iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** III **Month of publication:** March 2017

DOI: http://doi.org/10.22214/ijraset.2017.3096

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Survey on Privacy Preserving in Authentication Protocol for Shared Authority Based Cloud Computing

Thoke Virendra Dilip[1], Prof. D. O. Shamkuwar[2], Prof. Amol R. Dhakne[3]
[1] *Department of Computer Technology, AITP, Vita.*
[2,3] *Department of Computer Engineering, Flora Institute of Technology, Khopi, Pune*

Abstract: ***Cloud computing is rising as a prevailing information interactive paradigm to appreciate users information remotely keep in an internet cloud server. Cloud services offer nice conveniences for the users to fancy the on-demand cloud applications while not considering the native infrastructure limitations. throughout the information accessing, completely different users is also in a very cooperative relationship, and so information sharing becomes important to attain productive edges. however security and privacy problems have become key considerations in information sharing among the multiple users in cloud storage. so as to avoid of these things, a system is projected during which a shared authority primarily based privacy-preserving authentication protocol (SecCloud) to resolve privacy and security issue for cloud storage..***
Keywords: Cloud computing, privacy preservation, shared authority, AES Algorithm.

I. INTRODUCTION

Cloud services offer nice readiness for the users to fancy the on-demand cloud applications while not considering the native infrastructure limitations. throughout the information accessing, completely different users is also in a very cooperative relationship, and so information sharing becomes glowing to attain productive edges. the prevailing security solutions in the main specialize in the authentication to appreciate that a user's privative information cannot be unauthorized accessed, however neglect a refined privacy issue throughout a user difficult the cloud server to request different users for information sharing. The challenged access request itself might reveal the user's privacy despite whether or not or not it will get the information access permissions. many schemes using attribute-based encoding (SecCloud) are projected for access management of outsourced information in cloud computing. It allows customers with restricted procedure resources to source their massive computation workloads to the cloud, and economically fancy the large procedure power, bandwidth, storage, and even acceptable package which will be shared in a very pay-per-use manner. Despite the tremendous edges, security is that the primary obstacle that stops the wide adoption of this promising computing model, particularly for patrons once their confidential information square measure consumed and made throughout the computation. To combat against unauthorized data leak, sensitive information need to be encrypted before outsourcing thus on offer finish to- finish information confidentiality assurance within the cloud and on the far side. However, standard encryption techniques in essence forestall cloud from activity any significant operation of the underlying cipher text-policy, creating the computation over encrypted information a really exhausting downside. The projected theme not solely achieves quantifiability attributable to its hierarchical data structure. As a result, there do exist varied motivations for cloud server to behave undependably and to come incorrect results, i.e., they will behave on the far side the classical semi honest model

II. EXISTING SYSTEM

There square measure already well-known existing security solutions in the main specialize in the authentication to appreciate that a user's privative information cannot be unauthorized accessed, however neglect a refined privacy issue throughout a user difficult the cloud server to request different users for information sharing. The challenged access request itself might reveal the users privacy. the prevailing systems outline shared authority primarily based privacy-preserving authentication protocol that permits security and privacy within the cloud storage. In this, shared access authority is achieved by anonymous access request matching mechanism with security and privacy issues. Attribute primarily based access management is adopted to appreciate that the user will solely access its own information fields; proxy re-encryption is applied by the cloud server to supply information sharing among the multiple users.

A. Disadvantage of Existing System

The cloud is in and of itself not secure from the perspective of consumers while not providing a mechanism for secure computation outsourcing thus to shield the sensitive input and output data of the workloads. The varied motivations for cloud server to behave undependably and to come incorrect results, i.e., they will behave on the far side the classical semi hones model.

III. PROPOSED SYSTEM

The projected theme are ready to shield user's privacy against every single authority with whole attribute set is split into N disjoint sets and controlled by every authority, so every authority is responsive to solely a part of attributes. thus the projected theme are tolerant against authority compromise, and compromising of up to (N −2) authorities doesn't bring the complete system down. we'll offer elaborated analysis on security and performance to indicate feasibleness of the theme. Shoulder surfing is direct observation techniques, like trying over someone's shoulder, to induce passe-partout and knowledge. Shoulder surfing are provided at intervals the system with SecCloud.

