EasyChair Preprint

№ 3606

Privacy Preserving Of Cloud Storage Security

Adarsh Pandey and A. Daniel

June 14, 2020

Privacy-Preserving of Cloud Storage Security

Adarsh Kumar Pandey [a], Dr.A.Daniel[b]
[a] *Department of Computer Science & Engineering, Galgotias University, Greater Noida, Uttar Pradesh 201310*
[b]*Assistant Professor, Galgotias University.*

Abstract- The Terminology Cloud Computing has been speculated as to the subsequent descent of Information technology architecture. In disparity to traditional infrastructure and solution, where the information technology services are relying on physical, logical and self-controls, Cloud Computing tends towards the System software and databases to the large data hub and data centers, at where the controlling and management of data and their services may not be completely steadfast. These prime and unique features, however, create many security challenges that are not completely well interpretable and well understandable. In this research paper, we mainly deal with Cloud Data Storage Security, which always be the most precious factor for the quality of service. The cloud computing innovations take a lead towards the clients data for an assurance for security of the clients' data in the cloud storage or cloud servers which consist with the huge amount of distinct data, we proposed a most effective model, flexible, trustworthy and reliable compact distributed design and sample cases of cloud era with two main protruding features and solutions of storage security which mainly conflicting to its cloud architecture and there services provided by the CSP. By make a use of the identical tokens with the unique distributed authentication and verification of deleted coded data, our design achieves the unification of storage fineness assurance and data flaw localization, it means the identification of maltreating servers. Assam of the previous work done, the new design further helps to secure potential astir operations on the data sets or blocks, consisting with the data updation, deletions and connectivity. The vast security and performance abstraction show that the promises design is highly adaptable and resilient in terms of any failure, malicious data changes, any malware attack on data set or block, and most for the server machinate attacks.

Keywords- Cloud Computing, Storage Security, Machinate Attacks, Malware, CSP.

I. Introduction:

The Cloud Computing Technology, which is the most vast and graceful technology for every IT and Internet-based service provider and as they make a use of modern computer technology in terms of the cloud sources are completely magnificent .The constantly being inexpensive and more impressive processors, together with SaaS (Software as a Service) Computing architecture, that are transforming the whole data hubs and data centers into pools of computing resources and computing services on a spacious scale. The raise of network bandwidth and reliable, resilient network connections make this presumable that the users or clients can sign high quality services from data and application software that transmigrated merely on remote data centers.

Astir data into cloud source offers major facility to clients since they didn't concern about the involution of direct hardware management. The precursor of Cloud Computing vendors, Amazon S3 (Amazon Simple Storage Service) and Amazon EC2 (Amazon Elastic Cloud Compute) are the well-known best examples. In cloud computing the mainframe of internet-based online cloud services gives us a spacious amount cloud storage area and uniquely optimizable cloud computing

resources and there utility , the cloud computing technology provides a podium type of shift, however, cloud computing technology repelling and modifying the amenability and also the usage of local machines at server side and client side both, for data conservation at the same point of time. the valuable results of the cloud sources for clients are at the edge of the tenderness of the resources and CSP (Cloud Service Providers) for the utility, availability and integrity of their chained data and bit about the metadata. Recently downtime of Amazon Simple Storage Service (S3) is such a great and inclusive example.

