ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Efficient Data Storage Security in Cloud Computing

Dr S Durga Bhavani[1], Gudlanarva Sudhakar[2], Ujjwal Karna[3]

M. Tech ,Ph D, Director & Professor, School of Information Technology(JNTUH), Hyderabad, Telangana, India[1]

M. Tech (SE), (Ph D), Lecturer, School of Information Technology(JNTUH), Hyderabad, Telangana, India[2]

M.Tech Student, Department of Computer Networks & Information Security, School of Information technology (JNTUH), Hyderabad, Telangana, India[3]

ABSTRACT: Cloud processing is the figuring innovation which gives assets like programming, equipment, administrations over the web. Cloud computing gives calculation, programming, information get to and capacity benefits that don't require end-client learning of the physical area and setup of the framework that conveys the administration. Since the information transmission on the web or over any systems are defenceless against the programmer assault. Cloud based information capacity frameworks have numerous complexities with respect to basic, private, delicate information of customer. The trust required on distributed storage is so far had been restricted by clients. The information stockpiling in the cloud has been a promising issue in these days. This is because of the way that the clients are putting away their significant information and data in the cloud. The clients ought to believe the cloud specialist organizations to give security to their information. The cloud specialist organizations likewise giving the security however not up to a total level. The assault of noxious insiders into the cloud and to take the information has been expanded. Information store is fundamental future that cloud benefit gives to the organizations to store gigantic measure of capacity limit. Yet at the same time many organizations are not prepared to actualize distributed computing innovation because of absence of legitimate security control approach and shortcoming in insurance which prompt to many test in distributed computing. This paper deals about the study on various issues identified with information stockpiling security on single cloud and also multi cloud what's more, adaptation to internal failure.

KEYWORDS: Cloud; cloud computing; multiple cloud; service provider; data storage; data security; audit policy; data correctness; data availability; data integrity.

I. INTRODUCTION

Cloud computing is the cutting edge in the Internet's innovation which gives the client everything regarding administrations like figuring energy to registering framework, applications, business forms according to the need of client over the web. The "cloud" in distributed computing can be characterized as the arrangement of equipment, systems, stockpiling, administrations, and interfaces that join to convey parts of processing as an administration [1]. Distributed computing has four primary elements: versatility, self-administration of provisioning and need base utilization instalment.

a. Organization Models
There are four diverse sending models [2] of distributed computing.

1. Open Cloud: Open or outer cloud is one of sort of cloud in which client can utilize the recourses according to the need and pay for utilization. This kind of cloud likewise has different specialist co-ops who give conventional distributed computing administrations to clients and charged for it.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

2. Private Cloud: Private cloud is the sort of cloud in which the cloud is worked in just a single association or created for one association and oversaw by them or outsider administration gives. Essentially this sort of cloud is for the inner motivation behind association which is worked in topographically circulated.

3. Crossover Cloud: Crossover Cloud can be made up with the mix of two sort of cloud like private and open cloud or the mix of cloud virtualization server with physical equipment. This sort of cloud is much cost costly contrast with open cloud.

4. Group Cloud: In the event that few associations have comparative sort of prerequisite, they can share the cloud then this kind of cloud foundation is made conceivable in market. This cloud is additionally exorbitant in contrast with open cloud however gives high level security.

b. Cloud computing: Distributed computing is offered in various structures: open mists, private mists, and half and half mists, which join both open and private [3].

1. Cloud Software as a Service (SaaS) :Programming as a Service gives programming or application which can be utilized over the web and client does not have not mindful of any data with respect to working framework, physical equipment. This kind of use can be get to by means of web and through program at client side. Client can have just some of control setting for application.

2. Cloud Platform as a Service (PaaS) : Stage as a Service give the setup of customer's product bundles and different devices which set up on specialist co-ops' physical equipment over the web. So entire foundation is occur on specialist co-ops' surroundings and client can get to that product after validation prepare passes effectively. This client can free from the equipment disappointment issue by receiving this administration.

