© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Cloud Aided Shred Data with Digital Signature User Revocation

P. Deivendran, S. Abdul Rahman, P. R. Kishore, K. S. Rajeshwar Katoch
Information Technology, Velammal Institute of Technology
Velammal Knowledge Park, Panchetti, Chennai, Tamilnadu, India

ABSTRACT

Storage and Sharing of data in cloud can be easily modified by user. To overcome this data modification in cloud signature is provided to each individual who access the data in cloud. Once the data is modified by the user on a block, the user must ensure that the signature is provided on that specific block. When the user gets revoked from accessing the cloud the existing user of the cloud must re-sign the data signed by the revoked user. To re-sign the data they must download the entire data and sign it. This difficulty is rectified with the novel public auditing mechanism idea of proxy re-signatures. In addition to this, security of the data is also enhanced with the help of public verifier who is always able to audit the integrity of shared data without retrieving the entire data from cloud.

Keywords: *:* WWW, component, formatting, style, styling, insert

I. INTRODUCTION

Cloud computing is internet based computing in which large groups of remote servers are networked to allow sharing of data processing tasks, centralized data storage, online access to computer services or resources. As a metaphor for the Internet, "the cloud" is a familiar cliché, but when combined with "computing," the meaning gets bigger and fuzzier. Some analysts and vendors define cloud computing narrowly as an updated version of utility computing: basically virtual servers available over the Internet. Others go very broad, arguing anything you consume outside the firewall is "in the cloud," including conventional outsourcing. Cloud computing comes into focus only when you think about what IT always needs: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT's existing capabilities. RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private. It is based on the fact that finding the factors of an integer is hard. Once the information is changed by the user on a block, the user should make sure that the signature is provided there on specific block. Once a user gets revoked from accessing the cloud the present user of that cloud should re-sign the information signed by the revoked user. To re-sign knowledge the user should transfer the complete data and sign it. A novel public auditing mechanism plan of proxy re-signatures. Additionally to present, the security of information is additionally increased with the assistance of a public admirer world health organization is often ready to audit the integrity of audit the integrity of shared information while not retrieving the whole data from the cloud.

II. METHODS AND MATERIAL

System Architecture

The system architecture comprises seven modules:

1. Shared data in cloud
2. Revocation of users
3. Proxy Re-signatures
4. Construction of HAPS
5. Construction of PANDA
6. Extension of PANDA
7. Performance Evaluation

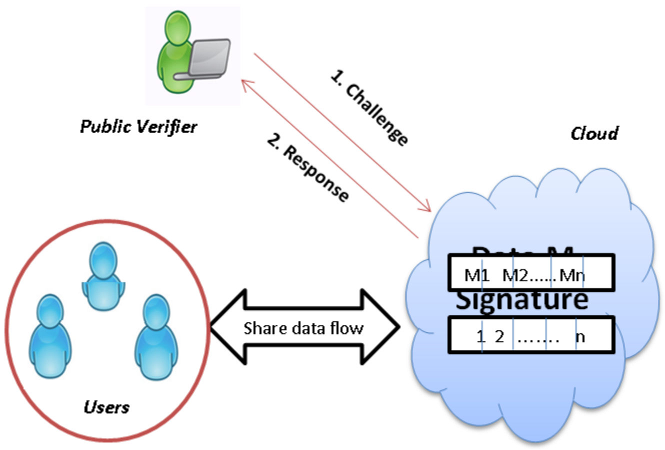

Figure 1: System Architecture

System Description

The major functional components are briefly described below:

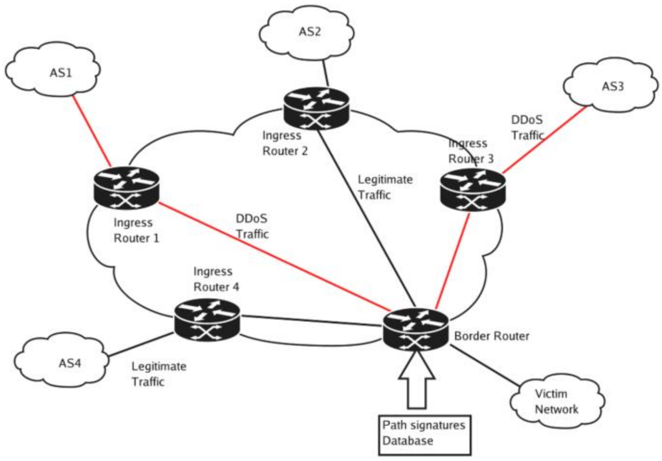

Figure 2 : A sample line graph(Font 8pt Times New Roman, Bold and Centered).

A. Shared Data in Cloud Module

Cloud providers promises a secure and reliable environment to the users, the integrity of data in the cloud may still be compromised, due to the existence of hardware/software failures and human errors. To protect the integrity of data in the cloud in this module a number of mechanisms have been proposed. In these mechanisms, a signature is attached to each block in data. Once a user modifies block of data shared data, he/she also needs to compute a new signature for the modified block. This module also implements a mechanism of checking data integrity in the cloud without downloading the entire data, referred to as public auditing.

