Enterprise Cloud Storage and Computation Security

Rajeev Yadav, PhD
Professor, CSE Deptt
RCEW College, Jaipur

Shreya Sharma
Assistant Professor, CSE Deptt
RCEW College, Jaipur

Avinash Sharma, PhD
Professor, CSE Deptt
RCEW College, Jaipur

ABSTRACT
Cloud computing acts as a computing paradigm that aims to provide huge amount of computing in a fully virtualized manner by aggregating resources and thus offering a single system view. Cloud Computing is also delivered as utility assuring customized and quality of service guaranteed computation environments for cloud users. While an enterprise organization is composed of different departments like finance, admin etc these departments are segregated as sub network zone which are thus interconnected via network. Securities are essential for authorization of storage and computing. In this paper we have proposed a privacy cheating discouragement and computation auditing approach that bridging secure storage and computation auditing in cloud. Privacy cheating discouragement is designated by verifier signature, batch verification and probabilistic sampling techniques.

General Terms
Enterprise Cloud Computing, Auditing Protocol, Verifier signature.

Keywords
Secure computation auditing; Secure storage; Privacy-cheating discouragement; Designated verifier signature; Batch verification; Cloud computing.

1. INTRODUCTION
In today's world organizations with its operations, services and management are becoming dependent on their enterprise networks. An enterprise network is a communication backbone which connects each and every computer of an organization with all possible locations. Interconnection among department in different scale is again an area of great importance thus it becomes a necessity to have some security constraints over the complete networking scenario. In such a case these networks consist of logical group of network elements correlated to different departments thus interconnected via interface routers most probably layer-3 network devices.

Current researches in cloud computing focuses on the cloud storage security .whereas the computation security receives. In order to save computation resources the cloud servers may not perform computations but may pretend to do so, Again in the centralized architectures, basic emphasis is layered on the fact that the cloud servers represent a single point o failure as shown by recent meltdown of Google's Gmail systems [25].

With Byzantine [11] failure or also external attacks the cloud may execute some unreliable computations' in the manner to hide computations. Such a cheating behaviour of cloud servers if detected may lead to useless results. Again view of accountability. There must be some secure computation mechanisms which may be placed in order to need of deciding whether the cloud servers or users to be implied responsible for the problems that may occur in any secure cloud paradigm .Suspecting a problem with customers software is quite natural and vice versa. Sometimes because of limitations in the computation and communication resources the cloud users may not afford much to spend on cost incurred from auditing or verification.

In order to prevent cloud users from spending a huge cost from expensive verifications it is required to introduce a trusted auditor who can conduct cloud auditing on the behalf of the users. Although public auditing of secure storage in cloud has already been proposed in the context, the public auditability has gained less attention. [33, 34]

There are again some related references for secure remote computations in distributed systems [24].However these proposed schemes target at secure cloud computations Also , privacy preserving is a critical issue for secure cloud computing when some of existing researches [20,29] have taken into consideration. In order to achieve secure auditing computing in cloud there is one straightforward method required i.e., to double click each result. The overall inputs and computing results are given to the auditor, which follows an identical procedure to compute the results and then perform comparisons with the one provided by the cloud providers although these schemes may lead to a waste of I/O and computing resources. Consider data transfer via bottlenecks rank in the top of ten obstacles which may prevent overall success in cloud computing [1].

Using a Commitment based sampling (CBS) technique a conventional grid computing is introduced however it does have much privacy issues here in this paper we have introduced novel approach by integrating CBS with designated verification technique.

