ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

A Survey on Public Data Integrity Auditing With Division and Replication of Data in Cloud System

Vedwati G. Patil[1], Prof.Shubhangi Suryawanshi[2]

M.E. Student, Dept.of Comp. Engg., G. H. Raisoni Institute of Engineering & Technology, Pune, Maharashtra, India

Assistant Professor, M.E. Student, Dept. of Comp. Engg., G. H. Raisoni Institute of Engineering & Technology, Pune, Maharashtra, India

ABSTRACT: Outsourcing data to be another authoritative control will be done in distributed system, ascend to security concern. This data trade off happen because of assaults by different types of users and nodes inside the cloud system.In this paper we be proposesa public data integrity auditing of data and group revocation with division and replication of data in cloud system that will be collectivel1y approaches the security and performance issues. In the procedure, as per user input file partition into sections, and reproduce the divided information on the cloud storage nodes. Each of the node store just a small byte part of that file information record that guarantees that even in the event of a fruitful assault, no important data is uncover to the assailant. More thinking like, the nodes putting away the section is isolated with separation by the method for diagrams T-shading to restrict an assailant of speculating the areas of the section.Recently some researches consider the problemof secure and efficientpublic data integrity auditing for shared dynamic data. However,these schemes are still not secure against the collusion of cloudstorage server and revoked group users during user revocation inpractical cloud storage system. We figure out thecollusion attack in the exiting scheme and provide an efficient publicintegrity auditing scheme with secure group user revocation basedon vector commitment and verifier-local revocation group signature.We design a concrete scheme based on the scheme definition.Our scheme supports the public checking and efficient user revocationand also some nice properties, such as confidently, efficiency,countability and traceability of secure group user revocation.

KEYWORDS: file fragmentation, file replication,Public integrity auditing, dynamic data, victor commitment,group signature, and cloud computing.

I. INTRODUCTION

Security is the most important aspects among those the wide-spread adoption eclipse of cloud computing. Cloud security problem supported due to core technology implementation as like virtual machine (VM) escape or session riding, etc. The service offerings by cloud as SQL injection or less authentication system and cloud characteristics like information recovery vulnerability and Internet protocol vulnerability, data storages, etc. To secure cloud all the participating entities must be provides security. In the cloud security of the assets does not completely depend on an individual's security measures because an any given system with one or more units, the highest level of systems security is equal to level of the weak entity and so the neighboring entities may provides an opportunity to an attacker. The off-line data storage cloud utility requires users to move data in clouds virtualized and shared environment that may result in various security procedures. Pooling and elasticity of cloud storage allows the physical resources to be the shared maximum users. Shared resources may be reassigned to other users at same instance of time that may result in data compromise through data recovery techniques. The information similarly, cross-tenant virtualizes network accessing may also compromise data Safety and data integrity. Inapplicable media sanitization can also hack customer's private data. The Unauthorized information/data accessing by user and processes must be prevented. This system is useful to user for successfully store the fragramts. In such criteria, the security mechanism must be the substantially increasing an attacker's/hacker effort to retrieve a reasonable amount of data even after the successful attack in the cloud storage.The sufficient amount of loss information present public data integrity auditing with division

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

and replication of data in cloud system that judicially fragments user text files into small part and replicates them at strategic locations within the cloud.

In this paper, we propose a public data integrity auditing with division and replication of data in cloud system. In our mechanism, by utilizing the idea of proxy re-signatures, once a user in the group is revoked, the cloud is able to re-sign the blocks, which were signed by the revoked user, with a resigning key. As a result, the efficiency of user revocation can be significantly improved, and computation and communication resources of existing users can be easily saved. Meanwhile, the cloud,who is not in the same trusted domain with each user, is only able to convert a signature of the revoked user into a signature of an existing user on the same block, but it cannot sign arbitrary blocks on behalf of either the revoked user or an existing user. By designing a new proxy re-signature scheme with nice properties which traditional proxy re signatures do not have, our mechanism is always able to check the integrity of shared data without retrieving the entire data from the cloud. Moreover, our proposed mechanism is scalable, which indicates it is not only able to efficiently support a large number of users to share data and but also able to handle multiple auditing tasks simultaneously with batch auditing. In addition, by taking advantages of Shamir Secret Sharing, we can also extend our mechanism into the multi-proxy model to minimize the chance of the misuse on re-signing keys in the cloud and improve the reliability of the entire mechanism

