A Survey on Public Batch Auditing Protocol for Data Security

Vinod Bharat
H.O.D of Computer Dept.
Dr.D.Y.Patil School of engineering Academy Ambi, Savitribai Phule Pune University,Pune,Maharashtra

Sandeep Mali
Dept.Computer Engineering
Dr.D.Y.Patil School of engineering Academy Ambi, Savitribai Phule Pune University,Pune,Maharashtra

Kishor Sawant
Dept.Computer Engineering
Dr.D.Y.Patil School of engineering Academy Ambi, Savitribai Phule Pune University,Pune,Maharashtra

NileshThombare
Dept.Computer Engineering逸
Dr.D.Y.Patil School of engineering Academy Ambi, Savitribai Phule Pune University,Pune,Maharashtra

ABSTRACT
The cloud provides storage for user to store their data remotely. But there is a problem with the auditing protocol, which was proposed. There is a new paradigm of storage service, which makes the integrity protection for outsourced data. There are also other integrity auditing protocols that has been already proposed but their focus was singleton cloud storage. These protocols don't support batch editing of cloud storage. There is a another auditing protocol for public which will provide integrity of multi-cloud storage. In this protocol there is a third party auditor which will simultaneously verify multiple auditing requests from different users on different storage of data files or different cloud storage servers. This protocol will achieve quick identification of corrupted data by implementing recoverable coding approach and homomorphicciphertext verification. It will also provide privacy preserving public auditing for data integrity. The total editing time can be reduced by batch auditing protocol and communication cost can be maintained low using same protocol. Analysis of extended security and performance shows this protocol is efficient and secure.

Keywords
Cloud Computing, Multi-cloud computing, Data Security in Cloud, Public Batch Auditing.

1. INTRODUCTION
In the early years, Cloud storage services are getting widely used because of their property of storing data remotely [1]. Cloud computing service provider provides perfect quality of services that can be used by the user. At this side is the good quality of the cloud computing there is another side which leads to difficulties which includes corruption of data, hardware failure, or by human errors [2].Due to these kinds of the problems arises in single cloud computing, multi-cloud computing is preferred by the users. Multi-cloud computing provides the facility of storage of data in multiple or more than single cloud. This storage of multi cloud computing resolves the problem of Data Integrity. Still user dose not made a choice of the use multi-cloud computing easily.

Manually it is not possible to check the data integrity, bothside, i.e. from users and the cloud service provider. Therefore the third party is a solution which, must, have to provide the service for checking the data integrity ensuring the user and service provider. By this, the user does not have to worry about the data integrity [5], [6].

On such basis in recent years multiple auditing protocols have been getting introduced such as Provable Data Possession [7]. These kinds of protocols are used for insuring about data integrity. But disadvantage of these protocols is that they cannot work on multiple cloud environments. The multi-cloud environment in which third party auditor can receive multiple authorized request from different data users. If the request can be get handled in sequential queue or in the batch manner way it will be the great efficient work. There are only several protocols which handle the data integrity in the multi - cloud system [6], [8]. These kinds of protocols work efficiently when the data of the particular user and the appropriate key is stored. If for any reason the data and key gets vanished there will be no use of such auditing protocol. In this condition it makes possible not recover the data with the use of this protocol.

2. CLOUD COMPUTING
2.1 Single Cloud Computing
Cloud computing is an approach to provide a virtual system in which user get the services like storing their data at remote locations and retrieving this data at any time anywhere. In cloud computing user does not have to worry about the how the data is stored or it is handled. Remotely stored data on cloud computing are totally handled by the cloud service provider. A cloud service provider is responsible for the managing the data [1]. one of the most important thing in ID industry is Data. Because of such advantage in Cloud computing, it is getting very famous, widely in the various sectors of the IT Industries. Cloud computing provides the service like IaaS (infrastructure as a service), PaaS (Platform as a service) and SaaS (Software as a service) [2]. A provider of IaaS provides computer physical or more often virtual machines. IaaS cloud provides frequently offer extra assets,

for example, a virtual-machine plate picture library, document, or item stockpiling, firewalls, load balancers, IP addresses, virtual neighborhood (VLANs), and programming packs. In the PaaS models, cloud suppliers convey a registering stage, ordinarily including working framework, programming-dialect execution environment, database, and web server. In the product as an administration (SaaS) model, clients obtain cloud computing is access to application programming and databases. Cloud suppliers deal with the foundation and the stages that run the applications. SaaS is some of the time defined as "on-demand programming" and is typically estimated on a pay-per-use premise [5].

As the cloud computing having the advantages simultaneously, it also has the drawbacks. One of the major issues about cloud computing is about data security.The data security issue arises at the user end. The main security issues where Data Integrity, Data availability and most important one is Services.

