|| Volume 3 || Issue 9 || September 2018 || ISSN (Online) 2456-0774

INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

# A Survey on Attribute-Based Cloud Data Integrity Auditing for Secure Outsourced Storage

**Harshu S Pawar[1], Prof. Nagaraju Bogiri[2]**
*Department of Computer Engineering K.J. College of Engineering & Management Research Pune*
*pawarharshu@gmail.com[1], mail2nagaraju@gmail.com[2]*

*Abstract*— **Cloud computing has changed the way computing takes place. It is the technology that enables outsourcing of computing and storage to a public cloud maintained by cloud service providers. Despite a long list of merits of cloud storage, it triggers many security risks at the same time. Data integrity is one of the challenges in secure cloud storage is a fundamental and pivotal element in outsourcing services. Using outsourced data auditing protocol verifiers efficiently check the integrity of the outsourced files without downloading the entire file from the cloud. Due to this reduce the communication overhead. The existing protocol based on public key infrastructure or an exact identity. We proposed attribute-based cloud data integrity auditing protocol. Where users can choose some arbitrary attributes to generate private keys and upload files to cloud server. Moreover, the data owners can specify the set of auditors who are able to check the integrity of the outsourced data. We formalize the system model as well as the security model of this new primitive to ensure the security named soundness of cloud data integrity auditing.**

***Keywords:*** *Cloud Storage, Data Integrity, Cloud computing.*

## I INTRODUCTION

Cloud computing, called on demand computing. Data centered stored and processes users data by third-party and with their storage solutions provided to users Cloud computing allows and enterprises with various capabilities. Resources are continuously catering and freed with nominal manageable effort. Cloud computing is a highly demanded service or utility today due to the positive points such as high computing power, low cost of services, high performance, scalability, accessibility and availability. Distributed resources shared by using cloud computing through the network because of this the security problems are arising. The user wants secure transmission and data storage. The transmission of data is failing due to the hackers attack. The cloud computing, data storage has many challenging issues that effect on the security and overall performance of the overall device [2] [3]. Depository storage needs guarantees regarding the authenticity of knowledge on storage, specifically that storage servers obtain information. Its low to observe that information are altered or erased once accessing the information, as a result of it will be late recapturing lost or broken information.

Depository storage servers remain large amounts of knowledge, very little of that is fetched. They have to store information for the long duration during that; there could be a risk of data due to human or machine errors. Previous solutions don't fulfill these needs for proving knowledge possession. Some schemes supply a weaker guarantee through imposing storage complexity. Additionally, all present methods need the server to fetch the whole file, that isn't possible once addressing large amounts of knowledge [4].

The cloud service providers might act untrustworthily, endeavoring to cover information loss or corruption for status or economic explanations. Consequently it is good for customers to advance an effective protocol to perform periodical confirmations of their stored expertise to assurance that the cloud to be definite maintains up their knowledge adequate. As of late, regeneration codes have picked up repute considering that of their reduce restore bandwidth whilst provides fault tolerance. Regeneration Coding has been heavily used for providing high availability and reliability while launching low storage overhead in storage framework. It's a process of data security [3][5]. Regeneration Coding has been heavily used for providing high availability and reliability while launching low storage overhead in storage framework. It's a process of data security. This process secures information from damaged into fragments, improved, encoded and preclude duplicate data portions and stored across distinct areas or storage media The goal of erasure coding is to regenerate corrupted information through making use of understanding in regards to the data saved someplace else within the array in the disk storage approach.

