IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 11-13

Public Auditing And Energy Saving Task Scheduling Strategy In Cloud Computing

Mr.K.Lakshminarayanan.M.E., Assistant Professor
Department Of Cse.,Mailam Engineering College,Mailam

Abstract : *Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user. Specifically, our contribution in this work can be summarized as the following three aspects:*

I. Introduction

Cloud Cloud storage is now gaining popularity because it offers a flexible on- demand data outsourcing service with appealing benefits: relief of the burden for storage management, universal data access with location independence, and avoidance of capital expenditure on hardware, software, and personal maintenances, etc. Nevertheless, this new paradigm of data hosting service also brings new security

Many mechanisms dealing with the integrity of outsourced data without a local copy have been proposed under different system and security models up to now. The most significant work among these studies are the PDP (provable data possession) model and POR (proof of retrievability) model, which were originally proposed for the single-server scenario by Ateniese respectively. Considering that files are usually striped and redundantly stored across multi- servers or multi-clouds, explore integrity verification schemes suitable for such multi-servers or multiclouds setting with different redundancy schemes, such as replication, erasure codes, and, more recently, regenerating codes. In this paper, we focus on the integrity verification problem in regenerating-code-based cloud storage, especially with the functional repair strategy. code-scenario; designed and implemented a data integrity protection(DIP) scheme for FMSR based cloud storage and the scheme is adapted to the thin-cloud setting. However, both of them are designed for private audit, only the data owner is allowed to verify the integrity and repair the faulty servers.

In particular, users may not want to go through the complexity in verifying and reparation. The auditing schemes in, imply the problem that users need to always stay online, which may impede its adoption in practice, especially for long-term archival storage.

II. Existing System

In the Existing System, To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud userThe third party auditing process should bring in no new vulnerabilities towards user data privacy.

Disadvantage Of Existing System

1. High energy consumption.
2. Meta-heuristic based algorithm is used for scheduling the data.
3. Waiting time for a particular task is high.
4. Online burden..

III. Proposed System

In In the Proposed System, in this paper, we utilize the public key based homomorphic authenticator and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. To support efficient handling of multiple auditing tasks. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. We also show how to extent our main scheme to support batch auditing for TPA upon delegations from multi-users and task scheduling algorithms in cloud computing mainly include the

improved heuristic task scheduling algorithms, the meta-heuristic task scheduling algorithms, and the queuing theory-based algorithms.

Advantage Of Proposed System

1. To reduce the energy consumption.
2. Highly secured and efficience.
3. Public auditability.
4. Authenticator regeneration.

IV. Architecture Diagram

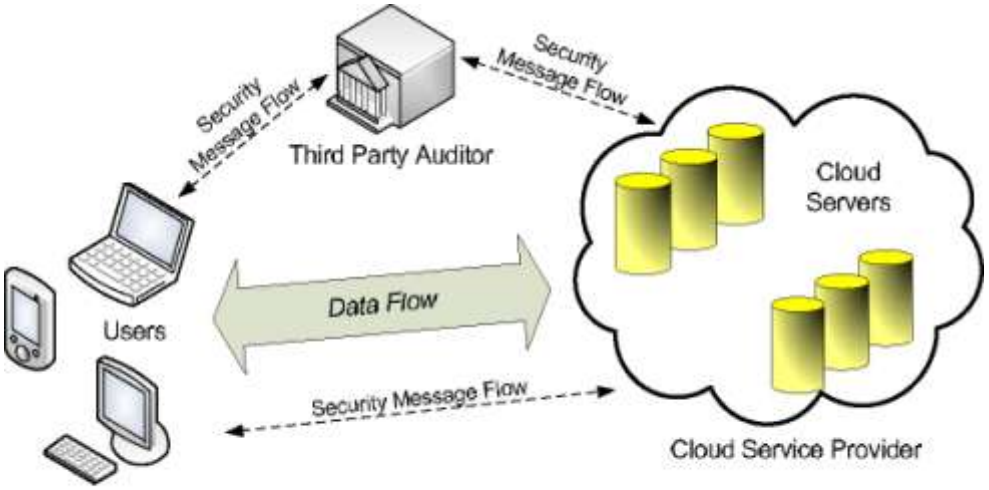

Fig. 1: The architecture of cloud data storage service

V. Algorothm

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. Conclusion

In this paper, we propose a public auditing scheme for the regenerating- code-based cloud storage system, where the data owners are privileged to delegate TPA for their data validity checking. To protect the original data privacy against the TPA, we randomize the coefficients in the beginning rather than applying the blind technique during the auditing process. Considering that the data owner cannot always stay online in practice, in order to keep the storage available and verifiable after a malicious corruption, we introduce a semi-trusted proxy into the system model and provide a privilege for the proxy to handle the reparation of the coded blocks and authenticators. This authenticator can be efficiently generated by the data owner simultaneously with the encoding procedure. Extensive analysis shows that our scheme is provable secure, and the performance evaluation shows that our scheme is highly efficient and can be feasibly integrated into a regenerating-code-based cloud. We model the task scheduling of a heterogeneous cloud computing system using the vacation queuing theory. We analyze the average sojourn time of tasks and the average power of compute nodes in the heterogeneous cloud computing system under steady state. We present a task scheduling algorithm based on similar tasks. Simulation results show that the proposed algorithm can ensure task performance, while reducing the energy cost of a cloud computing system effectively. Our future work will focus on designing and developing a green resource management software storage system.

References

[1] G. Lovasz, F. Niedermeier, and H. De-Meer, Performance tradeoffs of energy-aware virtual machine consolidation, Journal of Networks Software Tools and Applications, vol.16, pp. 37–38, 2013.
[2] J. X. Chen, Energy efficient design of cloud data center,Cloud IDC, vol. 57, pp. 481–496, 2011.
[3] O. Philippe and L. Jorge, Deep network and service management for cloud computing and data centers: A report on CNSM 2012, Journal of Network and Systems Management, vol. 21, pp. 707–712, 2013.
[4] Y. S. Jing, A. Shahzad, and S. Kun, State-of-the-art research study for green cloud computing, Journal of Supercomputing, vol. 65, pp. 445–468, 2013.