In the projected theme, de-duplication are added wherever the server can store solely one copy of every file, in spite of what number users asked to store that file, relying upon the disc space of cloud servers.

A. Advantages of Projected System

The outsourced computation workloads usually contain sensitive data, like the business money records, proprietary analysis information, or in person diagnosable health data are often secured victimization non-public computing.

IV. LITERATURE REVIEW

Cloud computing is promising data technology design for each enterprises and people. It launches a lovely information storage and interactive paradigm with obvious benefits, as well as on demand self-services, omnipresent network access, and placement freelance resource pooling . Towards the cloud computing, typical service design is something as a service (XaaS), during which infrastructures, platform, software, et al. square measure applied for omnipresent interconnections. Recent studies are worked to market the cloud computing evolve towards the web of services. Later, turning into key considerations with the increasing quality of cloud services. Standard security approaches in the main specialize in the sturdy authentication to appreciate that a user will remotely access its own information in on-demand mode. alongside the variety of the applying needs, users might want to access and share every other's approved information fields to attain productive edges, that brings new security and privacy challenges for the cloud storage. Existing System: the prevailing security solutions in the main specialize in the authentication to appreciate that a user's privative information cannot be unauthorized accessed, however neglect a refined privacy issue throughout a user difficult the cloud server to request different users for information sharing. The challenged access request itself might reveal the users privacy despite whether or not or not it will get the information access permissions.

Proposed System: Aim to integrity auditing and secure de-duplication on cloud data which are achieving using new secure system as SecCloud & SecCloud+[1]. In that, removing of integrity and de duplication done using ABE algorithm said by Jingwei Li,Jin Li,Dongqing Xie and Zhang Cai. Amol D Shelkar, Prof. Rucha R. Galgali [2], proposed Data Privacy issue can be proposed by Anony Control and Anony Control-F attribute entity scheme revocation. In proposed scheme we add user revocation in users to enable activating and deactivating users to enhance efficiency of system and adding more feasibility. Revoked users are maintained in the revoke user list, will decide which user should may in cloud storage server to access data or which will remove. The data access privilege will be depending upon misbehavior of user in cloud server.

Attribute Based Encryption (ABE) is predominantly used to secure the cloud storage. Anony Control-F that inherits from the basic user revocation algorithm. It also facilitates file accessing permission like user grant, file creation, file deletion and user revocation in cloud computing. this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners.[3]. M. Satishkumar,B. UdayKumar,Ch.ArunKumar [4], enhancing Attribute-based Encryption (ABE) is a cryptographic conducting tool to guarantee data owner's direct control over their data in public cloud storage ABE is a public-key based one to many encryption methodologies which allows users to encrypt and decrypt data based on user attributes with various schemes of ABE like KP-ABE, CP-ABE. Anony Control and Anony Control-F, also we analyzed how data access privilege and data sharing can be controlled by using various schemes of ABE.

