# Public Auditing In Cloud Environment For Secure Data Sharing

Jesudoss A.[1], Lakshmanan. L.[2], Christy A.[3], Mercy Theresa M.[4], Jayaprakash S.[5]
{jesudossas@gmail.com[1],laks14@yahoo.com[2],
ac.christy@gmail.com@gmail.com[3]}

AffiliationAssociate Professor, Dept. of CSE, Sathyabama Institute of Science and Technology, Chennai[1]
Professors, Dept. of CSE, Sathyabama Institute of Science and Technology, Chennai[2,3]

**Abstract.** The Cloud storage resembles a service offered by the cloud computing which involves maintaining, managing and backing up data remotely and there by making it accessible for multiple users across the network. Since the user's data can be altered by external users, storing data with in the cloud tends to be a serious thought for the users. To resolve the above issue an approach of data auditing is presented that performs data integrity using the CA (Cloud Auditor) component. The research aims to build an auditing scheme that being effective, secure and capable of public auditing and maintaining integrity and confidentiality of data. A novel successive single cloud data auditing has been proposed where in user provides uninterrupted declarations to the user and evaluates the information which is being strongly founded by adopting the new data audit validating protocol.

**Keywords:** Cloud computing, auditor, advanced encryption standard, message digest algorithm, encryption, decryption, simple Mail transfer protocol.

## 1 Introduction

This Cloud computing has gained popularity because of various services it offers. Data stockpiling and administration via internet being few of them. Numerable cloud services and arrangements can be acquired by multiple devices, for instance, computers, tablets and smart mobile phones. Since the data processing being quiet adaptable and sharing taking place among numerable users via cloud-based applications and administrations, fulfilling security requirements tends to be tedious and extremely complex. The cloud computing must ensure data integrity related to the information uploaded by the users in the cloud, keeping the data secured and provide strong data-distribution for every access. The cloud computing foundation relies upon outsourcing the computing task to some third-party. Though there may be chances of security risk concerning integrity, availability and confidentiality of information/service. The user's records are assigned to the verifier by the Cloud environment for checking data integrity, which can affect the user's security. The research proposes the need of remote information integrity checking for safe guarding the user's information within the cloud.The priorwork aims to deal with the issue of data integrity audition referring to the single-cloud storage domain compared to a heterogeneous cloud domain which is a hybrid of multiple internal, private, or external/publiccloud resources. In a cloud environment, the data is distributed by the clients, copy document blocks and the copied file blocks are outsourced to multiple Cloud Service Provider (CSP) servers. The above framework is not capable enough to effectively provide data integrity checking in an environment where the information is

ICASISET 2020, May 16-17, Chennai, India

DOI 10.4108/eai.16-5-2020.2303943

being distributed across multiple servers. This most crucial concern for the users in selection of the cloud storage services is identifying the best effective method that can assure the integrity of remotely externalized data. The traditional techniques of data auditing checking relies upon hash table apart from digital signatures, hence they are not feasible enough for auditing cloud information remotely due to prohibited data transmission and computational overhead to recuperate the out sourced records. For the successful verification of remote data integrity without recuperating the whole outsourced report, the model of initial probabilistic checking is being presented that relies upon the methods of signature cryptography and symmetric encryption. The research work presents an auditing checking which being the verification of cloud data integrity related to the audition plan relying upon symmetric keys and signature. Herein, the outsourced information can be audited by the clients in a single test reaction interaction, using minimum transmission cost. Moreover, it permits public verification and supports maintenance of dynamic information using which the data can be altered and deleted by the users with reduced execution overhead. Security analysisand execution evaluation concerning data integrity, fault confinement and transmission cost, reveals better performance of the cloud data integrity verification.

Following is the journal classification: Section 2 discusses works of previous author. Section 3 put forth the proposed auditing representation and outlook of various stages. Experimental outcome are depicted in Section 4. The conclusion is presented in Section 5 along with the research work for future.

