

A Survey on Batch Auditing Systems for Cloud Storage

Darshan Kumar G¹, Dr. K.Thippeswamy²

¹ Student, Department CS&E, VTU Centre for PG Studies, Mysuru, Karnataka.

² Professor & Head of Department CS&E, VTU Centre for PG Studies, Mysuru, Karnataka.

Abstract – As the Emergent technology in the IT world, Cloud Computing has spread over different facets of IT industry in software, platform & Infrastructure as service streams. The skill allows us to store the data in the place where we are allow access it anywhere and anytime we need. Its popularity is in its peak because of its potential and services given to use for cheap cost by Cloud Service Providers. as the technology is more complex and its internal organization is clumsy still today, many challenges it has faced and still facing in the terms of availability and many more but most challenges are faced regarding the security of e data stored by the user in cloud. There are many methodologies are introduced for overcoming the security issues .Auditing systems are the system which is intended to work on the security issues which utilizes complex and secure algorithms .Public Auditing & Private Auditing are the auditing systems used. This paper shows the Batch Auditing systems from the beginning and present ongoing researches on it.

Key Words: Cloud Computing, Security Issues, Batch Auditing, Cloud Service Providers, Public Auditing, Private Auditing.

1. INTRODUCTION

With the entry of cloud computing, which give foundation, stage, programming and different administrations for cloud clients, individuals can without much of a stretch access to less expensive and all the more capable processors and capacity. Client can facilitate the weight of putting away colossal information in neighborhood frameworks, with the cloud computing worldview client can ready to store the information into cloud and can recover at whatever point client needs. The cloud demonstrate has inspired industry and the scholarly community to receive distributed computing to have a wide range of uses running from high computationally concentrated applications down to light weight administrations. As per a Gartner study on distributed computing incomes, the cloud market was worth USD 58.6B in 2009 , is required to be USD 68B in 2010 and will reach USD 148B by 2014. These incomes infer that cloud computing is a promising stage. Then again, it builds the assailants' enthusiasm for finding existing vulnerabilities in the model. Regardless of the potential advantages and incomes that could be picked up from the distributed computing model, the model still has a considerable measure of open issues that effect the model respectability and inescapability. Merchant secure, multi-tenure and disconnection, information administration, benefit

compactness, flexibility motors, SLA administration, and cloud security .

The Cloud computing paradigm is built on several important modules among them the most important are :

- Cloud User
- Cloud Service Provider and
- Third party Auditor

The First two components are the basic and more important, Cloud User is one who Uses the services provided by the Cloud service providers. And the basic, managing services, maintaining & storing data are done by cloud service provider who provides services for user. The third party auditor comes when the cloud is seen in the security perspective of both user and Provider. He is the entity who is independent and has connected to both User and the cloud service provider, and has the most experience and capability on the verification which is the aim of auditing and solution to the security issues.

2. RELATED WORKS

There are many papers, Methods, Techniques are proposed in the view of Auditing for security purpose of cloud storage. Before that let us know the Existing auditing systems in use:

- Public Auditing
- Private Auditing

These two types of auditing are most popular.

Private auditing allows user to challenge the provider to check the integrity of his data .In single task high efficiency is achievable in this case but it is burden to user although efficiency is high.

Public auditing scheme allows data owner i.e. user to delegate a component who is expertise in it and most promisable and trustworthy next to Provider. And with the help of Component he/she can check their integrity .the component is TPA known as Third Party Auditor.

According to Ateniese's the Provable data Possession model, defines the public auditing using the technique which uses RSA based homomorphic tag. This is the first model to define the public auditing. The Tag length is 1024 bits long and also it solves the private validation problem.

According to Juels and Kaliski the method which uses the BLS signature and pseudorandom function which they proposed popularly known as "Proof of Retrivability" in which the

signature length is 160bits long .and query time to challengers is limited to limit secret keys.its working is high potential and heavy they can't be done is smaller platforms like mobiles,cellphones etc....

According the Shah who is from HP company puts a new plan to this and gives ""Auditing to keep online storage services honest" where the concept of TPA came to existence .he says the user need to delegate the Thirdparty who is expertise in this atsk i.e. TPA.the MAC keys are used in this plan.

"privacy- preserving public data auditing by using homomorphic authenticator with random masking" is the new method realized by Wang in this technique user need not be online always.

Wang improves the "Proof of retrievability" model and uses Merkle Hash Tree to complete dynamic data operations such as data modification, data insertion and data deletion for cloud data storage.

Moreover, Wang also explores the technology of Bi-linear aggregate signature to realize batch auditing. The data dynamic auditing scheme meets the users' demand of data operation and greatly improves Cloud Computing's computing efficiency when dealing with huge amount of data.

At present the Aggregate signature technique is used in verification.the technique is composed of Bi-linear aggregate signature technique where the data from different users are digitally signed by the different signers are aggregated into single signature if the aggregate signatures passes the verification then the data correspond to that signature are not affected.if in case it doesn't pass the verification then it is the job of TPA to verify it one by one.