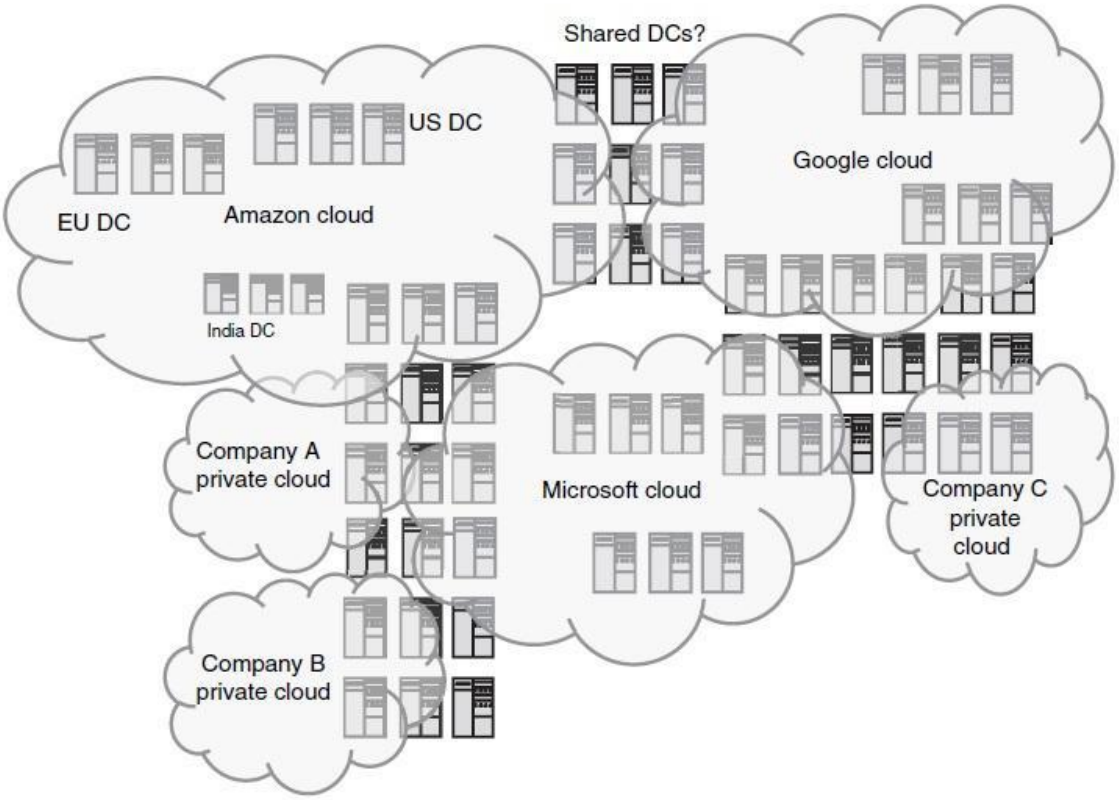

Fig 1: Enterprise Cloud System

2. RELATED WORK

Security and privacy issues in Enterprise cloud computing has received extensive attentions recently. The research is categorized in Enterprise cloud storage security and Enterprise cloud computation security. Enterprise Cloud storage security mainly addresses the secure outsourced storage issue.

First defined a model of provable data possession was first defined by ateniese et al[2] that allow a client to process the original data without retrieving at which may be stored at a cloud server. Here data is first verified by untrusted server an than processed. RSA-based homomorphic tags for auditing outsourced data were utilized but they don't have dynamic data storage.

Later a partially dynamic version of the pdp scheme using symmetric key cryptography was proposed. Although it does not support public audit ability [2].

A proof of retrievability was proposed by Juels et al. [22] where spot-checking and error-correcting codes ensure possession and retrievability for data file on archive service system.

Public verifiability and dynamic data storage operations using third party auditor for improving retrievability model by using classic merkle hash tree [26].

Finally the scheme was proposed for achieving public verifiability as well as the dynamic data storage operations in [33] using public cloud.

The first construction of dynamic provable data possession was proposed by Erway et al. [15] which use pdp extended model to achieve the required possession of data. Data using rank-based authenticated skip lists is updated, compared with cloud storage and computation which may receive less attention now days. Here in the related work includes Remote computation audit and verifiable computation was included.

A ringer scheme in distributed computing was proposed where the supervisor could send some precomputed result participant without disclosing the input [17].

In A distributed computing model a remote audit mechanism was used for verifying whether the remote host performed the assigned task successfully.

In the same manner as our prior work [35, 16] verifiable Computation notation were introduced and thus a notion of formalized verifiable Computation, which allows weak client to outsource the computation to the function of various dynamically-chosen inputs.