## 2 Related Works

Y. Jia et.al surveyed how the harm related to the disclosure of client's key can be minimized in CSA and offers the fore most workable resolution concerning the same. The definition was made official and "the security model concerning auditing protocol using key-exposure resilience and recommend this protocol". For the development purpose, the author adopts the "Binary tree structure along with the approach of pre-order traversal for updating client's secret keys. [1].

Assad Abbas et.al, put forth the sophisticated overview related to the techniques and approaches that are adopted to attend the challenging problem of privacy. The privacy preserving techniques can be divided into2 types: cryptographic and non-cryptographic. Encryption approaches that utilizes public-key encryption are computationally less effective in contrast to symmetric key approaches. Resultant, it's highly required to develop more functional and efficient data search approaches with out having to compromise on the cloud privacy in general and the e-Health clouds specifically [2].

Tao Jiang et.al, faces collusion attack in the present approach. It offers an effective public integrity auditing approach using secure group user revocation relying upon the vector commitment and verifier-local revocation group signature. A powerful scheme is being developed on the basis of scheme definition. The proposed scheme aids in public checking and user revocation in an efficient manner and offer the benefits of count ability, efficiency, confidentiality and traceability of secure group user revocation [3].

Boyang Wang et.al, proposes a novel mechanism of public auditing to achieve integration of shared data, keeping in accord the efficient user revocation. The cloud makes use of proxy re-signatures, and gets permitted to re-sign blocks instead of the current users at the time of user revocation, as a result the current users can avoid downloading and re-sign the blocks by

their own. Moreover, there is a public verifier who audits the integrity of shared data without any need to fetch the overall cloud data, even if the cloud resigns a portion of shared data [4].

Mazhar Ali et.al, proposes the approach of SeDaSC (Secure Data Sharing in Clouds) which offers: 1) data confidentiality and integrity 2) access control 3) sharing/forwarding of data without making use of computer bounded re-encryption 4) insider threat security and 5) forward and backward access control. SeDaSC makes use of one encryption key for encrypting a file. For every user, two separate key shares are being generated, but the user receives just one share. Allowing to acquire only one share of a key helps the SeDaSC methodology to oppose internal threats. A trusted third party (referred to as cryptographic server) saves the other part of the key share. The performance and functionality of SeDaSC is verified by adopting high-level Petri nets, the Satisfiability Modulo Theories Library and a Z3 solver [5].

Jiawei Yuan et.al, recommends a new scheme of data integrity checking depicted by multi-user modification, collusion resistance and a fixed computational cost of integrity checking for cloud users. It's made possible due to the novel layout of polynomial-based update techniques of authentication tags and proxy tags. The proposed scheme aids in effective and secured public checking and user revocation. But, this being still impractical to imbibe because of the involvement of enormous computing cost on the users. Moreover, collusion between cloud servers that misconduct and the users that are revoked is unconsidered [6].

Thiyagarajan et.al, focuses on how to safeguard and secure the data and the processes. For the cloud data that is outsourced, the AES Algorithm is employed. The multi-server data compression algorithm and effective automatic data reading protocol are adopted for effective checking. With the help of such algorithms, the user is permitted to restrict the unauthorized individuals in accessing user's files. [7].

AishwaryaPokala et.al, proposes and have designed two novel techniques. First being the AES (256 bit) Encryption at the Network Level and second being, establishing a shared platform among the user, cloud provider and TPA (Third Party Auditor). The AES Encryption algorithm permits the encryption and decryption of data, while it's transmitted across the network [8].

Guangjie Han et.al, recommends the BRTCO where the author ensures the efficiency concerning the objects. For reducing the amount of boundary nodes, the tracking service is being offered that yields in precise output. To obtain energy efficiency in the course of data transmission, the clustering method is adopted. And for competing with the cluster heads, the strategy of report node selection is built [9].

