IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 69-72
www.iosrjournals.org

PRIVACY & DATA INTEGRITY FOR SECURE CLOUD STORAGE

Almas Ansari[1], Prof.Chetan Bawankar[2]
1 (Student, M.Tech Dept. Computer Science & Engineering J.D. College of Engineering, Nagpur, India)
2 (Asst. Prof Dept. Computer Science & Engineering J.D. College of Engineering, Nagpur, India)

ABSTRACT: *Cloud computing is clearly one of today's most enticing technology areas due, at least in part, to its cost-efficiency and flexibility. However, despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. In this paper, we characterize the problems and their impact on adoption. In addition, and equally importantly, we describe how the combination of existing research thrusts has the potential to alleviate many of the concerns impeding adoption. In particular, we argue that with continued research advances in trusted computing and computation-supporting encryption, life in the cloud can be advantageous from a business intelligence standpoint over the isolated alternative that is more common today. A third party service provider, stores & maintains data, application or infrastructure of Cloud user. Relinquishing the control over data and application poses challenges of security, performance, availability and privacy. Security issues in Cloud computing are most significant among all others. Information Technology (IT) auditing mechanisms and framework in cloud can play an important role in compliance of Cloud IT security policies. In this paper, we focus on cloud security audit mechanisms and models.*

1. INTRODUCTION

Today, the 14th largest software company by market capitalization (Salesforce.com) operates almost entirely in the cloud, the top five software companies by sales revenue all have major cloud offerings, and the market as a whole is predicted to grow to $160B by 2011 (source: Merrill Lynch). Yet, despite the trumpeted business and technical advantages of cloud computing, many potential cloud users have yet to join the cloud, and those major corporations that are cloud users are for the most part putting only their less sensitive data in the cloud. Lack of control in the cloud is the major worry. One aspect of control is transparency in the cloud implementation - somewhat contrary to the original promise of cloud computing in which the cloud implementation is not relevant. Transparency is needed for regulatory reasons and to ease concern over the potential for data breaches. Because of today's perceived lack of control, larger companies are testing the waters with smaller projects and less sensitive data. In short, the potential of the cloud is not being realized.

When thinking about solutions to cloud computing's adoption problem, it is important to realize that many of the issues are essentially old problems in a new setting, although they may be more acute. For example, corporate partnerships and offshore outsourcing involve similar trust and regulatory issues. Similarly, open source software enables IT departments to quickly build and deploy applications, but at the cost of control and governance. Finally, virtual machine attacks and Web service vulnerabilities existed long before cloud computing became fashionable. Indeed, this very overlap is reason for optimism; many of these "cloud problems" have long been studied and the foundations for solutions exist.

Third-party data control: The legal implications of data and applications being held by a third party are complex and not well understood. There is also a potential lack of control and transparency when a third party holds the data. Part of the hype of cloud computing is that the cloud can be implementation independent, but in reality regulatory compliance requires transparency into the cloud. All this is prompting some companies to build private clouds to avoid these issues and yet retain some of the advantages of cloud Computing.

II. LITERATURE REVIEW

Data outsourcing in Cloud Computing is fastbecoming economically viable for large enterprises. In fact,this data outsourcing is ultimately retrieving user's controlover its own data and does not provide any assurance ondata integrity and availability. On behalf of cloud user, athird party auditor (TPA) who has resources and experiencethat a user does not have can be emplaced to audit theintegrity of large data storage. But user data privacy is stillexposed to a TPA, which is required to be secured againstunauthorized leakage. Wang and Sherman et al. [2] haveproposed a public auditing system of data storage securityby developing a

privacy preserving auditing protocol. Bywhich auditor can audit without having knowledge of user'sdata contents. Wang and Sherman also proposed a batchauditing protocol where multiple auditing tasks fromdifferent users can be performed simultaneously by a TPA.

Cloud computing provides development, deliveryand consumption of IT services over a distributed networkenvironment. These services are interdependent on eachother and failure of one service can cause unavailability ofother service resulting loss of revenue, damaging repute ofthe enterprise providing services and unreliability over thecloud. To minimize the risks of cloud outages there is a direneed for 'cloud governance' model that could control andmanage cloud-based services and storage.

In this paper[8], Zhiyun and Meina et al. have proposed a cloud basedgovernance model that securely manages and controls theimplementation of cloud services according to recognizedpolicies, service management policies and their auditprocedures. Elements of operational governance modelincludes: Authentication, i.e. enforcement of identity andaccess management system. Authorization, it enablesimplementation of a role-based authorization model. Audit,the collection of information related to the compliance ofcloud security and service management policies.Monitoring, the preparation of individual and aggregate datatransaction reports, summaries and graphs.