The growth of cloud computing encourages the endeavours and organization to subcontract their data to third-party cloud service providers. This will progress the storage drawbacks of resource limit local devices. In recent times, various profitable cloud storage services, such as the simple storage service, data backup services, realistic cloud basedSoftware Google Drive are built for cloud application. Ever since the cloud servers may return unacceptable results, it's because of servers' hardware failure or software failure. Sometimes human maintenance may lead to problems. And malicious attack will lead to unacceptable loss or result of data. To prevent from this situation, we are in need of data integrity and accessibility. This data integrity and accessibility are helps to protect data of cloud users. It also helps to provide privacy to the users' data. The improvements and enhancements in cloud computing motivates organization as well as enterprises to outsource their data to third party cloud service providers (CSP's) which will result in improvements the data storage limitation of resource constrain local devices. In market, already some cloud storage services are available like simple storage service (S3) [1] on-line data backup services of Amazon and software like Google Drive, [2] Dropbox, [3] Mozzie, [4] Bitcasa and [5] Memopal built for cloud application. In some cases cloud server sometime returns invalid results such as hardware/software failure, malicious attack and human maintenance. Security and privacy of cloud user's data should be protected by data integrity and accessibility. To overcome the security issues of today's cloud storage services, simple replication and protocols like Rabin's data dispersion scheme are not sufficient for practical application. For achieving the integrity and availability of remote cloud storage, some various solutions and their different variants have been proposed. In these solutions, when a scheme supports modification of data, it is known as dynamic scheme, otherwise static one. A scheme is publicly verifiable that means the integrity check of data can be performed not only by data owners, but also by the third party auditor (TPA).

II. RELATED WORK

1.On the characterization of the structural robustness of data center networks.

In this paper, Author studied the structural robustness of the state-of-the-art data center network (DCN) architectures [1]. Our results revealed that the D-Cell architecture degrades gracefully under all of the failure types as compared to the FatTree and ThreeTier architecture. Because of the connectivity pattern, layered architecture, and heterogeneous nature of the network, the results demonstrated that the classical robustness metrics are insufficient to quantify the DCN robustness appropriately. Henceforth, signifying and igniting the need for new robustness metrics for the DCN robustness quantification. Author proposed deterioration metric to quantify the DCN robustness. The deterioration metric evaluates the network robustness based on the percentage change in the graph structure.

2.Energy-efficient data replication in cloud computing datacenters

This paper reviews the topic of data replication in geographically distributed cloud computing data centers and proposes a novel replication solution which in addition to traditional performance metrics, such as availability of network bandwidth, optimizes energy efficiency of the system. Moreover, the optimization of communication delays leads to improvements in quality of user experience of cloud applications [2]. The performance evaluation is carried out using GreenCloud – the simulator focusing on energy efficiency and communication processes in cloud computing data

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

centers. The obtained results confirm that replicating data closer to data consumers, i.e., cloud applications, can reduce energy consumption, bandwidth usage, and communication delays significantly.

3.An analysis of security issues for cloud computing

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. Author presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. Virtual networks are also target for some attacks especially when communicating with remote virtual machines [3].

4. **Privacy-preserving public auditing for data storage security in cloud computing**

Motivate the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol [4]. Our scheme enables an external auditor to audit user's cloud data without learning the data content. This scheme is the first to support scalable and efficient privacy preserving public storage auditing in cloud. Scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner. TPA would not knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also reduce the user's fear of their outsourced data leakage. TPA may concurrently handle multiple audit sessions from different users for their outsourced data files.

5. Efficient public integrity checking for cloud data sharing with multi-user modification.

The author designed dynamic public integrity auditing scheme with group user revocation. Yuan and yu not consider data secrecy of group users in their scheme that means scheme efficiently support plaintext data update and integrity auditing not cipher text data [5]. Design polynomial authentication tag and adopt proxy tag update technique. If data owner share group key with group users and defection or revocation occur any group user will force to other group user to update their shared key. Sometime data owner not take part in user revocation phase, where many time cloud server update the data and provide data legally last.