RajatSaxena et.al, proposes an improvised and effective technique of integrity verification related to data (termed as "Cloud Audit"). The technique has the following essential components, a PHC variant (Paillier-homomorphic-cryptography) system along with combinatorial batch codes and Homomorphic tag. [10].

J. Noorul Ameen et.al has developed an auditing model to be utilized for CSS to provide effective privacy-preserving auditing service. The auditing protocol is then outspreads to help perform the data dynamic operations to carry put safe auditing concerning the random oracle model. Additionally, the auditing protocol is improvised to enable batch auditing for both multiple owners and multiple clouds with no involvement of trusted organizer [11].Swapnali More et.al, adopts a Third Party Auditor (TPA), in order to achieve privacy preserving and public auditing for cloud. The TPA performs the auditing without fetching the data copy, resultant, privacy is maintained [12].Li and his colleagues has put forth a feasible method of verifiable data ownership which utilizes a sequence number (SN)- chunk number (BN) vector

for assisting data block change. The method is made successful using decreased estimation, stockpiling/data storage and communication overhead [13][17].Ni and his colleagues presents a security-assurance checking rule related to the dispersed stockpiling as analysed. It's possible for the dynamic attacker to modify the proof of checking processso as to mislead the verifier and acquire the information, resultant, the cloud records that are inaccessible are not corrupted, though the reports are deteriorated [14][18].

S. Raghavendra and his partners proposes MSIGT (Most Significant Index Generation Technique) which improvisesviable and secured token generation period considering MSD (Most Significant Digit) radix sort. An analytical system is enhanced for encoding the mentioned keywords for obtaining secured token generation. As a result the information owner is offered with the advantage of reduced cost [15]. Jesudoss et al proposes a security mechanism for securing the application over the web [16].

# 3 Proposed Work

## 3.1 Overivew

The cloud storage system involves 3 types of network entities. The proposed mechanism of public auditing permits integrity of shared data by including the user revocation effectively. The cloud environment involves: data owner, group users and auditor. It is a medium which offers the services of storage of data with the group users. Group users involves users who being the shared data owner and are responsible for managing other group users membership. Entire set of group users are allowed to access and alter data. The auditor symbolizes a party responsible for validating data integrity which is stored in the cloud. Since the proposed scheme permits public integrity checking, any cloud user can be the auditor as long as they possess access to the encryption and decryption keys. According to the proposed framework, the group users can upload or create data. It's presumed that data is being saved in file format that is subsequently split into a no: of blocks. To perform integrity checking, every data block is linked using an authentication-tag which being produced by the 16-bit key in data owner send via SMTP. The auditing integrity checking relies upon the hash table. When a block is being added or altered by the user, the respective authentication tag is updated by the user with its own key without actually interacting with the user.

