Achieving Secure Cloud Data Storage without using of Trusted Third Party Auditor: A Review

Hiren Patel
Department of Computer Engineering
S. P. College of Engineering
Visnagar, India

Dhiren Patel
Department of Computer Engineering
S. V. National Institute of Technology
Surat, India

ABSTRACT
Cloud computing is a model where computing resources are rendered on rental basis with the use of clusters of commodity computers. In one of the services offered by cloud viz. Storage as a Service, users outsource their data to cloud without having direct possession or control on it. As the cloud service provider is not completely trustworthy, it raises issues such as data security and privacy. Achieving secure cloud data storage is one of the major security issues. The issue can be addressed into two directions viz. first which makes use of trusted third party auditor (TTPA) and other which do not. In this paper, we review various recently proposed approaches to ensure data storage correctness without using TTPA

General Terms
Security and Protection - Authentication and Access Control et. al.

Keywords
Cloud Computing, Data Storage Correctness, Privacy, Security, Trusted Third Party Auditor.

1. INTRODUCTION
Advancement in Internet bandwidth, processors' computing capabilities and networking technologies has motivated many organizations to outsource their computing, networking and storage need. Cloud computing is a novel paradigm where organizations or individuals use the services offered by cloud on rental basis and enjoy the advantage of cost-saving on initial investment to setup private storage infrastructure, to purchase higher versioned processors or networking elements quite often. But while taking pleasure in having numerous benefits, the fact that the most important asset of an organization or individual, the confidential data, is not under the owners' direct physical control, makes them worry. So the issues of privacy and security are to be addressed before convincing users to go for cloud. The main goals are to protect confidentiality and integrity of users' data stored on cloud. Confidentially is about prohibiting the cloud service provider (or any unauthorized user) to gain knowledge of the users' data. Integrity is about forbidding unauthorized alteration to users' data. And if at all, one or both of these violate, the same should be brought into the urgent notice of the data owner.

Recently, many researchers have attended the issue of data storage security in cloud which we broadly categorize into two groups; one which make use of trusted third party auditor (TTPA) and other that do not. Normally TTPA is a reliable independent component which is trusted by both the cloud users and server and has no incentive to conspire with either the cloud server or user during the auditing process. Trusted third party auditor is claimed to have the skill and competence that normal cloud users may not have. In order to save time and reduce computation/communication overhead, many researchers recommend the support of trusted third party (TTP). By leaving the resource consuming cryptographic operations on TTP for achieving confidentiality and integrity, cloud users can be worry-free. But issues such as TTP becoming bottleneck, data leakage, introduction of new vulnerabilities, scalability, accountability, performance overhead, dynamic data support, extra hardware cost incurred etc. have motivated many researchers to address the data storage security problems without using trusted third party auditor, where the cloud user may be comprised of extra application or tool which helps it periodically checks the data integrity. In this article, we review recently proposed such approaches which aim to achieve data storage correctness in cloud computing without making use of trusted third party auditor.

The paper is structured as follows. Section 2 depicts the review of various recent approaches which aim to achieve secure data storage through cryptographic primitives without using trusted third party auditor. Section 3 illustrates issues related to motivations and functionalities of the approaches which do not use trusted third party auditor. Section 4 exemplifies challenges involved in such approaches. We conclude in section 5 with future scope of the work followed by list of references.

2. REVIEW OF RELATED APPROACHES
In this section, we review various recently proposed data storage correctness approaches which do not utilize trusted third party to achieve secure data storage.

