Available online at www.sciencedirect.com

ScienceDirect

Materials Today: ProceedingsXX (2016) XXX–XXX

materialstoday: PROCEEDINGS

www.materialstoday.com/proceedings

PMME 2016

# ANALYSIS AND DESIGN OF AN OPTIMIZED SECURE AUDITING PROTOCOL FOR STORING DATA DYNAMICALLY IN CLOUD COMPUTING

Raman Kumar[a] and Gurpreet Singh[b]

[a,b]*Department of Computer Science and Engineering*
[a,b]*D A V Institute of Engineering and Technology, Jalandhar, Punjab*
[a,b]*er.ramankumar@aol.in*

**Abstract**

The remote server (Cloud Service Provider (CSP)) store their data on cloud servers and users can access their data from cloud servers while implementing the concept of cloud computing. Because of some security constraints in data outsourcing, the latest concept of data hosting service also arises new security challenges; those challenges can be handled by third party auditing service to check the data integrity in the cloud server. There are few existing remote integrity checking methods those can serve for static stored data but not able to work dynamically. In this paper, we develop three-tier security architecture for storing multimedia files which include role base access control, encryption, and signature verification. Therefore, an enhanced secure dynamic auditing protocol is proposed, which can store data correctly in the cloud. In the proposed scheme, both the combiner and the third party auditor (TPA) can verify the integrity of the information that they are receiving from each other. Therefore, the proposed an optimized secure dynamic auditing protocol is secure and efficient against various conspiracy attacks.

Selection and Peer-review under responsibility of International Conference on Processing of Materials, Minerals and Energy (July 29th – 30th) 2016, Ongole, Andhra Pradesh, India.

*Keywords:*Cloud Computing, Communication overhead, Time cost of individual client, Packet delivery ratio, Energy level, Average delay, Packet delivery time and Throughput

## 1. Introduction

The cloud computing is a well nourishing paradigm. The NIST definition characterized on important aspects of cloud computing and broad comparisons of cloud computing services and deployment strategies. The service and formation models defined form a simple taxonomy not predetermined to constrain any particular method of implementation, service delivery, or business operation. The hybrid cloud management platform performs some


Selection and Peer-review under responsibility of International Conference on Processing of Materials, Minerals and Energy (July 29th – 30th) 2016, Ongole, Andhra Pradesh, India.

imperative functions like Interfacing to multiple clouds, Unify the interface, Abstract, cloud agnostic workload blueprints, Stack provisioning, Policy management.

### *1.1. Essential Characteristics*

On-demand self-service: On-demand service is the methodology, by which recourses are allocated on runtime and this type of transition happens immediately, although it depends on the cloud provider, what kind of architecture and recourses they have.
Broad network access: Broad network access means that access to the private cloud can be enhanced to the other level like employees can use Smartphone, tablets and other devices to access the company recourses and work upon them through those devices.
Resource pooling: The cloud provider pooled a lot of resources on their side over the cloud. They authorize the uses to request those available resources at any time like on-demand, self-service. The customer could alter their level of service at any time without even interacting with the cloud provider.
Rapid elasticity. By rapid elasticity, consumers can request additional space in the cloud and another type of services as per their requirements. At cloud side administering the multiple requests is a demanding and precise administration.
Measured service. The services provided by the cloud server and requested services by the customer on real-time or self-service basis can be measured by the mechanism, which should maintain the transparency between the service provider and the user as cited in figure 1.

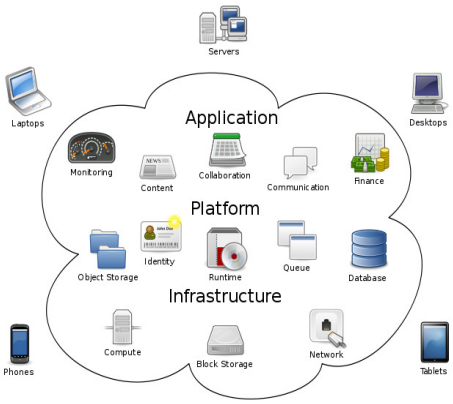


Figure-1: Overall view of cloud computing

### *1.2. Service Models*

Software as a Service (SaaS), the user can access the programs like a web browser or other type of programs, which are at the cloud side. The applications on the cloud can be shared by multiple clients through thin client interface, such as web browser and program interface. Platform as a Service (PaaS), consumer acquire operating environment created using programming languages, libraries, services, and tools which are supported by the provider. Infrastructure as a Service (IaaS), customer can access hardware and software resources provided by the cloud service provider. These are the services like storage, server, network components etc.