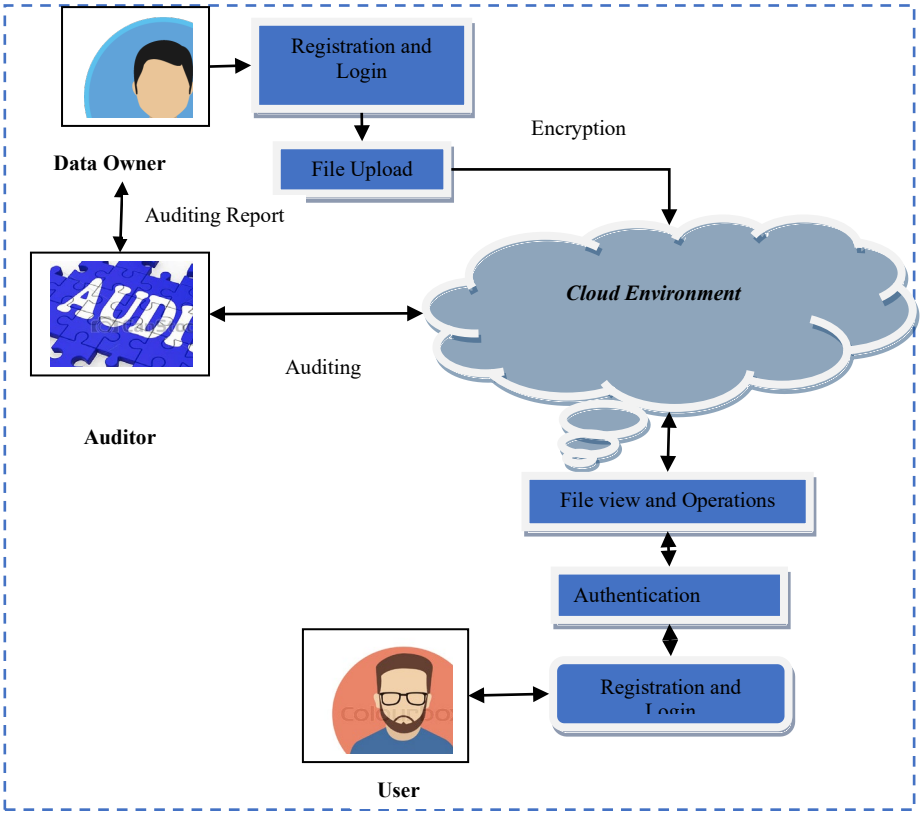


**Fig. 1.** Overall Proposed Architecture

### 3.2 Cloud Environment

The cloud services are founded on three technical models that includes: (PasS) Platform as a service, (SasS) Software as a service and (IasS) Infrastructure as a service. The above services are being offered to the users on the basis of the request and need of the applications. CSPs has built three unique layers for imbibing various technologies in cloud environment. These include:

Infrastructure as a service: This service is responsible to perform management task and store cloud resources. Generally, cloud functions on virtual resources allowing the users to access multiple virtual resources which includes: hardware, servers, software etc... which aids in satisfying the application's necessities.

Platform as a service: This level offers a platform for building software and applications. It simplifies management and utilization of user's application. It involves both software and hardware equipment's provided by the SPs. Application frameworks are taken into account for supporting(SasS) Software as a Service.

Software as a service: Most superior service is offered at this stage, enabling the cloud users to work together with the application. No installation of hardware and software resources takes place at user's end. It can be considered as end user's application, with no need to target on infrastructure management and service maintenance.

### 3.3Data Owner

The data owner possess data collection which needs to be transmitted to cloud environment. Before transmitting or forwarding, the data owner encrypts the data with the help of encryption algorithm. Advanced standard encryption algorithm are being utilized for this purpose. The encryption and decryption 16- bit authentication key is send via SMTP (Simple Mail Transfer Protocol).

### 3.4Public Auditing

Cloud computing allows to access multiple computing resources and managing the third party via internet. The data content from the auditing process gets stored in the cloud. The chance masking and the authenticator ensures that numerous users from various audit session was attended by the auditor. The cloud storage auditor targets on the data security in the CSP, the authenticator just utilizes the data files. The auditing strategy must not include any new un-trusted towards user data privacy as depicted in the existing work, to securely present an efficient auditor.

### 3.5 Advanced Encryption Standard

The AES algorithm carries out encryption that involves well-stated series of steps which are being employed as a method. The plaintext resembles the original information, whereas the cipher text being the information that is encrypted. The entire plaintext information is contained in the cipher text message, but is non-readable by a human or computer unless there is an accurate technique to decrypt it; it is usually depicted as a random crap for the ones who are not supposed to access it.

### 3.6 MD5

MD5 being a popularly utilized decryption algorithm and hash function, generating 128-bit hash value. 16-bit hash value is being retrieved. Though MD5 was formerly built to be adopted as a cryptographic hash function, it's reported to be affected by extensive vulnerabilities. But can be still employed as a checksum to validate data integrity, though purely towards accidental corruption. It's revealed that the MD5 hash function security is immensely compromised. Basically, hash functions are adopted to produce fixed-length or constant output data that symbolizes as a brief reference to the actual data. This being especially significant in case when the original data is very clumsy to be utilized as a whole.

