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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

A Survey on New Approach for Integrity Checking on Cloudstorage Data

Neha R. Patil[1], Prof. S. R. Patil[2]

Department of Computer Engineering, A. C. Patil College of Engineering, Kharghar, Navi Mumbai, India

Department of Computer Engineering, A. C. Patil College of Engineering, Kharghar, Navi Mumbai, India

ABSTRACT: Outsourcing data to a third-party administrative control, as is done in cloud computing, it gives rise to security concerns. The data compromise may occur due to attacks by other users and nodes within the cloud. Therefore, high security measures are required to protect data within the cloud. Cloud storage can make data users store and access their files any time, from any where and with any device. To ensure the security of the outsourced data,data user needs to periodically check data integrity. There are existing auditing schemes that are based on PKI.There is auditor to check integrity but for that he need to must validate the certificates of data user before auditing data integrity.Thus, It result in a large amount of computation cost. Especially, it brings heavy burden to the auditor in the multi user setting. Overcome this problem, in this paper, we propose an efficient ID based auditing protocol for cloud data integrity based on IDBased Cryptography. It supports batch auditing in the multi-user setting. Finally, extensive security and simulation results show that our ID-based auditing protocols are secure and efficient especially it reduces the computation cost of the auditor in the multi-user setting. It improves security by creating of replica of each file block and store it on different nodes. If the attackerattacks on the cloud, then he/she will not get any information of file as every block of files are spread on the nodes except adjacent nodes. Thus purpose of this work is to develop an auditing scheme which posses the capabilities such as privacy preserving, public auditing, maintaining the data integrity along with confidentiality. And also it must support batch auditing and data dynamics operations. Thus the new auditing scheme is been developed by considering all these requirements.

KEYWORDS: cloud security, ID-based auditing; Security proof, The CDH problem, Data integrity checking

I. INTRODUCTION

Cloud computing can be considered as a new computing standard that can provide services on demand at a minimal cost. The well-known and commonly used services models in the cloud paradigm are Software as a Services, Platform as a Servicesand Infrastructure as a Services and Storage as a Services. Here the mainly focus on Storage as a Services. Storage as a Service is one of the important services of cloud computing in which data is remotely maintained, managed and backed up. The service is available to users over a network, which is usually the internet. It allows the user to store files online so that the user can access them from any location via the internet. The provider cloud makes them available to the user online by keeping
the uploaded files on an external server. This gives cloud storage service provider ease and convenience, but can potentially be costly. Cloud storage has its benefits, but it is also important to remain secure while taking advantage of cloud technology.
In short, issues in cloud data security include data privacy, data protection, data availability, data location and secure transmission. The security challenges in the cloud include threats, data loss, services disruption and outside malicious attacks. Data integrity in the cloud system means preserving information integrity. The data should not be lost or modified by unauthorized users. Cloud computing providers are trusted to maintain data integrity and accuracy. Therefore security, integrity, privacy and confidentiality of the stored data on the cloud should be considered and are important requirements from user's point of view. To achieve all of these
requirements, new techniques or methods should be developed and implemented.Although cloud storage provides great advantages and conveniences for the users, it faces many new security challenges since the user no longer possesses

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

their data locally. The users might worry whether their data are lost or corrupted due to hardware errors and software bugs.

II. MOTIVATION

In PKI the auditor must validate the certificates of data user before auditing data integrity. Thus, it results in a large amount of computation cost. Especially, it brings heavy burden to the audit.
Existing system need to obtain public key certificate from certificate authority (CA) andverify the validity of public key certificate, it increase computation cost and communication overhead. Proposed IBC allows data user to obtain public keys without the corresponding privatekeys. That is, contrary to traditional public key derivation schemes, IBC does not requireto compute the private key before producing the public key. Indeed, data users can directly use ID based public keys to encrypt data before storage at no extra cost of communication.Here in IBC permits to data user to use the same ID based public key under the different PKG, That is, a ID based public key corresponds to multiple private keys. Thus, it alleviates data users storage burden to public keys.

III. OBJECTIVE

1. Develop a system an ID-based public auditing protocol by combining the ID-based cryptography with homomorphic authenticator technique.
2. Develop the system support batch auditing in the multi-user setting.