### *1.3. Cloud Computing Communication*

A cloud computing provides flexible services to the client devices by which clients can access the resources those are pooled over the cloud server. Service model used in this paper is Storage-as-a-service, by which clients those are registered to a particular cloud server can place their local data onto the remote storage available on the cloud side. A large number of data owners already started the adoption of SaaS service to store their local data onto the cloud

server by which they eliminate the limitation of storage on a local machine and reduce maintenance cost. The existing SaaS service providers are Microsoft with Sky Drive, Google Documents and DropBox, etc. They assure data availability and integrity to the user on different systems/locations/networks. Cloud storage is very useful service of a cloud computing (CC) by which data owners (clients) able to migrate their local data over the remote cloud server. Anyhow this paradigm also arises many security challenges [3]. Because data is not safe in any infrastructure, no matter what the cloud service provider uses optimal security measures (CSP) even CPS could be dishonest. They could delete the client's rarely used data and also pretend that the data is correctly stored in the cloud. Therefore, Clients need to be assured that data is efficiently and correctly stored onto the remote server. Many authors proposed different types of dynamic auditing protocols. They can support the dynamic operations on the stored data over cloud. But these security protocols may leak the data to the third-party auditor during checking the integrity of data stored at cloud server as it will request the server to access the linear combination of data blocks.

## 2. Previous Work

The previous work for the proposed hypothesis as listed below:

M. Lillibridge et al. (2003) [2] In this paper Peer-to-peer backup technique is introduced that enables computers to back up their data cooperatively. Each computer has a set of partners each hiding its backup data. It's a highly reliable method because multiple copies of data available on different computers. Periodically challenges are sent to determine the integrity of data stored on cooperative computers. Inexpensive: it appears to be a cheaper than existing Internet backup services.

Y. Deswarte et al. (2004) [3] In this paper focus in on checking the integrity of files on remote server. The challenge-response protocol used for checking integrity the correctness of stored data. The random checksum is calculated and then verify result by comparing it with the local checksum stored on verifier side. Precomputed responses are used in this integrity paradigm.

A. Juels et al. (2007) [5] In this Proofs of retrieve ability (POR) is used to enable backup service on prover side to generate proof that a data owner (verifier) can retrieve the target file F. This method is designed to handle the large size of files F. In POR, the communication cost, memory accessed by prover and storage requirement of the data owner are independent than the large file F. This method of verification is based on challenge and proof paradigm. The key generator protocol is used to generate keys and save them to verifier side and also File Encoder is used to encode the file F and save it to the prover side. The main goal of POR is to do security checks without users having to download the entire file F.

T.J.E. Schwarz et al. (2006) [6] In this paper, the algebraic signature and hash function used with of algebraic property for the verification of remote data. They use the algebraic property in which signature of parity gives the same result as parity of signature. To make this property feasible in this verification method they blind the data and parity by XORing them with pseudo-random stream and for verification small size of a message is used for verification. It verifies the random data without the need of a challenger.

D.L.G Filho et al. (2006) [7] In this paper, the protocol described is based on a hash function which helps to identify any infiltration during the process of data transfer. In this verification method verifier does not need to have data to in hand during execution of protocol but rather a small hash of that data. This scheme is very flexible but gives a low performance.

F. Sebe et al. (2008) [8] In this paper data is stored in the vault (cloud server) and intrusion detection system (IDS) is introduces to check whether there is server corruption happening in the system or not. In DIT various checks are done like runtime check, network based and host based fraud check, etc. By which infiltration in the model through various attacks become tough.

C. Wang et al. (2010) [9] In this paper, they introduced a network architecture to cop up with security issues regarding remote cloud storage. They represent improved cryptographically desirable properties of public auditing and advantage-disadvantage of their practical significance in the situation of cloud computing. They did the in-depth analysis over existing cloud storage security paradigm.

