iJRASET
International Journal For Research in Applied Science and Engineering Technology



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 6 **Issue:** V **Month of publication:** May 2018

**DOI:** http://doi.org/10.22214/ijraset.2018.5415

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887*
*Volume 6 Issue V, May 2018- Available at www.ijraset.com*

# A Multiuser Model of Privacy-Preserving Auditing for Storing Data Security in Cloud Computing

Akash Udaysinh Suryawanshi[1], Dr. J. Naveen Kumar[2],
[1, 2]*Department of Computer Engineering, Bharati Vidyapeeth (Deemed to be University), College of Engineering, Pune, India.*

***Abstract*: *In cloud computing frequently referred to as basically, the concept of data security for accessing the data to control effectively. These systems give a secure cloud storage environment for privacy preserving mechanism. The data integrity accessing method is a very effective for the information which is stored in the cloud storage system, so data outsourcing mechanism to allocate in cloud server or each unauthorized user. Typically, cloud computing described as just "the cloud computing" as the conveyance of request processing of the information. yet, for security auditing process of this shared information in cloud, to save the identity information of the users remaining part is the big challenge. This paper presents the best method of this system for privacy preserving so as to authorize the reviewing data of the users in cloud storage. That's why, we easily access the shared information in the cloud. This system truly focuses on the verification of data is necessary for reviewing process to check the integrity of shared data. During this system, the signature identity method is processed for every chunk is stored as securely as a TPA.The final output observed in this system confirms the integrity of data on that system though reviewing the common data which are present in cloud.***

***Keywords***: ***Cloud Computing, Cryptography, Data integrity, Privacy-Preserving, Third-party public auditing etc.***

## I. INTRODUCTION

Initially in cloud computing this paper proposes, to satisfy the requirement of data storage ability for processing the data in cloud server also need the data outsourcing for data owners. Thus, cloud service provides the services of data integrity, but the safety of owner's data is still most important concern while storing and accessing information in cloud storage. In cloud storage system to produce the most significant security related problems to easily access the information. To maintain the integrity of data in cloud storage, however, is subject to skepticism and scrutiny. This is only because as the information stored in cloud storage can be easily lost or corrupted on any system platform. To maintain the reliability of information on cloud, third party auditor (TPA) is introducing that best method to perform public auditing so it's reviewing process offers with great computation as well as conversation capacity of that common authentication of clients. Cloud computing has turned into a very important part of IT industry.

The user can store his information on cloud and recover it at whatever point he needs to develop it. This maintains a strategic distance from the cost of information support and there is no compelling reason to actually store information on one's pc. Every individual from the gathering can get to information through the web and there is no compelling reason to make various duplicates of information for individual users. In cloud computing this type of model brings numerous security challenges like information privacy, verification, and access control.

At that time, when information is put away on the cloud then honesty of that information is being put in danger because of following reasons. To begin with, cloud framework is solid than individualized computing gadgets however it has numerous issues like inner and outer dangers to information honesty Second, if information isn't gotten to or once in a while got to then this information can be disposed of by cloud specialist organization and they shroud this information misfortune to keep up the notoriety. Third, cloud is financially alluring for huge informational indexes however does not give information trustworthiness ensure, here it is important to give uprightness to data put away on the cloud. At the same time as clients never again physically have the capacity of consumer information; the information reliability is not a valid collection of knowledge therefore presently downloading each one of the information because of the price of input /output operation or cost of sending request under the overall system.

The responsibility of information correctness is very costly for outsourced transmission of information. Particularly; clients might not have any desire to experience the intricacy in checking the information trustworthiness. Open inspecting administration (Third Party Auditor) is actualized to reduce client's multifaceted nature and guarantee information uprightness. Outsider assessor (TPA) has capacities to verify the trustworthiness of the information put away inside the cloud that is semi-trusted gathering data for clients.

©IJRASET: All Rights are Reserved

So it is important to give integrity to data put away on cloud without uncovering client's information and character which is called privacy preserving auditing.

