ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Byte Level Encryption and Authentication Algorithms for Data Revocation in the Cloud

K.kiran
M.Tech Student,
Department of Computer Science Engineering,
Chilukuri Balaji Institute of Technology.

P. Dharshan
Associate Professor & HOD,
Department of Computer Science Engineering,
Chilukuri Balaji Institute of Technology.

Abstract:

Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. Cloud storage services may be accessed through a co-located cloud computer service, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems.

In Cloud services the data uploaded by the users and they are easily modified by the users. In previous approaches the data revocation done without any authentication of the users to other documents uploaded by other users. Here there are two problems rising such as authentication and integrity, security to uploaded data. For this problem we introduced an architecture which consists of secure authentication and the secure storing of the data by using byte level encryption and authentication algorithms.

Keywords:

Data Storage, Data Revocation, Authentication, Encryption, Cloud Computing.

Introduction:

Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network.

At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand.

This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server).

This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rack space, etc. are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications.Cloud storage is based on highly virtualized infrastructure and is like broader cloud computing in terms of accessible interfaces, near-instant elasticity and scalability, multi-tenancy, and metered resources. Cloud storage services can be utilized from an off-premises service or deployed on-premises.

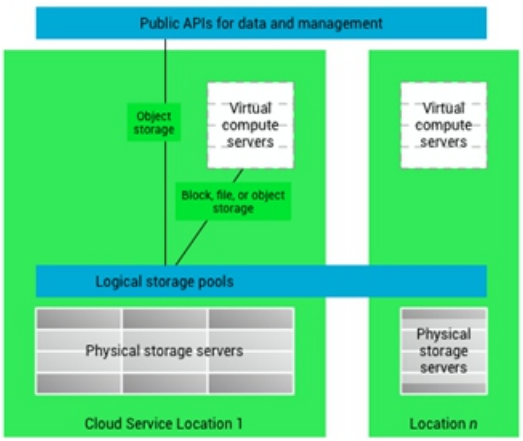
Cloud storage typically refers to a hosted object storage service, but the term has broadened to include other types of data storage that are now available as a service, like block storage.Object storage services like Amazon S3 and Microsoft Azure Storage, object storage software like Openstack Swift, object storage systems like EMC Atmos and Hitachi Content Platform, and distributed storage research projects like OceanStore[5] and VISION Cloud [6] are all examples of storage that can be hosted and deployed with cloud storage characteristics.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Cloud storage is:

Made up of many distributed resources, but still acts as one - often referred to as federated storage clouds Highly fault tolerant through redundancy and distribution of dataHighly durable through the creation of versioned copies Typically eventually consistent with regard to data replicas.

High level cloud storage architecture



Existing System:

With shared data, once a user modifies a block, shealso needs to compute a new signature for the modifiedblock. Due to the modifications from different users, differentblocks are signed by different users. For securityreasons, when a user leaves the group or misbehaves,this user must be revoked from the group. As a result,this revoked user should no longer be able to accessand modify shared data, and the signatures generatedby this revoked user are no longer valid to the group. Therefore, although the content of shared data isnot changed during user revocation, the blocks, whichwere previously signed by the revoked user, still needto be re-signed by an existing user in the group. As aresult, the integrity of the entire data can still be verifiedwith the public keys of existing users only.

Disadvantages:

1.In resigning of the users the data van be modified another users without any authentication.

2.In many situations the key generations between the cloud and users leads to complication.

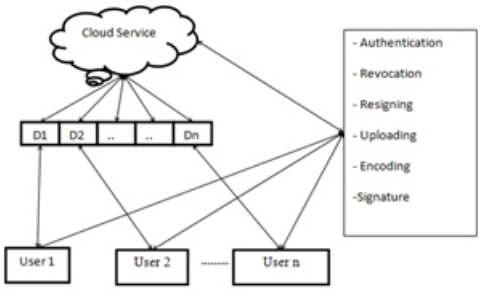
3.There are some security issues at the time of uploading the documents after resigning.

Problem Statement:

With relinquish trends in cloud, Data integrity is one of the critical issue, as there is lack of identity privacy, where the users are unacquainted with the auditor of the data, over geographically scattered datacenters. This features of cloud computing evolved various concerns related to user's identity, data integrity and users availability. Ultimately this influences to propose an enhanced model in order to audit the data integrity and keeping the identity privacy with efficient user revocation while sharing.

Proposed System:

In our work we introduced a novel framework to store and authenticate the users. We introduced a cryptographic algorithm such as byte level session based symmetric algorithm. We designed architecture as shown below:



In this users which are upload documents are should register in the cloud service and get authenticated. The User selects a file and encode the encrypted file by using the above mentioned algorithm as shown below:

Algorithms:

Encoding Algorithm:

Step 1. The input file i.e. the plain text is considered as a binary stream of finite no. of bits.