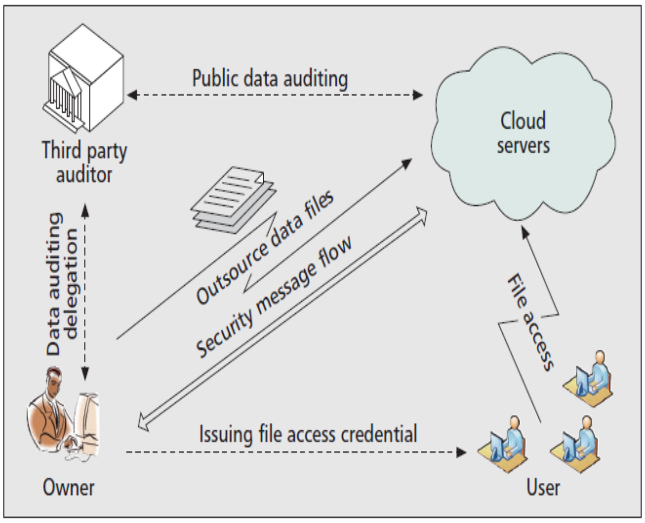

***Figure 1: cloud data storage service***

Public auditing is the service which is used to ensure integrity of the data stored in the cloud and save the cloud users' computation resources. To perform the auditing task the TPA known as a third party auditor used to audit the stored data on the cloud. TPA verifies the correctness of the cloud data on demand without retrieving a copy of the whole data. The TPA, has expertise and capabilities that can periodically check the integrity of all the data stored which provides a much easier and affordable way for the users to ensure their storage correctness in the cloud [6].

Figure 1 show the cloud data storage service consists of four different entity data owner, user, cloud server (CS), and TPA. TPA is the trusted entity. It's used to access the cloud storage security. The cloud data storage provides the availability, on demand sharing and relative low cost into the group of trusted users. For updating the stored data, the data owner indirectly interacts with the cloud server. Here to focus on how the publicly auditable secure cloud data storage services.

## II LITERATURE SURVEY

Yong Yu, Yannan Li, Bo Yang, Willy Susilo, Guoming Yang and Jian Bai [1], Cloud computing has changed the way computing takes place. It is the technology that enables outsourcing of computing and storage to a public cloud maintained by cloud service providers. Despite a long list of merits of cloud storage, it triggers many security risks at the same time. Data integrity is one of the challenges in secure cloud storage is a fundamental and pivotal element in outsourcing services. Using outsourced data auditing protocol verifiers efficiently check the integrity of the outsourced files without downloading the entire file from the cloud. Due to this reduce the communication overhead. The existing protocol based on public key infrastructure or an exact identity. In this paper proposes an attribute-based cloud data integrity auditing protocol.

*Table 1: Literature Survey*

| Sr. No | Paper Title | Author | Method Proposed | Disadvantages |
|---|---|---|---|---|
| 1 | Attribute-Based Cloud Data Integrity Auditing for Secure Outsourced Storage | Yong Yu, Yannan Li, Bo Yang, Willy Susilo, Guoming Yang and Jian Bai, | Using outsourced data auditing protocol verifiers efficiently check the integrity of the outsourced files without downloading the entire file from the cloud. | Low efficiency of system for establishing relevance of the learning content. |
| 2 | Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage | Y. Yu, M.H. Au, Y. Mu, S.H. Tang, J. Ren, W. Susilo and L.J. Dong. | Present "zero-knowledge privacy" to ensure the third party verifier. The client data cannot learn from available information. | Less Accurate. |
| 3 | Privacy-Preserving Public Auditing Protocol for Low Performance End Devices in Cloud | Jiangtao Li, Lei Zhang, Joseph K. Liu, Haifeng Qian, Zheming Dong | Proposes privacy-preserving public auditing protocols. This protocol based on online/offline signatures. | Performance of this method is not good. |
| 4 | Privacy-assured outsourcing of image reconstruction service in cloud | Wang C, Zhang B, Ren K, et al, | Proposes an outsourced image recovery service (OIRS). OIRS design under the compressed sensing framework. | Budget limitation. |
| 5 | An Ensemble Approach to Link Prediction | Liang Duan, Charu Aggarwal, Shuai Ma, Tiejun Ma, Jinpeng Huai | Present a privacy-preserving, similarity-based text retrieval scheme that prevents the server from precisely reproducing the term composition of queries and documents, and anonymize the search results from unauthorized observers. | Relevance was not established. |
| 6 | Toward publicly auditable secure cloud data storage services | C. Wang, K. Ren, W. Lou, and J. Li, | Proposes publicly auditable cloud data storage. This service helps to data owner. | Effectiveness of system is low for computer assisted instructor. |