3. Cloud Infrastructure as a Service (IaaS) : In this sort of cloud, client can have entire virtual server and client can get to it as he can get to it neighborhood like begin, stop, and get to and arrange the server. In this kind of administration, client pays just for the limit and model he needs them.

c. Advantages of Cloud Computing
1. Lessening in capital use on equipment and programming organization.
2. Area freedom, the length of there is access to the Internet.
3. Expanded adaptability and market readiness as the brisk organization model of distributed computing builds the capacity to re-arrangement quickly as required.
4. Permits the undertaking to concentrate on its center business.
5. Expanded upper hand.
6. Expanded security at a much lesser cost when contrasted with customary independent applications because of centralization of information and expanded security-centered assets.
7. Simple to keep up as they don't need to be introduced on every client's PC.

The cloud benefits that are executed or those that will be actualized will dependably be joined by a few dangers. Learning about these dangers might turn out to be the initial step to avoid them. Consequently security is the central concern of a few customers who craving to influence cloud administrations. In a wide range of cloud, security issues touch base from numerous points of view in distinctive stages, for example, client's confirmation, open source arrangement, virtual foundation, SLA, information stockpiling and asset request [5]. Out of these, Cloud based information stockpiling frameworks have numerous complexities with respect to basic/classified/delicate information of customer. The trust required on Cloud stockpiling is so far had been constrained by clients [6].

The overview of related research work done on the cloud information stockpiling security is talked about in the paper. The examination traverses the security challenges as for the kind of sending, administration and normal system issues.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

II. RELATED WORK

An Ateniese et al to consider public auditability in their defined provable data possession (PDP) model for ensuring possession of data files on untrusted storages. They implemented the scheme which utilizes the RSA based homomorphic authenticators for auditing outsourced data and suggests randomly sampling of a few blocks of file. Though, the public auditability in their scheme demands the linear combination of sampled blocks exposed to external auditor. The protocol which they proposed when used directly, is not privacy preserving, and therefore, leaks user data information to the auditor. 2) Secondly, Juels et al.[4] described in proof of retrievability (PoR) model, where spot checking and error correcting codes are used to ensure both possession and irretrievability of data files on remote archive service systems. However, the number of audit challenges a user can perform is a permanent priori, and public auditability is not supported in their main scheme. Although they describe a straight forward Merkle-tree construction for public PoRs, this approach only works with encrypted data. Shacham et al.[12] Design an improved PoR scheme built from BLS signatures with full proofs of security. Similar to the construction i they use publicly verifiable homomorphic authenticators that are built from provably secure BLS signatures [19]. Public retrievability is achieved based on the elegant BLS construction. yet again, their approach does not support privacy-preserving auditing for the same reason as Shah et al.propose allowing a TPA to keep online storage onest by first encrypting the data then sending a number of precomputed symmetric-keyed hashes over the encrypted data to the auditor. The auditors verify both the integrity of the data file and the server's control of a previously committed decryption key. This scheme only works for encrypted files and it suffers from the auditor easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it. State fullness and bounded usage, which may potentially bring in on-line burden to users when the keyed hashes are used up.

3) Atenieseetal. Propose a partially dynamic version of the prior PDP scheme that uses only symmetric key cryptography. However, the system imposes a priori bound on the number of audits and does not support public auditability. Consider a similar support for partial dynamic data storage in distributed scenario. The proposed challenge-response protocol can both determine the data correctness and locate possible errors.
In a subsequent work, Wang et al. propose to combine BLS based homomorphic authenticator with MHT to support both public auditability and fully data dynamics.

4) Simultaneously, Erway et al.[16] developed a skip lists based scheme to enable provable data control with fully dynamics support. However, all their protocol requires the linear combination of sampled blocks just as, and thus does not support privacy- preserving auditing on users outsourced data. While all above schemes provide methods for efficient auditing and provable assurance on the correctness of remotely stored data, none of them meet all the requirements for privacy-preserving public auditing in Cloud Computing, as supported in our result. More importantly, none of these schemes consider batch auditing, which will greatly reduce the computation cost in the TPA when coping with large number of audit delegations.

