A Formation of Cloud Data Sharing With Integrity and User Revocation

Mr. Butkar Umakant .D
Miss :-Sasane Minal M
Miss :-Salpure Sonali S.
Shri Saibaba Institute of Engineering Research & Allied Sciences, Rahata

Abstract

The advent of the cloud computing makes storage out sourcing become a rising trend, that promotes the secure remote information auditing a hot topic that appeared within the analysis literature. Recently some analysis take into account the matter of secure and economical public information integrity auditing for shared dynamic information. However, these schemes area unit still not secure against the collusion of cloud storage server and revoked cluster users throughout user revocation in sensible cloud storage system. during this paper, we tend to make out the collusion attack within the exiting theme and supply associate economical public integrity auditing theme with secure cluster user revocation supported vector commitment and verifier-local revocation cluster signature. we tend to style a concrete theme supported the our theme definition. Our theme supports the general public checking and economical user revocation and conjointly some nice properties, like with confidence, efficiency, countability and traceability of secure cluster user revocation. Finally, the protection and experimental analysis show that, compared with its relevant themes our scheme is additionally secure and economical.

Keyword:- *Public integrity auditing ,dynamic data, vector commitment, group signature, cloud computing*

Introduction:- The development of cloud computing motivates enterprises and organizations to source their information to third-party cloud service suppliers (CSPs), which can improve the storage limitation of resource constrain native devices. Recently, some business cloud storage services, like the straightforward storage service (S3) on-line information backup services of Amazon and a few sensible cloud based mostly code Google Drive, Dropbox , Mozy , Bitcasa , and Memopal , are designed for cloud application. Since the cloud servers might come AN invalid end in some cases, like server hardware/software failure, human maintenance and malicious attack, new varieties of assurance integrity and accessibility area unit needed to shield the safety and privacy of cloud user's data. to beat the higher than crucial security challenge of today's cloud storage services, easy replication and protocols like Rabin's information dispersion theme area unit removed from exercise. The formers area unit pare of entities and there's no collusion among them. Also, the auditing value of the theme is linear to the cluster size. Another plan to improve the previous scheme and build the theme economical, scalable and collusion resistant is Yuan and Yu, WHO designed a dynamic public integrity auditing theme with cluster user revocation. The authors designed polynomial authentication tags and adopt proxy tag update techniques in their theme, that build their theme support public checking and economical user revocation. However, in their theme, the authors don't contemplate the information secrecy of cluster users. It implies that, their theme might expeditiously support plaintext information update and integrity auditing, whereas not cipher text information. In their theme, if the information owner trivially shares key among the group users, the defection or revocation any cluster user can force the cluster users to update their shared key. Also, the information owner doesn't participate within the user revocation section, wherever m the cloud itself might conduct the user revocation section. during this case, the collusion of revoked user and also the cloud server can offer probability to malicious cloud server wherever the cloud server might update as several time as designed and supply a legal data finally. To the most effective of our data, there's still no answer for the higher than downside publicly integrity auditing with cluster user modification. The deficiency of higher than themes motivates U.S. to explore the way to style AN economical and reliable scheme, whereas achieving secure cluster user revocation. To the end, we have a tendency to propose a construction that not solely supports cluster encryption and decoding throughout the information modification process, however additionally realizes economical and secure user revocation. Our plan is to use vector commitment theme over the info. Then we have a tendency to leverage the uneven cluster Key Agreement (AGKA) and cluster signatures to support cipher text information base update among cluster users and economical cluster user revocation severally. Specifically, the cluster user use the AGKA protocol to encrypt/decrypt the share info, able to} guarantee that a user within the cluster are going to be able to encrypt/decrypt a message from the other cluster users. The cluster signature can stop the collusion of cloud and revoked cluster users, wherever the information owner can participate within the user revocation section and also the cloud couldn't revoke the information that last changed by the revoked user.

Literature Survey:-

1) Tao Jiang, Xiao Feng Chen, and Jian Feng Ma: Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation,

This paper represent secure and efficient public data integrity auditing for sharing dynamic data against the collusion attack, Provide secure group user revocation base on VC(Vector Commitment) and VLR(Verifier -local revocation)group signature. Organizations outsource own data to third party CSP(Cloud Service providers).contribution of these scheme: Propose efficient data auditing scheme by using VC and AGKA (Asymmetric group keyagreement),GS(Group signature)to support ciphertext group user revocation
and encrypt/decrypt share database. CSM (Cloud storage model) indicate three entities:
1. CSS (Cloud storage server): share privilege to access and modify number of group users.
2. GU (Group user) who are authorized to access and modify the data by the data owner.
3. TPA: any entity which able to conduct data integrity of share data storage in cloud server.

