International Journal on Recent Researches In Science, Engineering & Technology
(Division of Computer Science and Engineering)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. It is an absolutely free (No processing charges, No publishing charges etc) Journal Indexed in JIR, DIIF and SJIF.
Research Paper
Available online at: www.jrrset.com

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
Volume 2, Issue 12, December 2014.
JIR IF : 2.54
DIIF IF : 1.46
SJIF IF : 1.329

A SURVEY OF PUBLIC AUDITING FOR SECURE DATA STORAGE IN CLOUD COMPUTING

S Satish Babu[1], C.Vijayakumar[2], J.Vijaybabu[3]
[1]Professor, Department of Computer Science and Engineering, Mahendra Engineering College, Mahendhirapuri, Namakkal District, Mallasamudram, Tamilnadu, India.
[2,3]Assistant Professor, Department of Computer Science and Engineering, Mahendra Engineering College, Mahendhirapuri, Namakkal District, Mallasamudram, Tamilnadu, India.

Abstract: Utilizing distributed storage, cloud computing clients can remotely store information and requesting quality of applications and services from a common pool of configurable computing assets, without the burden of nearby information stockpiling and support. However, the clients do not have physical ownership of the outsourced information creates the information responsibility security in distributed computing environment of an impressive assignment, particularly for clients with compelled computing assets. The clients should be the capacity to utilize the distributed storage without worrying over the need to check its honesty. Subsequently, empowering public auditability for distributed storage is basic significance with the goal that clients can fall back on an Outsider Evaluator (OE) to verify the trustworthiness of outsourced information and be effortless. To safely present a compelling OE, the evaluating procedure should acquire no new vulnerabilities toward client information security, and initiate no extra online load with client. In the paper, propose Privacy Protecting Public Auditing (PPPA) algorithm for a safe distributed storage. Additionally stretch out the outcome to empower the OE to perform reviews for numerous clients at the same time and productively. Broad security and execution investigation demonstrate the proposed strategies are provably secure and effective.
Keywords: distributed storage, Outsider Evaluator (OE), public inspecting, information storage, cloud computing, Privacy Protecting Public Auditing (PPPA).

Introduction

Cloud generation information innovation has been imagined the enterprises, because of its not insignificant rundown of remarkable benefits in the information technology history: requesting individual service, universal framework access, area independent of asset pooling, fast asset flexibility, utilization based on cost and transmission of hazard. One crucial part of this outlook changing is information are unified or outsourced to the cloud computing environment. Distributed computing creates benefits more engaging than any other time in recent memory; it carries new and testing protection hazards to clients' outsourced information. Because, cloud service suppliers (CSS) are dividing regulatory substances, information outsourcing is giving up client's control over the destiny of their information.

The accuracy of the information in the cloud computing is being put in hazard owing to the following explanations. First, the fact of the infrastructures under the cloud computing are substantially more capable and dependable than individualized computing gadgets and it are confronting the wide scope of both inside and outside hazards for information reliability. Second, there do different inspirations for CSS to carry on faithlessly to the cloud clients with respect to their outsourced information status. Coordinating the homomorphic direct evaluating with random

masking and protocol ensures the OE couldn't take in any information about the information content stored in the cloud computing server (CCS) during the effective inspecting procedure. The collection and mathematical properties of the authenticator additionally advantage of design for the group inspecting.

Related Work

CSS may recover capacity for economic related reasons by disposing information and it are infrequently accessed, or still conceal information misfortune occurrences to keep up a reputation [1] [2]. So, the outsourcing information to the cloud computing is financially alluring for extensive term huge scale storage and it doesn't instantly provide some assurance on information respectability and accessibility. In the issue, if not appropriately addressed, may hinder the accomplishment of cloud design. Clients never physically have the capacity of their information's conventional cryptographic primitives with the end goal of information protection insurance can't be straightforwardly embraced [3]. Supporting clients to assess the hazard of their bought in cloud computing data services, the inspect outcome from OE would be useful for the cloud specialist suppliers to enhance cloud-based service stage, and even fill for independent assertion purposes [4]. Public inspectability permits an external party, in spite of the client himself, to check the rightness of remotely stored information. Since, a large portion of the strategies [5] don't consider the security protection of clients' information against outside examiners. There are legal controls such as the US Health Insurance Portability and Accountability Act (HIPAA) [6], additionally requesting the outsourced information not to be spilled to outside parties. Abusing information encryption before outsourcing [7] could be alleviate the protection concern of information evaluating and it could excess when utilized decoded/public cloud information (e.g., outsourced libraries and logical informational indexes), because of the superfluous handling load for cloud clients.