5) Portions of the work presented in the paper[1] they have previously appeared as an extended abstract they have revised the paper[2] a lot and improved many technical details as compared The primary improvements are as follows: First, they provide a new privacy-preserving public auditing protocol with enhanced security strength in we also include an additional (but slightly less efficient) protocol design for provably secure zero- knowledge leakage public auditing scheme Second, based on the enhanced main auditing scheme, they provide a new provably secure batch auditing protocol. All the experiments in their performance evaluation for the newly designed protocol are completely redone. They extended main scheme to support data dynamics and provide discussions on how to generalize their privacy-preserving public auditing scheme in which are lacking in [2]. Finally, they provide formal analysis of privacy-preserving guarantee and storage correctness; only heuristic arguments are sketched in [2]. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. A. Frequently used algorithms The Four basic algorithms are used frequently to set up the system environment.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

1) Key generation 2) Sign Generation 3) Gen proof 4) Verify proof, which user uses key generation algorithm to set up the sheme. Verification metadata is generated by the sign generation algorithm, where signature or identity of user is generated. Genproof algorithm is run on the cloud server to check the data storage correctness in the cloud, and for auditing the proof TPA uses to audit the proof. Algorithms for preserving privacy between the user and the cloud.Homomorphic Linear Authenticator (HLA) with random masking technique is used. These techniques guarantee that during auditing process TPA will notdemand for the local copy of data and will not be able to learn any knowledge about the data. Algebraic properties of the authenticator are taken in such a manner that they are helpful for batch processing and auditing process in further extension the entire document should be in Times New Roman or Times font. Type 3 fonts must not be used. Other font types may be used if needed for special purposes.

III. IMPLEMENTATION DETAILS

We consider a cloud data storage service involving three different entities, as illustrated in the cloud user, who has large amount of data files to be stored in the cloud; the cloud server, which is managed by the cloud service provider to provide data storage service and has significant storage .To completely guarantee the information respectability and spare the cloud clients calculation assets and additionally on the web trouble, it is of basic significance to empower open Examining administration for cloud information storage, with the goal that clients may turn to an third party auditor (TPA) to review the outsourced information when required. The TPA, who has aptitude and abilities that clients don't, can occasionally check the honesty of the considerable number of information put away in the cloud for the benefit of the clients, which gives a considerably more simpler and reasonable path for the clients to guarantee their capacity rightness in the cloud. Additionally, notwithstanding help clients to assess the danger of their subscribed cloud information benefits, the review result from TPA would likewise be advantageous for the cloud specialist co-ops to enhance their cloud based administration stage, and even serve for autonomous intervention purposes. In a word, empowering open evaluating administrations will assume a vital part for this beginning cloud economy to wind up noticeably completely settled; where clients will require approaches to survey hazard and pick up confide in the cloud.

Proposed Architecture

To empower security safeguarding open examining for cloud information stockpiling under the previously mentioned show, our convention configuration ought to achieve the accompanying security what's more, execution ensure:
1) Public auditability: enable TPA to confirm the rightness of the cloud information on request without recovering a duplicate of the entire information or acquainting extra on-line load with the cloud clients.
2) Storage rightness: ensure that there exists no conning cloud server that can pass the review from TPA without in fact putting away client’s information in place.
3) Privacy-safeguarding: ensure that there exists no chance for TPA to get clients information content from the data gathered amid the inspecting procedure.
4) Batch evaluating: empower TPA with secure and productive evaluating capacity to adapt to different reviewing assignments from most likely vast number of various clients at the same time.
5) Lightweight: enable TPA to perform evaluating with least correspondence and calculation overhead. We are presenting an assaulting module which will keep ceaselessly track on the information adjustment in the cloud if any, and will illuminate the client about the adjusted information.
Assaulting module will be as little code to adjust the database straightforwardly with the goal that passage is subverted. This code will dwell on cloud server. Likewise the clock is going to be actualized where errand might be plan for one time execution, or for rehashed execution at standard interims and furthermore we adjust some proficient servers for better execution and increment the speed of execution, for example, tomcat server.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