Kamara et al. [7] describe higher level cryptographic storage architecture in form of illustration in order to demonstrate how cryptographic techniques can be used to achieve secure data storage in cloud with three components viz. data processor (to process data before sending to cloud), data verifier (to verify the integrity of data stored on cloud) and token generator (to generate token which can be used to pass on credentials to data users at the time of data sharing). Authors also describe various ways to implement the core components of the architecture with standard modern encryption and encoding techniques such as searchable encryption, attribute based encryption and proof of storage techniques. Hota et al. [8] and Sanka et al. [9] address the issue of data security and access control. In [8], authors propose and use a modified Diffie-Hellman key exchange protocol between cloud service provider and cloud user for secretly sharing the symmetric key for secure data access and claim the approach to be efficient and secure. In [9], authors offer capability based access control technique to ensure cloud

accessibility of valid users only. In both the papers, there are mainly three entities viz. data owner (who generates the data and is having all rights on her data along with capacity to transfer rights to other users), data user (who uses data generated by cloud owner based on credentials received from the data owner) and the cloud service provider (central component which acts as data repository and serves the request received from data owner and user after making necessary credential verifications). Authors also presented proof of concept implementation of the cryptographic algorithms in a cloud computing environment using Java RMI. Sravan et al. [10] address the issue of integrity of data stored on cloud. Authors provide a scheme to check data integrity and proof to provide data storage correctness. The scheme can be employed by cloud user and agreed upon by both the cloud provider and cloud user. Due to lightweight in nature, authors claim the scheme to be useful to thin client where computing and storage capacity are limited. In the scheme, special blocks (sentinels) are randomly inserted into the original file and the file is stored on cloud after encryption. At the time of verification, the user challenges the cloud by specifying positions of a collection of sentinels and asking for associated sentinel values. If the file is modified there is quite a possibility that the sentinels are suppressed and in turn the cloud may not respond correctly to the user/verifier. To make the sentinels indistinguishable from original file blocks, authors make use of standard encryption techniques. The limitation of the scheme is that it works on static data only and cannot support dynamic data operations. Also the number of queries by the client is fixed apriori which is very large in practical situation. Shraer et al. [11] present a scheme which claims to achieve data integrity and consistency for remote storage accessed by multiple clients, without significant overhead and without any trusted third party components. The scheme, further, claims not to introduce extra communication overhead due to client-to-client coordination. The model is comprised of two components viz. verifier and commodity storage service at cloud premise. The verifier's responsibilities include integrity and consistency verification, where as commodity storage service allows client to store & retrieve her data. Though the limitation of the model is it does not take the issues of privacy and confidentiality into consideration. Unlike many other approaches which make use hash values for integrity verification, Jianhong et al. [12] propose an RSA-based assumption data integrity check way by combining identity-based cryptography and RSA digital signature for efficient data integrity verification. Authors claim to achieve public verifiability for integrity check. They adopt the blockless approach to authenticate the block tags instead of original data blocks in the verification process. Without specifying a specific scheme or model, Agudo et al. [13] emphasize the use of advance cryptographic techniques such as searchable encryption and secure outsourced computation to achieve secure data storage in cloud computing. Without losing confidentiality of the data, authors realized the significance of allowing operations such as searching on encrypted data. Authors also stress to verify computational output along with data privacy. Chuang et al. [14] propose an Effective Privacy Protection Scheme (EPPS) which provides appropriate privacy protection based on user's privacy requirement without compromising the performance. Authors categorize users' data based on its degree of importance and accordingly suggest the encryption algorithms. Key update frequency is also calculated from data sensitivity requirement to improve performance. Authors also analyze various symmetric key encryption algorithms such as AES (with variable keys), RC4, Blowfish etc. to measure computation time & security score. The issue of integrity verification is not covered in the article. The white paper [15] identifies the key security concerns in cloud computing viz. data leakage, customer identification, data snooping, key management and performance. The article proposes hybrid cryptographic approach i.e. to use faster symmetric key encryption algorithms (E.g. AES) to protect confidentiality of data in rest and recommend slower yet effective asymmetric key encryption algorithms (E.g. RSA) to protect the sensitive keys. The article demonstrates Nasuni product architecture based on OpenPGP encryption framework. Tribhuwan et al. [16] propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of user's data by utilizing the homomorphic token with distributed verification of erasure-coded data. The scheme claims to achieve the integration of storage correctness insurance and data error localization. The paper introduced a two-way handshake scheme based on token management. Xiong et al. [17] propose a scheme named CloudSeal to securely share and distribute contents to achieve end-to-end content security. The scheme ensures the data confidentiality with flexible access control policies for cloud users and efficient content distribution. It makes use of modern cryptographic primitives such as symmetric encryption, proxy based re-encryption, secret sharing and broadcast revocation mechanism. Talib et al. [18] propose an integrity layered architecture on multi-agent system architecture to achieve integrity of data stored on cloud. The paper introduces provably-secure and practical backup cloud data regularly that provide reconstruct the original cloud data by downloading the cloud data vectors from the cloud servers. Ranchal et al. [19] propose an approach for identity management to use identity data on untrusted hosts. The approach is based on the use of predicates over encrypted data and multi-party computing for negotiating a use of a cloud service. It uses active bundle-which is a middleware agent that includes personally identifiable information, privacy policies, a virtual machine that enforces the policies, and has a set of protection mechanisms to protect itself. An active bundle interacts on behalf of a user to authenticate to cloud services using user's privacy policies.

