of audit services. Security solutions also introduced to avoid the malicious users while outsourcing in the cloud.

Efficiency and Security: PDP scheme , perform symmetric key operations in setup and verification phases.

Dynamic Data Support: To supports secure and efficient dynamic operations on outsourced data blocks,that are uptation modification, deletion and append.

TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, further extend our privacy-preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency.

The security of identity-based cryptography is based on the assumption that the particular bilinear maps chosen are one-way functions, meaning it is easy to calculate their result given a pair of operands but hard to calculate the inverse.

III. PROPOSED SYSTEM DESIGN

This architecture illustrates in figure 1 the proposed system contain owner, user, CSP and TTP. Whenever owner store the information in encrypted format using keys.TTP is a controller of owner,user and CSP. The users are using this system by receiving the message and getting information from CSP.CSP is indirect mutual trust between owner and user.

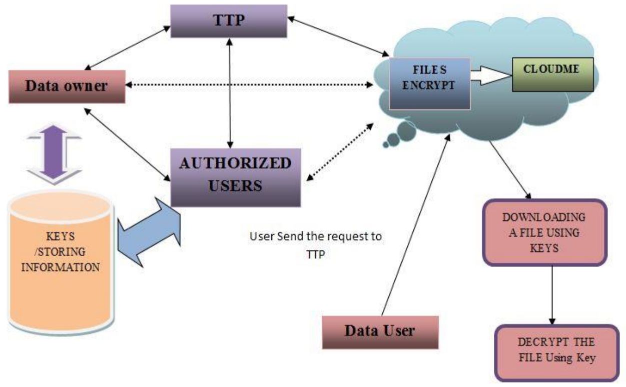
TTP
FILES ENCRYPT
CLOUDME
Data owner
AUTHORIZED USERS
KEYS /STORING INFORMATION
User Send the request to TTP
DOWNLOADING A FILE USING KEYS
Data User
DECRYPT THE FILE Using Key

Fig .1. Architecture Diagram

For System Process

User Side

Fig .2. User Side Process

CSP Side

2. CSP ask User for authentication just like login page.
4. Verify password if correct send a file that he wants to access. Else move to step 2.
7. CSP check the signature for authenticity and compute the message digest to find encrypted file which is compare with encrypted file of another message.
8. If correct it will change previous file with this one and move to step12.
9. Else ask the client to follow the step 8.
10. CSP sends a same message to client after addition of his signature.

Fig .3. CSP Side Process

Symbol	Meaning
SN	Serial number
BN	Block Number
KV	Key Version
F	File
M	Modification

TABLE I. NOTATION OF SYMBOLS

A. CloudMe

CloudMe (formerly icloud) is a file storage service operated by CloudMe that offers cloud storage, file synchronization and client software. It features a blue folder that appears on all devices with the same content, all files are synchronized between devices. The CloudMe service is offered with a freemium business model and provides encrypted SSL connection with SSL Extended Validation Certificate. CloudMe provides client software for Microsoft Windows, Mac OS X, Linux, Android, iOS, Google TV, Samsung Smart TV and web browsers.

As a cloud sync storage provider, CloudMe has a strong focus on the European market and differentiates itself from other storage providers with mobility and media features like Samsung SmartTV support.

1. User request to access a file from CSP.
3. User authenticates CSP by his password
5. User decrypts the file by applying decryption algorithm
6. If User modify the file he will send file to CSP and TTP with a message like *Md* as (*F*',$,*M*) and *F* ' here M denotes for modification F ' for encrypted file, *Md* for message digest file and $ for signature.
11. If file is same as previous one, drop this packet and move to step 1 or step 13.
12. Else ask CSP to follow step 11 again.
13. Exit ' F

Recently Novell announced support for the CloudMe service in their Dynamic File Services Suite. Novosoft Handy Backup version 7.3 also announced support for CloudMe. There are many third party mobile apps and software available for CloudMe, many using the WebDAV support of CloudMe.

The users can enhance the use of CloudMe by having iPhone or Android phone. Once CLoudMe is installed on the device, one can easily access the data all over the network. If the user makes changes in the cloud, then all the required changes will be made to other data as well. For instance, if a photo is taken with CloudMe iPhone application and saved in the CloudMe folder, then it will also be available on the computer drive as well. CloudMe can also be installed on multiple computers at the same time, for example, on home and work computer so that you can have all the files available on both the computers. There is no longer a need to have a USB-memory stick with you. Further, CloudMe allows the user synchronize multiple folders simultaneously. Now you can keep your photos, music, videos and documents all organized in the same folder as you always wanted to have but now with an additional CloudMe features.

CloudMe also setup the folders so that they can be automatically synchronized. As now everything will be available in CloudMe, one can feel safe if something goes wrong in the computer. The user can also share the files while on the go directly from a Smartphone or tablet. There is a CloudMe Web share feature that allows the user to share links to files or folders through instant messaging or emails. CloudMe also supports direct sharing to Google, Twitter and Facebook. The user can also add Web Share feature as a favorite so that he or she can always has access to what is being shared throughout the network. In the Cloud Me upload the encrypted but the the encrypted files should be a Proxy Re-Encryption to evaluate storage, communication, and computation overheads.