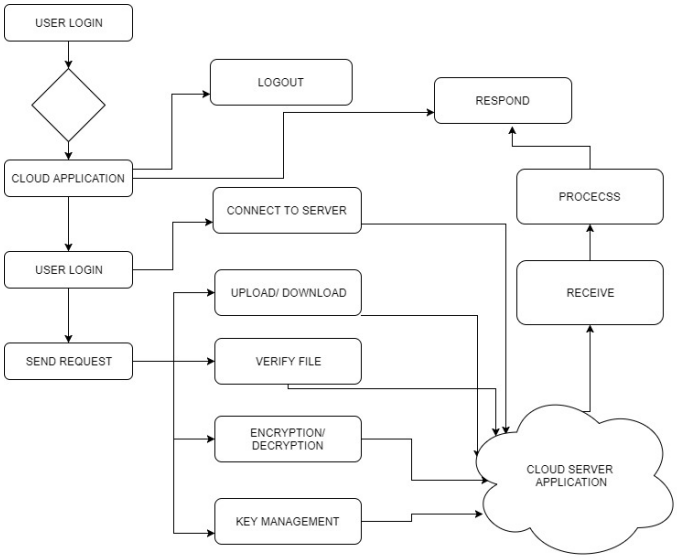

Figure 1: Architecture Diagram

B. Security Preserving Module

Homomorphic authenticators are unforgeable check metadata produced from singular information pieces, which can be safely amassed in such approach to ensure an inspector that a direct mix of information pieces is properly processed by confirming just the totalled authenticator. Thus, to accomplish protection safeguarding open evaluating, we propose to extraordinarily incorporate the homomorphic authenticator with irregular cover method. In our convention, the straight blend of examined obstructs in the server reaction is veiled with arbitrariness produced by a pseudo arbitrary capacity (PRF) [9].

C. Group Reviewing Module

Through the association of protection saving open inspecting in Cloud Computing, TPA may agree recently handle numerous reviewing appointments upon vary went client demands. The individual inspecting of these undertakings for TPA can be and extremely troublesome and wasteful. Group examining not just enables TPA to play out the numerous examining undertakings in the meantime, yet in addition incredibly decreases the calculation cost on the TPA side This is a direct result of collecting K confirmation conditions into decreases the quantity of very costly paring operation from 2k, as required in individual reviewing, to K+1, by which spares an extensive measure of reviewing time[9].
Information dynamic help is accomplished by supplant data file in calculation of square authenticator and by utilizing extraordinary compared to other information structure i.e. MHT (Merkle hash tree). Supporting information progression for security saving open hazard reviewing is additionally of preeminent significance. Presently we appear how our fundamental plan can be adjusted to expand upon the possible work to help information progression, including square level operations of adjustment, erasure and inclusion.
We can acknowledge this procedure in our outline to accomplish security safeguarding open hazard inspecting with help of information progression. [9]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

