IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. III (May-Jun. 2016), PP 50-56
www.iosrjournals.org

Personality Based Dispersed Provable Information Ownership in Multi Distributed Storage

S Supriya[1], K Anusha[2]
[1]M.Tech Scholar (CSE) in Department of Computer Science Engineering.
[2]Assistant Professor, Department of Computer Science and Engineering, Qis Institute of Technology, Ongole, AP, India.

Abstract: *The cloud storage administration has turned into a speedier benefit development by giving its components to customer's information. Security protection and information respectability are the two principle issues confronted by single cloud administration suppliers. Henceforth dispersed cloud environment, multi cloud is utilized. In the current framework, when customer stores his information on multi-cloud servers, the disseminated storing and respectability checking are at danger. Provable information ownership is a technique for guaranteeing the respectability of information away outsourcing. The proposed ID-DPDP convention ready to furnish customer's character with his private key and provably secure under the hardness presumption of the standard CDH issue.. It will check customers information kept securely without downloading the entire information. This convention kills testament administration, productive and adaptable. The earth of cloud computing has formed into a fundamental subject in a considerable amount of ranges. The conveyed storing and additionally honesty checking is essential for a typical circumstance, when customer develop his data on the servers of multi-cloud. Strategy of trustworthiness checking must be pragmatic to make it suitable in backing of limit constrained end gadgets along these lines, in view of disseminated calculation, we will learn circulated model of remote information honesty checking and set forward the comparing solid technique in multi-cloud storage. Thus in our work we start novel affirmation model of remote information honesty known character based circulated provable information ownership inside multi-cloud storage. On the premise of customer's approval, proposed strategy can comprehend private check, assigned confirmation and additionally open check. The anticipated strategy is provably clever and ensured. Other than auxiliary point of interest of end of endorsement administration, character based convention of conveyed provable information ownership is also capable and adaptable. To improve the adequacy, personality based provable information ownership is all the more striking and consequently, more supportive to ponder.*

Keywords: *Multi-cloud storage, Cooperative Provable Data Possession, Hash Index Hierarchy.*

I. Introduction

With the appearance of new advancements like Web Services and Virtualization, cloud computing turned into a reality. With cloud computing individuals can get three sorts of administrations, for example, stage as an administration, programming as an administration and foundation as an administration. The cloud organization models incorporate private cloud, open cloud, group cloud and half and half cloud. The private cloud is the cloud inside an association's system. Open cloud is the cloud available to whole world through web in light of specific guidelines. The group cloud is among organizations secretly while the crossover cloud is the blend of two or more sorts of cloud. As the cloud is turning out to be more famous, there are developing security concerns. These security concerns prompted the examination in the zone and numerous scientists proposed conventions and systems to guarantee cloud information security. The cloud administration suppliers deal with contend security of cloud information. Be that as it may, as the cloud is in trusted (got to through Internet), parcel of examination went on capacity security in cloud. A portion of the papers and their procedures are quickly given here. In [1] conveyed confirmation conventions are developed for guaranteeing information storing security in cloud computing. This is accomplished by executing a conveyed examining component which guarantees that the information progression of all cloud clients are guaranteed and tried for uprightness. In [2] an outsider examining instrument is actualized with a specific end goal to secure cloud storage. Nonstop accuracy of information is the SLA (Service Level Agreement) executed in this paper. Open reviewing of this paper helps in information uprightness of different cloud clients. In [3] another methodology is displayed. It is known as appropriated responsibility for information sharing. It is accomplished by actualizing a JAR which has information and security component other than availability records for different cloud clients. In [4] multi mists are actualized to protect information of customers. At the end of the day it is the billow of mists for enhancing power of capacity security. In [5] a novel methodology is utilized to store, recover and forward information in the cloud. It utilizes secure deletion code to guarantee information security and encryption instruments for sending information to other honest to goodness clients. In [6] helpful provable information ownership idea is utilized. It guarantees that cloud environment works helpfully and secure information. In [7] security to cloud information is given utilizing Sobol Sequence. This paper executed a dispersed confirmation convention that transfers on deletion code. In [8] likewise open inspecting is actualized for cloud storage security. The outsider examiner checks for information trustworthiness and guarantees that the information is not messed around with in the server. Whatever is left of this paper is dedicated to survey three papers relating to information storing security issues in cloud. All papers accepted that, the cloud storage is not secure as the administration supplier may erase information or the cloud proprietor does not unveil capacity issues in the cloud. In this manner, on the premise of disseminated calculation, we will learn appropriated checking of remote information uprightness show and give relating solid convention in multi-cloud storage. Out in the open key foundation, convention of provable information ownership requires open key declaration dispersion and overseeing and it will bring about significant overheads as the verifier will ensure the testament when it checks remote information respectability. In cloud computing, generally of verifiers just contain low calculation capacity. Character based open key cryptography can dispose of complex testament administration. To improve adequacy, character based provable information ownership is all the more striking subsequently, it will be critical to learn personality based disseminated provable information ownership [3][4]. The anticipated personality based convention of dispersed provable information ownership is provably secured in hardness supposition of standard computational Diffie-Hellman trouble. Also to auxiliary advantage of disposal of authentication administration, our character based disseminated provable information ownership is in addition capable and adaptable.