Juels et al. [11] describe a "proof of retrievability" (PoR) model, where spot-checking and error-correcting codes are used to ensure both "possession" and "retrievability" of data files on remote archive service systems. However, the number of audit challenges a user can perform is fixed a priori, and public auditability is not supported in their main scheme. Although they describe a straightforward Merkle-tree construction for public PoRs, this approach only works with encrypted data.

III. PROBLEM DEFINATION

A. The System and Threat Model

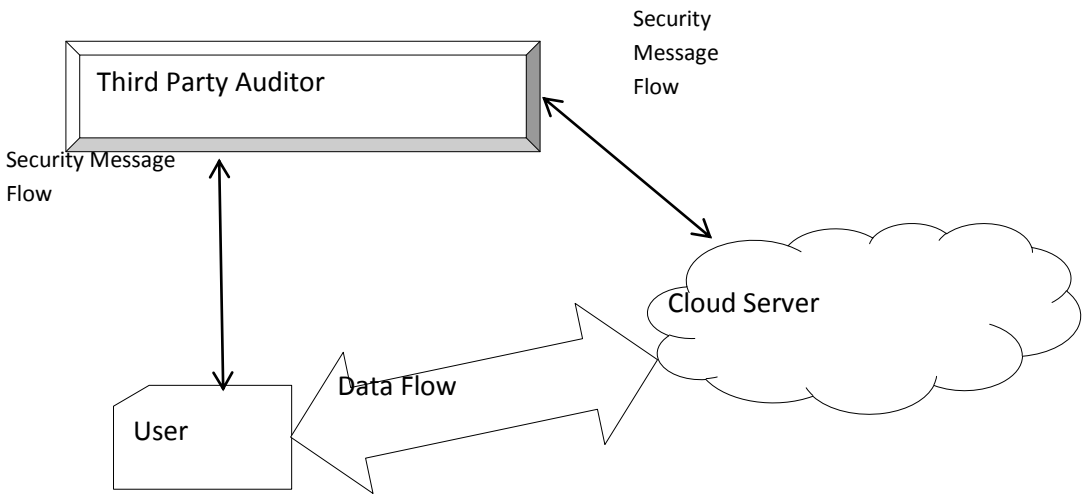


Fig. 1: The architecture of cloud data storage service

We consider a cloud data storage service involving threedifferent entities, as illustrated in Fig. 1: the cloud user(U), who has large amount of data files to be stored in thecloud; the cloud server (CS), which is managed by cloudservice provider (CSP) to provide data storage service andhas significant storage space and computation resources (wewill not differentiate CS and CSP hereafter.); the third partyauditor (TPA), who has expertise and capabilities that cloudusers do not have and is trusted to assess the cloud storageservice security on behalf of the user upon request.

B. Design Goals

To enable privacy-preserving public auditing for cloud datastorage under the aforementioned model, our protocol designshould achieve the following security and performanceguarantee:
1) Public auditability: to allow TPA to verify thecorrectness of the cloud data on demand without retrievinga copy of the whole data or introducing additional on-lineburden to the cloud users;
2) Storage correctness: to ensurethat there exists no cheating cloud server that can pass theaudit from TPA without indeed storing users' data intact;
3) Privacy-preserving: to ensure that there exists no wayfor TPA to derive users' data content from the informationcollected during the auditing process;
4) Batch auditing: toenable TPA with secure and efficient auditing capability tocope with multiple auditing delegations from possibly largenumber of different users simultaneously;
5) Lightweight: toallow TPA to perform auditing with minimum communicationand computation overhead.

