Global Journal of Engineering Science and Research Management

SECURITY ANALYSIS OF DATA DISTRIBUTION FOR MULTIOWNER IN CLOUD COMPUTING USING EFFICIENT STORAGE TECHNIQUES

C.Geetha[*1] P.Prasenna[2] P.RoobanJeyanth[3] R.Hariharan[4]
[1*] PG student ,M.Tech[I.T].,Department of Information Technology,Vel Tech University ,Chennai ,India.
[2]Assistant Professor, Department of Information Technology, Vel Tech University, Chennai, India.
[3]PG student, M.Tech [I.T]. Department of Information Technology, Vel Tech University, Chennai, India.
[4]Assistant Professor, Department of Information Technology, Vel Tech University, Chennai, India.
*Correspondence Author: **C.Geetha**

Keywords: Third Party Auditor, Multi Owner data sharing Scheme, Digital forensics, Offensive Decoy Technology and Digital Signature method.

Abstract
Cloud computing has an added advantages when compared to Cluster and Grid Computing then provides an economical and efficient solution for sharing group resource among cloud users. Due to the burden of local data storage and maintenance, user depend the Third-party auditor (TPA) to check the integrity of outsourced data and be worry free. Nowadays trusting the TPA for sharing the outsourced data in a cloud storage is still a challenging issue because TPA also can theft the outsourced data while sharing the data in multiple user so security issues arises rapidly. To overcome the cloud security issues, in this project propose a three efficient storage techniques or schemes (i) multi owner data sharing scheme (MOS) for creating dynamic groups in the cloud (ii) Digital signature method for file processing and (iii) Applying the Digital Forensics method, it monitoring the user behavior and providing decoy files using Offensive Decoy Technology. These three proposed schemes will provide the solution for highly securable and efficient.

Introduction
CLOUD service providers offer users efficient and scalable data storage services with a much lower marginal cost than conventional methodologies. It is normal for clients to influence cloud storage services to share data with others in a gathering, as information offering turns into a standard peculiarity in most cloud capacity offerings, including Dropbox, I Cloud and Google Drive.

The integrity of data in distributed storage, then again, is liable to suspicion and investigation, as data stored in the cloud can easily be lost or corrupted due to the inevitable hardware/software failures and human mistakes. To aggravate this matter even, cloud administration providers may be hesitant to inform users about these data errors in order to maintain the reputation of their services and avoid losing benefits. Accordingly, the honesty of cloud information ought to be verified before any information use, for example, pursuit or processing over cloud data.

The traditional approach for checking data correctness is to retrieve the whole information. Unquestionably, this customary methodology is data integrity by checking the correctness of signatures (e.g., RSA) or hash values (e.g., MD5) of the whole information. Unquestionably, this customary methodology is able to successfully check the correctness of cloud information. However, the efficiency of using this traditional approach on cloud data is in doubt.

The main reason is that the size of cloud data is extensive by and large. Downloading the whole cloud information to check data integrity will cost or even waste users amounts of computation and correspondence assets, particularly when information have been undermined in the cloud. Additionally, many uses of cloud data (e.g., data mining and machine learning) do not necessarily need users to download the entire cloud data to local devices. It is on account of cloud suppliers, for example, Amazon, can offer clients processing services directly on large-scale data that already existed in the cloud.

A public verifier could be an information client (e.g., scientist) who might want to use the owner's data via the cloud or a third-party auditor (TPA) who can provide expert integrity checking services. Moving a step forward, Wang et al. composed a propelled examining system, so that amid open reviewing on cloud information, the substance of private information fitting in with a personal user is not disclosed to any open verifiers.