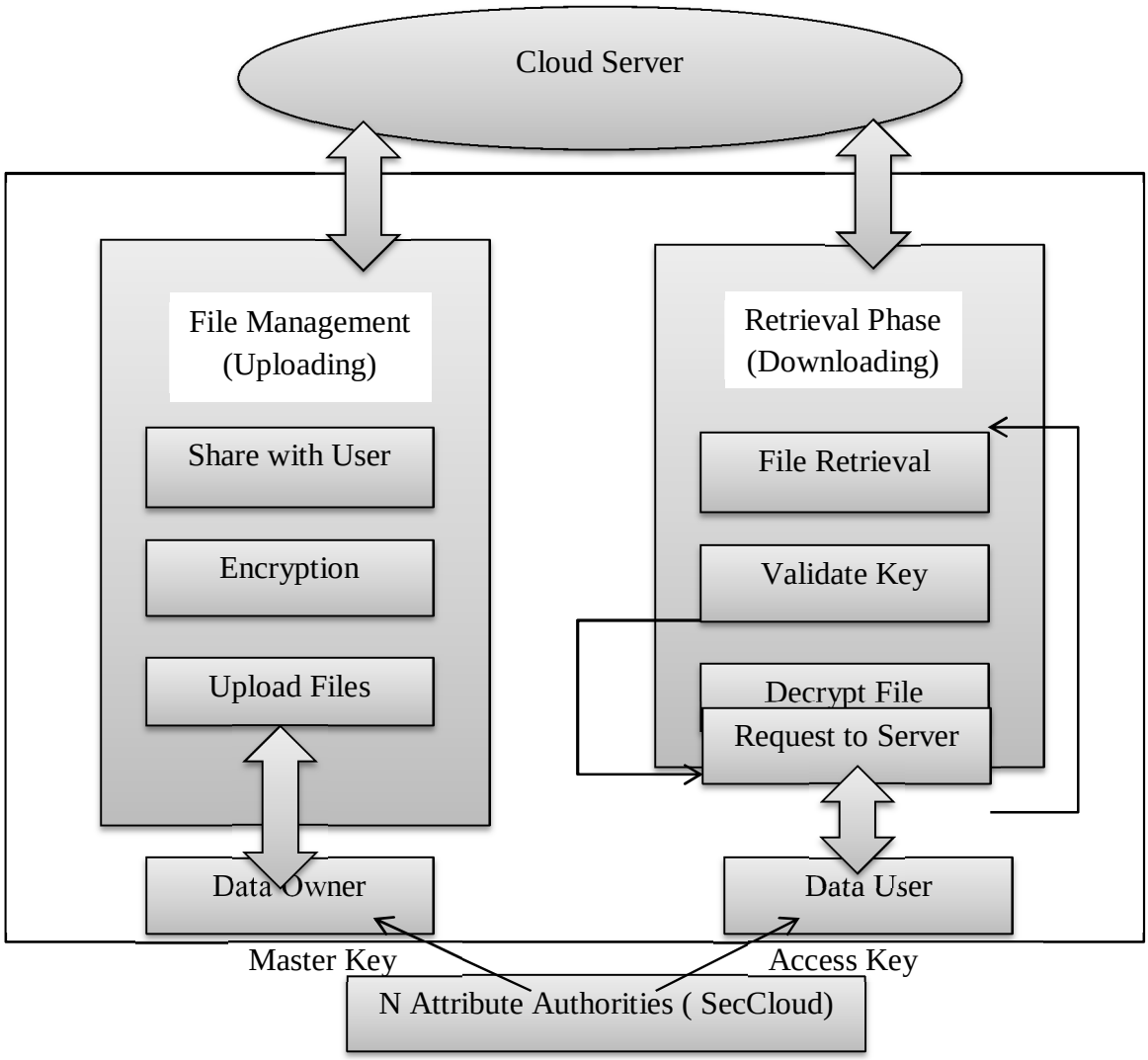
Access control schemes are not feasible in cloud computing because of their lack of flexibility, scalability, and fine-grained access control. This paper extensively surveys all ABE schemes and creates a comparison table for the key criteria for these schemes in

Volume 5 Issue III, March 2017
ISSN: 2321-9653

cloud applications which is proved by Muhammad Yasir Shabir, Asif Iqbal, Zahid Mahammad, and Ataullah Ghafoor[5]. The techniques of Two-to-One Recoding (TOR), and sampling on lattices, we propose a new Key-Policy Attribute-Based Encryption (KP-ABE) scheme for circuits of any arbitrary polynomial on lattices, and prove that the scheme is secure against chosen plaintext attack in the selective model under the Learning With Errors (LWE) assumptions shown by Jain Zhao, Haiying Gao and Junqi Zhang[6]. S. Keelveedhi, M. Bellare, and T. Ristenpart, Dupless [7] provide An architecture that provides secure deduplicated storage resisting brute-force attacks, and realize it in a system called DupLESS. In DupLESS, clients encrypt under message-based keys obtained from a key-server via an oblivious PRF protocol