## II. RELATED WORK

In this proposed system we define the method of preserving the information security is a new significant attribute in a cloud environment. This cloud infrastructure utilizes sharing the information. So cloud is a common server on that system.

Therefore, the data might look a major possibility of a declaration or any access by unauthorized users. In this system we have been sharing the information on cloud resources with the help of user's security purpose is a most demanding challenge.

So distributing a secure method of Multi-tenancy in the cloud server, separation of information is required to make sure all customer data have divided from others information.

When the information is transferred between other countries, so it could face various types of policy and authorized system on cloud storage. Facts of information integrity can be used for providing the users security and performing protection mechanism of knowledge.

This author [1] predictable a protected cloud storage framework methodology of supporting security preserving open inspecting and performs reviewing for different users at the same time.

In this paper the expected system of privacy conserving examining of private knowledge gives security to knowledge in cloud server and also checks the exactness of information. This system utilizes AES secret writing formula used for encoding the information by putting away in the cloud server.

We used SHA1 formula for checking reliability of information on the way to approve capability accuracy of information. User will confirm trustworthiness of their knowledge that holds on the cloud server utilization TPA.

This author [2] gives the effective method of dynamic provable data possessions (DPDP) which are based on category information with the use of authenticated users.

In this paper, the author decrease the storage information of those signatures of their common reviewing mechanism for the shape of device this is exploited. In addition to the author used index hash tables for clients to offers active operations.

This approach makes use of public mechanism proposed throughout is able to preserve customers private records from the TPA. Similarly, to function a couple of reviewing duties from distinctive users correctly, they completed their mechanism of system to permit auditing by TPA for the information of cloud.

Those Authors [3] has proposed best methodology of machine for providing auditing facts which is stored on cloud server. In addition to offerings without load of neighborhood statistics capacity, the cloud computing offers on require best utility of data and protection but information is now not in user ownership, then presenting reliability is a powerful scheme.

On this manner authors advocate a at ease cloud garage gadget helping privacy maintaining free reviewing and perform inspecting for many users simultaneously.

The assignment of reviewing the facts exactness in cloud surroundings can be privacy meant for big length outsourced facts. Specifically, customers might not have any desire to experience the many-sided quality in confirming the statistical reliability public reviewing service be applied to reduce the user's problem and assurance facts of reliability.

## III.SYSTEM DESCRIPTION

In the presented system we define two effective methods of system which are very important for authentication purpose. In this system we design workflow of this privacy preserving method to easily provide secure cloud storage infrastructure for a cloud. In this paper, we used the data integrity method for secure data stored on the cloud.

In this system we used AES algorithm for privacy preserving data on that server. In this workflow of system, the user first login into application. After login successful User has done authentication with the help of secret key which is sent in Email, so verification done by the user.

After that authentication data owner has file upload operation performing on server with the help of the AES Encryption algorithm, then get better security for this algorithm of encryption. Again the users download operation also performing on that server.

That's why we get proper privacy preserving mechanism through this effective system. In this way; we implement this useful system for future purpose. We implement the system workflow (Fig: 1) is as given below:

©IJRASET: All Rights are Reserved

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887*
*Volume 6 Issue V, May 2018- Available at www.ijraset.com*