IV. REVIEW OF LITERATURE

1.Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud [4], Juels et al. solve this open problem and propose the first POR scheme with public verifiability and constant communication cost: in proposed scheme, the message exchanged between the prover and verifier is composed of constant number of group elements; different from existing private POR constructions, scheme allows public verification and releases the data owners from the burden of staying online. We achieved these by tailoring and uniquely combining techniques such as constant size polynomial commitment and homomorphic linear authenticators. Thorough analysis shows that proposed scheme is efficient and Practical. And prove the security of our scheme based on the Computational Diffie-Hellman Problem, the Strong Diffie-Hellman assumption and the Bilinear Strong Diffie-Hellman assumption.

2 .Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources. While data outsourcing relieves the owners of the burden of local data storage and maintenance, it also eliminates their physical control of storage dependability and security, which traditionally has been expected by both enterprises and individuals with high service-level requirements. In order to facilitate rapid deployment of cloud data storage service and regain security assurances with outsourced data dependability, efficient methods that enable on-demand data correctness verification on behalf of cloud data owners have to be designed. In [2] Wang et al. propose that publicly auditable cloud data storage is able to help this nascent cloud economy become fully established. With public audit ability, a trusted entity with expertise and capabilities data owners do not possess can be delegated as an external audit party to assess the risk of outsourced data when needed.
Such an auditing service not only helps save data owners computation resources but also provides a transparent yet cost-effective method for data owners to gain trust in the cloud. We describe approaches and system requirements that should be brought into consideration, and outline challenges that need to be resolved for such a publicly auditable secure cloud storage service to become a reality.

3 The cloud computing, upsurges the capabilities of the hardware resources by optimal and shared utilization. The above mentioned features encourage the organizations and individual users to shift their applications and services to the cloud. Even the critical infrastructure. The migration of users assets (data, applications, etc.) outside the administrative

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

control in a shared environment where numerous users are faces the security concerns. In [1] Ali et al. has given survey details the security issues that arise due to the very nature of cloud computing. Moreover, the survey presents the recent solutions presented in the literature to counter the security issues.

4 .Introduce a model for provable data possession(PDP) that allows a client that has stored data at an Untrusted server to verify that the server possesses the original data without retrieving it.In [3] the model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDPmodel for remote data checking supports large data sets in widely-distributed storage systems. Remote data integrity checking is of crucial importance in cloud storage. It can make the clients Wang[5] verify whether their outsourced data is kept intact without downloading the whole data. In some application scenarios, the clients have to store their data on multi-cloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifiers cost. From the two points, propose a novel remote data integrity checking model: IDDPDP (identity-based distributed provable data possession) in multi-cloud storage. The formal system model and security model are given. Based on the bilinear pairings, a concrete ID-DPDP protocol is designed. The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational DiffieHellman) problem.

5 .The Cloud storage service has made the users to access their data anywhere anytime without any trouble. Available systems that provide support for the remote data integrity are useful for quality of service testing but do not deal with server failure or handling misbehaving servers. In [6],Ahire et.al. Proposed system ensures storage integrity in the server where the cloud users data is stored. It achieves strong cloud storage security and fast data error localization with the results provided by the auditing mechanism that is carried out by the Third Party Auditor.
Also it further supports secure and efficient dynamic operations on outsourced data. Third Party Auditor carries out the public auditing in-order to maintain the integrity for the data stored in cloud. The user delegates the integrity checking tasks of the data stored in the cloud storage to the Third Party Auditor, who then does the auditing process. Erasure correcting code is used in
the file distribution and depend ability against Byzantine failure. Data integrity in ensured with the help of verification key along with erasure coded data which also allows handling of storage correctness and identification of misbehaving cloud server.

6.In this paper, Ali et al.[7] propose Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. n the DROPS methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Moreover, the nodes storing the fragments, are separated with certain distance
by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments. Furthermore, the DROPS methodology does not rely on the traditional cryptographic techniques for the data security; thereby relieving the system of computationally expensive methodologies. We show that the probability to locate and compromise all of the nodes storing the fragments of a single file is extremely low. We also compare the performance of the DROPS methodology with ten other schemes. The higher level of security with slight performance overhead was
observed.

7 .proposed ID-RDPC model suitable for company-oriented cloud storage. And it is not ID-based auditing since data tag generation algorithm is not ID-based signature, but a PKI-based signature. It also increases computation cost[8].