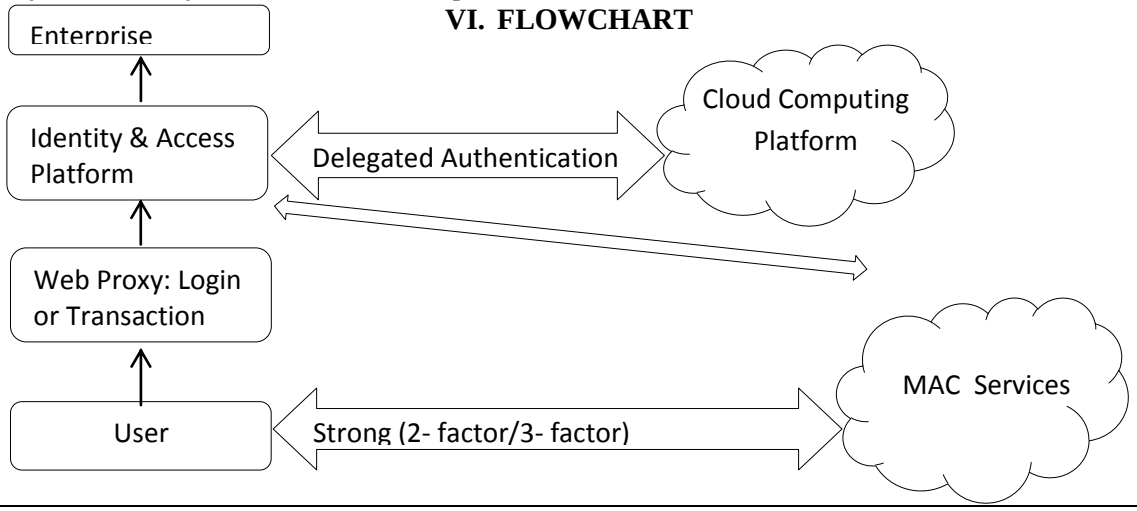
IV. THE PROPOSED SCHEMES

In the introduction we motivated the public auditabilitywith achieving economies of scale for cloud computing. Thissection presents our public auditing scheme for cloud datastorage security. We start from the overview of our publicauditing system and discuss two straightforward schemes andtheir demerits. Then we present our main result for privacypreservingpublic auditing to achieve the aforementioned designgoals. Finally, we show how to extent our main scheme tosupport batch auditing for TPA upon delegations from multiusers.Our public auditing system can be constructed from the
above auditing scheme in two phases, Setup and Audit:
• Setup: The user initializes the public and secret parametersof the system by executing KeyGen, and preprocessesthe data file F by using SigGen to generatethe verification metadata. The user then store the data file F at the cloud server, delete its local copy, and publishesthe verification metadata to TPA for later audit. As partof pre-processing, the user may alter the data file F byexpanding it or including additional metadata to be storedat server.
• Audit: The TPA issues an audit message or challengeto the cloud server to make sure that the cloud serverhas retained the data file F properly at the time of theaudit. The cloud server will derive a response messagefrom a function of the stored data file F by executingGenProof. Using the verification metadata, the TPAverifies the response via VerifyProof.

V. ALGORITHM

A public auditing scheme consists of four algorithms (KeyGen, SigGen, GenProof, VerifyProof).
KeyGen: key generation algorithm that is run by the user to setup the scheme
SigGen: used by the user to generate verification metadata, which may consist of MAC, signatures or other information used for auditing
GenProof: run by the cloud server to generate a proof of data storage correctness
VerifyProof: run by the TPA to audit the proof from the cloud server

VI. FLOWCHART



VII. CONCLUSION

In this paper, we propose a privacy auditingsystem for data storage security in Cloud Computing. Weutilize the homomorphic authenticator and random masking toguarantee that TPA would not learn any knowledge about thedata content stored on the cloud server during the efficientauditing process, which not only eliminates the burden ofcloud user from the tedious and possibly expensive auditingtask, but also alleviates the users' fear of their outsourced dataleakage. Considering TPA may concurrently handle multipleaudit sessions from different users for their outsourced datafiles, we further extend our privacy-preserving public auditingprotocol into a multi-user setting, where TPA can perform themultiple auditing tasks in a batch manner, i.e., simultaneously.Extensive analysis shows that the proposed schemes are provablysecure and highly efficient.

REFERENCE:

[1] Cong Wang ; Chow, S.S.M. ; Qian Wang ; KuiRen ;Wenjing Lou "Privacy-Preserving Public Auditing for Secure CloudStorage", IEEE Transactions on Computers Volume: 62 , Issue: 2 2013 ,PP no : 362 - 375
[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.
[3] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html, June 2009.
[4] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.
[5] M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions," http://www.techcrunch.com 2006/12/28/gmail-disasterreportsof- mass-email-deletions/, 2006.
[6] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors," http:// www.techcrunch.com /2008/07/10/mediamaxthelinkup-closesits-doors/, July 2008.
[7] Amazon.com, "Amazon s3 Availability Event: July 20, 2008," http://status.aws.amazon.com/s3-20080720.html, July 2008.
[8] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.
[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.
[10] M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, 2008.
[11] Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.
[12] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing," http://www.cloudsecurityalliance. org, 2009.
[13] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107, Dec. 2008.
[14] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.
[15] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," http://aspe.hhs.gov/ admnsimp/pl104191.htm, 1996.
[16] R. Curtmola, O. Khan, and R. Burns, "Robust Remote Data Checking," Proc. Fourth ACM Int'l Workshop Storage Security and Survivability (StorageSS '08), pp. 63-68, 2008.
[17] K.D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 43-54, 2009.
[18] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," J. Cryptology, vol. 17, no. 4, pp. 297-319, 2004.
[19] A.L. Ferrara, M. Green, S. Hohenberger, and M. Pedersen, "Practical Short Signature Batch Verification," Proc. Cryptographers' Track at the RSA Conf. 2009 on Topics in Cryptology (CT-RSA), pp. 309-324, 2009.
[20] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), pp. 1-10, 2008.