3. SPECIFICATION AND IMPLEMENTATION

3.1 System Architecture of Enterprise Cloud

In Fig 1, Consider a general Enterprise cloud computing model composed of number of cloud servers. These servers are under control of one or more cloud service providers (CSP).Cloud servers are responsible to process huge amount of storage and computing The CSP allocates resources via customized service level agreements [28]. For instance, in order to perform batch processing tasks by using abstraction programming techniques such as MapReduce and hadoop.CSP divides these large task into multiple small sub tasks which allow parallel execution of hundreds of cloud servers .Consider a cloud user such as mobile phone, laptop,aaple ipad, having low resource computation and storage in comparison to other cloud servers.

The cloud user (CU) submits storage and computation requests to the CSP on demand. Similarly for secure auditing schemes we consider the existence of verification agencies (VA) which are selected and trustworthy for cloud users. These are responsible for auditing the cloud services on data storage and computations. VAs have powerful computations and storage tendency to thus to perform the auditing operations than other CUs.

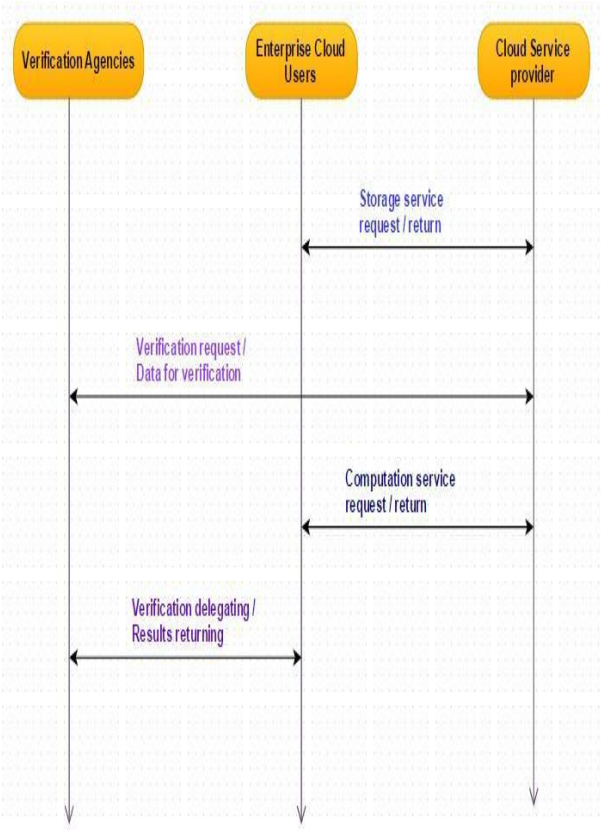

Fig 2: Enterprise Cloud Computing UML

In the Fig 3, A secure environment for cloud computing storage is represented, here Client requests for set of computations and storage via an interface which can be either web browser or any Application programming Interface, here request is redirected to master node .Here we have used master/slave model for communication where one master server controls one or more slave servers, once a relationship is established the control direction is always from master to slave.