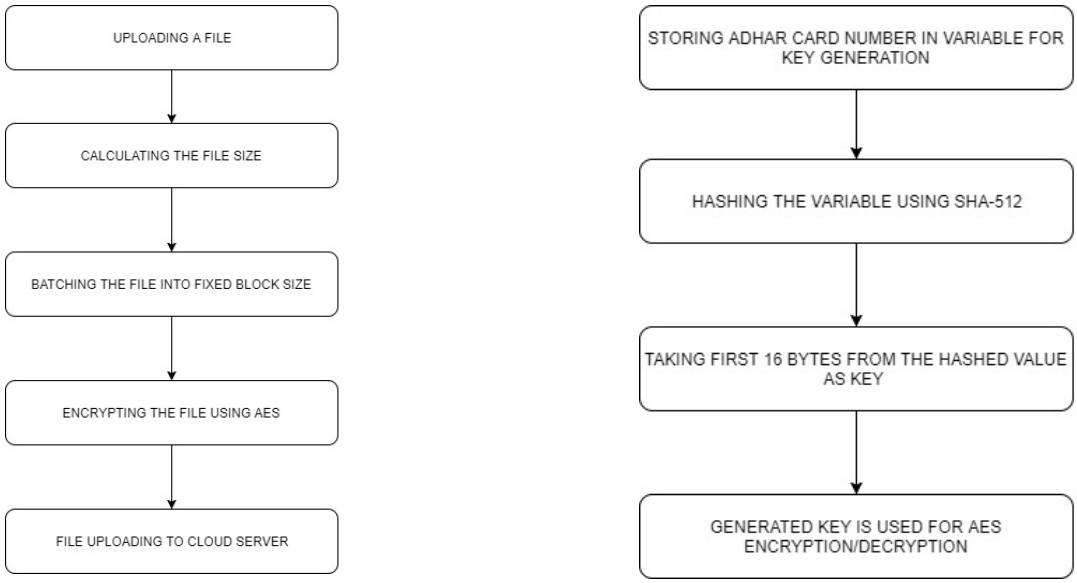

Figure 2: Steps in Uploading a File & Key Management

D. Confirm Module

This module confirm that whether record is interrupted or changed and advise client as needs be by giving alarm messages., additionally log records of the document change are moreover recorded for client perspective. Check module keeps following the cloud information exchange in given time length. We had additionally endeavoured to demonstrate the security by shoe the document change by assailant module. Aggressor module will adjust the substance of the information document and subsequent to executing the confirm module this change is distinguished and followed, and Hence keep away from the record from downloading; we firmly can state that the framework is sheltered.

E. Utilization of AES

We had executed every one of the calculations utilizing AES encryption systems which were already executed as RSA based encryption techniques the advantages of utilizing AES are as decrepit Some factors that are broke down by considering bundle estimate while utilizing AES, by which we expect that our system will give effective outcome then past created framework. Thus, AES encryption and unscrambling speed is a great deal more less and in this manner said to be more effective than RSA. What's more, numerous more advantages of utilizing AES are said in [13].

S. No	Factors Analysed	AES	RSA
1	Key Length	128	1024
2	Simulation Speed	High	Low
3	Power Consumption	Low	High
4	Hardware & Software Implementation	Highly Efficient	Not Efficient
5	Security	Highly Secure	Min Attack

Figure 3: Comparison of AES & RSA

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

F. Utilization of SHA

SHA remains for secure hashing calculation it produces 20 bytes160 bit hash value. This gives message authentications also, jelly the uprightness amid exchange.

Confirmation Requirements:

1) Masquerade – Insertion of message from deceitful source
2) Content Modification – Changing substance of message
3) Sequence Modification – Insertion, erasure and reordering arrangement.
4) Timing Modification – Replaying substantial sessions

IV. RESULT ANALYSIS

After usage of AES instead of RSA alongside secured hash work we got more proficient outcome. With the best encryption system calculation i.e. AES, system should demonstrate the proficient execution in its execution, the security safeguarding ought to be accomplished along these lines, that TPA ought to not request the duplicate of entire information and won't any learning from the information or putting more weight on the end client. The performance of the system is improved by using tomcat server which is easy to handle and has higher processing capabilities. Attacking module used should be able to find Found that compared to individual auditing, batch auditing indeed helps reducing the TPA computation cost by 20 the altered data in the cloud when the data is stored or updated dynamically. As there is less number of expensive operation required for batching such as modular exponentions and multi applications.In the wake of directing group inspecting test with expanded no of undertaking from 1 to 2000, with interims of 8. It was precent.

Total File Size(kb)	No. of blocks of the file(4kb)	Total uploading time using AES(ms)	Total uploading time using RSA(ms)
6.49	2	35181	37586
160	41	18838	33802
628	158	101179	156283

Figure 4: Result Table

We had additionally attempted to bolster information flow alongside protection preserving. Some factors that are examined by considering parcel measure while utilizing AES, by which we expect that our framework will give proficient outcome then past created framework. Consequently, AES encryption and decoding speed is a great deal more less also, consequently said to be more proficient then RSA. What's more, numerous more advantages of utilizing AES are said in [13] The graphical representation of the outcome are appeared in the following graph in which transferring time is spoken to on y-axis,the blue line (Series1) represent the qualities for AES while red (series2) shoes an incentive for RSA, while information measure is spoken to on x-axis,it demonstrates that chart of RSA goes high which demonstrates the required more opportunity for uploading the record then AES. Results are gone up against the framework which has the accompanying setup Intel centre i3 processor,1.66 GHz spped,32 bit working system,2gb Slam ,500gb hard plate. Result may change on various setups.