B. Identity-Based Proxy Re-Encryption

An application of proxy reencryption to the distribution of key material within a cryptographic filesystem. Each file stored on an trusted file server is encrypted using a symmetric key; these keys are encrypted under a public master key which is stored alongside the encrypted material. When a user wishes to decrypt a file, The owner provides access control for the encrypted material,and provide a decrypt secret Key.

We propose a significant security improvement to the access control in cryptographic storage, using proxy cryptography to reduce the amount of trust in the access control server. In our approach, keys protecting files are stored encryptedunder a master public key. When a user requests a key, the access control server uses proxy cryptography to directly re-encrypt the appropriate key to the user without learning the key in the process. Because the access control server does not itself possess the master secret, it cannot decrypt the keys it stores. The master secret key can be stored offline, by a content owner who uses it only to generate the re-encryption keys used by the access control server. we describe our implementation and provide a performance evaluation of our constructions.

IV. Result And Discussion

This paper explains Register and upload the files ,the upload files using keys, To maintain the privacy of outsourced data in a secure manner. Indirect mutual trust between CSP and data owner. The owner is capable of not only archiving and accessing the data stored by the csp, but also updating and scaling this data on the remote servers.The above discussion explains how to manage seurind data transmission in cloud computing. This ID based encryption process improving the communication between the owner and user.

V. Conclusion And Future Work

In this paper we have shown overheads on storage, communication and the computation of our data. This will improve the performance of communication and storage security. The user can get the most of CloudMe when it is set up on all the devices, including PC or Mac. It makes sure that all your stuff is stored, without which you cannot live such as contacts, photos, videos and important documents. It also keeps everything up-to-date on all the devices. If the user wants to update a contact, add a calendar event or delete an email, then changes will be everywhere. It is designed for all types of systems so that all users can easily download it and get access to all the required files. In future we are plan to develop our cloud service provider's data storage management system without the excessive overheads which explained in previous, and to add more features in this service.

References

[1]. Amazon elastic compute cloud (Amazon EC2), http://aws.amazon.com/ec2/.

[2]. Ayad Barsoum ,Anwar Hasan, Ontario, Canada "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems" Digital Object Indentifier 0.1109/TPDS.2012.337 1045-9219/12/$31.00 © 2012 IEEE

[3]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in CCS '07: Proceedings of the 14th ACM Conference on Computer and Communications Security, New York, NY, USA, 2007, pp. 598–609.

[4]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," Cryptology ePrint Archive, Report 2009/081, 2009, http://eprint.iacr.org/

[5]. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in SecureComm '08: Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, New York, NY, USA, 2008, pp. 1–10.

[6] . W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in Proceedings of the 2009 ACM workshop on Cloud computing security, ser. CCSW '09. ACM, 2009, pp. 55–66.

[7]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM, 2010, pp. 525–533.

[8]. K. D. Bowers, A. Juels, and A. Oprea, "HAIL: a high-availability and integrity layer for cloud storage," in CCS '09: Proceedings of the 16th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2009, pp. 187–198.

[9]. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, “MR-PDP: multiple-replica provable data possession,” in *28th IEEE ICDCS*, 2008, pp. 411–420.

[10]. A.F. Barsoum and M. A. Hasan, “Provable possession and replication of data over cloud servers,” Centre For Applied Cryptographic Research, Report 2010/32, 2010, http://www.cacr.math.waterloo.ca/techreports/2010/cacr2010-32.pdf.

[11] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, “MR-PDP: multiple-replica provable data possession,” in *28th IEEE ICDCS*, 2008, pp. 411–420.

[12] A. F. Barsoum and M. A. Hasan, “On verifying dynamic multiple data copies over cloud servers,” Cryptology ePrint Archive, Report 2011/447, 2011, 2011, http://eprint.iacr.org/.

[13]. Matthew Green Giuseppe Ateniese"Identity-Based Proxy Re-Encryption"Information Security Institute Johns Hopkins University 3400 N. Charles St. Baltimore, MD 21218{ateniese,mgreen}@cs.jhu.edu.

[14]. Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. “Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage”, in the 12th Annual Network and Distributed System Security Symposium, pages 29–43, 2005. Full version available at http://eprint.iacr.org/2005/028.

[15]. Ran Canetti, Shai Halevi, and Jonathan Katz. “Chosen-ciphertext security from Identity Based Encryption.” in Proceedings of Eurocrypt ’04, volume 3027 of Lecture Notes in Computer Science, pages 207–222. Springer-Verlag, 2004.

M. Ruban Raja Rathinam is a M.E., Candidate in the Department of Computer Science and Engineering at Mount Zion College of Engineering and Technology, Pudukkottai. He received his B.E. degree in computer science from Maharaja Engineering College, Coimbatore in 2012. He has undergone his project regarding “Access control with Authentication for Securing Data in Clouds”. He had published a paper in International Journal of Emerging Technology and Advanced Engineering ” An Efficient Communication Service in Wireless Networks” in Journal of Wireless Network Application.

Asst.Prof **K. Shanmugapriya** received her M.E in computer science (2012) from JJ College of Engg&Tech, Trichy & B.E in Computer Science (2010) from Arasu Engineering College, Kumbakonam, Tamilnadu, India. She is having 2 Years of Experience in Teaching & Currently working as Assistant Professor in the Department of Computer Science and Engineering in MZCET, Pudukkottai.