Step 2. This input binary string breaks into blocks with different lengths like 8 / 16 / 32 / 64 /128 / 256 / 512 …… (2k order where k = 3, 4, 5, ….)as follows:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

First n1 no. of bits is considered as x1 no. of blocks with block length y1 bits where n1 = x1 * y1.
Next n2 no. of bits is considered as x2 no. of blocks with block length y2 bits where n2 = x2 * y2and so on.
Finally nm no. of bits is considered as xm no. of blocks with block length ym bits
where nm = xm * ym with ym = 8. So no padding is required.
Step 3. For each block with length n, a unique number (ranging from 1 to 3*n) is generated forthe position of each bit using the following function
f1(p) = p + n * [{ n + p * (-1)^ (n % 3) } % 3] ;
where, n = block length under considerationp = position of the pth bit(-1)^ (n % 3) means that (n% 3) is the power of (-1).
(n % 3) returns the remainder when n is divided by 3.
Step 4. The new position of each bit is generated to form the next intermediate block using thegiven function
f2(q) = (q + 2) / 3 ; where, q = generated unique no. using f1(p) for pth bit
Step 5. The block of length n (=2k) be regenerated after n/4 (=2k-2) no. of iteration. Any of theintermediate blocks generated in this process may be used as encrypted string.
Step 6. The cipher text is formed after converting the encrypted binary string into characters.

Decoding Algorithm:

Step 1. For decryption process, the input file i.e. the cipher text is considered as a binary stream.
Step 2. After processing the session key information, this binary string is broken down intoblocks of different length as similar as encryption process.
Step 3. Since a block of length n (=2k) is regenerated after n/4 (=2k-2) no. of iteration, so theprocess is symmetric in nature. If n1 no. of iteration is used for encryption then (n/4 – n1) no.of iteration is used for decryption.
Step 4. The plain text is reformed after converting the decrypted binary string into characters.
We provide resigning by using captcha authentication which means the system can display the authentication images and then the user have to enter respective codes. If the user enters correct value the user is allowed to resign.

Signature Generation Algorithm:

Before stored data into cloud the user will generate authentication code for identify valid user will stored data into cloud. The generation of authentication code is used for sha1 hash function. Using sha1 function we can generate authentication code and append authentication to file stored into cloud.

Conclusion:

We proposed a novel authentication method for resigning and uploading data by using secure methods. The data which is used by another user have to authenticate to cloud service to access another user's files. By using this method we achieve more authentication issues and signature generation problems. When a user in the group is revoked, we allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with re-signatures. Experimental results show that the cloud can improve the efficiency of user revocation, and existing users in the group can save a significant amount of computation and communication resources during user revocation.

References:

[1] Wang, B. ; State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, Shaanxi, P.R. China ; Li, B ; Li, H., Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud, Services Computing, IEEE Transactions on (Volume:8 , Issue: 1)

[2] P. Mell and T. Grance, "Draft NIST working definition of cloud computing".

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2011.

[4] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and S. Chen, "Dynamic Audit Services for Outsourced Storage in Clouds," IEEE Transactions on Services Computing, accepted.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[5] S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham and Aamir M. Mirza, "Implementation of EAP with RSA for Enhancing The Security of Cloud Computig", International Journal of Basic and Applied Science, vol 1, no. 3, pp. 177-183, 2012

[6] Balkrishnan. S, Saranya. G, Shobana. S and Karthikeyan.S, "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", International Journal of computer science and Technology, vol. 2, no. 2, ISSN 2229-4333 (Print) | ISSN: 0976-8491(Online), June 2012

[7] K. Kiran Kumar, K. Padmaja, P. Radha Krishna, "Automatic Protocol Blocker for Privacy-Preserving Public Auditing in Cloud Computing", International Journal of Computer science and Technology, vol. 3 pp, ISSN. 0976-8491(Online), pp. 936-940, ISSN: 2229-4333 (Print), March 2012

[8] Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J.,"Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing", Bioinfo Security Informatics, vol. 2, no. 2, pp. 49-52, ISSN. 2249-9423, 12 April 2012

[9] J. Yuan and S. Yu, "Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud," in Proceedings of ACM ASIACCS-SCC'13, 2013

[10] H. Shacham and B. Waters, "Compact Proofs of Retrievability,"in the Proceedings of ASIACRYPT 2008. SpringerVerlag,2008,pp.90–107.

[11] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,and D. Song, "Provable Data Possession at Untrusted Stores,"in the Proceedings of ACM CCS 2007, 2007, pp. 598–610.