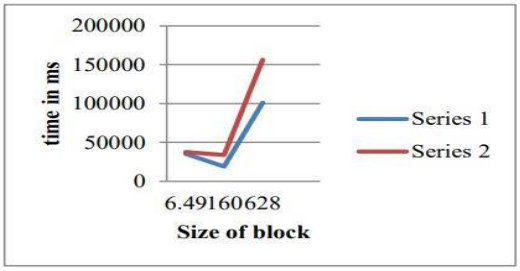

Figure 5: Graph Size of block vs Time(ms)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

V. CONCLUSION

In this paper, we propose a privacy-preserving public auditing system for data storage security incloud computing.Although the computational time is increased but the privacy is preserved the data is stored in the cloud by using the most prominent algorithm AES. We use the homomorphic straight authenticator and arbitrary veiling to ensure that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the load of cloud user from the tedious and possibly expensive auditing task, but also reduces the users fear of their outsourced data leakage.Considering TPA may simultaneously deal with different review sessions from various clients for their outsourced information records, we additionally expand our privacy-preserving public auditing protocolinto a multi-client setting, where the TPA can play out different inspecting assignments in a bunch way for better effectiveness. We had beaten the greater part of disadvantages of the current framework by securing information flow and execution change. General examination demonstrates that our plans are provably secure and profoundly effective. Our preparatory analysis led case further shows the quick execution of our plan on both the cloud and the examiner side. We leave the undeniable usage of the system on business open cloud as a vital future degree.

REFERENCES

[1] Cong Wang, Member, IEEE, Sherman S.M. Chow, Ian Wang, Member, IEEE, KuiRen, Senior Mem-ber, IEEE, and Wenjing Lou, Senior Member, IEEE. ”privacy preserving and public auditing in secure cloud storage” IEEE transaction on 2013.
[2] P. Oreizy, N. C. Wang, Q. Wang, K. Ren, and W.Lou.”Privacy Preserving Public Auditing for Storage Security in Cloud Computing” proc.IEEE INFOCOM 10, Mar 2010.
[3] Q.Wang, C.Wang, K. Ren, W. Lou, and J. Li. ”Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing” IEEE Trans.Parallel and Distributed Systems vol. 22, no. 5, pp. 847-859, May 2011.
[4] K.D.Bowers, A. Juels, and A.Oprea. ”Proofs of Retrievability: Theory and Implementation” Proc. ACMWorkshop Cloud Computing Security (CCSW09).pp. 43-54, 2009
[5] P. Mell and T. Grance.”Draft NIST Working Definition of Cloud Computing”Availableat:hhttp://csrc.nist.gov/groups/SNS/cloudcomputing/index.html”2009.
[6] Cloud Security Alliance,”Top Threats to Cloud Computing” http://www.cloudsecurityalliance.org 2010.
[7] Cloud security alliance” security guidance for critical areas of focus in cloud computing” Available at: http://www.cloudsecurityalliance.org. Inc. Amazon Spot-Instances http://aws.amazon.com/ec2/spotinstances/ Dec.2009.
[8] S.H. Clearwater, R. C.Wang, Q.Wang, K. Ren, and W. Lou. ”Towards Secure and Dependable Storage Services in Cloud Computing” IEEE Trans. Service Computing, vol. 5, no. 2, 220- 232, Apr.-June
[9] Q.Wang, C.Wang, K. Ren, W. Lou, and J. Li. ”Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing” IEEE Trans Parallel and Distributed Systems, vol.22, no. 5, pp.847-859, May 2011. [10] F. Sebe, J. Domingo-Ferrer , A. MartAśnez-Balleste , Y. Deswarte, and J.J. Quisquater. ”Efficient Re-mote Data Possession Checking in Critical Information Infrastructures ” IEEE Trans. Knowledge and Data Eng. vol. 20, no. 8, pp. 1034-1038, Aug. 2008.
[11] M. Stonebraker, R. Devine, M. Kornacker, W.Litwin, A. Pfeffer, A. Sah, and C. Staelin,Proc.Third M.A. Shah, R. Swaminathan, and M. Baker.”Privacy-Preserving Audit and Extraction of Digital Contents ” Cryptology ePrint Archive, Report 2008/186, 2008.
[12] H. Shacham and B. Waters. ”Compact Proofs of Rerievability” Proc. Int Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt) vol. 5350, pp. 90107. Dec. 2008.
[13] ” International journel of science and research india online” ISSN:2319-7064
[14] D. Boneh, B. Lynn, and H. Shacham, ”Short Signatures from the Weil Pairing” J. Cryptology, vol. 17,no. 4, pp. 297-319, 2004.
[15] M. A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, ”Auditing to Keep Online Storage Services Honest” Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS 07), pp. 1-6, 2007