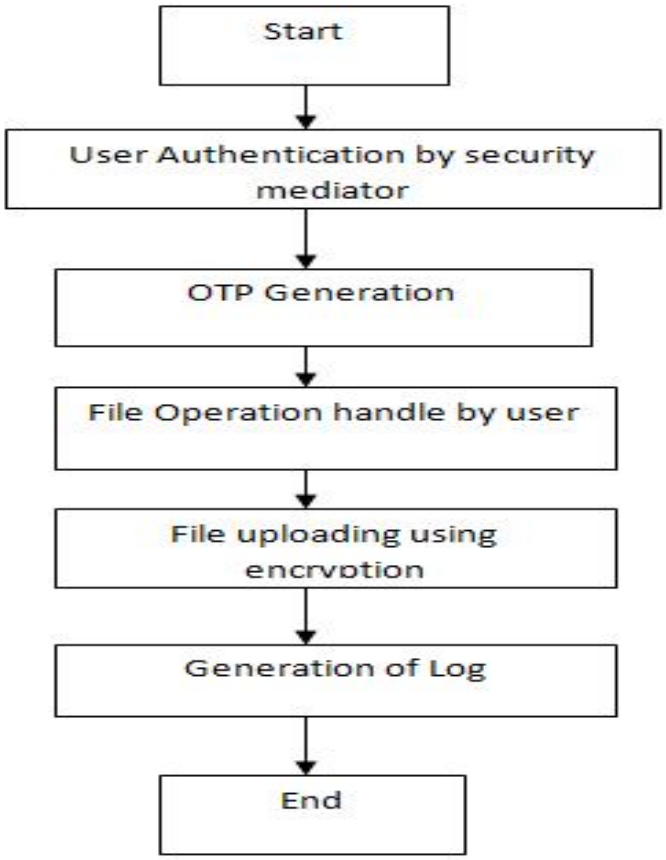



Figure 1: System workflow

We implement a few module of system which is described in given below:

*A. Authentication-Secret key Generation*

This type of module has to Implement an interface for authentication of user interaction. For system, application has been developed to register users to record of entries verification with cloud system. When executing an application, the user has entered the username, password, address, age, mobile no and email id for successful registration of user. When a user enters in the authentication module then user login into the system through providing his credentials. The key generation module is required the information owner characteristics that generates a secret key which is sent on email id once user registers into the system. After that system executes the successfully and authentication of user for key generation. So the user is ready to login in to the cloud system when Successful authentication of user for generation of secret key.

*B. Formation of File Upload and Download*

This module of the system handles completely different groups for various information. Using this module owner will upload information and consumer will download that same information. The information upload and download operations are finished by data owner for sharing information. At the same time, once user authentication done data owner upload the information. In this module encoding done using an elgamal encoding method and also the same time each key sends to TTP and AAs.

*C. Data chunk*

Data chunk mechanism defines a portion of information which is utilized for various multimedia samples like as PNG, IFF, MP3 and AVI.Every chunk in that system which consist of a header that indicates different specifications (E.g.: type of chunk, comments and size of information).In this term, there is a variable region which incorporates the data that are decrypted by the program from that specified requirement in the description. Data chunks can also be a very significant particle of information which is downloaded

©IJRASET: All Rights are Reserved

by P2P programs. In cloud computing system, a chunk is place of the information which is sent to a processor or any parts of the computer devices for processing the information. For Ex: a sub-set of rows of a matrix.

In this system, Chunk is managing the information on cloud and packet set used in Stream Control Transmission Protocol (SCTP).The SCTP packets are composed of shared headers and chunked information vary by continuously, so data chunks are described in RFC 4960, which update the version of RFC 2960 and RFC 3309.In below shows how to chunked the data in multidimensional shape.

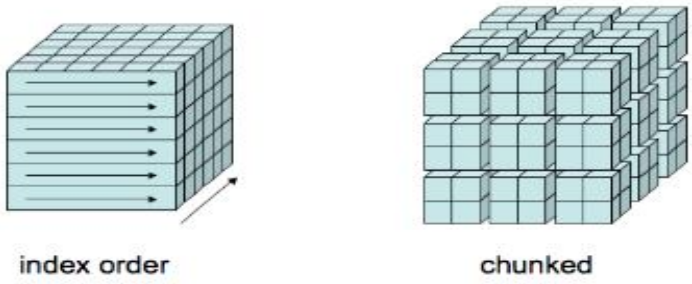



Figure 2 :Examples of data chunk

*D. Benefits of Chunking*

In this chunking method, we observe that the chunking of data is processed by user. Huge performance of the system extends or sufficient with excellent choices of chunk shapes and sizes increased in cloud system. That's why data chunking with supports to expanding the multidimensional information nearby various axes and efficient, per-chunk compression of data. So widely used this chunking method for processing of data. Therefore, processing a subset of a compressed variable cannot need uncompressing the entire variable are present in this system. For this purpose, we efficiently use this chunking phrase also described some benefits of chunking are given below:

*1)* The instruction required for this method is how to select chunk shapes and sizes for exact patterns of data access is missing.
*2)* Failure chunk shapes and sizes are presented for collection of data like as netCDF-4 and HDF5.So it work appropriately in a proper manner.
*3)* This is very expensive to revise the huge datasets of information that using for typical adjacent layouts of data to make use of chunking principle. EX: Chunking a 38GB variable can acquire hardly 20-30 Minutes.