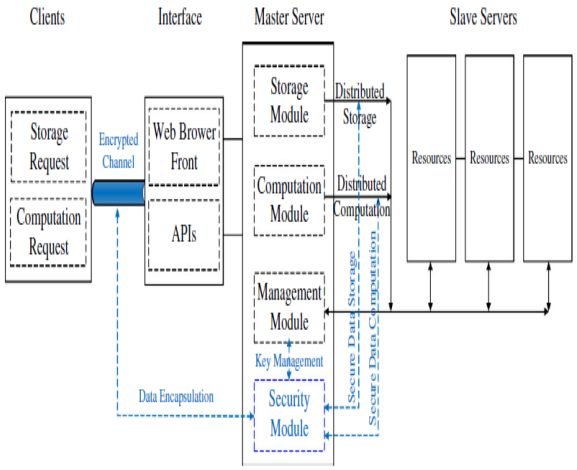

Fig 3: Secure Enterprise cloud computing storage environment

3.2 Step & Flow for Secure Enterprise Cloud Environment

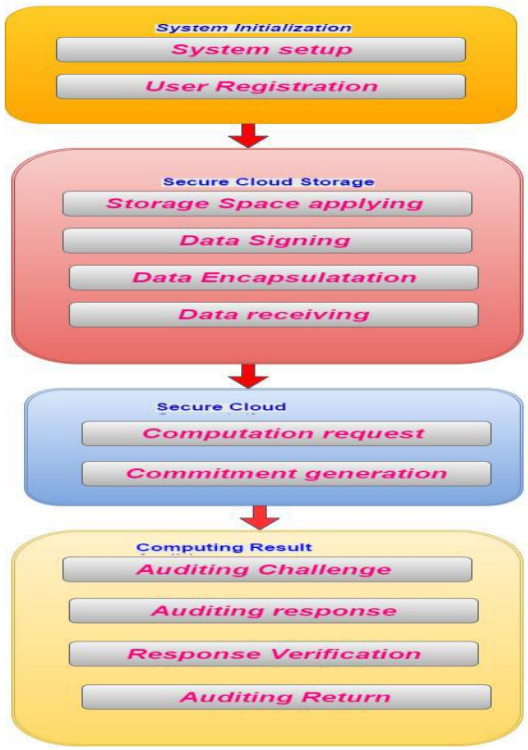

Fig 4: Enterprise Cloud Computing Security & privacy step

In Fig.4 and Fig.2, An enterprise security and privacy step and use case diagrammed is represented which can easily enable data storage auditing, the cloud user needs to sign each transmission block mi to generate authenticated Information. To preserve user's privacy in our model, CU makes a little modification of the traditional signature scheme according to

the designated verifier signature. Data Signing is done in two parts. The first part is compute signature using hash function and another signing using verifier signing. Fig 5 shows the performance analysis of cloud server and database per transaction with different size like 4 GB, 8 GB, and 16GB.

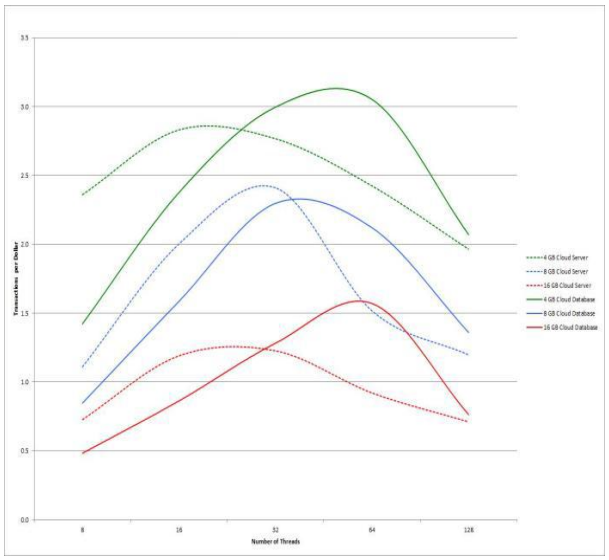

Fig 5: Performance Analysis

4. ACKNOWLEDGMENTS

This work was supported by the Research Lab of Computer Science & Engineering Department at RCEW Jaipur. We would like to thank anonymous reviewers who helped us in giving comments to this paper.

5. CONCLUSION

In Enterprise cloud has great influence on pay as you go or on demand services. With the help of Cloud computing, we can access huge amount of computing and storage for many enterprise all together. Security is the major key challenge in cloud computing in order to have secure enterprise network conventional and specific security network & design must be included into an Enterprise cloud network developer environment which may reduce the chances of intruders effecting the network. The security procedure provide practical effort of securing the cloud and an opportunity to re-architecture older application while at the same time there is always a risk of moving sensitive data and application to enterprise cloud network which may produce threats. Thus In this paper we have propose a privacy cheating discouragement and computation auditing approach, which can easily bridge secure storage and perform computation auditing in Enterprise cloud network. For authorizing and integrating a computation and storage security is the major constraint. Here privacy cheating discouragement is achieved by verifier signature batch verification and probabilistic sampling techniques.