3. MOTIVATIONS AND FUNCTIONALITIES

Most of the approaches discussed in previous section emphasis in having client application to make all necessary cryptographic operations (such as encryption or encoding) on data before sending them to cloud. The cloud service provider may allow the cloud user to download the client application and the application should take care of the entire consumers requirement through soft techniques. While downloading, the cloud user may ask the data owner for required credentials and the key to decrypt the data. For verification purpose, the consumer may send challenge to the server with some basic information about the data file, and the cloud service provider may compute a hash value and returns back to the consumer. Researchers expect this integrity verification phase to be lightweight in operational nature.

The major motivations behind using non-TTP approaches are as follows. First, as TTP is supposed to be a central, independent & reliable component, it may become bottleneck to the entire system. Any unusual activity in TTP may cause entire cloud system to go down or reduction in the performance. Apart from it, the situation of TTP being compromised cannot be ignored. In such a case, it may affect the functioning of whole cloud. The idea of keeping TTP's

functionalities in client application will avoid above mentioned situations and provides decentralized way of administrating the cloud. Second, cloud data owner can directly control the cryptographic operations to be performed on her data stored on cloud. Cloud data owner can specify privacy level of her data and also choose combinations of cryptographic operations from available options instead of TTP to decide what is good for her data. Third, as the data sent from cloud data owner premise is in encrypted form and the required credentials to decrypt the same are kept hidden from cloud service provider, during regulatory compliance, laws which make the data owner responsible for protection of her data can be followed. Fourth, during any legal investigation, cloud service provider cannot handover the data to any statutory body without consulting to data owner. Fifth, most of the approached studied above aim to achieve lightweight integrity verification, which in turn will be useful to thin client users.

It is recommended to provide non-TTP option using client application developed preferably on open source platform by the cloud service provider. Whenever the cloud user get herself registered with the cloud service provider, later allows the former to download a client application. After downloading and installing the application on client premise, the user may use the application for various functionalities such as encryption, encoding, transmitting, receiving, offering credentials to other users etc. We expect the client application to provide flexibility to user where she can have her own set of cryptographic primitives instead of already available options. In this way, we can increase user's faith in using the client application. Here, cloud users can remain offline but cloud service provider needs to remain online all time. Whenever a user comes online, she will have all pending requests popped on her screen regarding required credentials requested from other users. She can allow or deny the requests. She can even ask for credentials to other users' data. Though the keys (private/public) can be kept on client machine, to enhance security and portability, it is recommended to offer a USB dongle which can be kept under the owner's physical control and user can access the cloud from anywhere with the help of the dongle.

4. ISSUES AND CHALLANGES

Though briefly mentioned in above section, following are list of issues/challenges in using approaches mentioned above:

• Key generation/distribution: Every time a user encrypts a file, she has to generate a unique symmetric encryption key with the help of client application downloaded from cloud or using the one selected on her own. For a non-technical user, this may be little confusing operation during initial phase of cloud utilization.

• Performance: This is one of the main issues to be discussed with non-TTP approaches. The soft approach to perform cryptographic computing & communication operations may be as fast as compared to specially designed dedicated extra hardware in form of TTP for resource consuming cryptographic operations. Though one may perform these operation offline, to possible extent, to improve performance.