Y. Yu, M.H. Au, Y. Mu, S.H. Tang, J. Ren, W. Susilo and L.J. Dong [2], the author discussed about the remote data integrity checking. The server proves that the integrity of stored file using remote data integrity. In this the auditor to tell whether the client stored a data and link various parts of this file based on published metadata. They present "zero-knowledge privacy" to ensure the third party verifier. The client data cannot learn from available information.

Jiangtao Li, Lei Zhang, Joseph K. Liu, Haifeng Qian, Zheming Dong [3], for user various resources provided by cloud storage. A privacy-preserving public auditing protocol allows a third party auditor to check the integrity of the outsourced data. In this paper proposes privacy-preserving public auditing protocols. This protocol based on online/offline signatures. Results show that the protocol is more efficient.

Wang C, Zhang B, Ren K, et al [4], the author proposes an outsourced image recovery service (OIRS). OIRS design under the compressed sensing framework. For reducing the cloud storage overhead data owners only need to outsource compressed image samples.

Liang Duan, Charu Aggarwal, Shuai Ma, Tiejun Ma, Jinpeng Huai [5], in this paper present a privacy-preserving, similarity-based text retrieval scheme that prevents the server from precisely reproducing the term composition of queries and documents, and anonymize the search results from unauthorized observers. In the meantime, their plan preserves the relevance-ranking of the search server, and empowers accounting of the number of documents that every client opens. The effectiveness of the scheme is verified empirically with two real text corpora.

C. Wang, K. Ren, W. Lou, and J. Li [6], Cloud computing has changed the way computing takes place. In this paper proposes publicly auditable cloud data storage. This service helps to data owner for save the computation resources and it also provides a transparent yet cost-effective methods.

## III CONCLUSION

In this paper, they present an attribute-based cloud data integrity auditing protocol, for the first time, to simplify the key management issue in traditional cloud data auditing schemes. They formalize the system model and security model for this new primitive. Subsequently, a concrete construction is presented by involving the idea of attribute-based cryptography. Proposed protocol can achieve the property of soundness; attribute privacy-preserving and collusion resistance.

## REFERENCES

[1] Yong Yu, Yannan Li, Bo Yang, Willy Susilo, Guoming Yang and Jian Bai, "Attribute-Based Cloud Data Integrity Auditing for Secure Outsourced Storage", 2015.

[2] Y. Yu, M.H. Au, Y. Mu, S.H. Tang, J. Ren, W. Susilo and L.J. Dong, "Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage", 2015.

[3] Jiangtao Li, Lei Zhang, Joseph K. Liu, Haifeng Qian, Zheming Dong, "Privacy-Preserving Public Auditing Protocol for Low Performance End Devices in Cloud", 2016.

[4] Wang C, Zhang B, Ren K, et al, "Privacy-assured outsourcing of image reconstruction service in cloud", 2013.

[5] Liang Duan, Charu Aggarwal, Shuai Ma, Tiejun Ma, Jinpeng Huai, "An Ensemble Approach to Link Prediction", 2017

[6] C. Wang, K. Ren, W. Lou, and J. Li,"Toward publicly auditable secure cloud data storage services", 2010.

[7]Y. Y. Deswarte, J. J. Quisquater and A. Saidane "Remote integrity checking", 2004.

[8] G. Filho D L, Barreto P S L M. "Demonstrating data possession and uncheatable data transfer", 2006.

[9] A. Juels, B. S. Kaliski Jr. "PORs: Proofs of retrievability for large files" 2007.

[10] C. Wang, K. Ren, W. Lou, and J. Li,"Toward publicly auditable secure cloud data storage services", 2010.