II. Related Work

Security in cloud is essential. To check the accessibility and respectability of outsourced information in cloud stockpiles, specialists have recommended two essential methodologies called Provable Data Possession (PDP) [2] and Proofs of Retrievability (POR) [3]. Ateniese et al. [2] initially proposed the PDP model for guaranteeing ownership of records on untrusted MeghaPatil et al,/(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 982-985 www.ijcsit.com 982 stockpiles without recovering it. Customer keeps up steady measure of metadata to check evidence. This PDP approach has likewise given a RSA-based plan to a static case that accomplishes the ٖ (1) correspondence cost. They additionally proposed a freely unquestionable rendition, which permits customer (information proprietor) and also anybody other than proprietor, to challenge the server for information ownership. This property has had gigantic effect on application territories of PDP convention because of the partition of information proprietors and the clients. Be that as it may, these procedures are unstable against replay assaults in element situations. In addition, they don't fit for multi-cloud storage because of the loss of homomorphism property in the confirmation procedure. Ateniese et al. built up an element PDP arrangement called Scalable PDP [4]. This very effective and provably secure PDP procedure is construct totally in light of symmetric key cryptography without requiring any mass encryption. This PDP method permits outsourcing of element information, i.e. it bolsters operations, for example, erasure, piece change and affix, However, since it is based upon symmetric key cryptography, it is inadmissible for open (outsider) confirmation. Likewise, servers can cheat the proprietors by utilizing past metadata or reactions because of the absence of irregularity in the difficulties. The quantities of difficulties and redesigns are constrained and settled ahead of time and clients can't perform piece insertions anyplace. In view of past work, Erway et al. [5] proposed two Dynamic PDP plans with a hash capacity tree to acknowledge (log ٗ) correspondence and computational expenses for a ٗ -square record. The fundamental plan, called DPDP-I, keeps the downside of Scalable PDP, and in the "blockless" plan, called DPDPII, the information squares can be spilled by the reaction of a test, .However, these plans are likewise not powerful for a multicloud domain in light of the fact that the check way of the test piece can't be put away totally in a cloud [8]. Juels and Kaliski [3] introduced a POR plan, which depends generally on preprocessing steps that the customer conducts before sending a document to a CSP. Shockingly, these activities keep any effective augmentation for redesigning information. Shacham and Waters [6] presented an enhanced variant of this convention called Compact POR. This convention utilizes homomorphic property to total a proof into (1) authenticator esteem and (ي) calculation cost for ي challenge squares, however their answer couldn't keep the spillage of information pieces in the check procedure as a result of its static nature. Wang et al. [7] gave a dynamic plan (log ٗ) cost by coordinating the Compact POR plan and Merkle Hash Tree (MHT) into the DPDP. A few POR plans and models have been as of late proposed including [9], [10]. In [9] Bowers et al. presented a dispersed cryptographic framework that permits an arrangement of servers to take care of the PDP issue. This structure depends on an uprightness ensured blunder redressing code (IP-ECC), which redesigns the security and productivity of existing instruments. Notwithstanding, a record must be changed into particular sections with the same length, which are disseminated crosswise over servers.