V.EXISTING SYSTEM

Cloud storage paradigm is to let the data users upload the large data files to the cloud servers in order to relieve of the burden of storage and computation of data users. However, it results in a potential problem: data user no longer

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

possesses their data locally. Thus, it is very importance for the data user to ensure that their data are being correctly stored and maintained. There are existing auditing schemes that are based on PKI. There is auditor to check integrity but for that he need to must validate the certificates of data user before auditing data integrity. Thus, It result in a large amount of computation cost. Especially, it brings heavy burden to the auditor in the multi user setting. Scheme is not ID-based auditing since data tag generation algorithm is not an ID-based signature, but a PKI-based signature. In the PKI-based auditing system, there exists key management problem; the cloud user needs to manage its public key certificate. In general, for the security of the stored data, the mechanism can be used merely in such a situation: one key and one file. If they reuse their public private key pair to produce the tags of the data block for the different files, the cloud server can deceive them by forging the tag of the data block. Consequently, when the data user wants to store multiple data files in the cloud, it needs to remember multiple key-pairs for different files. Furthermore, if the data user loses the keys, it might no longer execute any integrity checking, except for retrieving the data files from the cloud to regenerate the verification meta-data. Thus, for a source-constrained cloud user, the key management of PKI-based data integrity checking scheme might become a difficult problem as multiple keys need to be stored at the user side.

Disadvantage-

1) Increase the computation cost.
2) An auditor, to execute auditing protocol, it first needs to retrieve the certificate of public key from CA, then to check the validity of public key's certificate.
3) Multiple keys need to be stored at the user side.

VI. SYSTEM ARCHITECTURE

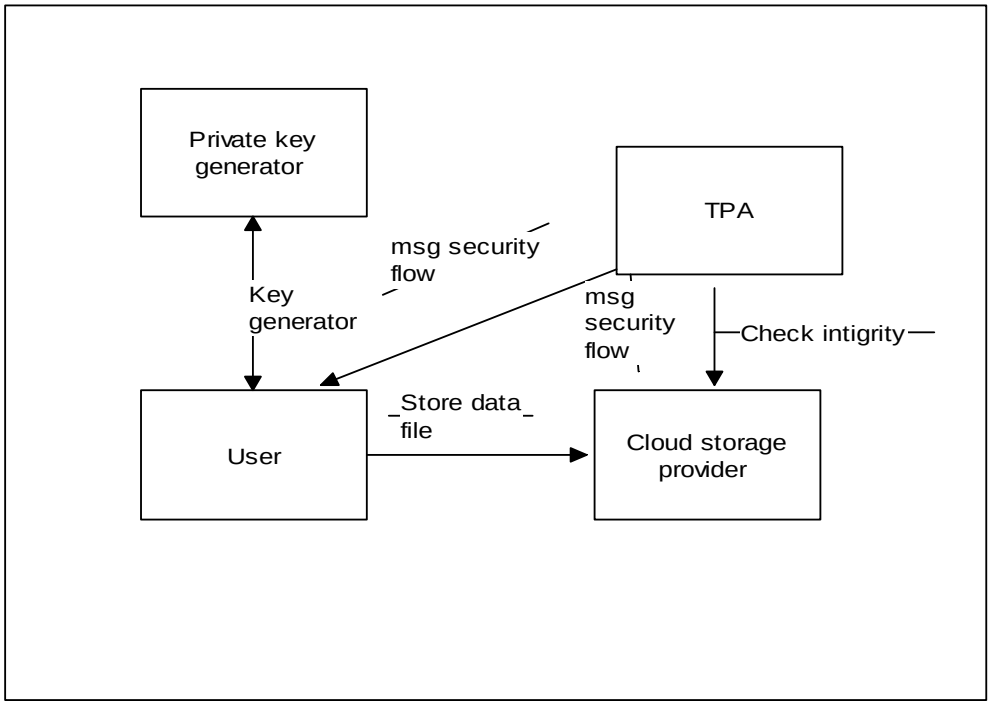

Fig.No.01) System architecture

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

VII. SYSTEM OVERVIEW

The system involves four entities: data users, the cloud server, the third party auditor and private key generator(PKG).Their roles are identified as follows:–

1. Data user: it is an entity which has a large amount of data files to be outsourced to the cloud storage for data maintenance and computation. In general, it is a resource-constrained entity. Here file will encrypt by encryption Aes algorithm and store in fragments in way owner of file will enter no. of fragments and according to that file will split. Also along with no. of fragment its replica will create and it will store on nodes. T-coloring: Fragment and its replica will store in order of t-coloring in way that fragment of one file will not stored in adjusant node .Also for replica. So hacker will not get any idea about the all fragment of one files storage location.

