ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

Data Security for Cloud Masses Based on Data Integrity

Aluri Srinivas Rao [1], K. Rama Krishnaiah [2]

[1]Student, Nova College of Engineering & Technology, Jupudi, Ibrahimpatnam, Krishna(Dt).

[2]Professor, Nova College of Engineering & Technology, Jupudi, Ibrahimpatnam, Krishna(Dt).

Abstract:

Cloud users store their data remotely and enjoy on-demand cloud applications without burden of local software and hardware management. Previously to address these issues a secure and dependable cloud framework was proposed that uses Data Protection as a service (DPaaS). DPaas is a suite of security primitive offered by the cloud platform. The File Distribution Preparation is a vital parameter to achieve dependable clouds. It stores content in multiple redundant disks (RAID) using Reed-Solomon erasure-correcting codes. One downside of Reed-Solomon erasure-correcting code is its harped performance to perform degraded reads from multiple data sources. So we propose to use a new class of rotated Reed-Solomon codes that perform degraded reads more efficiently than all known codes, but otherwise inherit the reliability and performance properties of Reed-Solomon codes. Although erasure codes tolerate multiple simultaneous failures, single failures represent 99.75% of recoveries especially with rotated Reed-Solomon codes. This robust, secure and dependable cloud framework offers an optimum cloud storage system considering the cloud users highlighted concerns. An implementation of the proposed framework validates the claim.

Index Terms: *Data integrity, dependable distributed storage, Cloud Computing, Data Protection as a Service, Reed-Solomon ensuring codes.*

I. INTRODUCTION

Cloud computing is used to describe the variety of different types of computing concepts that involves large number of computers that are connected through a real time communication network. Cloud computing is a jargon term without a commonly accepted non-ambiguous scientific or technical definition. In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time. The popularity of the term can be attributed to its use in marketing to sell hosted services in the sense of application service provisioning that run client server software on a remote location.

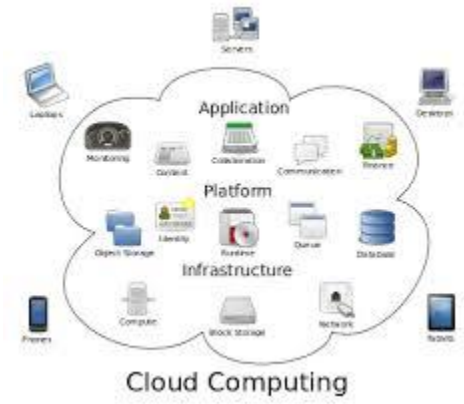

Figure 1: Cloud Architecture.

Building in data-protection solutions at the platform layer is an attractive option: the platform can achieve economies of scale by amortizing

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

expertise costs and distributing sophisticated security solutions across different applications and their developers. In our traditional technique we have to use Data Protection as a server (DPaaS). DPaaS enforces fine-grained access control policies on data units through application confinement and information flow checking. It employs cryptographic protections at rest and offers robust logging and auditing to provide accountability. Crucially, DPaaS also directly addresses the issues of rapid development and maintenance.

In this paper we propose new class of rotated Read-Solomon codes that perform degraded reads more efficiently. For demonstrational feasibility and clarity three different cloud entities are identified as follows

- Cloud User
- Cloud Server
- Third-Party Auditor/Adversary

The current system achieves the following performance parameters using Token Pre-computation, Correctness Verification and Error Localization, Error Recovery algorithms and Detection Probability against Data Modification, Identification Probability for Misbehaving Servers, File Distribution Preparation, and Dynamic data operation supporting techniques.

- Storage correctness
- Fast localization of data error
- Dynamic data support
- Dependability
- Lightweight

II. RELATED WORK

Even though the Cloud computing is emerging in these days and the number of providers and the clients are rapidly increasing there is much more concern about the security. There is tension between user data protection and rich computation in the cloud. Users want to maintain control of their data, but also want to benefit from rich services provided by application developers using that data. At present, there is little platform-level support and standardization for verifiable data protection in the cloud. On the other hand, user data protection while enabling rich computation is challenging.

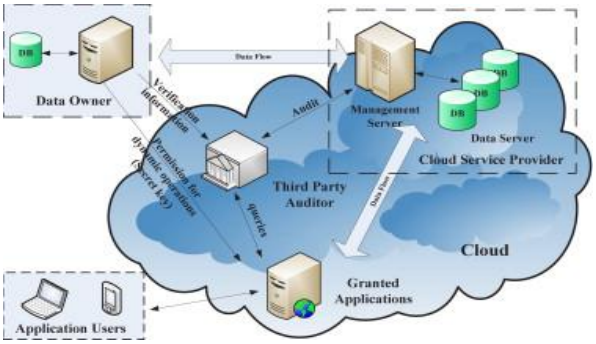

Figure 2: Cloud with third party storage device.

It requires specialized expertise and a lot of resources to build, which may not be readily available to most application developers. We argue that it is highly valuable to build in data protection solutions at the platform layer: The platform can be a great place to achieve economy of scale for security, by amortizing the cost of maintaining expertise and building sophisticated security solutions across different applications and their developers.