2) Madhuri R. Rokade et al, "Providing Data Utility on Cloud using Slicing approach and Dynamic Auditing Protocol using Third Party Auditor to maintain Integrity of Data" A method presents a new approach called slicing to privacy-preserving data. Slicing overcomes the limitations of generalization and bucketization and preserves better utility while protecting against privacy threats in cloud. That proposed an efficient and inherently
secure dynamic auditing protocol which audits the data present in the cloud periodically and also whenever auditor wants to check it. Also dynamic data changes are also audited. Furthermore, auditing scheme incurs less communication cost and less computation cost of the auditor by moving the computing loads of auditing from the auditor to the server, which greatly improves the auditing performance and can be applied to large-scale cloud storage systems.

3) C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing,"

Motivate the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol. Our scheme enables an external auditor to audit user's cloud data without learning the data content. This scheme is the first to support
scalable and efficient privacy preserving public storage auditing in cloud. Scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner. TPA would not
knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also reduce the user's fear of their outsourced data leakage.TPA may concurrently handle multiple audit sessions from different users for their outsourced data files; we further extend our privacy preserving public auditing protocol into a multiuser setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency.

4) J. Yuan and S. You, "Efficient public integrity checking for cloud data sharing with multi-user modification,"

The author designed dynamic public integrity auditing scheme with group user revocation. Yuan and you not consider data secrecy of group users in their scheme that means scheme efficiently support plaintext data update and integrity auditing not cipher text data. Design polynomial authentication tag and adopt proxy tag update technique. If data owner share group key with group users and defection or revocation occur any group user will force to other group user to update their shared key. Sometime data owner not take part in user revocation phase, where many time cloud server update the data and provide data legally last.

5) B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud,"

Oruta consider how to audit the integrity of shared data in cloud with static group. Group is predefined before shared data created in cloud. Membership of users is constant in the group. Original user decides who is able to share data to the cloud before outsourcing. Problem in these schemes is how to audit the integrity of shared data in cloud with dynamic group. New user added onto group but existing user can be revoked during data sharing.

6) D. Catalano and D. Fiore, "Vector commitments and their applications," in Public Key Cryptography

This paper introduce new simple and powerful commitment mechanism should not allow a sender to change mind about committed message. VC Scheme is collection of six-polynomial time Vs. allows to commit ordered sequence of q value (m1........mg) to single message Vc require position binding to satisfaction means two different value at the same position. Vs. require hiding updatable property, Use two algorithm to update the commitment and opening message. First algorithm allows committer who created commitment and want to updatechanging message. Second algorithm allows holders of an opening of message to update.

Existing System:-

Considering knowledge security, a customary approach to ensure it's to depend upon the server to implement the doorway management when verification, which means any unforeseen profit intensifying can uncover all knowledge. in a very mutual occupancy cloud computing surroundings, things prove to be way more terrible. knowledge from various customers are often expedited on separate virtual machines (VMs) but live to tell the tale a solitary physical machine. knowledge in AN objective VM may be taken by instantiating another VM co-occupant with the target one. on of documents, there square measure a progression of science plans that go equally as allowing AN outsider inspector to see the accessibility of records for the advantage of} the info supplier while not spilling something about the info, or while not talks the info provider's secrecy. Similarly, cloud shoppers presumptively will not hold the solid conviction that the cloud server is benefiting work relating to classification. A science arrangement, with incontestible security relied on number-theoretic presumptions is a lot of enticing, at no matter purpose the consumer isn't fantastically content with basic cognitive process the safety of the VM or the genuineness of the specialised workers. These shoppers square measure roused to encipher their knowledge with their own explicit keys before transferring them to the server. however there square measure many disadvantages within the existing system:-

- surprising privilege increase can expose all
- it's not economical.
- Shared knowledge won't be secure.

PROPOSED SYSTEM:-

In this paper, we tend to study the matter of constructing public authentication scrutiny for shared dynamic knowledge with cluster
user revocation. Our contributions are:
1) For cipher text info, we tend to explore on the secure and economical shared knowledge integrate auditing for multi-user operation.
2) we tend to intend AN economical knowledge auditing theme at the side of new options like traceability and countability by incorporating the vector commitment primitives, uneven cluster key agreement and cluster signature.
3) The analysis results show that our theme is secure and economical as we offer the safety and potency analysis of our theme which can end in back-up and knowledge storage in cloud.
4) The licensed duplicate sign up the hybrid cloud design is supported by many deduplication constructions and this licensed duplicate check theme relatively incurs minimum overhead than traditional operations.