Sr.No	Author	Paper Name	Description	Year
1	K. Bilal, M. Manzano, S.U. Khan, E. Calle, K. Li, and A. Zomaya,	On the characterization of the structural robustness of data center networks	In this paper, Author studied the structural robustness of the state-of-the-art data center network (DCN) architectures. Our results revealed that the D-Cell architecture degrades gracefully under all of the failure types as compared to the FatTree and ThreeTier architecture.	2013
2	D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya,	Energy-efficient data replication in cloud computing datacenters	This paper reviews the topic of data replication in geographically distributed cloud computing data centers and proposes a novel replication solution which in addition to traditional performance metrics, such as availability of network bandwidth, optimizes energy efficiency of the system.	2013
3	K. Hashizume, D. G. Rosado, E. Fernndez-Medina,	An analysis of security issues for cloud computing	We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. As described	2013

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

	and E. B. Fernandez,		in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users.	
4	J. Yuan and S. Yu	public integrity checking for cloud data sharing with multi-user modification	The author designed dynamic public integrity auditing scheme with group user revocation. Yuan and yu not consider data secrecy of group users in their scheme that means scheme efficiently support plaintext data update and integrity auditing not cipher text data	2014
5	C. Wang, Q. Wang, K. Ren, and W. Lou,	-preserving public auditing for data storage security in cloud computing	Motivate the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol. Our scheme enables an external auditor to audit user's cloud data without learning the data content. This scheme is the first to support scalable and efficient privacy preserving public storage auditing in cloud. Scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner.	2010

III. PROPOSED ALGORITHM

1. AES:

The Advanced Encryption Standard or AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.The origins of AES date back to 1997 when the National Institute of Standards and Technology (NIST) announced that it needed a successor to the aging Data Encryption Standard (DES) which was becoming vulnerable to brute-force attacks.This new encryption algorithm would be unclassified and had to be "capable of protecting sensitive government information well into the next century." It was to be easy to implement in hardware and software, as well as in restricted environments (for example, in a smart card) and offer good defenses against various attack techniques**.**

2. Data Partition Algorithm- To divide data into fragments

Algorithm for fragments replication
For each Ok in O do
Select Si that has max(Rik +Wik)
ifcolSi = open color and si>= ok then
Si←Ok
Si←si– ok
colSi←close color
Si←distance(Si; T) P /*returns all nodes at distance T from Si and stores in temporary set Si'*/
colSi← close color
end if
end for

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

IV. PROPOSED SYSTEM

This paper proposed system to realize efficient and secure Public data integrity auditing with division and replication of data in cloud system. The proposed model consists of the public data auditing. This technique will provide better data confidentiality compare to other methodologies. With data storage and sharing services in the cloud, users can easily modify and share data as a group. To ensure shared data integrity can be verified publicly, users in the group need to compute signatures on all the blocks in shared data. Different blocks in shared data are generally signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user. The straightforward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud.

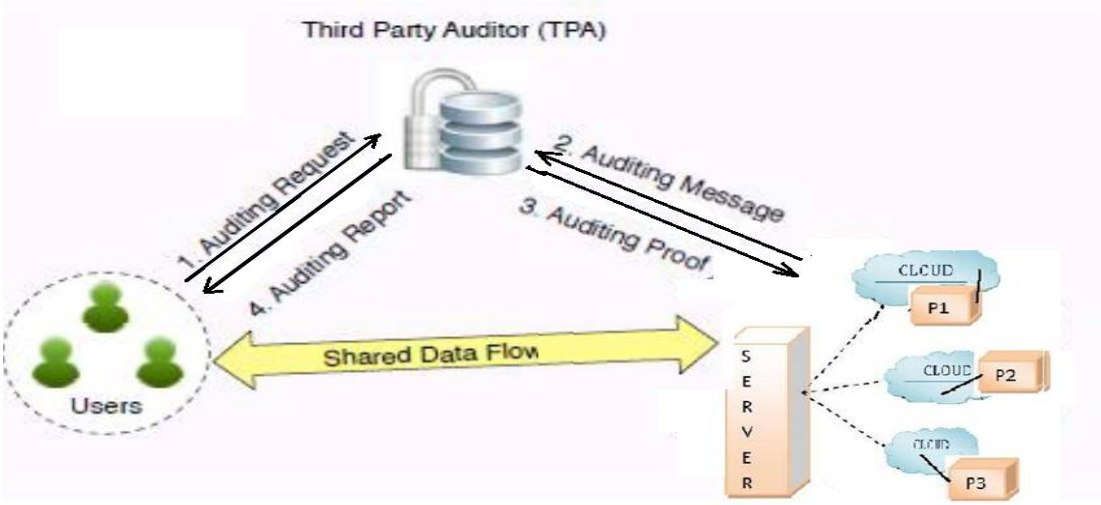

Figure 1: System Architecture

In this paper, we collectively rules the issues of security and performance as a secure the file.Division and Replication of Data in the Cloud storage that fragments user files into small part and replicates them at strategic locations with into the cloud storage nodes. The division of a file into fragments is performing based on the giving input criteria such that as the individual fragments do not contain any meaningful data. Each of the cloud node(we use the term node to represent storage capacity, physical, and the virtual machines) contains will be distinct fragment to increase the more data security on cloud.