III. Demonstrating Of Identity-Based Protocol Of Cloud Provable Data Possession

Cloud computing has end up being an essential subject in a few ranges. It takes data handling as an administration, and calms trouble for overseeing of capacity, all inclusive information access with self-governing geological areas. The issue to persuade cloud customers that their information is undamaged is specifically vital on the grounds that the customer's don't collect these information locally [3][4]. Checking of disengaged information uprightness is a primitive to handle this issue. For general circumstance, when customer amass his data on the servers of multicloud, the dispersed storing and honesty checking are crucial. Convention of respectability checking must be ingenious keeping in mind the end goal to make it suitable for limit constrained end gadgets therefore, in light of disseminated calculation, we will learn circulated model of remote information uprightness checking and set forward the relating solid system in multi-cloud storage. In personality based open key cryptography, our work concentrates on dispersed provable information ownership inside multi-cloud storage which can be made clever by wiping out declaration administration. The convention of solid character premise circulated provable information ownership development for the most part originates from signature, provable information ownership and in addition appropriated figuring. Information honesty checking representation is more adaptable other than high adequacy. In view of customer's approval, proposed ID-DPDP strategy can comprehend private confirmation, designated check and additionally open check. A personality based convention of appropriated provable information ownership includes four substances which are appeared in fig1. They are Client: a substance, which has colossal information to be put away on multi-cloud setting for safeguarding and calculation, can be additionally singular buyer or else enterprise. Combiner: an element, which gets capacity request and assigns square label sets to equal cloud servers [5]. At the point when accepting test, it parts test and issues them to a few cloud servers. Amid the getting of reactions from cloud servers, it consolidates them and forward joined reaction to verifier. Cloud Server: an element, which is administered by cloud administration supplier, has imperative storage room and calculation asset to maintain the customers' data. Private Key Generator: a substance, while getting character, it yields comparable private key.

IV. Cloud Types

Public cloud

A large organization owns the cloud infrastructure and sells cloud services to industries or public. Public cloud applications, storage, and other resources are made available to the general public by a service provider. These services are free or offered on a pay-per-use model.

Community cloud

Several organizations that have similar polices, objectives, aims and concerns share the cloud infrastructure. The common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally.

Hybrid cloud

Hybrid cloudis a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. It enables data and application Probability

Private cloud

The cloud infrastructure is owned or leased by a single organization and is operated solely for that organization Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally.

V. Cloud Architecture

It is a systems architecture involved in the delivery of cloud computing, involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue. Elastic provision implies intelligence in the use of tight or loose coupling as applied to mechanisms such as these and others. It have four basic steps,

1. Cloud infrastructure (eg. Billing VM)

2. Cloud service (eg. Queue)
3. Cloud platform (eg. Web Frontend)
4. Cloud storage (eg. Database)

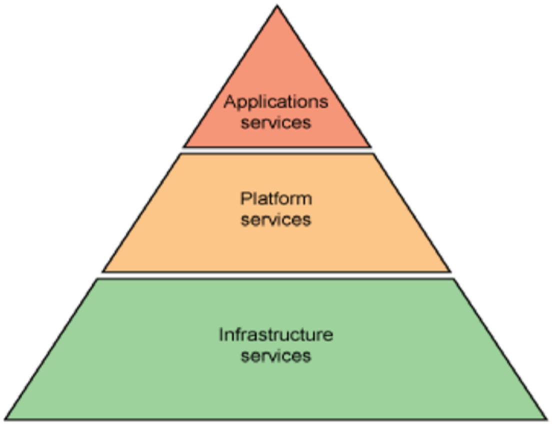

Fig 1. Cloud Architecture

DISTRIBUTED SERVERS:

The servers are not housed in the same location. Often, they are in geographically disparate location. But for cloud subscribers, it act as right next to each other. It gives service provider more flexibility in option and security. If any failure occurred at one site the service be still accessed from another site. If cloud need more hardware they need not throw more server in the safe room they simply add them at another site as a part of cloud.