Cloud computing promises lower costs, rapid scaling, easier maintenance, and service availability anywhere, anytime, a key challenge is how to ensure and build confidence that the cloud can handle user data securely. A recent Microsoft survey found that "58 percent of the public and 86 percent of business leaders are excited about the possibilities of cloud computing. But more than 90 percent of them are worried about security, availability, and privacy of their data as it rests in the cloud.

III. EXISTING SYSTEM

The platform also mediates ACL modifications, otherwise known as sharing or unsharing. A simple policy that the platform can enforce without having to know too much about the application is transitive: only currently authorized users can modify the ACL. For example, the creator is the first owner of a data unit, and at any time, any user with the owner status can add or revoke other authorized users. The support of anonymous sharing, in which possession of, say, a secret URL grants access to data, is also straightforward. DPaaS can accomplish user authentication either with a proprietary approach or

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

using open standards such as OpenID and OAuth. Because the platform mediates all interactions, symmetric encryption suffices. With AES hardware units in commodity CPUs exceeding throughput of 1 Gbyte/second/core, performance is unlikely to be a bottleneck for all but the most I/O-intensive applications. Once the system loads the data into the SEE, it doesn't need to be encrypted or decrypted again until storage.

IV. PROPOSED SYSTEM

One challenge in code attestation is how to establish a set of acceptable binaries in the presence of rapid software updates such as bug fixes and new features. One potential way is to log the history of software updates and perform verification a posteriori. For example, to increase the profit margin by reducing cost, it is possible for CSP(misbehaving) to discard rarely accessed data without being detected in a timely fashion. Similarly, CSP may even attempt to hide data loss incidents so as to maintain a reputation. The current system lacks dynamic updates to stored content in the clouds. The current system fails to provide integrity checking of the content by third party auditors. The current system lacks distributed data storage to address the issues of misbehaving cloud servers or failed cloud servers. Therefore, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, its lacking of offering strong assurance of data integrity and availability may impede its wide adoption by both enterprise and individual cloud users.

Uses SAAS based cloud computing applications over web that acts as a cloud server. The client is definitely user's browser. For demonstrational feasibility and clarity three different cloud entities are identified Cloud User, Cloud Server, and Third-Party Auditor/Adversary. The current system achieves the following performance parameters using Token Pre-computation, Correctness Verification and Error Localization, Error Recovery algorithms and Detection Probability against Data Modification, Identification Probability for Misbehaving Servers, File Distribution Preparation, and Dynamic data operation supporting techniques. This is an optimum cloud storage system considering the cloud users highlighted concerns.

V. EXPERIMENTAL RESULTS

In this section, we describe the protection details using third party auditors. Previous results describe the data security in cloud storage. In that authority is the main aspect for accessing results securely. For these conditions we are using Token Pre-computation, Correctness Verification and Error Localization, Error Recovery algorithms and Detection Probability against Data Modification, Identification Probability for Misbehaving Servers, File Distribution Preparation, and Dynamic data operation supporting techniques.

Whenever we are using above techniques are assumed in the cloud storage in the protection they are performed efficient security reasons in the sequence process. By this results are as follows.

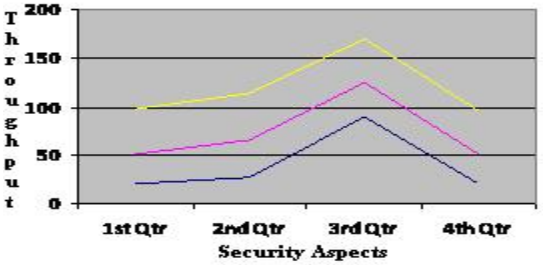

Figure 3: Data storage results with security advices.

We are storing information in the thirdy party auditor storages; it is just like act as a integrity checking process in the common cloud storage device. It is authorization technique for our previous results ignored to every result. Here we are maintaining security issues regarding our normal efficient encryption techniques present in the present scenario. Using above mention techniques in our proposed approach we are taking authorization process in cloud data storage.

VI. REFERENCES

1.N.Janardhan, Y.Raja Sree "Cloud Data Protection for the Masses" International Journal of Computer

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

Trends and Technology (IJCTT) - volume4Issue4 – April 2013.

2. Dawn Song, Elaine Shi, and Ian Fischer, *University of California, Berkeley*"Cloud Data Protection for the Masses" Umesh Shankar, *Google* IEEE,2012.

3. P. Maniatis et al., "Do You Know Where Your Data Are? Secure Data Capsules for Deployable Data Protection," *Proc. 13th Usenix Conf. Hot Topics in Operating Systems* (HotOS 11), Usenix, 2011; www.usenix.org/events/hotos11/ tech/final_files/ManiatisAkhawe.pdf.

4. A. Greenberg, "IBM's Blindfolded Calculator," *Forbes*, 13 July 2009; www.forbes.com/forbes/2009/0713/ breakthroughs-privacy-super-secret-encryption.html.