Dynamic Operation Implementation in storage of Cloud Computing

K.Hajarathaiah[#1], T. Seshu Chakravarthy[#2], G. Raphi[#3]

[#1] Assistant professor, Department of CSE, Narasaraopet Engineering College, Narasaraopet.

[#2]Assistant professor, Department of CSE, Narasaraopet Engineering College, Narasaraopet, seshuchakravarthy.thota@gmail.com.

[#3]Assistant professor, Department of CSE, Narasaraopet Engineering College, Narasaraopet, rafi1222@gmail.com.

Abstract: **Cloud data storage data maintains as security storage data. Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Although there are benefits, which inevitably poses new security risks toward the correctness of the data in cloud. Existing system controls the internal and external threats. New problems with existing system are generated in transmission time and also data loss accidents are generated here which leads to more incentives utilization. It can contains some disadvantages, for overcome those problems introduces the TPA (third party auditor) concept. In this paper, cooperative data centers or distributed data centers mechanism is used to over the problem of existing system. Here errors are blocked where it is occurred. Using dynamic operations implementation select another servers recover the error block of content. This is called as a distributed data collection cloud environment. It can give the clear data distribution content.**

Keyword: **Assurances, distributed clouds, cryptographic techniques, data dynamics, cloud computing.**

I. INTRODUCTION

Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology Cloud computing has a future information technology architecture for enterprises, ubiquitous network access, on-demand self-service, location independent resource pooling, usage-based pricing, rapid resource elasticity and transference of risk. Cloud Computing is transforming the very nature of how businesses use information technology as a disruptive technology with profound implications. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced to the Cloud.

Storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: universal data access with independent geographical locations, relief of the burden for storage management, and avoidance of capital expenditure on hardware, software, and personnel maintenances. The sharing of resources reduces the cost to individuals. Best definition for Cloud is defined as large pool of easily accessible and virtualized resources which can be dynamically reconfigured to adjust a variable load, allowing also for optimum scale utilization. The key driving forces behind cloud computing is the omnipresence of broadband and wireless networking, progressive improvements and falling storage costs in Internet computing software.

Since cloud service providers (CSP) are separate administrative entities and data outsourcing is actually relinquishing user's ultimate control over the fate of their data. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers. Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. The

internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift. From the perspective of data security that has always been an important aspect of quality of service and Cloud Computing inevitably poses new challenging security threats for number of reasons.

It is possible for CSP to discard rarely accessed data without being detected in a timely fashion. Although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it's lacking of offering strong assurance of data integrity and availability may impede its wide adoption by both enterprise and individual cloud users. The verification of cloud storage correctness must be conducted without explicit knowledge of the whole data files. The data stored in the cloud may not only be accessed but also be frequently updated by the users including insertion, modification, deletion and appending etc. It is also imperative to support the integration of this dynamic feature into the cloud storage correctness assurance that makes the system design even more challenging. It is more advantages for individual users to store their data redundantly across multiple physical servers so as to reduce the data integrity and availability threats. Last but not the least, the deployment of Cloud Computing is powered by data centers running in a simultaneous, cooperated and distributed manner.

II RELATED WORK

The survey of major cloud service providers to investigate the security mechanisms to overcome the security. We have considered 10 major cloud service providers, which provide their services in all major areas of cloud computing, including SaaS, PaaS and IaaS. The survey needs to be more exhaustive in order to analyze the complete state of art of security in cloud computing. Due to the fact that the scope of our work is not just to explore the state of art but to look at the major factors that affect security in cloud computing.

Security Issues on Cloud Computing Password Recovery 90% are using standard methods like other common services while 10% are using sophisticated techniques. The encryption 40% are using standard SSL encryption while 20% are using encryption mechanism but at an extra cost 40% are using advance methods like HTTPS access Data Location 70% have their data centers located in more than one country while 10% are located at a single location 20% are not open about this issue. The cloud computing is a model for information and services, which uses the internet infrastructure to allow communication between client side and server side applications. When making decisions to adopt cloud services privacy or security has always been a major deal with these issues the cloud provider must build up sufficient controls to provide such level of security than the organization would have if the cloud were not used.