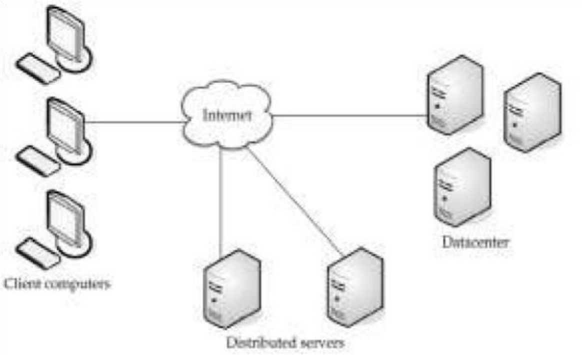

Fig 2. Distributed Servers

CLOUD ENTITIES:

End User **-** End Users need to access certain resources in the cloud and should be aware of access agreements such asacceptable use or conflict of interest and concerns transmission integrity.

System Architect **-**System architects are employed with writing the policies that pertain to the installation and configuration of hardware components such as firewalls, servers, routers, and software.

Developers **-**Developers build an application in the cloud need to access the infrastructure where the development environment is located and improve development through elasticity of resources.

Third Party Auditors (TPA) **-**Third party auditors are used by clients and providers alike to determine the security of the cloud implementation. Depending on the level of commitment to security and usefulness a cloud vendor may choose to submit itself to regular security assessments in an attempt to obtain accreditation. The accreditation process needs to be undertaken every three years.

CLOUD COMPUTING SECURITY:

There are many security issues in cloud and they are classify into main issues,
1. Security issues faced by cloud providers
2 .Security issues faced by their customers

Basic Principles in Information Security:

***Confidentiality* –**It is used to prevent disclosure of information to unauthorized person. It is necessary for maintaining the privacy of personal information.
***Integrity* –** The data should not get modified without knowingly. The data should remain intact unless it is modified by authorized person.
***Availability* –** The information must be available whenever it is needed. Ensure availability should always prevent DoS attacks.

VI. Proposed Model

An identity-based protocol of distributed provable data possession procedure is a collection of three algorithms such as Setup, Extract, TagGen in addition to an interactive proof system known as Proof. Setup algorithm will Input the security parameter, and it outputs system public parameters such as the master public key and master secret key. Extract algorithm Inputs public parameters and master public key, master secret key, as well as identity of a client, it outputs private key that corresponds to client with identity. TagGen algorithm will Input private key, block and a set of cloud servers it outputs the tuple. Proof is a procedure among Proof, Verifier and combiner. We put forward the corresponding concrete procedure in multi-cloud storage. The concrete identity-based protocol of distributed provable data possession construction mostly comes from signature, provable data possession as well as distributed computing. The signature relates client's identity by means of his private key. Distributed computing is generally utilized to accumulate client's data above multiple cloud servers. This computing is moreover employed to combine multi-cloud servers' responses to act in response to verifier's challenge. This procedure comprises Setup, Extract, TagGen, as well as Proof. In Extract, Private Key Generator creates private key in support of client which creates block-tag pair and uploads it towards combiner. Combiner distributes block-tag pairs towards various cloud servers consistent with storage metadata. Later verifier sends challenge towards combiner and combiner allocates challenge query to equivalent cloud servers consistent with storage metadata [6]. The cloud server's act in response to challenge and combiner collect these responses from cloud servers. The combiner sends combined response to verifier. Finally the verifier ensures whether aggregated response is applicable.