Proposed System

A distributed information storage service including three unique elements illustrated at Figure 1. The cloud computing client has expansive measure of information documents to be stored in the cloud environment. The cloud computing server (CCS) is controlled by the cloud specialist suppliers (CSS) to give information storage service and has storage space and calculation assets (won't separate CCS and CSS hereafter). The outsider evaluator (OE) has knowledge and capacities that cloud clients don't have and is trusted to survey the distributed storage benefit unwavering quality for the benefit of the client upon demand. Clients depend on the CCS for distributed information storage and protection. It may dynamically associate with the CCS to access and modify stored information for different application reasons. Clients have information locally and it is significance for clients to guarantee information's are accurately stored and preserved. The calculation asset save the online load conceivably carried by the periodic storage rightness confirmation and cloud computing clients alternate to OE for guaranteeing the capacity honesty of outsourced information while designing to maintain information private from OE.

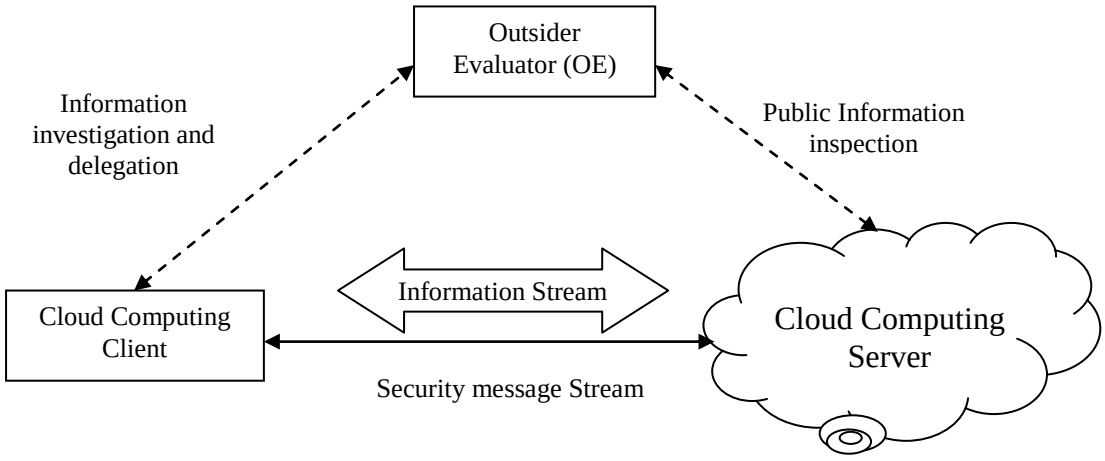

Figure.1 Architecture Diagram

The information honesty hazards accept to clients' information can originate equally inside and outside assaults at CCS. It contains programming faults, hardware disappointments, fault in the framework path, financially inspired hackers, malevolent or incidental management mistakes, and so on. Furthermore, CCS can act naturally intrigued. Particular advantages such as to control reputation, CCS selects to hide information dishonesty occurrences to clients. Utilizing outsider inspecting service gives a financially efficient technique to clients to pick up confide in cloud environment. The OE is accepting the business of inspecting is consistent and independent.

Result and discussion

PPPA proposed strategy represent mathematical model to improve security for distributed computing storage. In the methodology, protection methods work with cloud computing server and cloud client. Although, distributed computing storage is not trusted then also cloud computing client information will be in safe during information uploading and information retrieval. Its show following model separately such as communication cost, Encryption Time and Decryption Time.

Table 1 represents communication cost (%), encryption time (in sec) and decryption time (sec) for document file dataset. The strategy is investigated in terms of communication cost (%), encryption time (in sec) and decryption time (sec) and exhibit average values for respective aspects.

Table.1 Comparison of Communication Cost (CC) Encryption Time (ET) & Decryption Time (DT)

Learning Algorithms	**CC**	**ET**	DT
RSA	58.54	1.63	2.32
TRIPLE DES	63.7	1.47	0.83
DES	68.4	1.27	0.78
PPA	98	0.08	0.13

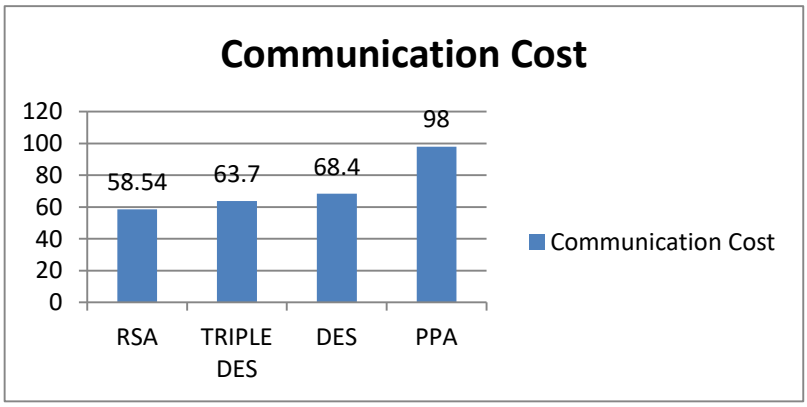

Figure.2 Comparison of Communication Cost (CC)