B. Revocation of User Module

The revocation of user in a group is carried out based on some security reasons or when a user leaves the group or misbehaves. This revoked user has no longer be able to access and modify shared data. In this module once the user gets revoked from a group the block of data accessed by the revoked user must be resigned by existing user using the public key. The integrity of the entire data can still be verified with the public keys of existing users only.

C. Proxy re-signatures Module

This proxy re-signature module allows a semi-trusted proxy to act as a translator of signatures between two users. The signature of two users gets interchanged. Meanwhile, the proxy is not able to learn any private keys of the two users The cloud act as the proxy in this module and convert signatures for users during user revocation. Efficiency gets improved during user revocation progress.

D. Construction of HAPS Module

Traditional proxy re-signature schemes are not block less verifiable, if we directly apply these proxy re-signature schemes in the public auditing mechanism, then a verifier has to download the entire data to check the integrity. Homomorphic authenticable proxy re-signature (HAPS) is a block less verifiable and non-malleable scheme. This HAPS scheme uses five different algorithms (KeyGen, Rekey, Sign, Resign and Verify) to enhance the block less data verification on shared data.

E. Construction of PANDA Module

A public auditing mechanism for shared data with efficient user revocation (PANDA) allows the original user to act as the group manager, who is able to revoke users from the group when it is necessary. This module allows the cloud to perform as the semi-trusted proxy and translate signatures for users in the group with resigning keys. The re-signing is performed by the cloud in this module which improves the efficiency of user revocation and saves communication and computation resources for existing users.

F. Extension of PANDA Module

In this module the verification of block of data is done by selecting a number of random blocks instead of choosing all the blocks in shared data. The original user who acts as the group manager, can keep a short priority list (PL) with only a small subset of users instead of the entire PL with all the users in the group, the total number of re-signing keys required in the cloud gets reduced. Batch auditing is implied in this module, a public verifier can perform multiple auditing tasks simultaneously with the mechanism of batch auditing.

G. Performance Evaluation Module

The main purpose of Panda is to improve the efficiency of user revocation. Task involved in resigning of block of data gets easier with the implementation of cloud resigning mechanism increasing the performance dramatically. Our mechanism is still quite efficient for supporting large groups. Our mechanism allows this verifier to perform batch auditing to improve the performance on multiple auditing tasks.

III. CONCLUSION AND FUTURE

Storage and sharing of information in cloud will be simply changed by users. to beat this knowledge modification in cloud signature is provided to every individual World Health Organization access the info in cloud. We planned a replacement public auditing mechanism for shared information with economical user revocation in the cloud. once a user within the cluster is revoked, we tend to enable the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures. Experimental results show that the cloud will improve the potency of user revocation, and existing users within the cluster will save a major quantity of computation and communication resources throughout user revocation.

In the future enhancement of cloud-computing scenario the users buy software from software providers and execute it at computing centres, a digital rights management (DRM) system has to be in place to check the software licenses during each software execution. However, the exposure of users to privacy invasion in the presence of DRM systems is problematic. We come up with a concept that unites software providers' and users' demands for a secure and privacy-preserving DRM system for cloud computing. The employment of proxy re-encryption allows for a prevention of profile building (under pseudonym) of users by any party.

IV. LITERATURE SURVEY

[1] C.wang Et AL in his paper he explains about the data blocks and the file encryption happening in the system. One of the important concerns that need to be addressed is to assure the customer of the integrity i.e. correctness of his data in the cloud.

[2] B.Wang Et AL he explained the Outsourcing of computation and storage resources to general IT providers (cloud computing) has become very appealing. They also bear new risks and raise challenges with respect to security and privacy aspects.

[3] G.Ateniese Et AL he proposed a portable personal electronic health record architecture which natively supports a greater level of privacy using an extended digital certificate-based approach.

[4] K.ren Et ALUsed the Continuity of Care Record standard (CCR), a personal health record created through the PcHR system was successfully shared across the IHE demonstration regional health information network (RHIN) and the patient's health information viewed in several commercial clinical information systems. Similarly, provider records were viewed from within the patient's record.

[5] Q.Wang Et AL in his paper tells that companies which so far have refrained from Cloud Computing because of Compliance concerns can use the new analysis approach to check for rule adherence, and Cloud providers can demonstrate compliance through certificates.

V. REFERENCES

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," in the Proceedings of ACM/IEEE IWQoS 2009, 2009, pp. 1–9.

[7] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," in the Proceedings of IEEE INFOCOM 2013, 2013, pp. 2904–2912.

[8] 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.

[9] K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," in the Proceedings of ESORICS 2009. Springer-Verlag, 2009, pp. 355–370.

[10] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in the Proceedings of IEEE INFOCOM 2010, 2010, pp. 525–533.