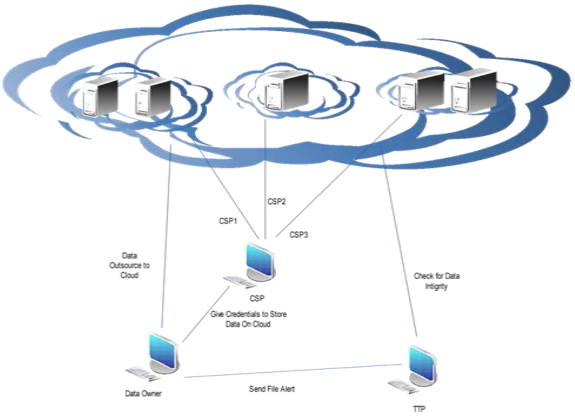

Fig.3 Proposed system Architecture

VII. Aes Algorithm

AES is a block cipher with a block length of 128 bits. • AES allows for three different key lengths: 128, 192, or 256 bits. Most of our discussion will assume that the key length is 128 bits. [With regard to using a key length other than 128 bits, the main thing that changes in AES is how you generate the key schedule from the key — an issue I address at the end of Section 8.8.1. The notion of key schedule in AES is explained in Sections 8.2 and 8.8.] • Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. • Except for the last round in each case, all other rounds are identical. • Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing.

AES Key Expansion AES Key Expansion
 Use four byte words called w Use four byte words called wi. Subkey = 4 words. . Subkey = 4 words.
For AES For AES-128:
 First subkey (w3,w2,w1,w0) = cipher keyFirst subkey (w3,w2,w1,w0) = cipher key
 Other words are calculated as follows: Other words are calculated as follows:

wi=wi-1 wi-4
for all values of i that are not multiples of 4. for all values of i that are not multiples of 4.
 For the words with indices that are a multiple of 4 (w For the words with indices that are a multiple of 4 (w4k):
1. RotWord: Bytes of w : Bytes of w4k-1 are rotated left shift (nonlinearity) are rotated left shift (nonlinearity)
2. SubWord: SubBytesfn is applied to all four bytes. (Diffusion) fn is applied to all four bytes. (Diffusion)
3. The result The result rsk is XOR'ed with w4k-4 and a round constant and a round constant rconk (breaks Symmetry): (breaks Symmetry):
w4k=rsk w4k-4 rconk
 For AES For AES-192 and AES 192 and AES-256, the key expansion is more 256, the key expansion is more

VIII. Cooperative Provable Data Possession Scheme

This work addresses the construction of an efficient PDP scheme for distributed cloud storage to support data migration and scalability of service, in which we consider the existence of multiple cloud service providers to cooperatively store and maintain the clients' data. It presents a *cooperative* PDP (CPDP) scheme based on homomorphic verifiable response and hash index hierarchy. Multi-prover zero knowledge proof system is used to prove the security of this scheme, which can satisfy knowledge soundness, completeness and zero-knowledge properties.

A. Hash index hierarchy:

To support distributed cloud storage, architecture used in cooperative PDP scheme as shown in fig. 2. Our structure has a hierarchy structure which resembles a natural representation of file storage. This structure consists of three layers to represent relationships among all blocks for stored resources. This hierarchy structure and layers are described as follows:
1) *Express Layer*: This layer offers an abstract representation of the stored resources;
2) *Service Layer*: This layer offers and manages cloud storage services; and
3) *Storage Layer*: This layer represents data storage on many physical devices.

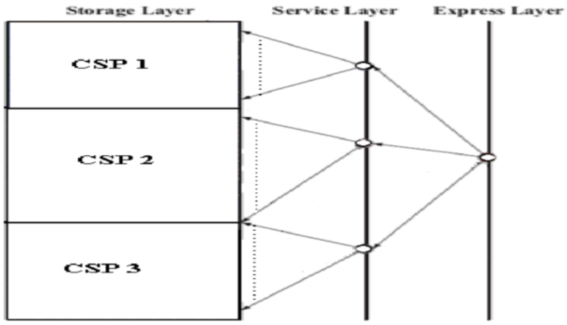

Fig.4 Hash index hierarchy.

This hierarchy used to organize data blocks from multiple CSP services into a large size file by shading their differences among these cloud storage systems. In Figure the resource in Express Layer are split and stored into three CSPs that are indicated by different colors are shown in Service Layer. After that each CSP fragments and stores the assigned data into the storage servers in Storage Layer. It also makes use of colors to distinguish different CSPs. Moreover, it follows the logical order of the data blocks to organize the Storage Layer.