G. Ateniese et al. (2007) [10] In this paper, they introduce a provable data possession (PDP) model that enable data

owner to place their local data over the remote cloud server. In this method data, M is further break up into data blocks and tags generated for each data blocks saved at the server, later data owner can verify that data is correctly stored on the server or not. The verify process took place by two-way communication by which data owner send the challenge to the server and then the server sends the proof to the data owner. After receiving the proof, data owner generates the result (0/1).In this method, they create the probabilistic proofs taking random number blocks from the entire file which reduces the I/O cost. The data owner (client) The challenge/response protocol transmits a small, keep the metadata of the entire data and later use it verify the proof sent by the server.
M.A. Shah et al. (2008) [11] In this paper they keep main focus on third party auditing means that they introduced service level agreement, which will be done between the server and client so that client can opt TPA for effective verification and security of the data stored on the remote cloud server. They explain the required fundamental properties for implementing TPA. They take a step forward to make TPA method a reality in cloud computing.
C.C. Erway et al. (2009) [12] In this paper again the focus is on the security and integrity of data stored on the remote untrusted server. They extend PDP technique in which client keep the small metadata of the larger file F, which been sent to the server and later uses that metadata to verify the proof to ensure data is correctly stored in the remote cloud server. They introduce dynamic provable data possession DPDP in which the result is based on the authenticated dictionaries where the entries are maintained in rank information table. By which the block level authentication can be provided, so client can perform insert, delete operation on the remote data. They validate the security by using some perquisites. We prove the security of our constructions using standard assumptions.

## 3. Proposed hypothesis

The related scheme has developed a method for secure and optimal auditing in storage while using cloud services. Many attacks can breach into storage credentials. To prevent the replay, reply and forge attack the methodology of ITable is introduced. The ITable consists of general information related to data and it is stored at the TPA and data owner side. The I stand for Index, which indicates the current data block number(mi) in the main data M.Dat. Tags are generated within the timestamp T, which is provided by Itable itself. At the initialization phase, the ITable will be generated by the data owner and it is managed by the TPA. When static or dynamic operations are performed over the data stored at cloud server and changes are updated on the ITable by the TPA. During the confirmation of auditing process, results are sent to the data owner and Itable will also be updated at owner side. This method is very much capable of preventing the attack, but a slighter limitation is a storage while performing operations which are critical so in this research will purpose a lighter detect based TagGen and Itable process which will be carried in packet header itself with 2 bit of information.
For proposed work, the focus will be on pseudonym based auditing and save auditing storage against different attacks. In the auditing process, the communication between the auditor and remote server is done through two-way communication where auditor sends challenge to a remote server and in response server sends the proof after accessing the challenge by this auditor ensures data is correctly stored at cloud side. Further auditing data will be updated according to the required storage solutions. After the confirmation of auditing process, TPA will send the result to the data owner. If the result sent by the TPA is true, then data owner is convinced that data remotely stored over cloud server is correctly stored. Then data owner may choose to delete the local copy of data. The pseudonyms are composed of the public key, private key and a certificate to maintain privacy. Through pseudonyms, users define their candid and certificate validate that user is a regular user. TTP save pseudonyms and actual ID of users to reveal the anonymity of the user in case of a problem it also used for storing results for whole auditing process. Then process the operations based on the traces like Itable generation and TagGen generation but storing the trace initial data in the header so that it will not create overhead to running processes. Network Simulator will be used for experimentation with dense network. Cloud server structure will have opted for experimentation with various users.

## 4. Results

For proposed work, a focus will be on pseudonym based auditing and save auditing storage against different attacks. In auditing process, the auditing protocol will process the operations based on the traces like Itable generation and TagGen generation but storing the trace initial data in a header so that it will not create overhead to

running processes. Network Simulator will be used for experimentation with a dense network. Cloud server structure opted for experimentation with various users as listed in figure 2.

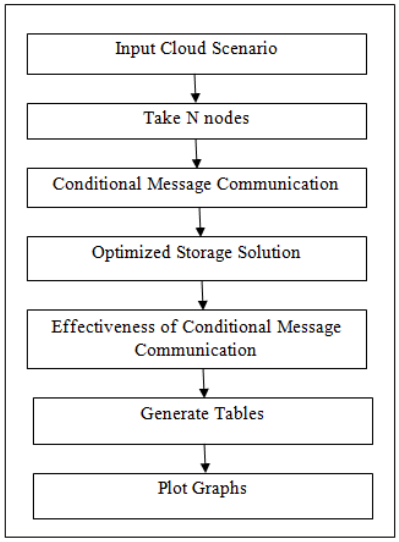


Figure 2 –Methodology used for enhanced secure dynamic auditing protocol

We tested my enhanced secure dynamic auditing protocol using following environment as configured in figure 3.