Major security challenge is that the owner of the data has no control on their data processing. Inclusion of the technologies like operating systems, databases, scheduling of resources, memory management, network, concurrency control etc arises the many security issues in the cloud computing. Top seven security threats to cloud computing discovered by "Cloud Security Alliance" (CSA) are

a. Abuse and Nefarious Use of Cloud Computing
b. Insecure Application Programming Interfaces
c. Malicious Insiders
d. Shared Technology Vulnerabilities
e. Data Loss/Leakage
f. Account, Service & Traffic Hijacking
g. Unknown Risk Profile

To ensure the remote integrity we have describe the proof of retrievability. Their scheme combines spot-checking and error correcting code to ensure both possession and retrievability of files on archive service systems.

Schwarz *et al.* [2] proposed to ensure static file integrity across multiple distributed servers, using erasure-coding and block level file integrity checks. From there distributed storage verification protocol we have adopted some ideas. Our schemes further support data dynamics and explicitly study the problem of misbehaving server identification that their did not.

K. Ren, C. Wang, and Q. Wang [3,4],Although virtualization and cloud computing can help companies accomplish more by breaking the physical bonds between an IT infrastructure and its users, heightened security threats must be overcome in order to benefit fully from this new computing paradigm. This is particularly true for the SaaS provider.

In Shacham[5] built on this model and constructed a random linear function based homomorphism authenticator which enables unlimited number of challenges and requires less communication overhead due to its usage of relatively small size of BLS signature.

Bowers et al. [6] proposed an improved framework for POR protocols that generalizes both Juels and Shacham's work. Later in their subsequent work, Bowers et al. [7] extended POR model to distributed systems. However, all these schemes are focusing on static data. The effectiveness of their schemes rests primarily on the preprocessing steps that the user conducts before outsourcing the data file F. Any change to the contents of F, even few bits, must propagate through the error-correcting code and the corresponding random shuffling process, thus introducing significant computation and communication complexity.

Recently, Dodis et al. [8] gave theoretical studies on generalized framework for different variants of existing POR work. Ateniese et al. [9] defined the "provable data possession" (PDP) model for ensuring possession of file on untrusted storages. Their scheme utilized public key based homomorphism tags for auditing the data file. However, the pre-computation of the tags imposes heavy computation overhead that can be expensive for an entire file. In their subsequent work, Ateniese et al. [10] described a PDP scheme that uses only symmetric key based cryptography. This method has lower –overhead than their previous scheme and allows for block updates, deletions and appends to the stored file.

III EXISTING SYSTEM

Previously many solutions are present for providing the cloud data security here. Those techniques are handling the internal and external threats here. It can spend more amount of energy levels utilization. Using some reputation techniques provides assurances as a security resource here. It is not provides the good security. After some days introduces the cryptographic concepts. It is not gives the good performance levels. Next some people are uses auditing systems. All previous are not gives the good solutions and correctness results also here. It is distributed data to any users with the help of static servers only. Data distribution is not effective using single server utilization. Single server is not transmitting guaranteed data delivery. Incase server is fail there is no possibility for collecting the data from another server. In cloud data storage, a user stores his data through a CSP into a set of cloud servers cooperated and distributed manner. The data redundancy can be employed with technique of erasure correcting code to further tolerate faults or server crash as user's data grows in size and importance. User an entity whose data to be stores and relies on the cloud for storage, server is an entity which manages by cloud service provider to provide data storage service has significant storage space and computing resources and third party is an optional Third Party Auditor who has expertise and capabilities that users may not have is trusted to assess and expose risk of cloud storage services on behalf of the users upon request. There are some lists of disadvantages in the existing system. They are Data errors in user's side, Storage errors, Error recovery techniques are not available here, Misbehavior server's detection is not available here, Deliver the unclear data.

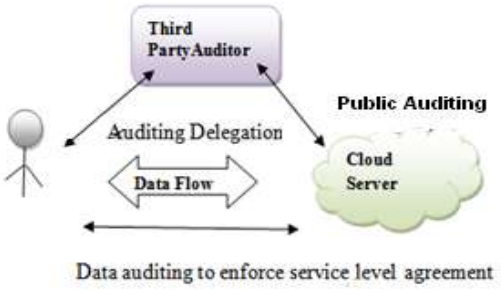

Fig 1.Data Auditing Diagram

IV PROPOSED SYSTEM

Newly we are proposing here multi servers data distribution with distributed protocols implementation. Any server is fail using cross server

storage collect the data and provides quality data distribution to users or customers. This is called as a data dynamic support procedure. It can remove the redundant problems and increases the quality data distribution. In any server failure data identifies and recover from replication server. Server show any problems under distribution of data, this failure data recover from another server. This is called as a verification and correctness data.