3. METHODOLOGY

The Bi-linear aggregate method is fast and efficient but it fails when the Aggregate signature do not pass the verification .at this moment the verifier should verify one by one ,which for small piece of data .Since the data is huge in realtime and the Many users are using it on same time . So a method or technique is need to overcome this problem. In this context ,a new method is proposed which uses the Map reduce framework for this [1]. In this proposed system Auditing is done in two phases

In first phase the user generates the public keys and private keys along with the data is upload to CSP(Cloud Service Provider).

In second phase the User request the TPA(Third Party Auditor) to check whether his/her file is safe or not. As soon as request is recived form user.TPA challenges the CSP .CSP sends the data related to TPA request which is called proof . TPA check the data and replies to user with TRUE/FALSE.

If not it should verify it . at this particular point the map reduce framework is introduce in order to map the signatures with data and reduce it to check TRUE/FALSE.

MAP function

Map(Text value, Context context)

Input: PKFile_1, ..., paramFile_1, ...

Output: <dataTag, PK_1>, ..., <dataTag, Para_1>, ...

REDUCE function

Input: K key-value pairs of <key, values>

Output: K results of <dataTag, true/false>

4. CONCLUSION

In this paper, we have come across different process of the advancement and advancement in the existing methods in batch auditing for cloud storage from the early days.the initial techniques from Provable data Possession to the Bi-linear aggregate signature technique.the security challenges are minimized to some extent but not completely.in this view we also seen the new technique of MapReduce framework incorporated in the existing Batch Auditing system.From early time the performance and efficiency are increased more but he integrity verification pace is still is in its slower rate.A new method can be introduced in view of process which computes parallely and many advancements can be made in various ,small,and complex part of cloud paradigm.

ACKNOWLEDGEMENT

I Thank my Professor & HOD Dr.K.Thippeswamy For his Vauable Guidelines.

REFERENCES

- [1] Yu Jin,Dong Yan,Heng He, 2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA).
- [2] Mohamed Al Morsy, John Grundy and Ingo Müller, "An Analysis of the Cloud Computing Security Problem," In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 2010.
- [3] Wang Q, Wang C, Li J, "Enabling public verifiability and data dynamics for storage security in cloud computing," Proceedings of the 14th European conference on Research in computer security Springer- Verlag, 2009, pp. 355-370.
- [4] Chen H F, Lin B G, Yang Y, "Public Batch Auditing for 2M-PDP Based on BLS in Cloud Storage," Journal of Cryptologic Research, 2014.

- [5] [Syam K P, Subramanian R, "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing," International Journal of Computer Science Issues, 2011.
- [6] Ateniese G, Burns R, Curtmola R, "Provable data possession at untrusted stores," Ccs'07 Proceedings of Acm Conference on Computer & Communications Security, 2007, pp. 1165-1182.
- [7] Fischlin M, "The Cramer-Shoup Strong-RSA signature scheme revisited," Proceedings of Pkc'03 Lncs, 2003, pp. 116-129.
- [8] Juels A, Kaliski B S, "Pors: proofs of retrievability for large files," In CCS'07 Proceedings of the 14th ACM conference on Computer and communications security, 2007, pp. 584-597.
- [9] Wang C, Wang Q, Ren K, "Privacy-preserving public auditing for data storage security in cloud computing," INFOCOM, 2010 Proceedings IEEE, 2010, pp. 1-9.

and Bachelor's Degree in Computer Science and Engineering from University B.D.T College of Engineering (UBDTCE), Davangere in the year 1998. He is currently heading the Department of Computer Science and Engineering, Visvesvaraya Technological University, PG Center, Mysore, He is having 18 years of Teaching and 3 years Research experience. He has published around 40 papers which include International Journals, International Conferences and Notional Conferences; he has conducted two national one International conference and many workshops successfully.

He is a Life member of India Society for Technical Education (LMISTE), Computer Society of India (CSI) & International Association of Engineers (IAENG). He is Reviewer Committee Member for the international Journal Bioinformatics and Data Mining. Mysuru.

BIOGRAPHIES



Darshan Kumar G Presently Pursuing his M.Tech Degree in department of CS&E at Visvesvaraya Technological University, PG Centre, Mysuru 570029. He completed B.E in CS&E branch at SJMIT Chitradurga, Karnataka in the year 2015. His M.Tech project Research on Map Reduce based Cloud Storage Batch Auditing. His area of interest in programming in C#, PHP, Web Development, Artificial Intelligence, Search Engine Optimization, Search engines, Research in Big Data.



Dr. K. Thippeswamy Received his Ph. D degree from the Department of CS&E in Jawaharlal Nehru Technological University, Ananthapur, Andra Pradesh in the year 2012, M.E degree in Computer Science and Engineering from University Visvesvaraya College of Engineering (UVCE), Bangalore in 2004.