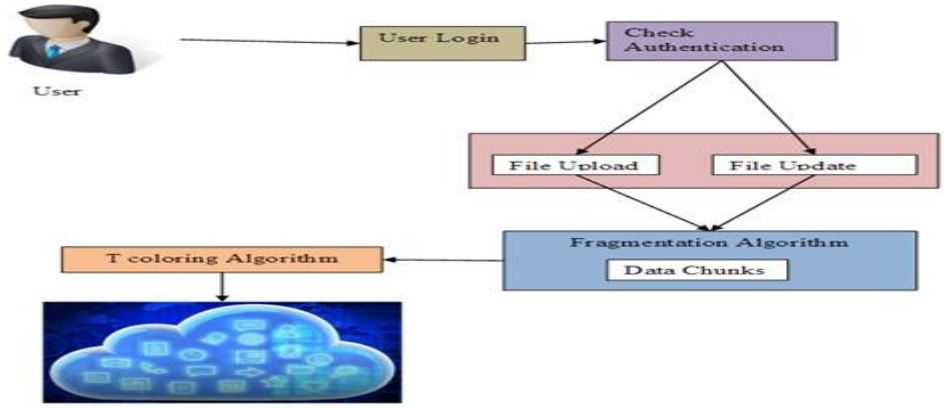

Figure 2: Fragmentations of File

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

V. CONCLUSION

In this paper, the proposed that Public data integrity auditing with division and replication of data in cloud systemmethodology is a distributed storage security conspire that by and large manages the security and execution as recovery time. The information record was divided and the parts are scattered over different nodes. The nodes were isolating by method for T-shading. The discontinuity and dispersal guaranteed that no noteworthy data was reachable by the enemy if there should a rise an occurrence of a fruitful assault. No node in to the cloud put away more than a solitary part of the same documents. It is important to build up a programming upgrade instrument that can recognize and overhaul the required sections just. User can uploading files, updates, modify, delete, etc. It gives the information related to the Division and replication of data in cloud Storage for optimal performance and security.In this paper, securely share the data file among thedynamic groups. Without revealing their identity membersin the same group can share the data efficiently.Cryptography is used for over all security. Whencompared to other algorithm key size is very small, it isnot able to hack easily. It is used for efficient revocationwithout updating private keys of remaining users. This paper proposed system to realize efficient and secure data integrity auditing for dynamic data. The proposedmodel consists of the public data auditing. This technique will provide better data confidentiality compare to othermethodologies.

REFERENCES

[1].K. Bilal, M. Manzano, S.U. Khan, E. Calle, K. Li, and A. Zomaya, "On the characterization of the structural robustness of data center networks," IEEE Transactions on Cloud Computing,Vol. 1, No. 1, 2013, pp. 64-77.
[2].D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, "Energy-efficient data replication in cloud computing datacenters," In IEEE Globecom Workshops, 2013, pp. 446-451.
[3]. J. Yuan and S. Yu, "Efficient public integrity checking for cloud data sharing with multi-user modification," in Proc. of IEEE INFOCOM 2014, Toronto, Canada, Apr. 2014, pp. 2121–2129.
[4]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. of IEEE INFOCOM 2010, CA, USA, Mar. 2010, pp no. 525533.
[5].K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, Vol. 4, No. 1, 2013, pp. 1-13.
[6] W. K. Hale, "Frequency assignment: Theory and applications,"Proceedings of the IEEE, Vol. 68, No. 12, 1980, pp. 1497-1514.
[7] K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B.Fernandez, "An analysis of security issues for cloud computing,"Journal of Internet Services and Applications, Vol. 4, No. 1,2013, pp. 1-13.
[8] M. Hogan, F. Liu, A.Sokol, and J. Tong, "NIST cloud computingstandards roadmap," NIST Special Publication, July 2011.
[9] W. A. Jansen, "Cloud hooks: Security and privacy issues incloud computing," In 44th Hawaii IEEE International ConferenceonSystem Sciences (HICSS), 2011, pp. 1-10.
[10] A. Juels and A. Opera, "New approaches to security andavailability for cloud data," Communications of the ACM, Vol.56, No. 2, 2013, pp. 64-73.
[11] G. Kappes, A. Hatzieleftheriou, and S. V. Anastasia is, "Dike:Virtualization-aware Access Control for Multitenant Filesystems,"University of Ioannina, Greece, Technical Report No.DCS2013-1, 2013.