We are mostly surrounded by the data so from the perspective of data security, which always play a vital role in every aspects of services either if it is a quality, attribute or any other aspect of services, Cloud Computing Technology occasionally pretense towards the new moderating and challenging security risks for some equipoised number of reason. [1] The main reason which is consisted with the traditional cryptographic fundamentals for the main objective of data security and the flow of the data modules along with the protection, cannot be primarily adopted due to the reason associated with clients, which loss there control of data under cloud computing. Hence Authentication and verification of exact and reliable frame of the data storage in cloud storage space must be conducted without having any other explicit information and knowledge of the complete data module (Unit). We are considering different and various aspects of data for each and every user or clients which stored in cloud storage for the future references (Usage) and the users demand for their data security tend towards long term and a contagious convincement for the purpose of data safety and controls over it, the main problem came with the verification and Chasity of the storage and data as well with the cloud storage server(s), which became more difficult to deal with and make a proper control over this. [2] The Second reason in this contrast is that cloud computing is not mainly use as storage unit or a data warehouse, which completely deal by any other third party or any other cloud service providers. Every cloud user who stored there data in cloud so this might be a frequent chance that the data which stored in cloud storage is updated by that users and this updating can be of any type either that user wants to insert some new and convergence data over it, delete some kind of meaningless data, reordered that data sequence or appending etc. To preserve and ensure the data module and storage module fineness under astir data update by the users is a very high priority based and have a more importance. However, these high priorities feature also cover the mainframe of the storage security and always makes an unpackable integrity towards the traditional insurance techniques, sometimes which is not as much as worth it and not entails us a unique and dynamic solution for this. [3] This might be the last reason; Cloud Computing deployment is purely deal by the data centers which processing the data in a sequential format and also running in a sequential pattern and this all cooperation pull together in a cyclic distributed manner. The data of each and every user is stored in various places which is set of a multiple physical location and the user's data which stored in cloud is redundantly stored to decrease the data integrity threats. So distributed protocols for storage and storage locations Chasity convincement will be most important aspects for the storage related issue in cloud computing to achieving a robust complete package of secure cloud data storage systems in the real world for the end users. However, this kind of vast, an emerging, meaningful and important area remains to be completely explored in today IT environment and for the future references this explored in literature as well.

In this research paper, we promise the most valuable, flexible and an effective distributed design and plotting pattern of data security with explicit astir scheme for data support to preserve and make surety about the fineness of clients' data in to cloud storage. We contrast on the deleted correcting code in the system which mainly deals with the file distributed system and consolidated

scaling map of cloud storage cardinalities. The file distribution system is a distribution preparation for stored data and storage area which consisted with redundancies and dependability of data on each set with each other. This unique design and storage overhead pattern decrease the communication and consolidation of storage over heading as compared to previous pattern of file distribution techniques proposed in traditional infrastructure. By make a use of the identical tokens with the unique distributed authentication and verification of deleted coded data, our design achieves the unification of storage fineness assurance and data flaw localization: if we got any type of data corruption in between storage fineness or correctness authentication and verification process, this system design often takes almost surety about the data errors and data mapping system throughout simultaneous localization, it means the identification of maltreating servers.

This complete work should be considered first in terms of our participation and the field which we choose to demonstrate the distributed data storage and some categorize factor of data storage in cloud computing. This whole participation is brief as in the main three aspects: -

[1] If we talk about the cloud computing and its predecessors then we only deal with the binary result and unitary data storage state throughout the storage access on the distributed servers, the main and most considerable factor is about the challenge response routine and protocol in this work and then again we deal with the localization of the compressing data errors controls and their operated format through the data mapping.

[2] Assam most certainly and primary wok of this conclusive storage medium and prior work to make them assure about the remote and the data integrity which called remote data integrity is the mainframe and key components of cloud storage and for their servers to the new design pattern for supporting, securing the most valuable and efficient astir operation on the data blocks and data sets which consisting with the insertion, deletion, updating, and more or like append.

[3] In this scenario of cloud computing technology the vast extensible security and execution analysis define that and brief about the reliability of new era technique in cloud data security and proposed unique design in completely resilient and most efficient towards the any failure in storage mode and also in any irrelevant maltreating data attack or any other modification in that data related to the cloud servers. Hence this proposed model is a bit about the real tracking of data security to ensure the real time tracking of unauthorized user then helps to get rid with them.

Now let us discuss about the paper pattern in this manual format, consisting with first section in which we have already described the introductory part of this research paper, In the next sections we will cover the following like System model and trade related to that model, After that we will brief about the Adversary model, In which we will mainly focus the guided media and their affects over it, Then next will be our design and some important kind of notations which is used in this paper. Finally we let you know about the whole description in details of our newly made design and some mapping cardinalities followed by the a brief overview which deal with the related work in this particular domain and their x-factor which demonstrate our enhancement or we may say the inheritances of this paper and at the end we gives you a elaborated conclusion and some kind of the most important remarks consisting the whole paper and all subsets.