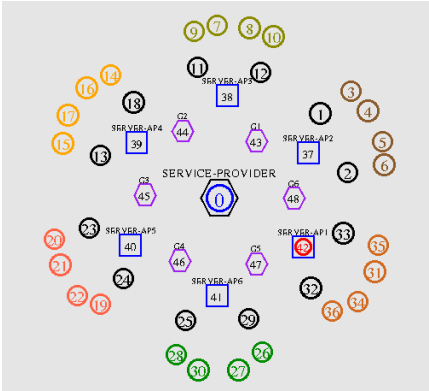


Figure 3 –Methodology used for enhanced secure dynamic auditing protocol

### 4.1. Communication cost

Communication cost basically an excess overhead of computation time, space and bandwidth as shown in figure 4.

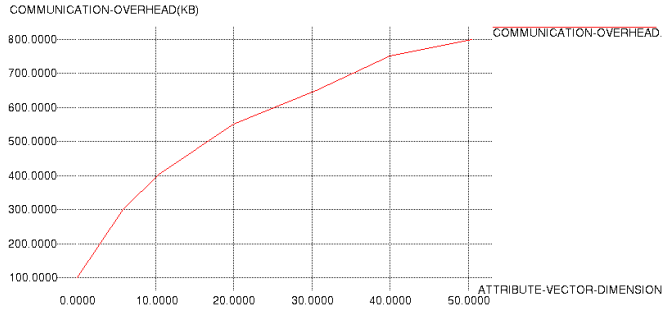


Figure 4 –Communication overhead versus attribute vector dimension for enhanced secure dynamic auditing protocol

### 4.2. Time cost of individual client

The time cost calculated for the individual client as shown in figure 5.

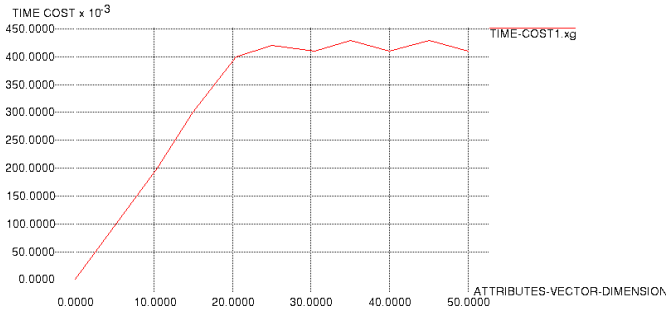


Figure 5 –Time cost of individual client for enhanced secure dynamic auditing protocol

### 4.3. Key generation time taken analysis

It calculates time for generation of keys include encryption and decryption as shown in figure 6.

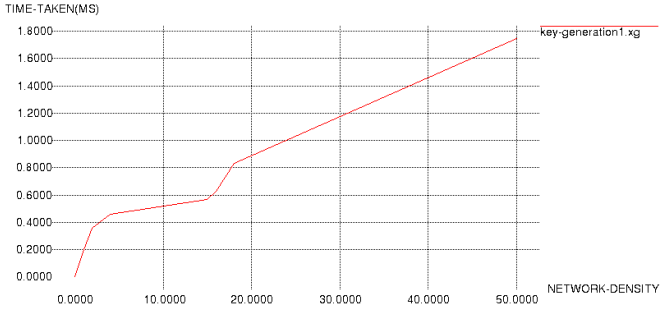


Figure 6 – Key generation time taken analysis for enhanced secure dynamic auditing protocol

### 4.4. Throughput

The throughput calculated for the proposed hypothesis as shown in figure 7.

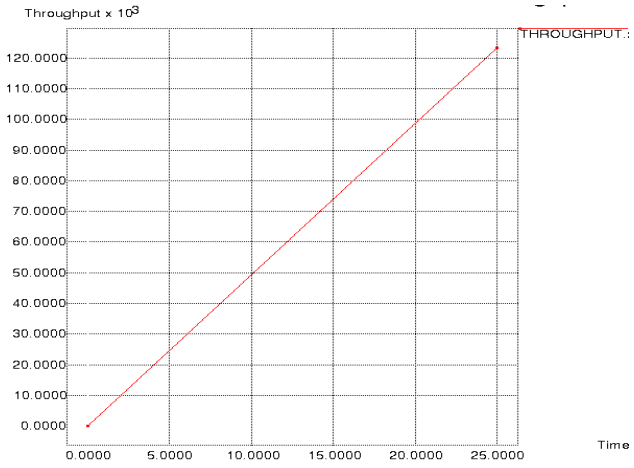


Figure 7 – Throughput for enhanced secure dynamic auditing protocol

### 4.5. Comparison of different dynamic auditing protocol

The analysis reports of different dynamic auditing protocol as listed below in table 1. We compare [1] to [12] and * schemes and invent robust architecture for security in the field of cloud computation.