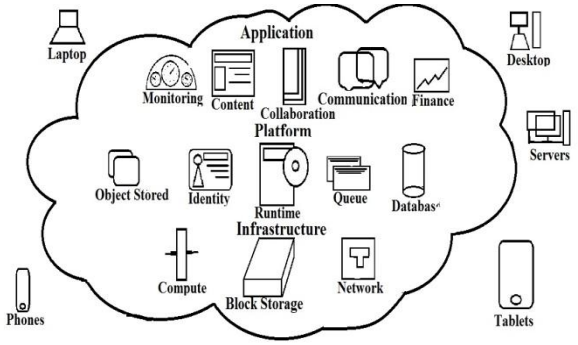

Fig. Single Cloud Computing

2.2 Multi-Cloud Computing

Multi-cloud is a collection or collaboration of two or more cloud computing services. Services like software as a service (SaaS), Infrastructure as services (IaaS) and Platform as a service (PaaS). Multi-cloud platform provides facility that you can collaborate public cloud, private cloud, and virtualized environment in your cloud strategy. Multi-cloud is nothing but a cloud of cloud or interrelated cloud.[17].Multi-cloud improves performance of organization by handling "vendor lock-in". Vendor of consumer attained "lock-in" in a single cloud so multi-cloud provides some strategy to release it into multiple cloud environment [1].

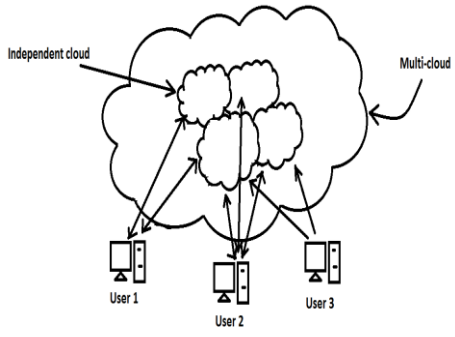

Fig .Multi cloud computing

3. SECURITY ISSUES IN CLOUD COMPUTING

3.1 Data Integrity

The data integrity problem is the one of the serious issue of cloud computing. When the cloud system store data it requires to perform a transition function like operation on storing data it may cause the noised data or data can be damaged in that operation. Data lost risk is not depending only on internal function, it may cause by external theft attack. The examples given by Cachinetearl.[12] data breaching of Google Docs it affects the electronic privacy information Center it forced to investigate cloud computing services of Google organization, Red Hat Linux's distribution server problem [18].

In Multi-cloud, number of cloud store data in a centralized manner or in exact opposite case the huge amount of data store or operate in the cloud because of large data it is difficult detect data loss issues [12]. To overcome this type of problem Byzantine fault-tolerant replication protocol are best protocol in cloud system [19].

3.2 Data Intrusion

Data intrusion is another major concern in cloud computing. It is an important data security risk that occurs with a cloud service provider (CSP). If any intruder can access the account username and password then they will be able to any operation or any kind of unwanted changes in the accounts private document.

3.3 Service availability

Availability of Service is again threat with cloud service provider. In the service availability it mentions the cloud service providers licensing or not, accessing anytime due to unforeseen reasons. Important documents or files are stored on the cloud server and cloud suddenly goes down, then important problem is it will be coming original data with all important documents or files.

4. PUBLIC BATCH AUDITING PROTOCOL

An efficient privacy-preserving public batch auditing protocol for integrity of the data in multi-cloud with identification of the corrupted data. Our work focuses on batch auditing protocol in multi-cloud. We use homomorphicciphertext verification for protecting data privacy against the third party auditor can't obtain any data content from the proofs. The proposed protocol achieves quick identification of the corrupted data by using a recoverable coding approach [6] [7].

Public auditing of cloud data with data privacy proposed by Want etin [6]. They also enable batch editing. Index hash tables to support dynamic data during the public auditing process [16]. After that proposed provable data possession protocol to gain integrity verification in multi-cloud, but it doesn't support batch verification.

Because some of operations are helping towards the encryption of stored data, the encryption method bounds the functionality of storage system. A third party auditor (TPA) performs tasks like shared data, dynamic data and its integrity in the cloud. Dynamic data support the data operation such modification, insertion, deletion. TPA handles multiple audit sessions from different user data and also audit the stored files and check the data uniqueness. The privacy preserving system provides secure data storage [6].

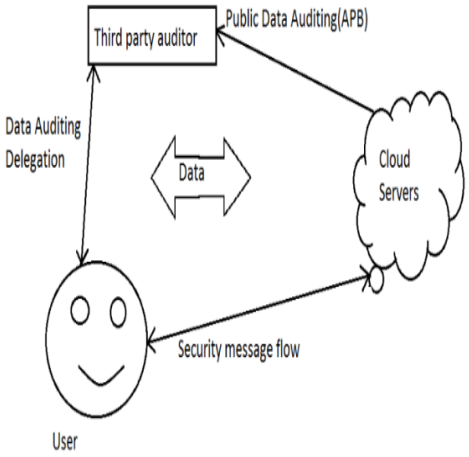

Fig. Public Batch Auditing Protocol

A user stores his data through a cloud service provider (CSP) into a set of cloud servers. For application purpose the user interacts with the cloud servers via CSP to access his data. User may need to perform block level operations on his data [12].

5. RELATED WORK

First in 2006 Jewels and Kaliski [10] introduced structure called as the POR (Proof of retrievability). The structure has the ability to maintain the data Integrity with the help of server and sentimental value. The resulting works [11], [12], [13] enhanced this work by giving a boundless number of information integrity check, taking less correspondence, or supporting secure and productive dynamic information operations.