## 4 Results and Discussion

In Cloud computing domain, data integrity tends to be extremely testing and hot security issue. Considering the importance of data integrity, the research explores unique data integrity methods along with their advantages and disadvantages. A quick comparison is being made among the methods by the study. Using the research work, managing remote cloud information is made feasible for numerous users. The performance of proposed workis checked in regard to updating, verifying and inquiring time cost. The proposed work is

analyzed and compared with prevailing work and it's elucidated that there is a low update-time-cost value compared to rest of the methods. Nevertheless the verify-time-cost value is increased because of integrity verification of the signature.

**Table 1.** Performance Comparison Table

| *S. No* | *Techniques* | *Time (ms)* | *Security (%)* |
|---|---|---|---|
| 1 | Parallel Homomorphic Encryption Algorithm (PHEA) | 2.8 | 90 |
| 2 | Triple Data Encryption Algorithm (3DES) | 3.63 | 82 |
| 3 | Elliptic-Curve Cryptography (ECC) | 3.8 | 80 |
| 4 | AES (Advanced Encryption Standard) +MD5 (Message Digest Algorithm) | 1.3 | 100 |

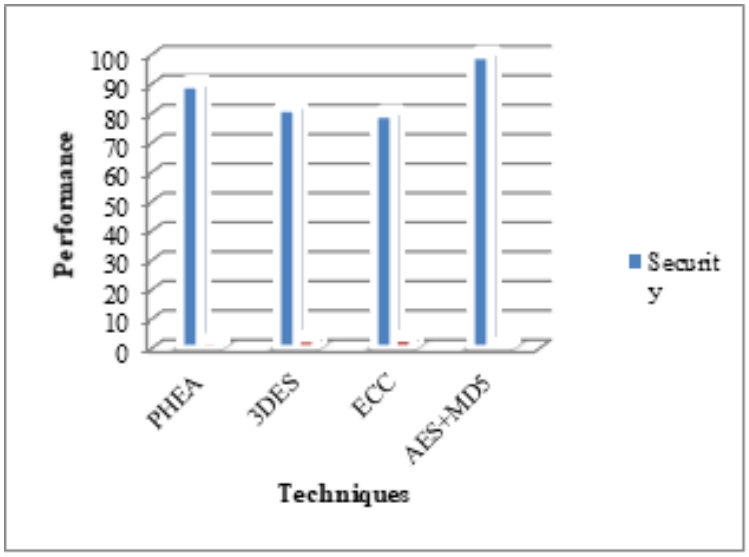


**Fig. 2.** Comparison of Performance Analysis

Figure 2 displays the performance analysis result of current techniques such asAES+MD5, PHEA, ECC and 3DES. The proposed approach of AES +MD5 yields effective performance in contrast to other approaches.

## 5 Conclusion

The research work proposes and illustrates data sharing within the cloud environment instead of employing cloud storage devices. Using this secure and efficient auditing technique, data can be safeguarded against the auditor. In contrast to the mask technique, the blend of cryptography method proves to be effective tool for securing huge amount of owner's data. Hence, any additional organizer is not required for auditing purpose in multi-owners storages. Since the auditing's computing load is moved from auditor to the server, the overall

computation and communication cost is reduced. Resultant, the cloud computing performance can be enhanced and can offer benefit in large-scale cloud sharing systems. In addition, the proposed method is quiet easy and assures owner's data security against corrupt auditors by generating intermediate values for data that is updated.

## References


[1] **Journal article:** Jia Yu; Kui Ren; Cong Wang; Vijay Varadharajan, Storage Auditing With Key-Exposure Resistance (2015), IEEE Transactions on Information Forensics and Security, Vol. 10, pp. 1167-1179.

[2] **Journal article:**Assad Abbas, Samee U. Khan "A Review on the State-of-the-Art Privacy Preserving Approaches in the e-Health Clouds", © IEEE, Journal of Biomedical and Health Informatics, p.p.1-12.