Another User will get his file after entering files secrete key which is sent by user on mail by Owner of the file. At time of downloading merging is performed by system

2. cloud server : it is an entity which has unlimited storage space and computation capability. And it is responsible for storing and maintaining the outsourced data and can provide the data access to the data user.

3. The auditor: it is a trusted third-party which has expertise and capabilities to provide data auditing service on behalf of data users with cloud servers. When auditor got knows the fragment is loosed at that time he will place fragment by its replica.

4. Private Key generator: it is responsible to set up the whole system parameter and issue private key for each data users. Cloud storage paradigm is to let the data users upload the large data files to the cloud servers in order to relieve of the burden of storage and computation of data users. However, it results in a potential problem: data user no longer possesses their data locally. Thus, it is of very importance for the data user to ensure that their data are being correctly stored and maintained. That is a reason why data users should be equipped with certain security measures so that they can periodically verify the integrity of the out sourced data even without the existence of local copies. Key will generate at the time of encryption.

VIII. CONCLUSION

In this paper, propose an ID-based publicauditing protocol by combining the ID-based cryptography with homomorphic authenticate or technique. This system increase the data confidentiality..Finally, This auditing protocol is also extended to support batch auditing in the multi-user setting. Proposed Out sourcing data to a third-party administrative control, as is done in cloud computing, gives rise to security concerns. The data compromise may occur due to attacks by other users and nodes within the cloud.Here we are storing user uploaded files replica,so when stored file is hacked by user then replica file can get user from another location.

REFERENCES

[1] M.Ali, S.U.Khan, A.V.Vasilakos, Security in cloud computing: Opportunities and challenges,Inf.Sci.305(1)(2015)357383.
[2] C.Wang,K.Ren,W.Lou,J.Li,Toward publicly auditable secure cloud data storage services,IEEENetw.24(4)(2010)1924.
[3] H.Wang,Identity based distributed provable data possession in multi clouds storage, IEEET. Serv. Compsut.8(2)(2015)328340.
[4] A.Juels,B.S.KaliskiJr.,Pors: Proofs of retrievability for largefiles,in:Proceedings of the 14thACMConference on Computer and Communications Security(CCS07),2007,pp.584597.
[5] H.Wang,Identity based distributed provable data possession in multi clouds torage,IEEET.Serv.Compsut.8(2)(2015)328340.
[6] Study and Implementation of Secure Storage Service in Cloud Computing Mrs. PramilaKailas Ahire, Prof. R.V. Patil, IJRACET, 2015.
[7] Mazhar Ali, Student Member, IEEE, Kashif Bilal, Student Member, IEEE, Samee U.Khan, Senior Member, IEEE, BharadwajVeeravalli, Senior Member, IEEE, Keqin Li,Senior Member, IEEE, and Albert Y. Zomaya, Fellow, IEEE "DROPS: Division and Replicationof Data in Cloud for Optimal Performance and Security", IEEE Trans. on CloudComputing., 2015.
[8] Jianhong Zhang Pengyan Li Jian Mao, IPad: ID-based public auditing for the outsourceddata in the standard model Springer Science+Business Media New York 2015-16
[9] S.G.Ateniese,R.Burns,R.Curtmola,J.Herring,L.Kissner,Z.Peterson,D.Song,Provable datapossession at untrusted stores,in:Proceedingsofthe14thACM Conference on Computer andCommunications Security(CCS07),2007,pp.598609.
[10] G.Ateniese, S.Kamara,J.Katz, Proofs of storage from homomorphic identification protocols,in:Proceedings of the International Conference on Theory and Application of Cryptologyand Information Security: Advances in Cryptology,2009,pp.319333.
[11] J.Zhang,W.Tang,J.Mao,Efficient public verification proof of retrievability scheme in cloud,Clust.Comput.17(4)(2014)14011411.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

[12] G.Calandriello, P.Papadimitratos, A.Lioy,J. P.Hubaux,Efficient and robust pseudonymousauthenticationinVANET,in:ProceedingsoftheVANET,2007,2007,pp.1928.
[13] E.C.Chang,J.Xu,Remote integrity check with dishoneststorageserver,in:Proceeding s ofthe13th European Symposium Researchin Computer Security(ESORICS08),2008,pp.223237.
[14] JianhongZhanga, Qiaocui Dong, Efficient ID-based public auditing for the outsourceddata in cloud storage, 0020-0255/ 2016 Elsevier Inc.