Global Journal of Engineering Science and Research Management

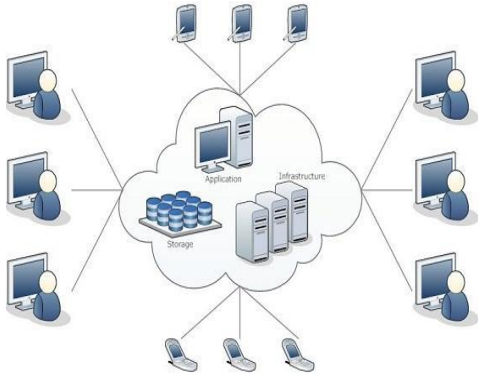

FIG 1: AN OVERVIEW OF CLOUD COMPUTING

We accept that imparting information among different users is perhaps one of the most engaging features that motivate distributed storage. Along these lines, it is additionally important to guarantee the integrity of shared data in the cloud is right. Existing open inspecting components can actually be extended to verify shared information honesty. On the other hand, another huge protection issue introduced in the case of shared data with the use of existing mechanisms is the leakage of identity privacy to open verifiers [1]. Case in point, Alice and Bob cooperate as a group and share a file in the cloud. The imparted document is separated into a number of little squares, where every square is autonomously marked by one of the two users with existing public auditing solutions. Once a block in this shared file is adjusted by a client, this client needs to sign the new piece utilizing his/her private key. In the end, diverse pieces are agreed upon by different users due to the modification introduced by these two diverse clients. At that point, so as to effectively review the honesty of the whole information, an open verifier needs to pick the proper public key for each block. As a result, this public verifier will inevitably learn the identity of the signer on each block due to the unique binding between an identity and a public key via digital certificates under public key infrastructure (PKI).

Failing to preserve identity privacy on shared data during public auditing will reveal significant confidential information (e.g., which particular user in the group or special block in shared data is a more valuable target) to public verifiers. After performing several auditing tasks, this open verifier can first learn that Alice may be a more important role in the group because most of the blocks in the shared file are always signed by Alice; on the other hand, this open verifier can likewise effortlessly find that the eighth block may contain data of a higher value (e.g., a final bid in a bartering), on the grounds that this square is much of the time changed by the two different users.

In order to protect these classified data, it is key and basic to safeguard identity privacy from public verifiers during open evaluating. In this paper, to fathom the above protection issue on shared data, we propose Privacy Preserving, a novel privacy-preserving public reviewing system. All the more particularly, we use ring marks to construct homomorphic authenticators in Privacy Preserving, so that a public verifier is able to verify the integrity of shared data without retrieving the entire data—while the identity of the signer on each block in shared data is kept private from the open verifier.

Likewise, we further amplify our system to support cluster inspecting, which can perform numerous evaluating undertakings simultaneously and improve the efficiency of verification for multiple auditing tasks. Meanwhile, Privacy Preserving is compatible with arbitrary veiling, which has been used in WWRL and can preserve data privacy from open verifiers. Additionally, we likewise influence file hash tables from a previous public auditing solution to support dynamic

Related work

One of the most fundamental services offered by cloud providers is information stockpiling. Give us a chance to consider a pragmatic information application A company allows its staffs in the same group or department to store and share files in the cloud. By using the cloud, the staffs can be completely released from the troublesome local data storage what's more, upkeep. Be that as it may, it likewise represents a noteworthy danger to the confidentiality of those stored files.

Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and private, for example, strategies for success. To protect information privacy, a basic solution is to scramble information records, and afterward transfer the encoded information into the cloud. Tragically, outlining a proficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following testing issues. At first, character security is a champion amongst the most significant obstacles for the wide deployment of distributed computing. Without the insurance of personality

Global Journal of Engineering Science and Research Management

security users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers.

Second, it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is characterized as the numerous holder way Compared with the single-manager way, where just the gathering director can store and modify data in the cloud, the various holder way is more adaptable in practical applications. All the more solidly, every client in the gathering is able to not just read information, additionally alter his/her a player in information in the entire data file shared by the organization. To wrap things up, gatherings are regularly dynamic practically speaking, e.g., new staff interest and current employee revocation in an organization. The progressions of participation make secure information sharing extremely difficult.

Security is one of the most significant obstacles for the wide deployment of cloud computing. In this project different kinds of security problem arises, still it is a challenging issue

- Due to the burden of local data storage and maintenance users depend the third-party auditor (TPA) to check the integrity of outsourced data and be worry free, nowadays TPA can also theft the outsourced data in a untrusted cloud.
- Cloud users distribute their cloud space to below user without any guarantee in a trusted manner. Let us consider a practical information application. An organization permits its staffs in the same group to store and share files in the cloud. By using the cloud, the staffs can be completely released from the troublesome local data storage and maintenance.

DISADVANTAGES

- Data theft attacks are possible
- Sharing their cloud space to other, misuse problem occur
- Security issues arises a major problem here

Digital monogram schemes

In discussed approach, a secure multi-owner data sharing scheme for dynamic groups in the cloud. By using the cloud, the staffs can be:

- We propose a secure multi-owner data imparting plan. It suggests that any client in the gathering can securely share data with others by the untrusted cloud.
- Our proposed scheme is able to support dynamic gatherings effectively. In particular, new allowed clients can specifically decrypt data files uploaded before their participation without contacting with information managers. Client disavowal can be effortlessly accomplished through a novel revocation list without updating the secret keys of the with information holders. Client disavowal can be effortlessly attained to through be constant and independent with the number of revoked users.
- We provide secure and privacy-preserving access control to clients, which ensures any part in a gathering to anonymously utilize the cloud asset. Additionally, the genuine personalities of information managers can be uncovered by the gathering supervisor when debate occurs.
- We provide rigorous security investigation, and perform far reaching recreations to illustrate the efficiency of our scheme in terms of storage and computation overhead.
- To overcome the existing security issues, in this project propose a three efficient storage techniques or schemes are Multi Owner scheme(MOS) for dynamic groups in cloud , digital signature for file processing and applying Forensic technique for providing decoy files using Offensive decoy technology.