Table 1 - A comparison on different dynamic auditing protocol

| Details | [1] | [2] | [3] | [4] | [5] | [6] | [7] | [8] | [9] | [10] | [11] | * |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Constant bandwidth cost | Yes | No | No | No | Yes | No | Yes | No | No | Yes | No | Yes |
| Protecting data privacy | No | No | Yes | No | No | No | No | No | No | No | No | Yes |
| Batch auditing | No | No | No | No | No | No | No | No | No | No | No | Yes |
| Data owner | No | No | No | No | No | No | Yes | No | No | No | No | Yes |
| Data dynamic support | No | Yes | Yes | Yes | No | Yes | No | Yes | Yes | No | Yes | Yes |

* An enhanced secure dynamic auditing protocol

## 5. Conclusion

The primary focus on pseudonym based auditing and saving auditing storage against different attacks. We process the operations based on the traces generation but storing the trace initial data in the header so that it may not create overhead to the running processes. In this paper, simulative analyses illustrated for an enhanced secure dynamic auditing protocol and prove efficient against various conspiracy attacks.

## Acknowledgements

The authors also wish to thank many anonymous referees for their suggestions to improve this paper.

## References

[1] Kan Yang, Student Member, IEEE, and Xiaohua Jia, Fellow, IEEE "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Transaction on Parallel and Distributed Systems, VOL. 24, NO. 9, Sep 2013

[2] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, "A Cooperative Internet Backup Scheme," Proc. USENIX Ann. Technical Conf., pp. 29-41, 2003.

[3] Y. Deswarte, J. Quisquater, and A. Saidane, "Remote Integrity Checking," Proc. Sixth Working Conf. Integrity and Internal Control in Information Systems (IICIS), Nov. 2004.

[4] M. Naor and G.N. Rothblum, "The Complexity of Online Memory Checking," J. ACM, vol. 56, no. 1, article 2, 2009.

[5] A.Juelsand B.S. Kaliski Jr., "Pors:Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security, P. Ning, S.D.C. di Vimercati, and P.F. Syverson, eds., pp. 584-597, 2007.

[6] T.J.E. Schwarz and E.L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. 26th IEEE Int'l Conf. Distributed Computing Systems, p. 12, 2006.

[7] D.L.G. Filho and P.S.L.M. Barreto, "Demonstrating Data Possession and Uncheatable Data Transfer," IACR Cryptology ePrint Archive, vol. 2006, p. 150, 2006.

[8] F. Sebe, J. Domingo-Ferrer, A. Martınez-Balleste ´, Y. Deswarte, and J.-J.Quisquater, "Efficient Remote Data Possession Checking in Critical Information Infrastructures," IEEE Trans. Knowledge Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008.

[9] C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[10] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song, "Provable data possession at untrusted stores," in ACM Conference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 598–609.

[11] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, J. Pieprzyk, ed., pp. 90-107, 2008.

[12] C.C. Erway et. al."Dynamic Provable Data Possession," Proc. ACM Conf. Computer and Comm. Security, E. Al-Shaer, S. Jha, and A.D. Keromytis, eds., pp. 213-222, 2009.

[13] Dhiraj Soni and Raman Kumar, "Multimedia Cloud Computing Security an Evolving Trend: Rudimentary Essentials Computing", International Journal of Advanced Trends in Computer Applications, (IJATCA), Vol. 2, Issue 7, pp. 19-25, 20th January 2016.

[14] Raman Kumar, Harsh Kumar Verma and Renu Dhir, "Cryptanalysis and Performance Evaluation of Enhanced Threshold Proxy Signature Scheme Based on RSA for Known Signers", Mathematical Problems in Engineering, Vol. 2013, Article ID 790257, 24 pages, 2013.

[15] Raman Kumar and Nonika Singla, "Cryptanalytic Performance Appraisal of Improved CCH2 Proxy Multisignature Scheme", Mathematical Problems in Engineering, Vol. 2014, Article ID 429271, 13 pages, 2014.

[16] Raman Kumar, Harsh Kumar Verma and Renu Dhir, "Analysis and Design of Protocol for Enhanced Threshold Proxy Signature Scheme Based on RSA for Known Signers", Wireless Personal Communications – An International Journal - Springer ISSN: 0929-6212 (Print) 1572-834X (Online), Volume 80, Issue 3 (2015), Page 1281-1345.