So mainly in this research paper, we promise the most valuable, flexible and an effective distributed design and plotting pattern of data security with explicit astir scheme for data support to preserve and make surety about the fineness of clients' data in to cloud storage. We contrast on the deleted correcting code in the system which mainly deals with the file distributed system and consolidated scaling map of cloud storage cardinalities.

II. Problem Statement

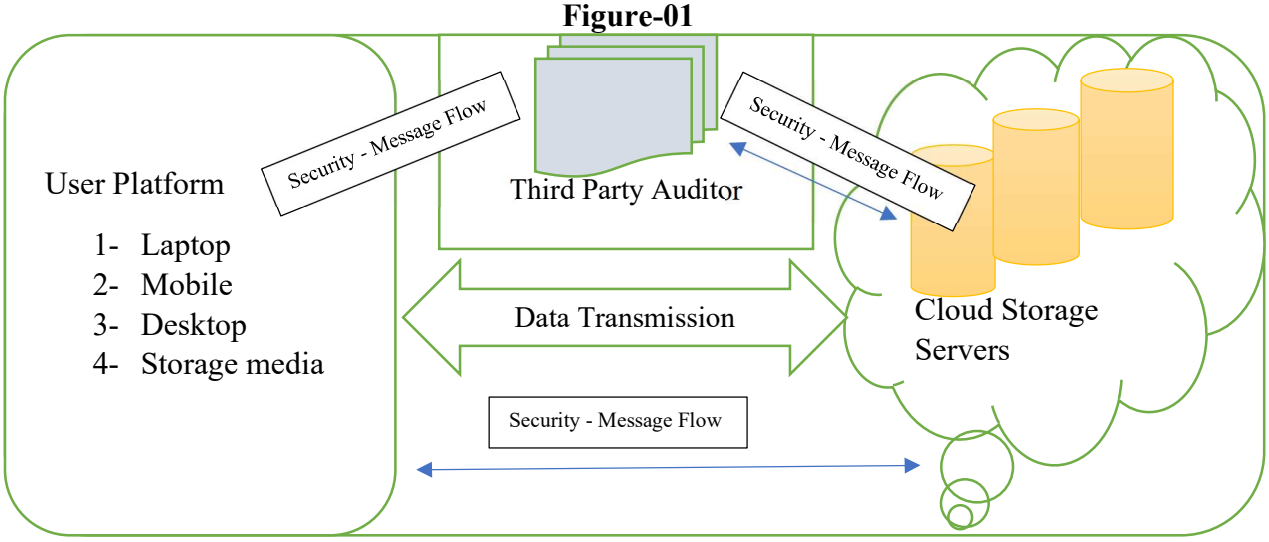
A. System Design/Model

The Architectural representation of cloud data storage network is shown in figure 1. In this figure there are mainly three separate network keynote or entities described as follow:

- Client/User: This representative is basically described in terms of a person who have their own data and wants to store that in the cloud and also he wants to completely become independent in term of computation of their data and this mainframe is always consisted with any particular individual or any consumer who is accessing it and an industry or any other organization who have their own platform.
- Vendor/CSP (Cloud Service Provider): A cloud vendor is a person who has proper idea about the all cloud services, delivery models and some kind idea about the important services and specialization in forming and managing the all cloud data storage servers which is mainly in distributed form and can owns and handle all cloud computing technological services by self and provide a reliable solution for any interruption.
- The Arbiter/TPA (Third Party Auditor): The Arbiter is a person who has a great and depth knowledge in user's related problems and also have a great specialization and professionalism, capabilities that any user doesn't have and the cloud service provider have a great trusted people like TPA, who is always trusted to get any type of access and can improve main risk mitigation of cloud data storage and easily can expose the unwanted access of any other invalid source from the storage hub on as per the demand by the clients.