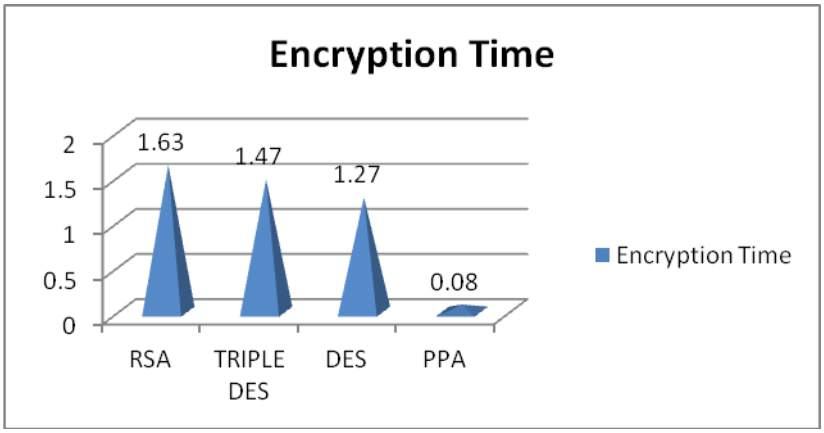

Figure.3 Comparison of Encryption Time (ET)

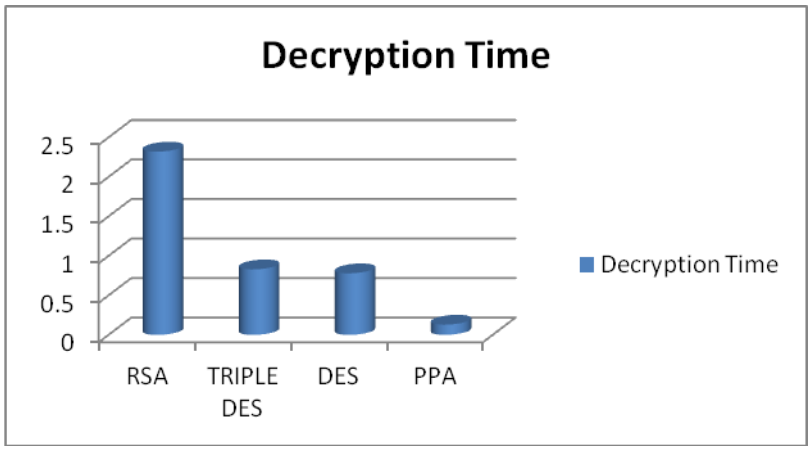

Figure.4 Comparison of Decryption Time (DT)

According to proposed Privacy Protecting Public Auditing (PPPA) protocol estimation outcome in figure 2 to 4 for document dataset. Privacy Protecting Public Auditing (PPPA) protocol is the best strategy. Communication cost, encryption time and decryption time PPPA show that it forever yields the best performance in both all graphical outcomes. In terms of communication cost, PPA establish as best methodologies. In terms of all estimated aspect with respective dataset, DES (Data Encryption Standard) is closest method to proposed method. However, DES outcome is too far contrast than proposed methodology. Consequently, it claims that PPPA is best methodology for document dataset.

Conclusion

A Privacy Protecting Public Auditing (PPPA) framework for information storage security in distributed computing environment. Utilizing the homomorphic direct evaluating with random masking and protocol ensures the OE couldn't take in any information about the information content stored in the cloud computing server (CCS) during the effective inspecting procedure. It is not reduces the load of cloud computing client from the dreary and conceivably costly evaluating operation and reduces the clients' dread of outsourced information leakage. Considering OE, simultaneously deal with numerous inspect sessions from various clients for outsourced information documents, and expand privacy protecting public inspecting convention into a multi-client setting, where the OE plays different examining operations in a group way for better productivity. Broad investigation strategies are provably secure and very effective.

References

[1]. 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.

[2]. 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.

[3]. A. 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.

[4]. M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[5]. 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.

[6]. 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," http://aspe.hhs.gov/admnsimp/pl104191.htm, 1996.

[7]. M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.