International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume2, Issue 8 (August '2016)

ENSURING DATA STORAGE USING PROVABLE DATA POSSESSION

Dr.G.Kesavaraj,
Professor &Head,
Department of Computer Science ,
Vivekanandha College of Arts and Science College for Women, (Autonomous),
Elayampalayam, Namakkal, Tamilnadu.

R.Divya,
M.Phil Scholar,
Department of Computer Science ,
Vivekanandha College of Arts and Science College for Women, (Autonomous),
Elayampalayam, Namakkal, Tamilnadu.

Abstract: Cloud computing delivers convenient, on-demand access to shared pools of data, applications and hardware over the internet. Cloud computing provides unlimited infrastructure to store and execute customer data and program. Due to this redundancy the data can be easily modified by unauthorized users which can be stored in the database. This leads to loss of data privacy and security to database. Extensive security and performance analysis shows that the proposed scheme ensures that cyclic redundancy check and time-tested practices and technologies for managing trust relationships in traditional enterprise IT environments can be extended to work effectively in both private and public clouds. Those practices include data encryption, strong authentication and fraud detection, etc.

Key words: cloud storage, cloud security, workflows, reliability

I.INTRODUCTION

Several Computing, which is an Internet-based development trends are opening up the era of Cloud and use of computer technology. Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) are both well known examples. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data. On the one hand, although the cloud infrastructures are much more powerful and reliable than personal computing devices, broad range of both internal and external threats for data integrity still exist. Examples of outages and data loss incidents of noteworthy cloud storage services appear from time to time. On the other hand, since users may not retain a local copy of outsourced data, there exist various incentives for cloud service providers (CSP) to behave unfaithfully towards the cloud users regarding the status of their outsourced data. For example, to increase the profit margin by reducing cost, it is possible for CSP 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.

II.OVERVIW OF CLOUD COMPUTING

The terms of Cloud Computing can be sometimes useful and sometimes misleading because people seem to think they understand the meaning of the term even when they don't. To illustrate the use of the term, someone I know told me of a meeting where he was explaining virtual private servers to group of non-technical people. The group was having trouble understanding some of the most basic concepts. He finally gave up and told the group that the servers were "in the Cloud." At that point, everyone in the group brightened and said they now understood. But they really didn't understand. They just thought they did because they thought they understood term Cloud Computing. But, in all likelihood, they did not understand that either. The presenter in this story was not trying to mislead people when he resorted to using "the Cloud" to help explain what he was discussing. Nevertheless, you may find intentional attempts to mislead if "Cloud" is added to products and services when those products and services really do not involve Cloud Computing. The term for this is cloud washing.

a) Its managed

One basic principle of cloud computing is that you no longer need to worry how the service you're buying is provided: with Web-based services, you simply concentrate on whatever your job is and leave the problem of providing dependable computing to someone else. Easily we manage the raw data.

b) It's "on-demand"

Cloud services are available on-demand and often bought on a "pay-as-you go" or subscription basis. So you typically buy cloud computing the same way you'd buy electricity, telephone services, or Internet access from a utility company. Sometimes cloud computing is free or paid-for in other ways (Hotmail is subsidized by advertising, for example).

TYPES OF CLOUD COMPUTING

Infrastructure as a Service (IaaS) means you're buying access to raw computing hardware over the Net, such as servers or storage. you buy what you need and pay-as-you-go, this is often referred to as utility computing. Ordinary web hosting is a simple example of IaaS.
Software as a Service (SaaS) means you use a complete application running on someone else's system. Web-based email and Google Documents are perhaps the best-known examples.

Platform as a Service (PaaS) means you develop applications using Web-based tools so they run on systems software and hardware provided by another company. So, for example, you might develop your own ecommerce website but have the whole thing, including the shopping cart, checkout, and payment mechanism running on a merchant's server.

III. OBJECTIVE OF THE RESEARCH WORK

Cloud computing is the most popular notion in IT today; even an academic report from UC Berkeley says "Cloud Computing is likely to have the same impact on software that foundries have had on the hardware industry." They go on to recommend that "developers would be wise to design their next generation of systems to be deployed into Cloud Computing". While many of the predictions may be cloud hype, we believe the new IT procurement model offered by cloud computing is here to stay. Whether adoption becomes as prevalent and deep as some forecast will depend largely on overcoming fears of the cloud. Cloud fears largely stem from the perceived loss of control of sensitive data. Current control measures do not adequately address cloud computing's third-party data storage and processing needs. In our vision, we propose to extend control measures from the enterprise into the cloud through the use of Trusted Computing and applied the cryptographic techniques. These measures should alleviate much of today's fear of cloud computing, and, we believe, have the potential to provide demonstrable business intelligence advantages to cloud participation. Our vision also relates to likely problems and abuses arising from a greater reliance on cloud computing, and how to maintain security in the face of such attacks. Namely, the new threats require new constructions to maintain and improve security.