In general, a client who wants to store their data in cloud storage, must have a CSP who can give an access from a set of cloud servers to the user so that by using this the user get the access of cloud server and can easily store their data. In cloud computing the whole process of any cloud services is completely running is simultaneous mode which is also have a form of distributed replica. The data redundancy in cloud storage and their integrity can be deputed with homomorphic techniques of cloud data storage which describe the penetrated and erasable data and make them in recoverable format in coded mode to get rid with the further track faults during the crashes of system, crashes of servers, or any unauthorized access over the cloud servers. Hence the client should have made a contact with cloud service provider so that by using some techniques and tools or application he gets their data back. If some server cracking issue is generating then sometimes client needs to perform a block level operation in his data to make them more secure and become resilient over any other x-servers. The main featured general operation consisting in block level operations are considered as update, insert, delete and somewhere as in form of append.

Figure-01



So above mentioned figure 1 is describing about the all three network entities containing with the user, cloud service provider and then finally with third party auditor. The work responsibilities about all three we have already discussed previously.

In Cloud Computing technology a user can never get any access of their data directly through cloud server, there is always a role of CSP and this is a small but most important factor about the users' data that is his data is completely safe and correctly stored and maintained. Because a user doesn't know about the security processes and their means, that's why they easily can make their data for storing in the cloud without keeping the replica of their data in contagious format of data set report or any other copies of it. If there is any case related to users access over the cloud servers then the TPA which is optional but more trusted, they helped them to understand proper about the time complexities, feasibility and all about the cloud resources and the processes that how they monitor their data in cloud storage medium. The TPA always stand with expertise with all cloud services and proper knowledge about the resources so that they can maintain the data and users query anytime and from anywhere. In this research paper and in our project design we considering that end to end communication which is also called point to point communication with the help of some channels among the cloud servers and the client authenticated and reliable area which is completely demonstrated under the cloud specialists where they can provide a guided media for each and every user so that they can easily communicate with us at anytime from anywhere and gives a practice with some kind of little overhead through this whole process. Remark this as an important keynote that in this paper we are not putting and demonstrating any kind of issue data privacy, we all know very well that in cloud computing the data privacy of any user is completely orthogonal and we don't address about it.

B. Adversary Design/Model:

Now in cloud computing storage technology there are mainly two sources of any threat attack on our cloud data storage. The first source is, the only cloud service provider itself in terms of if he/she become self-living or self-interesting, unworthy for their work and responsibilities, untrusted for their loyalty and position with some kind of inimical behavior. If a CSP wants to move or reallocate the data as per his/her choice so that is not a big issue to move that data as per desire and may sell the whole storage unit consisting with large amount of data for some kind of financial helps for itself or may provide a lower standard of cloud storage to store the data and save a huge amount from the infrastructure setup and maintenance. There is another possibility like a CSP wants to hide your confidential data in cloud storage and said to you that your data is lost due to some kind of maintenance errors and overloading of server's track on each other or a system failure due to any threat attack in our storage unit. So, this kind of things leads towards the security threats for our cloud data storage. The second source for security threat is, a person with a massive knowledge about the server attack process and a good capability to make a stable and unidentified settlement among the lot of cloud storage servers from various sources and encounter with the main hosted server afterward the attacker is completely able and free to do whatever he wants, either he wants to delete some data, modify the data, make a replica of the data he can do without having any valid identity. Attacker is completely hidden from the cloud service provider for a fix time duration. In this whole process of security threat, the attackers are thoroughly undetected and unauthorized for access of storage source. So, in this research paper we mainly focusing and considering only two category/types of hostile or adversary consisting with some of the standards and levels and this level is our capability and a strong source for this paper. There are following two types of it: [1] Feeble hostile/Adversary: In this kind of adversary the attacking source is mainly focused with the corrupting the client's data and stored files on each and every

Single Server Unit. If the attacking medium make a stable settlement with the host server then they can erase all the client's data over the server or make some kinds of modification in it, they can also use the fraud data to get a proper and safe data from the host server or source, there may a chance of interruption of the original data access from the storage by any user.