L. A. Dunning , R. Kresman[8], shown technique is used iteratively to assign these nodes ID numbers ranging from 1 toN. The new algorithms are built on top of a secure sum data mining operation using Newton's identities and Sturm's theorem. An algorithm for distributed solution of certain polynomials over finite fields enhances the scalability of the algorithms. Markov chain representations are used to find statistics on the number of iterations required, and computer algebra gives closed form results for the completion rates. S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg[9] introduce the notion of proofs-of ownership (PoWs), which lets a client efficiently prove to a server that that the client holds a file, rather than just some short information about it. Merkle trees and specific encodings, and analyze their security. We implemented one variant of the scheme.

V. SYSTEM ARCHITECTURE



Above Fig. shows the system architecture where the model of secure scheme is given. Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users' personally

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

identifiable information. The whole attribute set is divided into N disjoint sets and controlled by each authority, therefore each authority is aware of only part of attributes. A Data Owner is the entity who wishes to outsource encrypted data file to the Cloud Servers. The Cloud Server, who is assumed to have adequate storage capacity, does nothing but store them. Data users request access keys from all of the authorities, and they do not know which attributes are controlled by which authorities. When the Data users request their access keys from the authorities, authorities jointly create corresponding access key and send it to them. All Data users are able to download any of the encrypted data files, but only those whose access keys satisfy the privilege tree can execute the operation. The server is delegated to execute an operation if and only if the user's credentials are verified through the privilege tree.

A. Implementation Steps

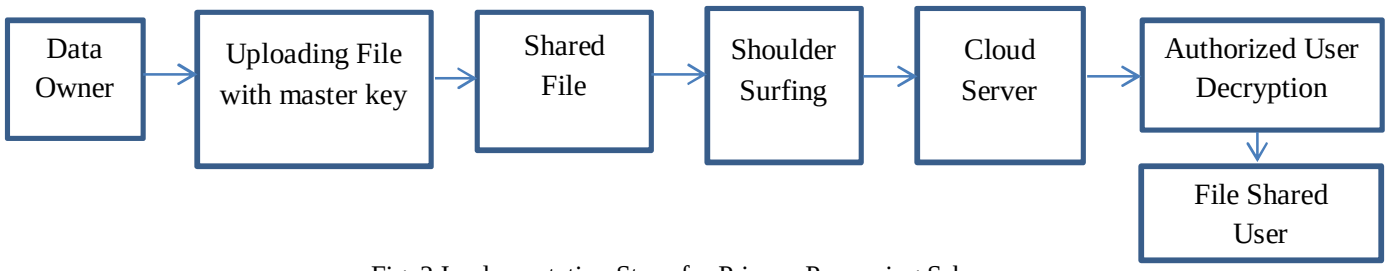


Fig. 2 Implementation Steps for Privacy Preserving Scheme

VI. AES ALGORITHM

Under a wide range of environments, AES performs consistently well in hardware and software platforms. These include 8-bit and 64-bit platforms and DSPs. Its inherent parallelism facilitates efficient use of processor resources and result in very good software performance. AES algorithm has speedy key setup time and good key agility. It requires less memory for implementation and also making it suitable for restricted-space environments. There are no serious weak keys in AES. It supports any block sizes and key sizes that are multiples of 32. The cipher text Statistical analysis has not been possible even after using huge number of test cases. No differential and linear crypt analysis attacks save been yet proved on AES. The fact that the cipher and its inverse use different components practically eliminates the possibility for weak and semi-weak keys in AES, which is an existing drawback of DES. Also, non-linearity of the key expansion practically eliminates the possibility of equivalent keys in AES. Amongst AES, DES and Triple DES for different micro controllers comparison is made then it shows that AES has a computer cost of the same order as required for Triple DES. Another performance evaluation reveals that AES has an advantage over algorithms- 3DES, DES and RC2 in terms of execution time (in milliseconds) with different packet size and throughput (Megabyte/Sec) for encryption as well as decryption. Also in the case of changing data type such as image instead of text, it has been found that AES has advantage over RC2, RC6 and Blow fish in terms of time consumption.