6. REFERENCES

[1] Y. Bartal, A. Mayer, K. Nissim, and A. Wool, ―Firmato: a novel firewall management toolkit," ACM Trans. Comput. Syst., vol. 22, no. 4, pp. 381-420, Nov. 2004.

[2] E. S. Al-Shaer and H. H. Hammed, ―Discovery of policy anomalies in distributed firewalls," in Proc. IEEE INFOCOM'04, pp. 2605-2626,Hong Kong, China, Mar. 2004.

[3] T. E. Uribe and S. Cheung, ―Automatic analysis of firewall and network intrusion detection system configurations," in Proc. ACM WorkshopFormal Methods Security Eng., pp. 66-71, Washington, DC, USA, Oct.2004.

[4] E. S. Al-shaer and H. H. Hamed, ―Firewall policy advisor for anomaly discovery and rule editing," in Proc. IFIP/IEEE 8th International Symp.Integrated Netw. Management, pp. 17-30, Colorado Springs, USA, Mar.2003.

[5] L. Yuan, J. Mai, Z. Su, H. Chen, C. Chuah, and P. Mohapatra,FIREMAN: a toolkit for firewall modeling and analysis," in 27th IEEE Symp. Security Privacy, Oakland, CA, USA, May 2006.

[6] A. X. Liu and M. G. Gouda, ―Complete redundancy detection in firewalls," in Proc. 19th Annual IFIP Conf. Data Applications Security,pp. 196-209, Aug. 2005.

[7] High level firewall language." [Online]. Available: http://www.hlfl.org/.Accessed on Apr. 2009.

[8] B. Zhang, E. S. Al-Shaer, R. Jagadeesan, J. Riely, and C. Pitcher,―Specifications of a high-level conflict-free firewall policy language for multi-domain networks," in Proc. 12th ACM Symp. Access Control Models Technologies (SACMAT 2007), pp. 185-194, France, June 2007.

[9] CISCO: Configuring IP access lists," CISCO White Papers 23602 edition, July 2007.

[10] Configuring ACL in Huawei switches," Huawei 3 Com Switch 4500G Release Notes, pp. 1-28, Feb. 2009.

[11] Alcatel-OS-LS-6200 User Guide," Part No. 060202-10, pp. 1-762, June 2007.

[12] J. D. Guttman and A. L. Herzog, ―Rigorous automated network security management," International J. Inf. Security, vol. 4, no. 2, pp. 29-48, 2005.

[13] Y. S. Mahajan, Z. Fu, and S. Malik, ―Zchaff 2004: an efficient SAT solver," in Proc. 8th International Conf. Theory Application Satisfiability Testing, pp. 360-375, Scotland, June 2005.

[14] C. C. Zhang, M. Winslet, and C. A. Gunter, ―On the safety and efficiency of firewall policy deployment," in 28th IEEE Symp. Security Privacy, pp. 33-50, Oakland, CA, USA, May 2007.

[15] P. Matousek, J. Rab, O. Rysavy, and M. Sveda, ―A formal model for network-wide security analysis," in Proc. 15th IEEE International Conf. Workshop ECBS, Belfast, Ireland, 2008.

[16] T. Hofmeister, U. Schoning, R. Schuler, and O. Watanabe, ―A probabilistic 3-SAT algorithm further improved," in Proc. 19th Annual

[17] Symp. Theoretical Aspects Computer Science (SATACS), pp. 192-202, 2002.

[18] O. Dubois, P. Andre, Y. Boufkhad, and J. Carlier, SAT Versus UNSAT,Second DIMACS Challenge, D. S. Johnson and M. A. Trick, editors,1993.

[19] L. Zhang and S. Malik, ―Towards symmetric treatment of conflicts and satisfaction in quantified Boolean satisfiability," in Proc. 8th International Conf. Principles

Practice Constraint Programming (CP 2002), pp. 200-215, 2002.

[20] S. Matsumoto and A. Bouhoula, ―Automatic verification of firewall configuration with respect to security policy requirements," in Proc.International Workshop Computational Intelligence Security Inf. Syst.(CISIS'08), pp. 123-130, Barcelona, Spain, Oct. 2008.