[2] Robust Hostile/Adversary: In security threat case this adversary is top most horrible and worst case ever and quite challenging also, in which cloud servers are purely quantized and in this case we considered that the conflicting and dissident can make a robust settlement with the internal sources of storage and he can try to make some internal changes in the data and data files with a consistent amount which is completely unchangeable from external sources and they can easily transmit the data from anywhere. In fact, there is another part of this in which all the localized servers through the host are start colluding with each other and start generating a rigid structure of data loss so that they can prevent themselves from mixing up with each other. In this case all server is start responding in a subsequent manner with same point of time so here data loss and data corruption chances are quite massive and its completely irreversible to get data back in a safe zone.

C. Model Objective:

In Cloud Computing Technology the data security is a huge goal for every cloud service provider, So, To assure about the data security and some special kind of data reliability for cloud storage from the previous discussed and mentioned design which is said an adversary design/model, in this paper we are planning to implement and design a new and specific format and mechanism for data assurance and a step forward to dynamic data authentication and verification, a malicious free operation in which we may achieve some special kind of goal with related to our paper and cloud storage related security also. The goals are as follows: [1] Storage Fineness: To assure the clients that all their data are completely kept in a most secure place and stored in very organized form so that there is no chance of a bit about data loss from anywhere, anytime in the cloud. [2] Instant localization of any type of data flaw: In this process we instantly detect the maltreating and unauthorized servers from our server side whenever any unauthorized wants to get the access and we prevent our data from corruption. [3] Astir data adherence: In this section we help our clients to maintain and use the same standard of data format for same set and we provide them a same level of storage fineness for all set either clients are modifying their data, delete their data or insert some special data from any source in the cloud. [4] Reliability: we provide dynamic access to our user so that they can enhance the usage and availability throughout any condition or any kind of unwanted failure, maltreating attacks, malicious data modifications, server collisions due to high trafficking or any kind of server colluding malware attack. It means we are completely reducing the data flaws and errors any kind of system failure, any maltreating attacks over the servers or any other clashes brought by unauthorized login or in case of server failure. [5] Convenience: To give authority to the users for performing the storage inputs from anywhere, anytime by just using and enabling the storage fineness and check all the details related to it and minimized the over heading of storage blocks and assuring all the storage cardinalities overhead.

D. Preliminaries:

To get the right access control over the data and secure the cloud data storage we just need to keep some important preliminaries in terms of the maltreating server. Malfunctioning, overheating of servers due to some external load by any malware so that we can easily localize them and block them from our local server and prevent the user's data over the cloud. The main key insight of the paper is to discuss about the generic cloud storage problem and causes of security threats and the possible ways to get rid with those all issue. The cloud computing technology always deal with the most challenges like security, availability, robustness, capex and opex.

III. Proposed Statement for Assuring Cloud Data Storage

Now a days every almost everyone using cloud services either in form if infrastructure, platform or software and all cloud users usage cloud data storage technique to store their data and access it wherever they want, they are not concern with the management of cloud storage and also there is no need to go in for locally. Therefore, the accuracy, fineness and exactness of data availability is being maintained and the all data sets or block which is stored in the cloud servers are completely guaranteed by the cloud service providers who keeps all the stats of data manipulation. The main key factor which is mostly effective and reliable is to get the details about the any unauthorized access over the servers, after detecting any unwanted access through our local server we prevent our whole cloud storage from unauthorized data changes and corruption which always happens due to any other server colluding with our localhost and makes a stable settlement with our system. Afterward, this cloud system is considered in a distributive manner so that when any such type of incompatibilities is founded then we try to moderate that servers from where all calls and requests are generating for the data error. So, this is a huge significance for us by using this, it's our first step towards the instant recovery of data storage and get rid with the all kind of unwanted and unauthorized data errors.