Last of all, the operating expense mechanism of the chunk data describes that we either have to acquire it correctly when the information of data is produced, but the data are very sufficient for that reason of the rate of a rechunking scheme for various study accesses is necessary. In order to, we would like to believe receiving a cloud computing stage with the help of a lot of memory, presently for the rechunking of data principle is more important to the different datasets which are used for chunking entire process.

*E. Challenges*

*1)* Internal and external warnings to data integrity.
*2)* Information loose due to hardware failure or cloud gap management for Non data backup mechanism.
*3)* Privacy loss due to data patterns for profit intent.
*4)* Data corruption with no recovery mechanism. i.e. Stock market data or shop store records.
*5)* Large calculation in the verification process for multiple user request in time complex and requires effective scheduling**.**

*F. Algorithm*

*1)* Encryption of Input file: encryption key + AES
*2)* Decryption of file: encrypted file + decryption key
*3)* Signature Generation: Run by client
*a) Input:* File Blocks F, secret key, generator g
*b) Output:* set of signature Φ.
*4)* Generate Proof: Run by cloud storage server
*a) Input:* Subset of file blocks mi, coefficient i
*b) Output:* Proof P

©IJRASET: All Rights are Reserved

## IV. CONCLUSION

We have implemented the effective method of privacy preserving public auditing mechanism for shared information in the cloud storage and check the correctness of information of the system. We handle the structure of the AES encoding algorithm for encoding the information by putting away it in the cloud storage system. Also, we can handle digital signature to organize homomorphism authenticators, so the TPA can review the integrity of common information. That's why, we improve the efficiency of verification for various reviewing tasks, and we further expand our mechanism to support groups of reviewing the information. And also we are planning to implement our proposed system on cloud servers. This result presents the efficiency of implementing work on this cloud storage system.

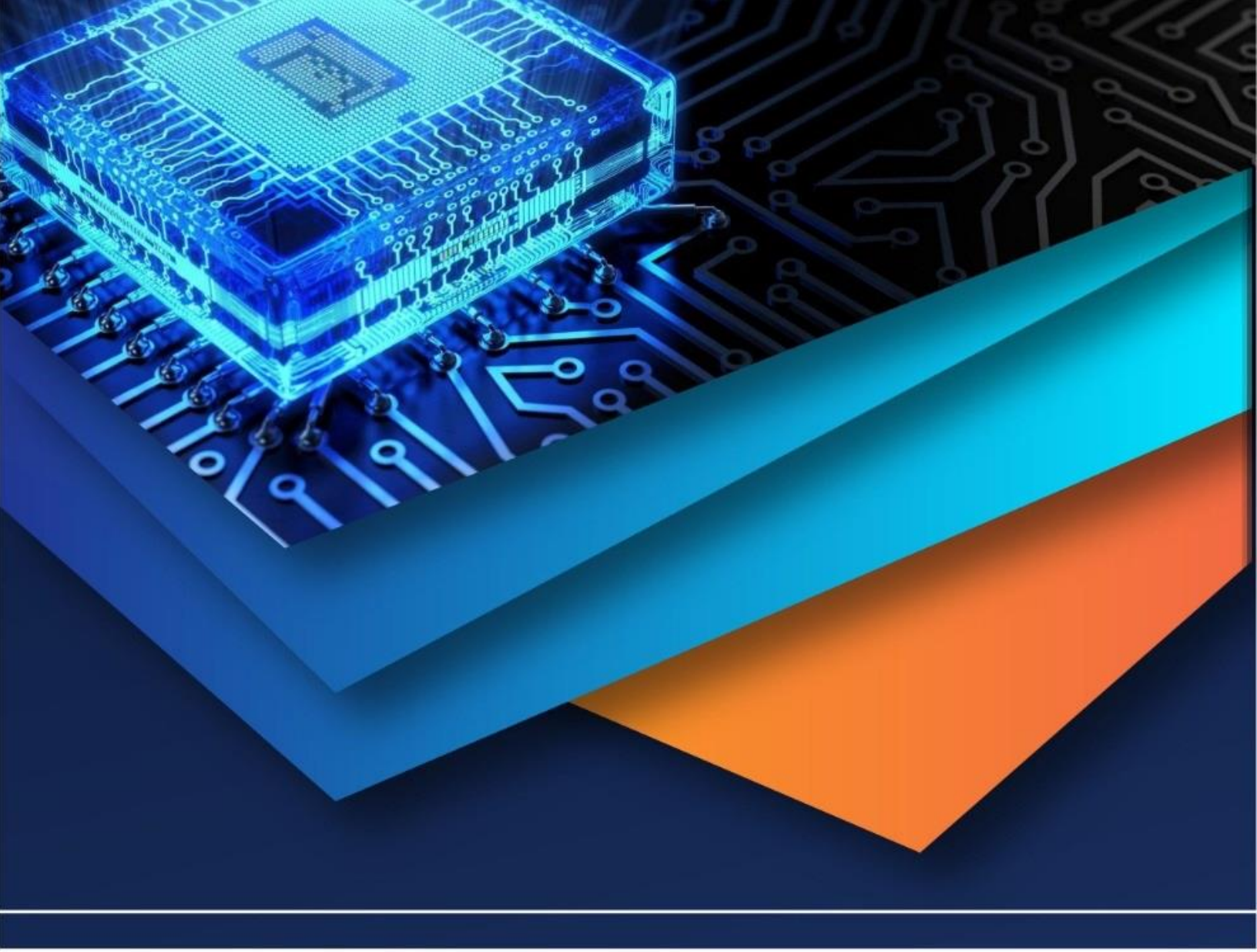
## V. ACKNOWLEDGMENT

To prepare proposed methodology paper on "A Multiuser Model of Privacy-Preserving auditing for storing data security in cloud" has been prepared by Akash Udaysinh Suryawanshi and Dr.J.Naveenkumar. Author would like to thank my faculty as well as my whole department, parents, friends for their support. Author has obtained a lot of knowledge during the preparation of this document.

## REFERENCES

[1] Ms. Kalyani B. Ghutugade, Prof. G. A. Patil, "Privacy preserving auditing for shared data in cloud", 2016 International Conference on Computing, Analytics and Security Trends (CAST) College of Engineering Pune, India. Dec 19-21, 2016.
[2] Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE:" Privacy-Preserving Public Auditing for Shared Data in the Cloud system", IEEE TRANSACTIONS ON XXXXXX, VOL. X, NO. X, XXXX 2012.
[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 525–533.
[4] X. Liu, B. Wang, Y. Zhang, and J. Yan, "Secure multi owner data sharing for dynamic groups in the cloud," IEEE Computer Society, vol. 24, no.6, June. 2013.
[5] S. Pearson, "Privacy, Security and trust in cloud computing," in Privacy and Security for Cloud Computing, ser. Computer Communications and Networks. New York, NY, USA: Springer, 2013, pp. 3–42.
[6] Henry C.H, Chen, Patrick P.C., Lee, "Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014.
[7] B. Wang, Sherman S.M., Chow, M. Li, H. Li, "Storing Shared Data on the Cloud via Security-Mediator", 2013 IEEE 33rd International Conference on Distributed Computing Systems
[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," Proc.IEEE INFOCOM, pp. 534-542, 2010.
[9] Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong, TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage, IEEE Transactions on parallel and distributed systems, VOL.24, NO. 06, October 2016.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)