[3] **Journal article:**Tao Jiang, Xiaofeng Chen, and Jianfeng Ma "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation", IEEE Transactions on Computers, 2015, p.p.1-12.

[4] **Journal article:**Boyang Wang, Baochun Li, and Hui Li "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud", IEEE Transactions on Services Computing, 2013, p.p.1-14.

[5] **Journal article:**Ali, RevathiDhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, Fellow, and Albert Y. Zomaya, Fellow, "SeDaSC: Secure Data Sharing in Clouds", © IEEE SYSTEMS JOURNAL, 2015, p.p. 1-10.

[6] **Conference proceedings paper:**Jiawei Yuan, Shucheng Yu "Efficient Public Integrity Checking for Cloud Data Sharing with Multi-User Modification", © IEEE Conference on Computer Communications, 2014, p.p. 2121-2129.

[7] **Conference proceedings paper:**B.Thiyagarajan, Kamalakannan.R "Data Integrity and Security in Cloud Environment Using AES Algorithm", © IEEE, ICICES, 2014.

[8] **Journal article:**AishwaryaPokala, A.Murugan "SURVEY ON DATA INTEGRITY FOR CLOUD SECURITY USING AES ALGORITHM", International Journal of Pure and Applied Mathematics, Volume 118, No. 22, 2018, p.p.251-255.

[9] **Journal article:**Guangjie Han, JiaweiShen, Li Liu, Lei Shu, BRTCO: A Novel Border Line Recognition and Tracking Algorithm for Continuous Objects in Wireless Sensor Networks, © IEEE Systems Journal, 2016 (SCI index, IF=2.114), DOI: 10.1109/JSYST.(2016).

[10] **Journal article:**RajatSaxena and SomnathDey "Cloud Audit: A Data Integrity Verification Approach for Cloud Computing", © Elsevier B.V, IMCIP-2016, 142 – 151.

[11] **Journal article:**J. NoorulAmeen, J. Jamal Mohamed, N. NiloferBegam" Dynamic Auditing Protocol for Efficient and Secure Data Storage in Cloud Computing", International Journal of Advanced Computer Technology, Vol. 3, no. 6, 2014, p.p. 932-937.

[12] **Conference proceedings paper:**Swapnali More, SangitaChaudhari "Third Party Public Auditing scheme for Cloud Storage", © Elsevier, 7th International Conference on Communication, Computing and Virtualization, 2016, p.p. 69 – 76.

[13] **Journal article:**C. Li, Y. Chen, P. Tan, and G. Yang, "Towards Comprehensive Provable Data Possession in Cloud Computing," Wuhan University Journal of Natural Sciences, vol. 18, no. 3, 2013, pp. 265–271.

[14] **Journal article:**J. Ni, Y. Yu, Y. Mu, and Q. Xia, "On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 10, 2014, p.p. 2760–2761.

[15] **Conference proceedings paper:**S. Raghavendra, C. M. Geeta, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik (2015), "MSIGT: Most Significant Index Generation Technique for Cloud Environment," in Proceedings of the Annual IEEE India Conference (INDICON), p.p. 1–6.

[16] **Journal article:**Jesudoss A. and Subramaniam N.P., " Securing cloud-based healthcare information systems using enhanced password-based authentication scheme", Asian Journal of Information Technology, Vol. 15, Issue 14, 2016, pp. 2457-2463.

[17] K. Vijayakumar, Chokkalingam Arun, “Integrated cloud-based risk assessment model for continuous integration”,Int. J. Reasoning-based Intelligent Systems”, Vol. 10, Nos. 3/4, 2018.
[18] K. Vijayakumar, S. Suchitra and P. Swathi Shri, “A secured cloud storage auditing with empirical outsourcing of key updates”, Int. J. Reasoning-based Intelligent Systems, Vol. 11, No. 2, 2019.