To track these kinds of massive problem inside our system and cloud storage, the most important and significant design is to assure cloud data storage which is already describes in this paper, and some out of the box scenario is described as in terms of the control over the system and servers. This kind of control always gives a great possible way for an individual which facilitate with internet connection services to get the complete access of data files as per the need. Cloud storage security increasingly attached with the lots of impactive tools and some kind of innovative technology with huge approaches. An immersive and signified advantages of cloud computing is that there are lots of in-built predecessors and quantized element consisted with peer to peer connections and stability which gives a unified source to the users. The initial section of this, is attached with a precise and specific tools, auditing and compliances based on the codes and rest of them are on behalf of the theory which is mostly required for our design to distribute the all data files from the servers to the host cloud servers. Therefore, another concept is came related to the storage issue and that is identical token. This identical token is considered as a process of some kind of computation function with the systems and use some distributed techniques to become stable throughout the process and this is comes under the family group of an universal hash and universal trace function and this is opt out for the preservation of the identical behavior and attributes of the data sets. This data sets are vastly semantic in cloud storage, which can consist with pure and exact integrated identity of the users. This authentication and verification process are also led in terms of preservation of storage and data sets. This methodology shows us that how to obtain a problem response novation for getting verified and become authorized for the storage access and fineness and also get the access about the all maltreating servers and some ransomware. So, at the end the process of get the access of our files and data sets back and error verification of deleted coded data, our design achieves the unification of storage fineness assurance and data flaw localization, it means the identification of maltreating servers and this is also categorize in following aspects which is consisted with some distribution techniques, token study, fineness and verification of data flaws with error localization, files protection and backup& recovery point.

A. File Sharing and distribution technique:

In cloud computing technology we all are well introduced with the terminology known as fault tolerance, so by using this in file distribution techniques we can correct the deleted coded data, it may cause by many types of subsequent and multiple tolerated failures in our cloud data storage.

B. Defiance Trace Precomputation:

In this aspects and terms of challenges or defiance to get the convincement of the cloud data storage and get rid with data flaws and concentric error affiance in the similar ways, this method completely relies on the precomputed inspections trace. The leading process will take place as per file distribution, in which system and clients will thoroughly precompute a dedicated numbers of computation chain of small inspection trace with separate subset, each and every trace casing with all of random set of data set and blocks. Afterward, if clients are requested and wants to know about the cloud storage security and storage assurance about their data in cloud, they took a set of unspecified random procreated set of blocks and disquieted block indices on cloud server with precomputed tokens to check the storage correctness. Now after getting some unspecified traces on cloud servers, all cloud servers start work separately as in form of a unique server itself and then they started compute a bit about unified source and unspecified data set thoroughly a unique set of data block with specified block and finally send it back to clients. The attributes and locale values of this all set and sources which should be similar match with concerned and specified traces which is precomputed by clients itself. Hence During this whole process, all cloud servers will purely operate casing the same data blocks and subsets of source indices.

C. Fineness verification and data flaws localization:

The terminology flaw localization is a main stream and key factor for detecting the flaws and terminating them from storage unit and system sources. In spite of different kind of old and various methods which can determine all the flaws explicitly for data localization and then gives us a unique binary result as an outcome for storage correctness and storage inspections. So this method consist with a separate set of schemas which outperforms all of those by unified the Chasity inspections and flaws localization in this defiance impedance protocol: the impedance values from cloud servers for each and every separate defiance not only considered and determining the Chasity of the distributed storage source, but also this is containing the whole details of process execution and information to locate the mainstream of potential data flaw(s).

D. File Protection and Backup recovery point:

Now a days our complete structure and layout pattern of file is in a form of systematic linear data set and the user can again reform the mainstream file just by downloading that media data and all data set and subset block of the structure. In this method our inspection methodology is mainly based on the random casing system and point to point checking system. So, the cloud storage unit and the whole data set is compatible with respect to servers' structure and assurance medium.
However, the whole reconstruction of system defined parameters is completely suitable for conveying the system protocols of cloud storage servers. Hence here are the main algorithm of recovery point of cloud data from cloud storage servers which we using in our implementation part and this pseudo algorithm is gives you a bit idea about the actual recovery point of data-

Algorithm -: \\ Process

% Let the data set and all data block, subsets corruptions have been detected among the % n type of error medium and data flaws.