IV.EXISTING SYSTEM

Recently the importance of ensuring the remote data integrity has been highlighted by the some research works. These techniques, while can be useful to ensure the storage correctness without having users possessing data, cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As a complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers to peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited.

DISADVANTAGES

a. Cannot address all the security threats in cloud data storage.
b. Do not consider dynamic data operations.
c. Security aspects in data managed by third party cloud providers are risk.
d. Traditional of cryptographic primitives for the purpose of data security protection.

V.PROPOSED SYSTEM

An effective and flexible distributed scheme is proposed with explicit dynamic data support to ensure the correctness of users' data in the cloud. Some part of the data is encrypted in the cloud storage with a symmetric key encryption. For example, the day to day transaction database records. Their aggregated values are encrypted in data owner storage which is less in size.

- Security risk is reduced.
- Data integrity is not violated.
- Redundant data is always similar.

Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

USING META DATA

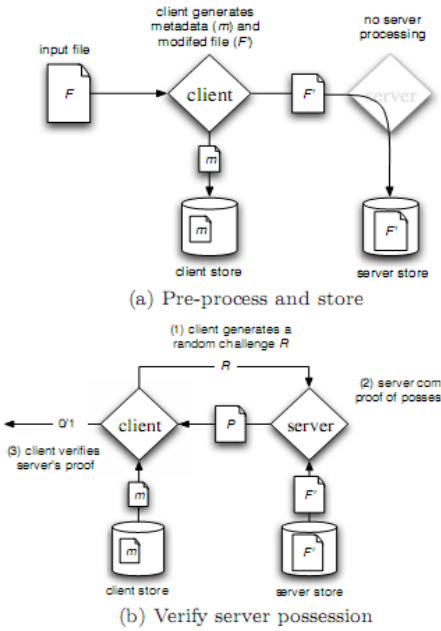

Figure 1: Provable Data Possession

We focused on the problem of verifying if an untrusted server stores a client's data. They introduced a model for provable data possession, in which it is desirable to minimize the file block accesses, the computation on the server, and the client-server communication. Their solutions for PDP fit this model: They incur a low (or even constant) overhead at the server and require a small, constant amount

of communication per challenge. Key components of their schemes are the homomorphic verifiable tags. They allow to verify data possession without having access to the actual data file. Experiments show that their schemes, which offer a probabilistic possession guarantee by sampling the server's storage, make it practical to verify possession of large data sets. Previous schemes that do not allow sampling are not practical when PDP is used to prove possession of large amounts of data. Their experiments show that such schemes also impose a significant I/O and computational burden on the server.

In the paper "Auditing to Keep Online Storage Services Honest" [19] the authors Mehul A. Shah, Mary Baker, Jeffrey C. Mogul, Ram Swaminathan (HP Labs, Palo Alto) stated that a growing number of online service providers offer to store customers' photos, email, file system backups, and other digital assets. Currently, customers cannot make informed decisions about the risk of losing data stored with any particular service provider, reducing their incentive to rely on these services. They argue that third-party auditing is important in creating an online service-oriented economy, because it allows customers to evaluate risks, and it increases the efficiency of insurance based risk mitigation. We describe approaches and system hooks that support both internal and external auditing of online storage services, describe motivations for service providers and auditors to adopt these approaches, and list challenges that need to be resolved for such auditing to become a reality. Many online services allow customers-both end users and businesses .

VI.CONCLUSION

Through this paper,the data management process becomes easy. The interface helps bank officials and cloud providers along with customers for accessing the data in the safest way.The new system eliminates the difficulties in the existing system. It is developed in a user-friendly manner.

VII.REFERENCE

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in Proc. of IWQoS'09, July 2009.

[2] Amazon.com, "Amazon Web Services (AWS)," Online at http://aws.amazon.com, Aug 2008.

[3] N. Gohringis, "Amazon's S3 down for several hours," Online at http://www.pcworld.com/businesscenter/article/142549/amazonss3 down for several hours.html, June 2008.

[4] A. Juels and J. Burton S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. of CCS '07, May 2007.

[5] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. of Asiacrypt '08, Dec 2008.

[6] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Cryptology ePrint Archive, May 2008.

[7] T. S. J. Schwarz and E. L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. of ICDCS '06, Apr 2006.

[8] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, "A Cooperative Internet Backup Scheme," Proc. of the 2003 USENIX Annual Technical Conference (General Track), Sep 2003.