Cloud data storage a user stores his data through a CSP into set of cloud servers which are running in a simultaneous cooperated and distributed. For application purposes user interacts with the cloud servers via CSP to extract his data. It is of critical importance to ensure users that their data are being correctly stored and maintained as users no longer possess their data locally. Users should be equipped with security means so that they can make continuous correctness assurance of their stored data even without the existence of local copies. To securely introduce TPA any possible leakage of user's outsourced data towards TPA through the auditing protocol should be prohibited.

Security Issues:

Cloud service providers operate complex systems; have sophisticated processes and expert personnel for maintaining their systems which small enterprises may not have access. Data Centralization in a cloud environment the service provider takes care of storage issues and small business need not spend a lot of money on physical storage devices also cloud based storage providers a way to centralize the data faster and potentially cheaper.

Incident Response like IaaS providers can put up a dedicated forensic server that can be used on demand basis. Forensic image verification time in some cloud storage implementations expose a cryptographic check sum or hash Logging in a traditional computing paradigm by and large logging is often an afterthought.

Aware security threads:

Abuse use of cloud computing is the top threat identified by the CSA. It was introduced by Cloud Security Alliance. Attackers can infiltrate a public cloud and find a way to upload malware to thousands of computers and use the power of the cloud infrastructure to attack other machines. Suggested remedies by the CSA:

a. Stricter initial registration and validation Processes
b. Enhanced credit card fraud monitoring and coordination
c. Comprehensive introspection of customer network traffic
d. Monitoring public blacklists for one's own network blocks

Insecurity in Programming Interface:

As software interfaces or APIs are what customers use to interact with cloud services. Those must have extremely access control, activity monitoring mechanisms, secure authentication and encryption especially when third parties start to build on them.

We put more focus on the support of file-oriented cloud applications other than non-file application data like social networking data. The cloud data we are considering is not expected to be rapidly changing in a relative short period. Users should be equipped with security means so that they can make continuous correctness assurance of their stored data even without the existence of local copies. Users can delegate the data auditing tasks to an optional trusted TPA of their respective choices in case of the users do not necessarily have the time, resources or feasibility to monitor their data online.

We assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable that can be achieved in practice with little overhead.

Design Goals:

We aim to design efficient mechanisms for dynamic data verification and operation to ensure the security and dependability for cloud data storage under the aforementioned adversary model. The following want to achieve by our design:

- Storage correctness
  To ensure users that their data are indeed stored appropriately and kept intact all the time in the cloud
- Fast localization of data error

To effectively locate the malfunctioning server when data corruption has been detected

- Dynamic data support
  To maintain the same level of storage correctness assurance even if users modify, delete or append their data files in the cloud
- Dependability
  To enhance data availability against Byzantine failures, malicious data modification and server colluding attacks
- Lightweight
  To enable users to perform storage correctness checks with minimum overhead

V SECURITY ARCHITECTURE

The aspects went on describing the problems and threats in related to security in cloud. The issues like security for data, virtualization security and prescribed format of SLA etc. There are many research people have keen interest in designing certain security architectures help for secure cloud computing. Gary Anthes [14-3] has described the various security research works in cloud. He brought forward the research works done in popular companies like HP, Microsoft and IBM. **T**here are many security risks involved in cloud computing and also some good solutions are also been designed by the researchers. The researchers pointed the following risk:

1. Researchers at HP laboratories are prototyping cells as a service to automate security management in cloud
2. IBM research people doing virtual machine introspection which puts security inside protected VM running on same machine
3. Microsoft research described about cryptographic cloud storage where the data is secured by user by encrypting format such that the provider cannot get what the data is present

In a general system at base OS level, there is a problem like a user at one guest OS may interact with other Guest OS. This will maintain security by preventing unnecessary logins into the other guest OS by weak passwords or weak SSH. We have proposed approach which checks whether their data has been attacked or any integrity loss is done or not over the cloud. These works help in securing the cloud systems, Virtualization, Data confidentiality and data storage security, there are still issues need to be discussed in secure data transmission between cloud Provider, service provider and cloud User. The secure data transmission works designed for storage networks for secure data transmission over IP Networks by developing Middleware works below application layer and selects suitable security approach based on the cluster of data items available in Application. That will help in securing the data as well as this works well than IPSec.