Multi Owner Data Sharing scheme (MOS):

Cloud users distribute their cloud space to below user without any guarantee in a trusted manner. Let us consider a practical information application. An organization permits its staffs in the same group to store and share files in the cloud.

Global Journal of Engineering Science and Research Management

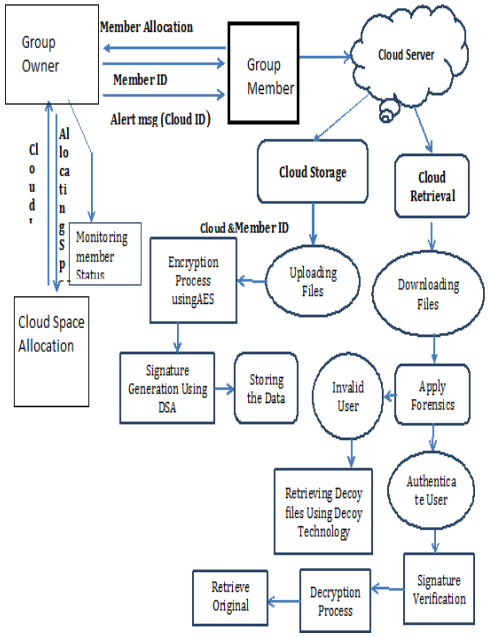

FIG 2: ARCHITECTURE DIAGRAM

By using the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. So they introduce Multi Owner Data Sharing scheme [7]. MOS means, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners and User revocation can be easily achieved whose break the terms and condition, it evade from misuse attack .

Digital Signature

Digital signatures are essential in today's modern world to verify the sender of a record's character. An advanced mark is spoken to in a computer as a string of double digits. The mark is PC utilizing a situated of rules and parameters (algorithm) such that the identity of the person signing the document as well as the originality of the data can be confirmed. The mark is produced by the utilization of a private key. A private key is known just to the customer. The mark is checked makes utilization of a public key which corresponds to (but not the same, i.e. numerically infeasible to deduct private key from public) the private key. With every user having an open/private key match, this is a case of open key cryptography Public keys, which are known by everybody, can be utilized to confirm the signature of a user. The private key, which is never imparted, is utilized as a part of mark era, which can only be done by the user.

Digital signatures are used to detect unauthorized modifications to data. Also, the recipient of a digitally signed document in proving to a third party that the document was indeed signed by the person who it is claimed to be signed by. This is known as non-repudiation, because the person who signed the document cannot repudiate the signature at a later time. Digital signature algorithms can be utilized as a part of messages, electronic trusts exchange, electronic information interchange, software distribution, information stockpiling, and pretty much any application that would need to assure the integrity and originality of data.

Element description

- **Group Owner**

Group Owner introduce the multi owner data sharing scheme .First Owner buy the Cloud Space from Cloud Server .Then they make the relation with member is said to be as multi owner scheme. After Membership, owner monitors all status for members. He has the rights to revoke the members using revocation method because of crossing the membership terms and condition.

- **Cloud Space Allocation:**

In this module, owner need to allocate their memory space(100 MB-GB) in cloud server by giving some amount to buy that particular space. Cloud server randomly generates cloud id for owner .After getting the cloud id, owner is allowed to store and retrieve their data in cloud server.

Global Journal of Engineering Science and Research Management

- **Monitoring Member Status:**

Owner monitoring the member status such as file monitoring, member details monitoring and available system monitoring.

- **Revocation method:**

Member breaks the terms and conditions, then automatically they will come to the revocation list. Owner will revoke that member because of storage overhead in membership. After Revoked member want to enter this process, again they will join the membership.

- **Group Member**

Member will join the membership by getting member id and cloud id. After Member is allowed to store and retrieve their data in cloud server.

- **Encryption & Decryption Process:**

In this process, the uploaded file and download file will be encrypting (plaintext into cipher text) and decrypting (cipher text into original text) using Blowfish algorithm

- **Signature Generation & verification**

The signature is generated by the use of a private key. A private key is known only to the user. The signature is verified makes use of a public key which corresponds to (but not the same, i.e. mathematically infeasible to deduct private key from public) the private key. With every user having a public/private key pair, this is an example of public-key cryptography. Public keys, which are known by everyone, can be used to verify the signature of a user. The private key, which is never shared, is used in signature generation, which can only be done by the user.