% Suppose there are N unspecified servers and also K unauthorized access through main server.

% Let there are M misbehaving malware

2- Recovery

% Download the unspecified server address and unauthorized access link

% Exterminate the server N and erase the linking process and get the physical address (MAC) of unified system source.
% Block the system calls and transmission and corrupt the transmitted data set.
% Generate the list report and quantify the main source of access.
% Gather all server and malware daemons
% Kill the daemons via daemon thread process
% Stop the server

End Process //

IV. Security Analysis and Performance Efficiency Evaluation:

In cloud computing technology, security section is the most important aspect for the clients and CSP both. Our designed method in terms of security and performance efficiency provide a system setup to evaluate the minimum downtime during the process execution. This method is completely containing the adversary design which is already described in this paper. In this section we also calculate the efficiency of our design by making usage as implementing our both module file sharing and distribution technique, defiance trace precomputation, inspection trace precomputation and this process gives us a correctness about the storage assurance. There are mainly two part of evaluation, which is goes through from the following aspects-

[1] Feeble hostile/Adversary Security Strength against the robust hostile adversary: In this kind compatibility of adversary which relies on both the attacked source and the attacker source which is mainly focused with the data modification probability with detection and replication of origin source of data storage or corrupting the client's data and stored files on each and every Single Server Unit. During the overtaking of weak and strong adversary together, If the attacking medium make a stable settlement with the host server then they can erase all the client's data over the server or make some kinds of data modification in it, so that they can also use some kind of replicated and adequate set of data or the fraud data to get a proper convincement and safe transmission of data from the host server or source via overlapping the adversary, there may a chance of interruption of the original data access from the storage by any user.

[2] Robust Hostile/Adversary Security with the feeble strength against strong design: In this portion we generally evaluate and analyze the mainstream of the security compatibility and security strength of main design and some of there schemas against the servers and client's interaction. Our design will provide a significant way to comprise the server collision attacks via different mode of attacks, so we make a use of parity block which provide a blinding facility for the data blocks and subset of the data and this can help us to get the easy mode of access and improve our security pattern for the dedicated system design. In security threat case this adversary is top most horrible and worst case ever and quite challenging also, in which cloud servers are purely quantized and in this case we considered that the conflicting and dissident can make a robust settlement with the internal sources of storage and he can try to make some internal changes in the data and data files with a consistent amount which is completely unchangeable from external sources and they can easily transmit the data from anywhere. In fact, there is another part of this in which all the localized servers through the host are start colluding with each other and start generating a rigid structure of data loss so that they can prevent themselves from mixing up with each other. In this case all server is start responding in a subsequent manner with same point of time so here data loss and data corruption chances are quite massive and its completely irreversible to get data back in a safe zone. By making all block as blinded parity block no any other malicious servers can get the data and data related information from anywhere in this world and this is a pure linear structure for parity block also, so this is a brief about the security and privacy preserving.

V. Related Works:

In this vast and most adoptable technology there are lot of work which is associated with it and this works are done by many researchers named [1] Juels et al, who explain and elaborate a pure and formal schemes for cloud computing security challenge which consisted with proof of accessibility (Retrievability) pattern for Chasity among the remote data storage medium and widely adopted data integrity technology. This design consists with peer to peer checking and inspection of data flaws and their access code to assure the both kind of security threat which is accessibility and possession of data blocks and subset or some file system and service system. [2] Shacham et al, constructed this design and built a random structure and pose that structure in a linear function format based some specific homomorphic inspector and some distributed authenticator which helps to provide the large number of storage queries with very tiny peer to peer communication mode.[3] Bowers et al, Bowers et al, Bowers et al, this man proposed an most efficient and enhanced modified framework for proof of accessibility protocols that mainly generalizes and signify the both combined work together which was done by Juels and Shacham. Afterward in continuation of this work done in this subsequent, Bowers et al, enhanced the same model which he proposed lastly with a specific distributed system. Overall, these main designs are mainly focusing and concentrating on the static data. The Chasity of their design data pattern and some of the primarily about the data set deals with some preprocessing processes that a source can confined before the outsourcing of their data block and whole data files. If there are any kind of data changes occur with related to contents of the data then few of them propagate through data flaws detection and some error detecting code, hence this complete process introduced a unified and magnified pre-computation process and some specific peer to peer communications complexity.