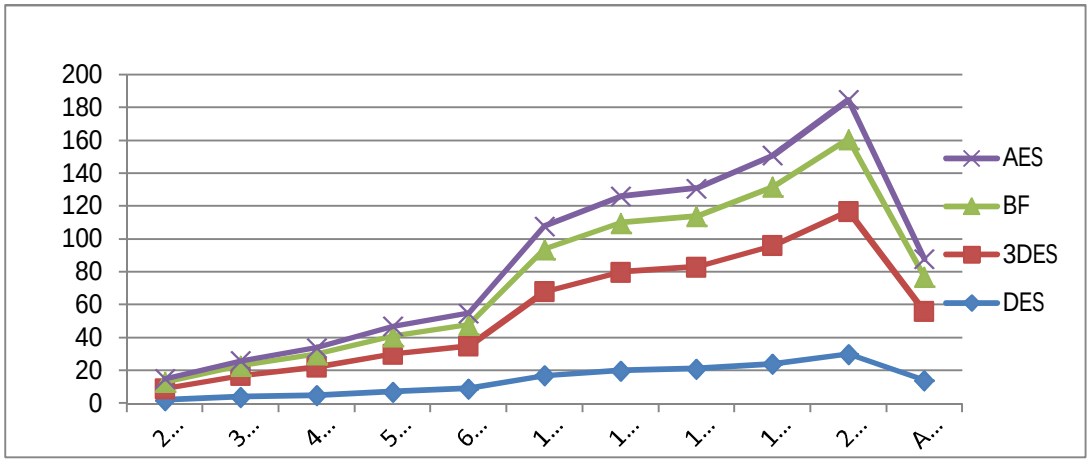


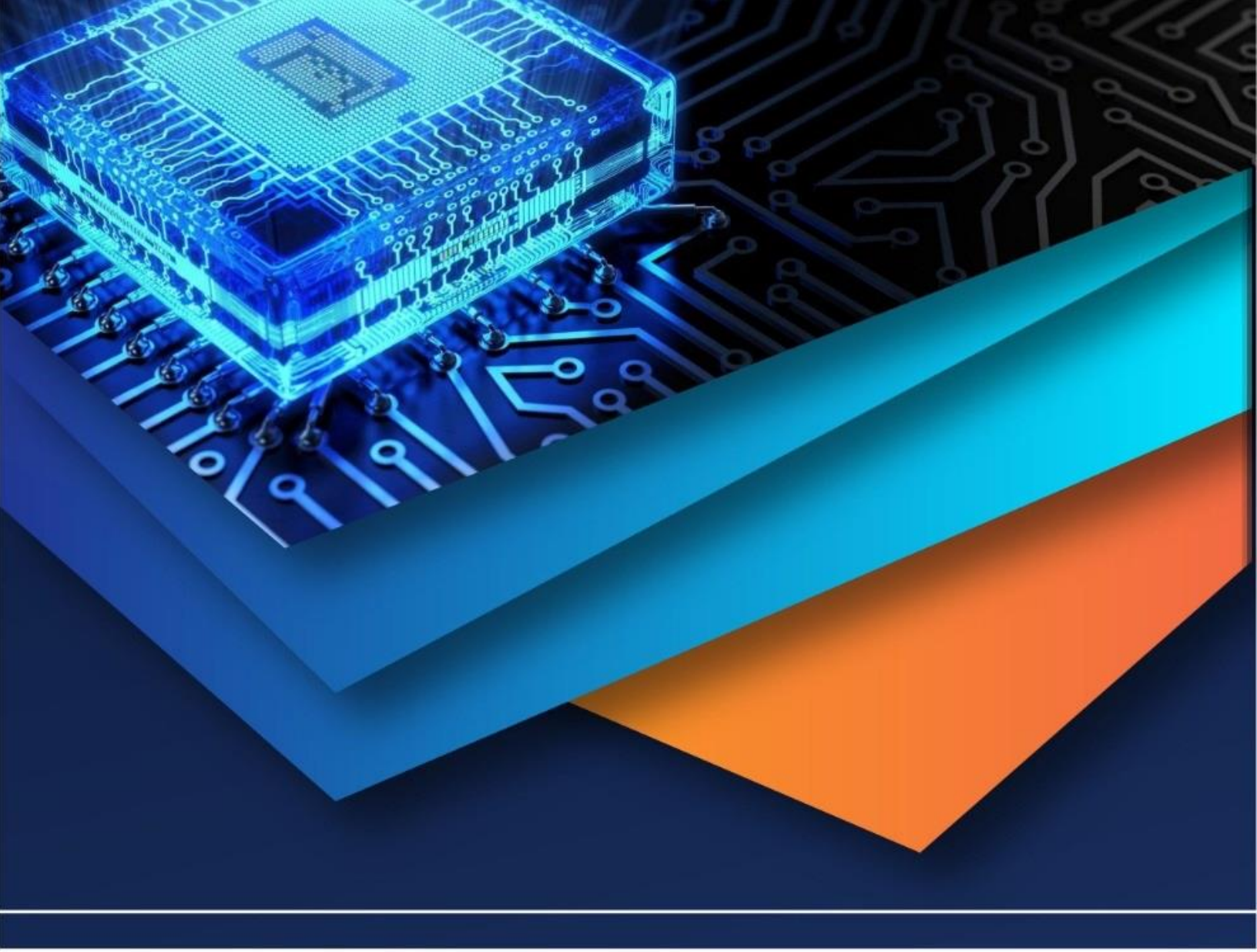
Fig. Comparison of Algorithm

VII. CONCLUSION

A. In our Approach, within the cloud computing to attain privacy-preserving access authority sharing.
B. Authentication is established to ensure information confidentiality and information integrity.
C. Data namelessness is achieved since the wrapped values square measure changed throughout transmission.
D. User privacy is increased by anonymous access requests to in camera inform the cloud server regarding the users access wishes.
E. Forward security is accomplished by the session identifiers to stop the session correlation

REFERENCES

[1] Jingwei Li,Jin Li,Dongqing Xie and Zhang Cai " Secure Auditing and Deduplicating Data in Cloud" DOI 10.1109/TC.2015.2389960, IEEE Transactions on Computers
[2] Amol D Shelkar, Prof. Rucha R. Galgali, " Data Access Privilege With Attribute Based Encryption and User Revocation", International Research Journal of Engineering and Technology (IRJET), Nov 2016.
[3] Praveen N.R and Renju Samuel," Enhanced Efficient User Revocation Mechanism on Top of Anonymous Attribute Based Encryption" , International Journal of Emerging Technology in Computer Science Electronics, AUGUST 2016.