B. Homomorphic Verifiable Response:

Homomorphic Verifiable Responses (HVR), which is used to integrate multiple responses from the different CSPs in CPDP scheme. If given two responses and for two challenges and from two CSPs, there exist an efficient algorithm to combine them into a response corresponding to the sum of the challenges ∪ then a response is called homomorphic verifiable response in a PDP protocol. Homomorphic verifiable response is the key technique of CPDP because it not only reduces the communication bandwidth, but also hides the location of outsourced data in the distributed cloud storage environment.

***C. Security Analysis*:**

Multi-prover zero-knowledge proof system is directly used for security, which satisfies following properties:

1) *Collision resistant for index-hash hierarchy:* The indexhash hierarchy in CPDP scheme is collision resistant, even if the client generates files with the same file name and cloud name collision doesn't occur there.
2) *Completeness property of verification:* In this scheme, the completeness property implies public verifiability property. Due to this property allows client as well as anyone other than client (data owner) can challenge the cloud server for data integrity and data ownership without the need for any secret information.
3) *Zero-knowledge property of verification:* This paper makes use of the zero-knowledge property to preserve the privacy of data blocks and signature tags. Initially, randomness is adopted into the CSPs' responses in order to resist the data leakage attacks.

Knowledge soundness of verification:

The soundness means that it is infeasible to fool the verifier to accept false statements. Often, the soundness can also be considered as a stricter notion of unforge ability for file tags to avoid cheating the ownership. This denotes that the CSPs, even if collusion is tried, cannot be tampered with the data or forge the data tags if the soundness property holds. Thus CPDP scheme can resist the tag forgery attacks to avoid cheating the CSPs' ownership.

IX. Conclusion

Cloud is designed to provide a service to the external users. To compensate their needs the resources should be highly available. In this survey, it gives overview about cloud availability and various integrity verification techniques. In addition, comparative study of various availability and integrity verification schemes and its methodology are classified along with their adaptation to single/multi cloud environment.This paper formalizes the ID-DPDP system model and security model. ID-DPDP protocol works efficiently in multi cloud environment. Besides of the elimination of certificate management, our ID-DPDP protocol has also flexibility and high efficiency. At the same time, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification based on the client's authorization.

AUTHORS:

S. SUPRIYA is a student of Computer Science &Engineering from QIS Institute of Technology, Presently pursuing M.Tech (CSE) in this college. She received B.Tech from JNTUK in the year of 2013.

K. ANUSHA, is working as Assistant Professor in QIS Institute of Technology, Ongole. She received M.Tech (CSE) from JNTUK. She is pursuing Ph.D. in Sri Padmavati Mahila Visva Vidyalayam, Tirupati.

References

[1]. P. Mell and T. Grance, "Draft nist working definition of cloud computing," Referenced on June. 3rd, 2009.

[2]. G. Ateniese, R. DiPietro, L. V. Mancini, G. Tsudik, "Scalable and Efficient Provable Data Possession", SecureComm 2008, 2008.

[3]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,D. Song, "Provable Data Possession at Untrusted Stores", CCS'07, pp.598-609, 2007.

[4]. C. C. Erway, A. Kupcu, C. Papamanthou, R. Tamassia, "DynamicProvable Data Possession", CCS'09, pp. 213-222, 2009.

[5]. F. Seb´e, J. Domingo-Ferrer, A. Mart´ınez-Ballest´e, Y. Deswarte, J.Quisquater, "Efficient Remote Data Integrity checking in Critical InformationInfrastructures", IEEE Transactions on Knowledge and DataEngineering, 20(8), pp. 1-6, 2008.

[6]. H.Q. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, 2012.

[7]. Y. Zhu, H. Hu, G.J. Ahn, M. Yu, "Cooperative Provable Data Possessionfor Integrity Verification in Multicloud Storage", IEEE Transactions on Parallel and Distributed Systems, 23(12), pp. 2231-2244, 2012.

[8]. Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, S. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds", CCS'10, pp. 756-758, 2010.

[9]. R. Curtmola, O. Khan, R. Burns, G. Ateniese, "MRPDP: Multiple-Replica Provable Data Possession", ICDCS'08, pp. 411-420, 2008.

[10]. A. F. Barsoum, M. A. Hasan, "Provable Possessionand Replication of Data over Cloud Servers", CACR,University of Waterloo, Report2010/32,2010.