• Multiple task handling & Batch Auditing: Dedicated TTP is specialized in handling multiple task handling and bath auditing issues. The client application may not give the same performance as TTP with available computing resources in presence of other applications running on client machines.

• Legal Dispute & Accountability: In case of any legal dispute between cloud user and service provider, as there is no trusted third party, we need to have mechanism which has been previously agreed upon by both of them. We even need to provide service level agreements (SLA) between the entities. These set of agreed upon rules and SLA shall be used to prove accountability of the fault.

• Data Dynamics Support: As cloud is not just a third party repository, users can update & share files. A file can updated simultaneously by many users & to keep a trail of the same and keeping an updated final status of a file is a challenging job for the client application. Performance should not be compromised while achieving this goal.

5. CONCLUSION AND FUTURE WORK

Data storage security is one of the important concerns in adopting Cloud computing. Secure data storage can be achieved with one of two directions viz. using trusted third party auditor and without using the same. Later option is explored in this paper. We have studied and analyzed various recently proposed approaches to accomplish data storage security without using trusted third party. In this article, we have pointed out various motivations, issues and challenges in adopting non-TTPA procedures to address cloud security concerns. Our future goal is to design a secure cloud storage system without using TTPA which addresses the issues mentioned.

7. REFERENCES

[1] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, V 3.1, Nov 2011.

[2] W. Jansen, T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication 800-144, December 2011.

[3] K. Raen, C. Wang, Q. Wang, "Security Challenges for the Public Cloud", Published by IEEE Computer Society, Jan/Feb 2012.

[4] "Nine Storage-Related Attributes of an Enterprise Cloud" – A white paper from SAVVIS, A CenturyLink Company, 2011.

[5] N. Virvilis, S. Dritsas, and D. Gritzalis, "Secure Cloud Storage: Available Infrastructures and Architectures Review and Evaluation," vol. 6863, S. Furnell, C. Lambrinoudakis, and G. Pernul, Eds. Springer Berlin / Heidelberg, 2011, pp. 74-85

[6] Hiren B. Patel, Dhiren R. Patel, Bhavesh Borsania, Avi Patel, "Data Storage Security Mode for Cloud Computing", in *Third International Conference on Advances in Communication, Network, and Computing – CNC 2012* organized by ACEEE. February, 2012.

[7] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proceedings of the 14th international conference on Financial cryptography and data security, 2010, pp. 136-149.

[8] C. Hota, S. Sanka, M. Rajarajan, S. Nair, "Capability-based Cryptographic Data Access Control in Cloud Computing", in *International Journal of Advanced Networking and Applications*, Volume 01, Issue 01, 2011.

[9] S. Sanka, C. Hota, and M. Rajarajan, "Secure data access in cloud computing," in 2010 IEEE 4th International

Conference on Internet Multimedia Services Architecture and Application(IMSAA), pp. 1-6, 2010.

[10] R. Sravan Kumar and A. Saxena, "Data integrity proofs in cloud storage," in *2011 Third International Conference on Communication Systems and Networks (COMSNETS)*, 2011, pp. 1-4.

[11] A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y. Michalevsky, and D. Shaket, "Venus: verification for untrusted cloud storage," in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, 2010, pp. 19-30.

[12] Z. Jianhong and C. Hua, "Security storage in the Cloud Computing: A RSA-based assumption data integrity check without original data," in *2010 International Conference on Educational and Information Technology (ICEIT)*, 2010, vol. 2, pp. 143 -147.

[13] I. Agudo, D. Nuñez, G. Giammatteo, P. Rizomiliotis, and C. Lambrinoudakis, "Cryptography Goes to the Cloud," in *1st International Workshop on Security and Trust for Applications in Virtualized Environments (STAVE 2011)*, 2011, vol. 187, p. 190-197.

[14] I.-hsun Chuang, S.-hao Li, K.-chieh Huang, Y.-hwang Kuo, "An Effective Privacy Protection Scheme for Cloud Computing" In *13th International Conference on Advanced Communication Technology (ICACT)*, 2011, pp. 260-265, Feb-2011.