- Cloud Server

In cloud server, we store and retrieve our personal and business information in safe manner.

- Apply Forensic Technique

  In Cloud Server, we apply forensic technique for all users. It will monitor the user behavior and intimate to server.

- Decoy Generation

Using the forensic technique [6] we can identify the hacker and providing decoy files to them using offensive decoy technology.
Digital Monogram Schemes

- Public key signature schemes
- The private-key signs (creates) signatures
- The public-key verifies signatures

- Only the owner (of the private-key) can create the digital signature. Hence it can be used to verify who created a message
- Anyone knowing the public key can verify the signature
- If they are certain of the personality of the owner of the public key
- The key distribution problem
- Usually don't sign the whole message. Since this would double the amount of information exchanged. Rather just a hash of the message. Digital signatures can provide non-repudiation of message starting point, following an uneven calculation is utilized as a part of their creation, gave suitable timestamps and redundancies are incorporated in the signature. Having looked at hash functions, can now consider how to use them to create a digital signature, used to confirm message integrity (actually integrity of the hash - but that should be good enough). With public key signatures, can also get non-repudiation of the origin.

DSA Monogram Creation

- to **sign** a message M
  - generate random signature key k, k<q
  - compute
    - $r = (g^k (\text{mod } p))(\text{mod } q)$
    - $s = k^{-1} \cdot SHA(M) + x.r \ (\text{mod } q)$

Global Journal of Engineering Science and Research Management

- send signature (r,s) with message
- to **verify** a signature, compute:
  - $w = s^{-1}(\text{mod } q)$
  - u1= (SHA(M).w)(mod q)
  - u2= r.w(mod q)
  - v = (gu1.yu2(mod p))(mod q)
  - if v=r then the mark is confirmed.

Signature creation is again similar to Elgamal with the use per message temporary mark key k, yet doing calculation first mod p, then mod q to reduce the size of the outcome. Note that the utilization of the hash capacity SHA is unequivocal here.

DSA Monogram Verification:

Does anybody have a DSA worked example with simple values on how to calculate r ,s and verify v == r. As this standard has been around awhile and is implemented in libraries e.g. the Java Cryptography Extension I'm finding it very hard to find an example of how the algorithm works.

Compute r=(gk mod p) mod q

Compute s=(k-1 * (x * r + i)) mod q

Verifying a signature; again i is the input, and (r,s) is the signature.

u1 = (s-1 * i) mod q

u2 = (s-1 * r) mod q

v = ((gu1 * yu2) mod p) mod q

If v equals r, the signature is valid.

Advantages:

- It implies that any user in the group can securely share data with others by the untrusted cloud. It is able to support dynamic gatherings proficiently. In particular, new allowed clients can straight forwardly decrypt data files uploaded before their participation without contacting with data owners and User revocation can be easily achieved whose break the terms and condition, it evade from misuse attack .
- It avoids the data theft attack using forensic (monitoring) to provide the fake files to attackers

Conclusions

In this paper we design a secure data sharing for three efficient storage techniques/schemes such as multi owner data sharing scheme (MOS) for creating dynamic groups in the cloud, digital signature method for file processing and applying the digital forensic method using offensive decoy technology In MOS means, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners and User revocation can be easily achieved whose break the terms and condition, it evade from misuse attack .In general a group signature scheme allows any number of the group creating signature whenever sharing the file in the cloud using digital monogram algorithm. It avoids the data theft attack finally applying the forensic technique for monitoring the unauthorized user to provide fake files using decoy technology it will decreases crime activities moreover it reduces the storage overhead problem .Extensive analysis proves that our proposed design assure the desired security requirements and guarantees efficiency as well.

Future enhancement

In future, we are planning to enhance our project by uploading the file like .PDF, .Excel and multimedia file formats. We are planning to send the member id via Email and SMS while creating a user.

Global Journal of Engineering Science and Research Management

References

1. *Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member, IEEE,Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE "Privacy-Preserving Public Auditing for Secure Cloud Storage"-Feb 2013.*
2. *E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.*
3. *M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.*
4. *Salvatore J. StolfoComputer Science DepartmentColumbiaUniversityNewYork , NY, USA" Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud"-2014*
5. *S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.*
6. *Ting Sang, Shanghai Jiao Tong University, Shanghai, 200240, China. "A Log-based Approach to Make Digital Forensics Easier on Cloud Computing"- 2013 Third International Conference on Intelligent System Design and Engineering Applications*
7. *Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud"- VOL. 24, NO. 6, JUNE 2013.*