International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 4 Issue: 3 16-Apr-2015,ISSN_NO: 2321-3337

# Cloud Aid Public Information With Digital Mark Client Revocation

S.P.Subha, D.Naveen raju
Student, Dept. of. Information Technology, Veltech University, India1.
Assistant Professor, Dept. of. Information Technology, Veltech University, India2.

**ABSTRACT--** *The Storage and sharing of data in cloud can be easily modified by users.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 a user gets revoked from accessing the cloud the existing user of that cloud must re-sign the data signed by the revoked user. To re-sign the data the user must download the entire data and sign it. This difficulty is rectified with the a novel public auditing mechanism idea of proxy re-signatures. In addition to this, security of the data is also enhanced with the help of a public verifier who is always able to audit the integrity of shared data without retrieving the entire data from the cloud*.

## 1 .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, and 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. 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 a integer is hard.

## 2. OBJECTIVE

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.

## 3. SYSTEM ANALYSIS

### 3.1 EXISTING SYSTEM

The shared data integrity in a cloud can be verified publicly when the users in the group compute signatures on all the blocks in shared data. When a user gets revoked form accessing the cloud the resigning of previously signed data in such case the existing system uses the straight forward method.This straight forward method reduces the efficiency, since the entire set of data has to be downloaded and it has to be resigned.To protect the integrity of data in the cloud, a Third party auditor (TPA) was used, who is able to provide verification services.

**demerits of existing algorithm:**

Re-sign of blocks by existing users during user revocation makes the users to download the entire block of data of revoked user and re-sign it.The technique using unique re-signing key to pair of users. This increases the complexity of key management and decreases the efficiency of user revocation.

### 3.2 PROPOSED APPROACH:

The drawback of re-signing gets rectified by utilizing the idea of proxy re-signatures.In the proposed system a novel public auditing mechanism is implied for the integrity of shared data with efficient user revocation in cloud(PANDA).PANDA enables the cloud to re-sign the blocks, which were signed by the revoked user with a re-signing key, this reduces the burden of the existing userTo provide additional integrity to the data in cloud the blocks of data are signed by user who created it. Once the block of data gets modified by a user, he/she must provide the private key in the block by overwriting the previous signature.

**Merits of proposed system:**

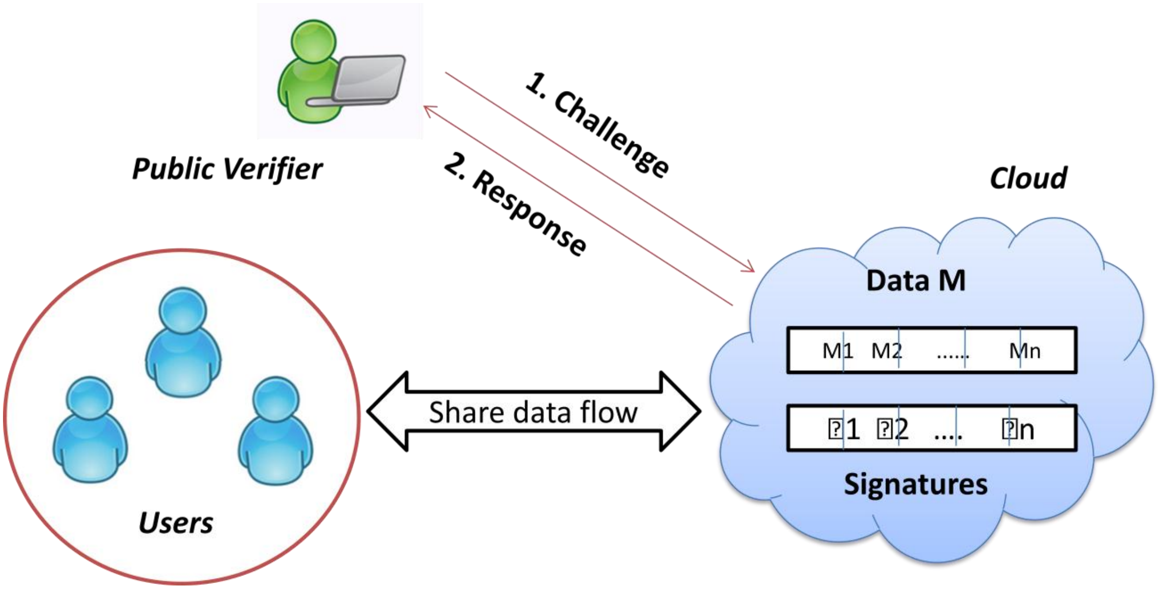
The major advantage of this system is that, the novel public auditing mechanism (PANDA ) dramaticatically increases the efficiency of the system by simplifying the time consuming task of re-signing the block of data, this is made possible using the proxy resigning technique..Semantic intelligent multi-attribute system used to make system as more secure .Used to update and store documents efficiently.

## 4. ALGORITHM AND DESIGN:

### 4.1 RSA-based Proxy Signature:

An original signer, who delegates her signing capability to a proxy signer. A proxy signer, who signs the message behalf of original signer. A verifier who verifies the proxy signature and decides to accept or reject. A trusted Party, who certifies the public key.

### 4.2 architectural and functionality architecture diagram:



## 5. IMPLEMENTATION:

### 5.1 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.

### 5.2 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.

### 5.3. Proxy re-signatures module:

This proxy resignature 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.

### 5.4. 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 algorithm(KeyGen, ReKey, Sign, Resign and Verify) to enhance the block less data verification on shared data

### 5.5 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.

### 5.6 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.

### 5.7. 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.

## 6. CONCLUSION

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.

## 7. FUTURE ENHANCEMENT:

In the future enhancement of cloud-computing scenario the users buy software from software providers and execute it at computing centers, 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

## REFERENCES

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

[2]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apirl 2010.

[3]. 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.

[4]. H. Shacham and B. Waters, "Compact Proofs of Retrievability," in the Proceedings of ASIACRYPT 2008. Springer-Verlag,2008,pp. 90–107.

[5]. 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.

[6]. Q. Wang, C. Wang, J. Li, 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.

[7]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,