In 2007 Ateniese et al. [7] Have developed the (PDP) provable data possession which gives the access to the user to keep the data integrity without having access to the full file. Again to improve the performance in Athens et al. [9] Formed another PDP with most effective way. But the problem with the algorithm is that it just gives little access to user which does not fill the requirement of the user.In other related work Wang et al. [5] Introduced the protocols which focus on the diting on privacy in cloud data. Also later Wang et al. [14] introduced the protocol, which takes the advantages of both BLS based homomorphism authenticator and MHT.

Zhu et al. [16] find file hash tables to help dynamic information amid auditing publicly. After that for the multi-cloud Zhu et al. [17] again introduced PDP for user to check the data integrity, but, it does not show the effect to the batch verified.

Like the above protocols introduced Curtmola et al. [18] find out PDP to multiple copies over the distributed storage system. After that Barsoum et al. [19] recommended pairing-based PDP on multi data protocol to support public checking of data integrity.

Wang Jinhai, Zhou Hao, Chen Xi, Lu Yilong [1] introduced the Efficient Public Batch Auditing Protocol, which uses cipher text verification for data privacy and assumption of corrupted data. The use of this protocol leads to reducing the communication time auditing time. This gives the highly secured protocol.

6. FUTURE SCOPE AND CONCLUSION

As shown in the paper, the cloud computing is the most growing technology in the IT sector. but as per the user requirement, there comes the important topic to be resolved is Data Security. The auditing the data is a solutionfor that kind of problem. In this parer shows the survey of the construction of the batch auditing protocol for multi-cloud system. In view of homomorphic authenticator and homomorphicciphertext check, we have proposed an open reviewing convention that TPA can productively confirm the privacy of particular information records in a cluster way, while the information security is still ensured against TPA. The future work will be the icing of the generic algorithm for the user key generation can be used in a more conventional way to maintain the privacy of users.

7. REFERENCES

[1] He Kai, Huang Chuanhe+, Wang Jinhai, Zhou Hao, Chen Xi, Lu Yilong, Zhang Lianzhen, Wang Bin, "An Efficient Public Batch Auditing Protocol for Data Security in Multi-Cloud Storage",8th ACGC, 978-0-7695-5058-9/13, DOI 10.1109,IEEE,2013.

[2] R. H. Katz, A. Fox, R. Griffith, A. D. Joseph, A. Konwinski,G. Lee, M. Armbrust, D. A. Patterson, A. Rabkin and M. Zaharia, "A view of cloud computing,"Commun. ACM, vol. 53, no. 4, pp. 50-58, 2010.

[3] B. Krebs. "Payment Processor Breach May Be Largest Ever,"Online at http://voices.washingtonpost.com/securityfix/2009/01/payment processor breach may b.html, Jan. 2009.

[4] M.A. AlZain, E. ardede, B.Soh, J.A. Thom, "Cloud Computing Security: From Single to Multi-Clouds,"inProc of the 45th Annual Hawaii International Conference on System Sciences, 2012, pp. 5490-5499.

[5] K. Yang and X. Jia, "Data storage auditing service in cloud computing: challenges, methods and opportunities,"World Wide Web,vol. 15, no. 4, pp. 409-428, 2012.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,"in Proc. IEEE INFOCOM, 2010, pp. 525-533.

[7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores,"inProc.ACM CCS, 2007, pp. 598-610.

[8] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing,"IEEE Transactions on Parallel and Distributed Systems, 2012 (to be printed) .

[9] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession,"in Proc. ICST SecureComm, 2008.

[10] Juels and B. S. Kaliski, "PORs: Proofs pfRetrievability for Large Files,"in Proc. ACM CCS, 2007, pp. 584-597.

[11] H. Shacham and B. Waters, "Compact proofs of retrievability,"in Proc. of Asiacrypt, 2008, pp. 90-107.

[12] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing,"in Proc. of IWQoS, 2009, pp. 1-9.

[13] K. D. Bowers, A. Juels, and A. Oprea, "Hail: a high-availability and integrity layer for cloud storage,"in Proc. of CCS, 2009, pp. 187-198.

[14] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing,"in Proc. of ESORICS, 2009, pp. 355-370.

[15] C. Wang, Q. Wang, K.Ren, Ni. Cao, W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing,"IEEE Transactions on Services Computing, vol. 5, no. 2, pp.220-232, 2012.

[16] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds,"in Proc. ACM Symposium On Applied Computing, 2011,pp.1550-1557.

[17] M. Vukolic,"The Byzantine empire in the intercloud", ACM SIGACT News, 41,2010, pp. 105-111.

[18] RedHat,https://rhn.redhat.com/errata/RHSA-20080855.html.

[19] J. Hendricks, G.R. Ganger and M.K. Reiter, "Lowoverhead byzantine fault-tolerant storage", SOSP'07: Proc. 21st ACM SIGOPS symposium on Operating systems principles, 2007, pp. 73-86.