VI COMPARATIVE STUDY

Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute poses many new security challenges which have not been well understood. Here, no user data privacy Security risks towards the correctness of the data in cloud compare to existing environment on cloud data storage security. We propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors, to ensure the correctness of users' data in the cloud.

Our scheme achieves the integration of storage correctness insurance and data error localization by utilizing the homomorphic token with distributed verification of erasure-coded data. The new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append and an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. The data stored in the cloud may be frequently updated by the users including deletion, insertion, appending and modification etc. To ensure storage correctness under dynamic data update is hence of paramount importance.

Analysis Work System Model

User: user has data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.

Cloud Service Provider has significant resources and expertise in building and managing distributed cloud storage servers.
Third Party Auditor (TPA) has expertise and capabilities that users may not have.

- ***File Retrieval and Error Recovery***

  Assuming that they return the correct response values when the user can reconstruct the original file by downloading the data vectors from the first m servers. We can guarantee the successful file retrieval with high probability.

- ***Third Party Auditing***

  User does not have the time, feasibility or resources to perform the storage correctness verification, at that instance user can optionally delegate this task to an independent third party auditor, making the cloud storage publicly verifiable. The auditing process should bring in no new vulnerabilities towards user data privacy as pointed out by the recent work, to securely introduce an effective TPA.

- ***Cloud Operations***

  1. ***Update Operation***

     We refer this operation as data update sometimes the user may need to modify some data block(s) stored in the cloud

  2. ***Delete Operation***

     Certain data blocks may need to be deleted after being stored in the cloud**.** The delete operation we are considering is a general one, in which user replaces the data block with zero or some special reserved data symbol.

  3. ***Append Operation***

     The user may want to increase the size of his stored data by adding blocks at the end of the data file in some cases which we refer as data append. We anticipate that the most frequent append operation in cloud data storage is bulk append.

VII CONCLUSION

We investigate the problem of data security in cloud data storage, which is essentially a distributed storage system. We propose an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append to achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users. A general cloud computing architecture uses the find the secure data storage analyze for the objects in different data for security issues Cloud data storage a user stores his data through a CSP into set of cloud servers which are running in a simultaneous cooperated and distributed. The data redundancy can be employed with technique of erasure correcting code to further tolerate faults or server crash as users data grows in size. Our future direction is to implement a novel explanation mechanism for the problem of having high false intruders can also be resolved by one such approach that uses a high rate of accuracy in the case of any business method with human- understandable can also improve the efficiency for secure storage analyzing the complex dataset.

VIII REFERENCE

[1] Cong Wang, Qian Wang, Kui Ren, Ning Cao, Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," in Proc. IEEE Transactions on Cloud Computing, april-june 2012, pp.1-14.

[2] T. Schwarz and E. L. Miller, "Store, forget, and check: Using algebraic signatures to check remotely administered storage," in Proc. of ICDCS'06, 2006, pp. 12–12.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in Proc. of IWQoS'09, July 2009, pp. 1–9.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in *Proc. of IWQoS'09*, July 2009, pp. 1–9.

[5] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of Asiacrypt'08, volume 5350 of LNCS, 2008, pp. 90-107.

[6] K.D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation,"Proc.

ACM Workshop Cloud Computing Security (CCSW '09), pp. 43-54, 2009.
[7] K.D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage,"Proc. ACM Conf. Computer and Comm. Security (CCS '09),pp. 187-198, 2009.
[8] Y. Dodis, S. Vadhan, and D. Wichs, "Proofs of Retrievability via Hardness Amplification,"Proc. Sixth Theory of Cryptography Conf. (TCC '09), Mar. 2009.
[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores,"Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, Oct. 2007.
[10] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession,"Proc. Fourth Int'l Conf. Security and Privacy in Comm. Netowrks (SecureComm '08),pp. 1-10, 2008.