[4] M. Satishkumar,B. UdayKumar,Ch.ArunKumar,"Attribute Based Data Sharing with At tribute Revocation to Control Cloud Data Access", International Journal of Computational Science, Mathematics and Engineering, February-2016
[5] Muhammad Yasir Shabir, Asif Iqbal, Zahid Mahammad, and Ataullah Ghafoor, " Analysis of Classical Encryption Techniques in Cloud Computing" , ISSN 1007-0214 09/10 pp102-119 Vol. 21, Number1, February 201
[6] Jain Zhao, Haiying Gao and Junqi Zhang," Attribute-Based Encryption for Circuits on Lattices ", ISSN 1007-0214 05/13 pp463-469 Vol. 19, Number 5, October 2014.
[7] S. Keelveedhi, M. Bellare, and T. Ristenpart, Dupless:" Server aided encryption for de-duplicated storage" , in Proceedings of the 22Nd USENIXConference on Security, ser. SEC13. Washington, D.C.: USENIX Association, 2013, pp. 179194
[8] L. A. Dunning and R. Kresman," Privacy Preserving Data Sharing With Anonymous ID Assignment " , IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 402413, 2013
[9] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Proofs of ownership in remote storage systems, in Proceedings "of the 18th ACM Conference on Computer and Communications Security. ACM, 2011, pp. 491500.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY