ARTICLE

PRIVACY-PRESERVING FOR A SECURE DATA STORAGE ON CLOUD USING PUBLIC AUDITING TECHNIQUE

Akash Udaysinh Suryawanshi*, J. Naveenkumar

Department of Computer Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, INDIA

ABSTRACT

In this paper, we describe the data security term as more important on the cloud, for the efficiently access control mechanism of information to preserve it. The data accessing mechanism are a very important method present in the cloud storage, so the data outsourcing is authorized on the cloud server for verification of information or various unauthorized users. Basically, cloud computing is utilized in request processing of data and access that request for preserving information. Cloud is used for putting away information it may be shared by various users. All time it is not possible to access all information and verify reliability, so is proposed to contain TPA to confirm the correctness of shared facts of that system. Data Security is done authentication of that the TPA could not obtain client's knowledge from the information captured along with the verification of inspecting process. However, for the security reviewing process of that shared information, to preserve the identification of user remaining part is the open challenge. This paper proposes the system for security preserving so as to permit reviewing the information of clients for common information access in cloud storage. These systems focus on the verification of information is necessary for auditing to check the correctness of common information. The reliability of this mutual information of the TPA can verify secretly without retrieving whole information. The Final output achieved through this experiment proves the capacity of this executed system while reviewing shared information

KEY WORDS
Cloud Computing, Cryptography, Data integrity, Privacy-Preserving, Third-party public auditing etc.

INTRODUCTION

In cloud computing, we efficiently satisfy the requirements of the information for storage capacity to preserve in the cloud system and provide the data outsourcing service for data owners. Thus, cloud service provides this service, but the safety of owner’s data is still most important concern while storing and accessing information in cloud storage. To provide security for information access is the most important problem in cloud storage. To maintain the integrity of data in cloud storage, however, is subject to skepticism. This is only for 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 the best method to perform public auditing so it’s reviewing process offers with great computation as well as conversation ability of that common authentication of clients. Cloud computing has turned into a very important part of IT industry. Application programming, database and touchy data user can store on a cloud.

The user can store his information on cloud and recover it at whatever point he needs to utilize 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. All individual from the gathering can get to information through the web and there is no credible reason to make various duplicates of information for individual users. The extraordinary requirement is used for the information protection and the capacity to search information, putting away information on the cloud without losing character Security.

Received: 27 May 2018
Reviewed: 16 July 2018
Accepted: 21 July 2018

The system shows the best methodology of provable data possession (PDP) technique to execute common reviewing information so the user to confirm the integrity of knowledge. This also helps to validate the correctness of information left out recovering the whole information which is stored on cloud system. The multiple users are sharing information among other users to motivate for cloud system. This may be very important features for clients. During the process of public auditing the single problem of system highlighted for collective information is stored on cloud system, so as to save identification of privacy from TPA.A particular user in the group which indicates the shared information for identities of signatures of users.

RELATED WORK

This author [1] presented 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 the information. This system utilizes AES secret writing formulas used for encoding the information by putting away the cloud server. We used the SHA1 formula for checking the reliability of information on the way to approve capacity accuracy of information. The user will confirm the trustworthiness of their knowledge that holds on the cloud server utilization TPA. Putting away knowledge can produce the acute would like in favor of knowledge Protection on the cloud and also the capability to look knowledge while not losing identity, privacy. Limitation of this implementation is that it doesn't keep the initial knowledge chunks as in systematic committal to writing schemes.

***Corresponding Author**
Email: akashsuryawanshiak@gmail.com
Tel.: +91-7720001020

The 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 decreases 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 offer active operations. This approach makes use of public mechanism proposed throughout is able to preserve customers' private records from the TPA. Similarly, they finished their mechanism of system to permit auditing by TPA for the information of cloud.

This Author [3] has proposed best methodology of machine for providing auditing facts which are stored on cloud servers. In addition to offerings without load of neighborhood statistics capacity, the cloud computing offers on requiring best utility of data and protection, but the information is now not in user ownership, then presenting reliability is a powerful venture. On this manner authors advocate an at ease cloud garage gadget helping privacy maintaining open reviewing and perform inspecting for numerous users simultaneously. Specifically, customers might not have any desire to experience the many-sided quality in confirming the statistics, reliability public auditing services (1/3 celebration inspector) be applied to decrease user's complications and guarantee facts reliability.

In this paper authors [4] proposed that cloud computing gadget affords a cost-effective for sharing grouping of cloud clients. In this paper, the authors suggested that ease multi-proprietor information sharing system methodology for active agencies inside the cloud server. As a result of utilizing the organization name and active communication encoding strategies, user cans percentage information namelessly through others. Meanwhile, the capacity in the clouds and encoding estimated value of this system is impartial throughout the range of repudiated cloud users.

The author [5] proposed the exceptional technique of sharing information in a multi-proprietor manner at the same time as maintaining data together with the identification of security from an allocated cloud is a most demanding problem of the system. In this method, we propose a multi-proprietor record of the system is stored in the cloud storage system for active corporations of the authorized user. As a result of utilizing the organization name and active communication encoding strategies, users can percentage information secretly through others. Meanwhile, the capacity in the clouds and encoding estimate value of this system is impartial throughout the range of repudiated cloud users.

This Author [6] conveys a machine with fundamental encryption and decoding strategies for supplying safety of this system. In repudiation, the unique records are first separated into various cuts, after which posted to the cloud system. The repudiation method is accelerated via disturbing handiest one portion accordingly in place of the complete facts. We have proposed a unique procedure for using the cloud storage to recover the information.

In this paper, [7] the author proposed the effective method of auditing structure for cloud system to understand the procedure of the complete system. Also proposes privacy preserving identity protocol for cloud storage. After this they expand their auditing mechanism to support the information of active operations that provably comfortable inside the random version of the system. The analysis and simulation result proves that their method of reviewing formalities is safe as well as especially it can reduce the estimated value of that inspector. It's far not possible for their scheme to help a systematic review for various proprietors, which substantially improves the overall performance of the system.

Those authors [8] have proposed to layout and implement a scalable and first-class-grained information get admission to system with KP-ABE method. The information title-holder makes use of an unsystematic key to encode a document, in which the unsystematic key is similarly encoded with a position of properties utilizing KP-ABE. At that point, the institution supervisor assigns a right to use shape and the relating secret key to approved customers, with the end goal that a consumer can handiest decode a secret message textual content condition and handiest on the off chance that the information documents properties fulfill the get right of entry to structure.

These authors [9] proposed an efficient method to get right of access to control the system of cloud storage for easily access information for authentication. This carries an individual factor of the block on each single safety or performance problem of a system towards unauthorized permission for every predefine characteristic. Very first layout of system is multi-authority access control structure addresses the problem via proposing the threshold (t, n) difficult for authentication of user verification or multiple user of this CP-ABE system. After this system proposes and realizes a strong and verifiable multi-authority to get right of entry to manipulate the machine in public cloud storage. A couple of scheme combines manage a uniform attribute used to access information.

ISSN: 0976-3104

MATERIALS AND METHODS

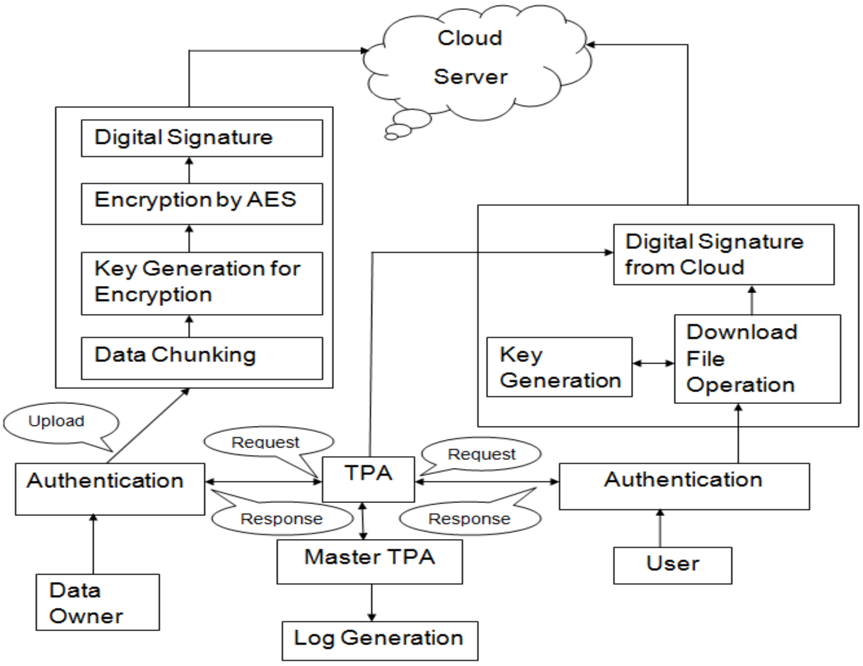

Fig. 1: System architecture

Modules Description

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 for record of entries verification with cloud system. When executes system, user has entered the username, password, address, age, mobile no and email id for successful registration of user. When the user is going in the authentication module then user login into the system through providing his credentials. So system verifies user confirmation for authentication of this user credentials. Key generation module is required the information owner characteristics that generates a secret key which is send on email id once user registers into the system. After that system executes the successfully and this module work properly. The system architecture is given in Fig-1.

Formation of file upload and download

This module handles completely different groups for various information. Using this module data owner will upload information and user will download that same information. The information upload and download operations is 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 elgamal encoding method and also the same time each key send to TTP and AAs. Lastly, user will offer the transfer request to cloud server for downloading the information, at the same TTP and AAS at verification has done on cloud.

Digital signature generation

This signature generation module is selected to analyze verification of information by user. Third party auditor needs authentication of information for verification of data integrity. So this module implements secure hash algorithm for finding hash function as verification of data. This type of function implements the efficient method or effective algorithm of signature generation. This algorithm taken as an input of information partition and generates hash value from hash function for each partition of data. So this module executed effectively for signature generation of data.

TPA (Third party Auditor)

This is final module of system. This module has represented to execute third party auditor (TPA), united nation industry verifies the information integrity of system. Once user will verify the information then he /she sends request to TPA.TPA generates a method by using theoretical information (file id, SHA1) that is hold on by data owner through information upload on server. As a result of verifying that proof, auditor

IIOAB JOURNAL ISSN: 0976-3104

involves realize reliability of that requested information. For data integrity verification of SHA1 algorithm is implemented in this system. Reviewing method are implemented in four parts like reviewing request, challenge generation, proof generation and verifies confirmation of data which is shown in following tasks:

- User sends the reviewing request to TPA.
- TPA sends reviewing message to cloud server as the same as information id.
- Auditing proof-cloud server responds with hash function of specific information .TPA compares cloud servers response hash with TPA stored in database hash of requested information.
- Reviewing report-whether information is degraded or not.

RESULTS

The final result of the implemented system shows that, we used following attributes for comparative analysis: After implementing several part of the system we have got system performance of this project. In this way we get results of this system, firstly user will register in that system then registered user only login into the system. After login successfully done, the user will again login into the system with a secret key. So information is secure on cloud server with the help encoding data stored in this cloud storage. The output of this system is divided into the following steps:
1. Encoded information and secret key are stored separately on cloud storage media.
2. Then decoding the information of file user have to enter OTP which is sent on authorized user e-mail and combination of OTP, So encoded information are used to generate original information on that system. This information is secretly saved in cloud so users easily access that information through database.
3. For accessing the information of the user is limited in read only mode and for insert, modify and delete the notification is sent to admin for preserving the security of the system.
4. Then encoding or decoding the original information is deleted.
5. For protecting the system, we are eliminating the TPA. The flow of the TPA will be done by admin and our proposed system. The user will easily upload that information and download the information on the server for data security. In this way, the secret information is stored on cloud server for preserving privacy of data integrity. The final result of the comparative analysis of this system is shown in following table [Table 1] so we design the appropriate graph [Fig. 2] of system which is based on following [Table 1]

Table 1: File size with respect to time (ms)

File Name	size	AES	DES
File1	84kb	199.014	20.0012
File2	15kb	48.027	3.0002
File3	1kb	40.0022	2.0001
File4	11kb	45.0026	6.0003
File5	207kb	161.0092	10.0006

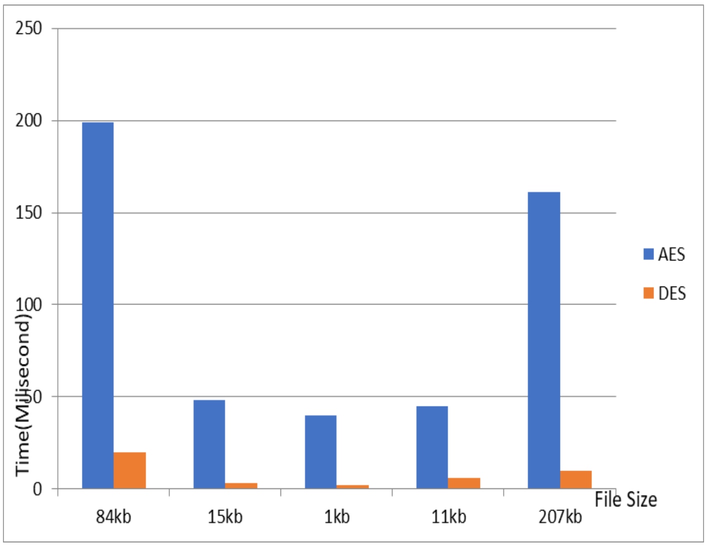

Fig. 2: Graph of performance result and analysis

CONCLUSION

As a result, we obtain the first publicly verifiable secure cloud storage framework which is secure without using the random method. Further, we improve our general structure to support user secrecy and third-party public auditing. To recover the efficiency of verification for various auditing tasks, we further expand our mechanism to support reviewing of data. One of the positive future works is to introduce, how to check the reliability of common information with effective groups, though still preserving the singularity of all blocks from the third party auditor in cloud system and also we are planning to implement our proposed system on the cloud storage system.

CONFLICT OF INTEREST

There is no conflict of interest.

ACKNOWLEDGEMENTS

To prepare proposed methodology paper on “Privacy-Preserving public auditing for secure data storage technique in cloud computing” has been prepared by Akash Suryawanshi and Dr.J.Naveenkumar Author would like to thank my faculty as well as my entire department, parents, friends for their support. Author has obtained a lot of knowledge during the preparation of this document.

FINANCIAL DISCLOSURE

None

REFERENCES

[1] Ghutugade KB, Patil GA.[2016] Privacy preserving auditing for shared data in cloud, 2016 International Conference on Computing, Analytics and Security Trends (CAST) College of Engineering Pune, India.

[2] Boyang W, Baochun L, Hui L. [2012] Privacy-Preserving Public Auditing for Shared Data in the Cloud system, IEEE International Conference on Computer Communications, 124-230.

[3] Wang C, Wang Q, Ren K, Lou W. [2010] Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, in Proc. IEEE International Conference on Computer Communications (INFOCOM), 525–533.

[4] Liu X, Wang B, Zhang Y, Yan J. [2013] Mona: Secure multi owner data sharing for dynamic groups in the cloud, IEEE Transactions on Parallel and Distributed Systems, 24(6): 1182- 1191.

[5] Pearson S. [2013] Privacy, security and trust in cloud computing, in Privacy and Security for Cloud Computing, ser. Computer Communications and Networks. New York, NY, USA: Springer, pp. 3-42.

[6] Chen HCH, Lee PPC. [2014] Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation, IEEE transactions on parallel and distributed systems, 25(2): 407- 416.

[7] Wang B, Sherman SM, Li CM, Li H. [2013] Storing Shared Data on the Cloud via Security-Mediator, 2013 IEEE 33rd International Conference on Distributed Computing Systems. 10.1109/ICDCS.2013.60

[8] Yu S, Wang C, Ren K, Lou W. [2010] Achieving secure, scalable, and fine- grained data access control in cloud computing, 2010 Proceedings IEEE INFOCOM, DOI: 10.1109/INFCOM.2010.5462174

[9] Wei Li, Xue K, Xue Y, Hong J, [2016] TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage, IEEE Transactions on parallel and distributed systems, 27 (5):