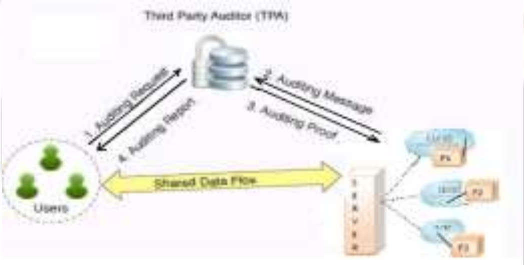

Fig: The cloud storage model

Advantages:-
1. Usability: All cloud storage services reviewed during this topic have desktop folders for Mac's and PC's. this permits users to pull and drop files between the cloud storage and their native storage.
2. Bandwidth: you'll avoid emailing files to people and instead send an online link to recipients through your email.
3. Accessibility: hold on files is accessed from anyplace via web affiliation.
4. Disaster Recovery: it's extremely suggested that companies have AN emergency backup arrange prepared within the case of AN emergency. Cloud storage is used as a back-up arrange by businesses by providing a second copy of necessary files. These files ar hold on at a foreign location and may be accessed through a web affiliation.
5. price Savings: Businesses and organizations will typically scale back annual in operation prices by exploitation cloud storage; cloud storage prices regarding three cents per G to store knowledge internally. Users will see extra price savings as a result of it doesn't need internal power to store data remotely.
Disadvantages:-
1. Usability: use caution once exploitation drag/drop to maneuver a document into the cloud storage folder. this can for good move your document from its original folder to the cloud storage location. Do a duplicate and paste rather than drag/drop if you would like to retain the document's original location additionally to moving a duplicate onto the cloud storage folder.
2. Bandwidth: many cloud storage services have a particular information measure allowance. If a corporation surpasses the given allowance, the extra charges can be important. However, some suppliers permit unlimited information measure. this is often an element that firms ought to contemplate once watching a cloud storage supplier.
3. Accessibility: If you've got no web affiliation, you've got no access to your knowledge.
4. knowledge Security: There ar issues with the protection and privacy of necessary knowledge hold on remotely. the chance of personal knowledge commingling with alternative organizations makes some businesses uneasy. If you would like to grasp a lot of regarding those problems that govern knowledge security and privacy, here is a stimulating article on the recent privacy debates.

5. Software: If you would like to be able to manipulate your files domestically through multiple devices, you'll have to be compelled to transfer the service on all devices.

Future Scope:-

In future we will keep replication of cloud data which is divide into the fragments.

Conclusion:- The primitive of verifiable information with economical updates is a crucial thanks to solve the matter of verifiable outsourcing of storage. we tend to propose a theme to understand economical and secure knowledge integrity auditing for share dynamic knowledge with multi-user modification. The theme vector commitment, uneven cluster Key Agreement (AGKA) and cluster signatures with user revocation square measure adopt to attain {the knowledge|the info|the information} integrity auditing of remote data. Beside the general public knowledge auditing, the combining of the 3 primitive alter our theme to source ciphertext information to remote cloud and support secure cluster users revocation to shared dynamic knowledge. we offer security analysis of our theme, and it shows that our theme give knowledge confidentiality for cluster users, and it's conjointly secure against the collusion attack from the cloud storage server and revoked cluster users. Also, the performance analysis shows that, compared with its relevant schemes, our theme is additionally economical in numerous phases.

References:-

1. Q.Wang, C.Wang, J. Li, K. Ren, and W. Lou. Enabling public verifiability and data dynamics for storage security in cloud computing. IEEE Transactions on Parallel and Distributed Systems, 22,847(2011)

2. Yan Zhu, Hongxin Hu,Gail-Joon Ahn and Mengyang Yu. Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage. IEEE Transactions on Parallel and Distributed Systems, 23, 12(2012)

3. Cong Wang, Sherman S.M. Chow, Qian Wang, KuiRen, and Wenjing Lou, Privacy-Preserving Public Auditing for Secure Cloud Storage, IEEE Transactions on Computers (TC), 10, 451(2012)

4. Kan Yang, Xiaohua Jia. Data storage auditing service in cloud computing: challenges, methods and opportunities. The journal of World Wide Web. 15, 409(2012)

5. Huaqun Wang. Proxy Provable Data Possession in Public Clouds. IEEE Transactions on Services Computing, P, P(2012)

6. G Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. Provable data possession at untrusted stores. In CCS '07, (2007) October598-609;Alexandria, VA, USA

7. R.Johnson, D.Molnar, D.song, and D.wagner. Homomorphic signature schemes. In Proc. of CT-RSA, (2002) Feb 244-262; San Jose,CA, USA

8. A.Juels and B. Kaliski. PORs: Proofs of retrievability for large files. In CCS '07, (2007) October584-597; Alexandria, VA, USA Shacham and B. Waters. Compact proofs of retrievability.In ASIACRYPT '2008, (2008) December 90-107;Melbourne, Australia

9. K. D. Bowers, A. Juels, A. Oprea, Proofs of Retrievability: Theory and Implementation, Proc. 2009 ACM Cloud Computing Security Workshop, (2009) November 43-54;Chicago, IL, USA

10. Y. Dodis, S. Vadhan, and D. Wichs.Proofs of retrievability via hardness application. In TCC'09, (2009)