[21] D. Gabby, Ch. Hogger, and J. Robinson, editors, ―Temporal Logic,"Handbook of Logic in AI and Logic Programming, vol. 4. Oxford University Press, 1995.

[22] Y. Venema, ―A modal logic for quantification and substitution," L. Csirmaz, D. Gabby and M. de Rijke, editors, Logic Colloquium 92, Veszprem, Hungary, Studies in Logic, Languages and Information. CSLI Publications, Stanford, pp. 293-309, 1995.

[23] P. Bera, P. Dasgupta, and S. K. Ghosh, ―A verification framework for analyzing security implementations in an enterprise LAN," in Proc. IEEE International Advance Computing Conf. (IACC 09), pp 1008-1015, Mar. 2009.

[24] S. K. Ghosh, ―Analyzing security policy implementations in enterprise networks–a formal approach," in Indo-US Conf. Workshop Cyber Security, Cyber Crime Cyber Forensic (ICSCF 2009), invited position paper, Kochi, India, July 2009.

[25] P. Bera, P. Dasgupta, and S. K. Ghosh, ―Formal analysis of security policy implementations in enterprise networks," International J. Computer Netw. Commun., vol. 2009, no. 2, pp 56-73, June 2009.

[26] M. Ahmed, H. Yanikomeroglu, and S. Mahmoud, ―Call admission control in wireless communications:a comprehensive survey,‖to be submitted to IEEE Wireless CommunicationsMagazine.

[27] M. Andrews, K. Kumaran, K. Ramanan, A. Stolyar, P. Whiting, and R. Vijayakumar, ―Providing quality of service over a shared wireless link,‖ IEEE Communications Magazine, vol. 39,no. 2, pp. 150–154, Feb. 2001.

[28] A. Eleftheriadis and D. Anastassiou, ―Meeting arbitrary QoS constraints using dynamic rate shaping of coded digital video,‖ in Proc. IEEE Int. Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV'95), pp. 95–106, April 1995.

[29] R. Guerin and V. Peris, ―Quality-of-service in packet networks: basic mechanisms and directions,‖Computer Networks and ISDN, vol. 31, no. 3, pp. 169–179, Feb. 1999.

[30] A. Sadeghi, T. Schneider, M. Winandy, Token-based cloud computing: Secure outsourcing of data and arbitrary computations with lower latency, in: Trust and Trustworthy Computing, Berlin, Germany, June 21–23, 2010.

[31] H. Takabi, J. Joshi, G. Ahn, Security and privacy challenges in cloud computing environments, IEEE Security & Privacy 8 (6) (2010) 24–31.

[32] C. Wang, K. Ren, J. Wang, Secure and practical outsourcing of linear programming in cloud computing, in: 30th IEEE Conference on Computer Communications (INFOCOM 2011), Shanghai, China, April 11–15, 2011.

[33] C. Wang, Q. Wang, K. Ren, W. Lou, Privacy-preserving public auditing for data storage security in cloud computing, in: 29th IEEE Conference on Computer Communications (INFOCOM'10), San Diego, California, USA, March 14–19, 2010.

[34] Q. Wang, C. Wang, J. Li, K. Ren, W. Lou, Enabling public verifiability and data dynamics for storage security in cloud computing, in: 14th European Symposium on Research in Computer Security (ESORICS'09), Saint Malo, France, September 21–23, 2009.

[35] L. Wei, H. Zhu, Z. Cao, W. Jia, A. Vasilakos, Seccloud: bridging secure storage and computation in cloud, in: 30th International Conference on Distributed Computing Systems Workshops (IEEE ICDCSW 2010), Genova, Italy, June 21–25, 2010.

[36] T. Yuen, W. Susilo, Y. Mu, How to construct identity-based signatures without the key escrow problem, International Journal of Information Security 9 (4) (2010) 297–311.

[37] J. Zhang, J. Mao, A novel ID-based designated verifier signature scheme, Information Sciences 178 (3) (2008) 766–773.