[4] Ateniese et al, described some verified provable and imposed data possessions type model which completely deals with the Chasity among the assurance possession of data files and some unauthorized and untrusted storage medium. This design pattern mainly utilized the public impedance and their key which is thoroughly based on the homomorphic keys and uniquely designed tags for auditing the subsequent data files, data blocks and then ensuring the public verification via these keys. So, overall, this design pattern needs some efficient and contributed sufficient pre-computations mode that can enhanced the process customizability and can be expensive and imposed for the whole subsequent pattern and file. In this subset of process execution, Ateniese elaborate an inherited model and unique design set for that users who can have a verified and unique symmetric homomorphic key. This model has a base head panel which is more reliable than the previous designed model and that allows users to disable the routine framework update, delete, and insert type of operations for the stored data in cloud servers and this is also very much supported in our model and work. However, this design concentrating on a unique screen and specific server scenario and propagated a physical address and some specific address route in data modifications and corruption. [5] Curtmola et al, proposed a model with their trajected data blocks to assure about the data security and data schemas for possessions of various replica of the data sets among the distributed storage medium. This is completely extending the previous designed model for subsequent data blocks to casing the various replicas of data without having any homomorphic key, during this process of executions this model provide a customizable copies of original data block who is actually maintained for the security purposes.

VI. Conclusion:

In this research paper, we mainly investigated and inspected the problem which relies with cloud data storage security and accessibility through cloud, which is mostly a distributed structure of storage system. To get an exact and unified Chasity of client's data in cloud computing, we designed and proposed an most efficient and effective design pattern with some new enhanced explicit kind of dynamic data support and accessibility, which is mainly consisted with block level security patches and some data operations like update, delete, insert. This model relies on the erasure modifications and corrections code in the data block and file system with distributed file structure preparations to provide a complete redundancy and parity among the data subsets. The file distribution technique guarantees the inadequate data compressibility and dependability by just using the public and homomorphic key and some newly made defiance traces with distributed inspections of deleted or modified data, our design pattern gets a significant integrations of storage Chasity and assurance of data flaws localizations, i.e., whenever any type of data modification and corruptions has been occur then this module of error detection and localizations during assurance of data storage medium is take place and verify the unauthorized source and unauthenticated access of the source throughout the process and this verification process will cover all the platform across various distributed servers. Hence this proposed model will guarantee a most important aspects of some malicious changes in client's data or any other server attack or in case of server collision with unified or untrusted source. We make sure that the data security in cloud computing technology is the most important aspect for now and forever in the world of technology and also in the area of storage and safety of data challenges. In fact, there are many researchers and their work in the area of this research problems are not completely identified. Hence third-party auditor will audit the cloud data storage without having any prerequisite demand by the user's time, feasibility and the cloud storage resources.

****

References:

[1] Amazon.com, "Amazon Web Services (AWS)," Online at http://aws. amazon.com

[2] N. Gohring, "Amazon's S3 down for several hours," Online at http://www.pcworld.com/businesscenter/article/142549/amazons s3 down for several hours.html

[3] A. Juels and J. Burton S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. of CCS '07, pp

[4] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. of Asiacrypt

[5] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Cryptology ePrint Archive Report

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. of CCS

[7] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. of SecureComm"

[8] T. S. J. Schwarz and E. L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. of ICDCS.